Integral dependence and integral extensions

We discuss the notion of an *integral element* of a ring S over a ring R. We define integral and module-finite extensions and discuss the relationship between these two notions. We define the integral closure of a ring in an extension ring and prove that integral closure commutes with localization. We then study the behavior of contraction of prime ideals from S to R when $R \subseteq S$ is an integral extension. In particular, we prove the lying over, going up, and going down theorems.

Let S be an R-algebra with structural homomorphism $f : R \to S$. An element $s \in S$ is called *integral* over R if for some positive integer d we have that

$$s^d = r_{d-1}s^{d-1} + \cdots + r_1 s + r_0 \cdot 1_S$$

for suitable elements r_j of r, i.e., $s^d \in Rs^{d-1} + \cdots + R1_S$. If we multiply by s, we see that s^{d+1} is in the R-span of $s^d, \ldots, 1_S$, and s^d is not needed, because it is in the R-span of its predecessors. Thus s^{d+1} is in the R-span of $s^{d-1}, \ldots, 1_S$. We may continue in this way to prove by a straightforward induction that s^t is in the R-span of $s^{d-1}, \ldots, 1_S$ for all t.

Thus, the fact that s is integral over R is equivalent to the assertion that the R-submodule of S spanned by the powers of s (including 1_S as the 0 th power) is finitely generated. (Note that any set of generators will involve only finitely many powers of s, and that these powers of s will lie among the elements $s^{d-1}, \ldots, 1$ for any $d \gg 0$.) Let A denote the image of R in S. Then another equivalent statement is that the ring $A[s]$ is a finitely generated A-module, and yet another is that s satisfies a monic polynomial (i.e., one with leading coefficient 1) with coefficients in A, say $s^d + a_{d-1}s^{d-1} + \cdots + a_1 s + a_0 = 0$ where every a_i has the form $f(r_i)$ for some element $r_i \in R$. From this definition, it is clear that s is integral over R if and only if it is integral over the image $A = f(R)$ of R in S. Thus, questions about integrality reduce, for the most part, to the case where $R \subseteq S$, and we usually assume this without much comment in the proofs.

Note that $1/2$ is not integral over $\mathbb{Z}$: its d th power is not a $\mathbb{Z}$-linear combination of lower powers for any d. On the other hand in $\mathbb{Z}[\sqrt{2}]$ the element $\sqrt{2}$ is integral over $\mathbb{Z}$: it satisfies the monic polynomial equation $x^2 - 2 = 0$. Note that $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$ is spanned over $\mathbb{Z}$ by 1 and $\sqrt{2}$.

S is said to be *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 said to be module-finite over R if S is finitely generated as an R-module. This is much stronger than the requirement that S be finitely generated as an R-algebra. If $R \subseteq S$ and S is module-finite over R, then S is called a *module-finite extension* of R. We want to explore the connection between module-finite extensions and integral extensions.

We need to extend aspects of the theory of determinants to arbitrary commutative rings. If (r_{ij}) is an $n \times n$ matrix with entries in R, we define

$$\det(r_{ij}) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) r_{1,\pi(1)} r_{2,\pi(2)} \cdots r_{n,\pi(n)}$$

where S_n is the set of permutations of $\{1, 2, \ldots, n\}$ and $\operatorname{sgn}(\pi)$ is 1 if π is an even permutation -1 if π is an odd permutation.

Certain facts about determinants follow from polynomial identities in the entries. To prove them for any ring, it suffices to prove them for polynomial rings over the integers, and since the problem remains the same if we think over the fraction field, we see that it is enough to prove the result over a field of characteristic 0. For example, suppose we want to prove that A and its transpose have the same determinant. If one knows this when A is matrix of indeterminates over $\mathbb{Z}$, one gets the general case by taking a homomorphism from $\mathbb{Z}[x_{ij}] \to R$ that maps x_{ij} to r_{ij} for all choices of i, j. The result that $\det(AB) = \det(A)\det(B)$ can be proved similarly: one starts with the case where A and B are two matrices of indeterminates. One can similarly prove that if two rows (or columns) are identical the determinant is 0, and that switching two rows or columns reverses the sign.

Let A_{ij} denote the submatrix of A obtained by deleting the i th row and j th column. The determinant of A_{ij} is called the i, j minor of A, and $(-1)^{i+j}\det(A_{ij})$ is called the i, j *cofactor*. The *classical adjoint* of A is the matrix whose i, j entry is the j, i cofactor of A: it is also referred to as the transpose of the cofactor matrix. We denote it $\operatorname{adj}(A)$. The determinant of a matrix can be found by multiplying each element of the i th row by its cofactor and summing: this called *expansion by minors* with respect to the i th row. There is a similar expansion with respect to any column. Then $A\ \operatorname{adj}(A) = \det(A)I_n$, where I_n is the $n \times n$ identity matrix. Each entry of the product on the left is the determinant of a matrix obtained by expanding with respect to a row. If the entry is off diagonal, the matrix whose determinant is being expanded has two rows equal. If the entry is on the diagonal, one gets one of the expansions for $\det(A)$ by minors. A similar argument using columns shows that $\operatorname{adj}(A)\ A = \det(A)I$.

These results are valid for any commutative ring R. If the case of a field of characteristic 0 is taken as known, they can be deduced from that case by the type of argument discussed above, using maps of polynomial rings.

The fact that for an $n \times n$ matrix A over a commutative ring R one has $\operatorname{adj}(A)\ A = \det(A)I_n$ has the following consequence:

Lemma. *Let $A = (r_ij)$ be an $n \times n$ matrix over R and let V be an $n \times 1$ column matrix such that $AV = 0$. Then* $\det(A)$ *kills every entry of V, i.e.,* $\det(A)V = 0$.

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

We note that if x is an indeterminate over the ring R and B is an $n \times n$ matrix over R, then $\det(xI_n - B) \in R[x]$ is a monic polynomial of degree n in x with coefficients in R. The product of the entries of the main diagonal provides a unique term of degree n in x, namely, x^n, while the product of any other n entries can involve x at most to the $n-1$ st power. As in the case of elementary linear algebra, this polynomial is called the *characteristic polynomial* of the matrix B. We can now prove:

Theorem. *Let S be module-finite over the ring R. Then every element of S is integral over R.*

Proof. We may replace R by its image in S, and so assume that $R \subseteq S$. Let $s_1, \ldots, s_n$ be a finite set of generators for S as an R-module. Since we may enlarge this set of generators as we please, we may assume that $s_1 = 1$. Let $s \in S$ be any element. Then for every i we have an equation

$$ss_i = \sum_{j=1}^{n} r_{ij} s_j$$

with coefficients r_{ij} in R, simply because ss_j is some element of S and so can be written as an R-linear combination of elements of $s_1, \ldots, s_n$. Let I_n be the $n \times n$ identity matrix, let V be the $n \times 1$ column vector whose entries are $s_1, \ldots, s_n$, and let $B = (r_{ij})$. Then these equations can be written in matrix form as $sIV = BV$ or $(sI - B)V = 0$. Applying the preceding Lemma with $A = sI - B$, we find that $\det(sI - B)$ kills all the entries of V, one of which is $s_1 = 1$, and so $\det(sI - B) = 0$. This implies that s is a root of the characteristic polynomial of B over R, and so s is integral over R. $\square$

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

Proof. Every element of t can be written as $\sum_{j=1}^{n} \sigma_j t_j$ for suitable elements $\sigma_j \in S$, and each σ_j can be written as $\sum_{i=1}^{m} r_{ij} s_i$ for suitable elements r_{ij} of R. Substituting in the expression for t shows that the elements $s_i t_j$ span T as an R-module. $\square$

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

Proof. Replace R by its image in S and so assume $R \subseteq S$. Let s, s' be elements of S integral over R. Then $R[s]$ is module-finite over R and, since s' is integral over R it is certainly integral over $R[s]$: use the same monic polynomial to see this. Thus, $(R[s])[s'] = R[s, s']$ is module-finite over $R[s]$, and so, by the preceding Corollary, it is module-finite over R. Thus, $s \pm s'$ and ss', which are in $R[s, s']$, are integral over R. $\square$

This depends on the characteristic polynomial method that was used to prove the Theorem above. A bit of further analysis of the proof shows that if s, s' satisfy monic polynomial equations of degrees m and n over R, the every element of $R[s, s']$ satisfies a monic polynomial equation of degree mn over R. It can be shown that, in general, one cannot do better.

If F is a finite algebraic field extension of the rational numbers the elements of F that are integral over $\mathbb{Z}$ are referred to as the *algebraic integers* of F, and form a ring o. The study of such rings is the branch of mathematics known as *algebraic number theory.*

We next observe:

Theorem. *Let S be an R-algebra. Then S is module-finite over R if and only if S is finitely generated as an R-algebra and integral over R. For S to be module-finite over R, it suffices if S is generated over R by finitely many elements each of which is integral over R.*

Proof. We have already seen that module-finite extensions are integral, and it is clear that they are finitely generated as R-algebras.

For the other half, it suffices to prove the final statement, and we may suppose that $R \subseteq S$ and that $S = R[s_1, \ldots, s_n]$. $R[s_1]$ is module-finite over R by one of our characterizations of when an element is integral, and S is module-finite over $R[s_1]$ by induction on n. The result now follows because a module-finite extension of a module-finite extension of R is module-finite over R. $\square$

A union of a family of sets, subgroups, submodules, subrings or subalgebras is called a *directed union* if any two of them are contained in a third. Then any finite union of them is contained in one of them.

Corollary. *S is integral over R if and only if it is a directed union of module-finite extensions of R.*

Proof. "If" is clear, since every element of S will be in one of the module-finite extensions and therefore integral over R. For "only if," note that S is the directed union of its finitely generated R-subalgebras, each of which will be module-finite over R. $\square$

Observe that $\mathbb{Z}[\sqrt{p} : p > 1 \text{ is prime}]$ is integral over $\mathbb{Z}$ but not module-finite (and hence not finitely generated as a $\mathbb{Z}$-algebra). In fact, adjoining the square roots of the several primes to even to $\mathbb{Q}$ does not introduce the square roots of any other primes. Similarly, if K is a field and x is an indeterminate, the ring $K[x^{1/2^n} : n \in \mathbb{N}]$ is integral over $K[x]$ but is neither module-finite nor finitely generated as an algebra over $K[x]$.

Let $f : R \to S$ be a ring homomorphism, V a multiplicative system in R, and W the image of V in S. Since the image of V in $W^{-1}S$ consists of invertible elements, there is a unique induced homomorphism $g : V^{-1}R \to W^{-1}S$ such that $g(r/1) = f(r)/1$ for all $r \in R$.

Lemma. *With notation as in the paragraph above, if S is module-finite over R (respectively, integral over R), then $W^{-1}S$ is module-finite (respectively, integral) over $V^{-1}R$.*

Moreover, if $R \subseteq S$ so that $W = V$, 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. If $S = Rs_1 + \cdots + Rs_k$ and $s/f(v) \in W^{-1}S$, then $s = r_1s_1 + \cdots + r_ks_k$ for suitable $r_j \in R$, and then $s/f(v) = \big(f(r_1)/f(v)\big)(s_1/1) + \cdots + \big(f(r_1)/f(v)\big)(s_1/1)$ which we may rewrite as $g(r_1/v)(s_1/1) + \cdots + g(r_k/v)(s_k/1) = (r_1/v)(s_1/1) + \cdots + (r_k/1)(s_k/1)$, because of the way the $V^{-1}R$-module structure is defined on $W^{-1}S$. Thus, $s_1/1, \ldots, s_k/1$ span $W^{-1}S$ as a $V^{-1}R$-module. For the integrality part, note that elements $1/f(v)$ are integral because they are in the image of $V^{-1}R$, while for elements $s/1$ one may take a monic polynomial satisfied by s over R and then $s/1$ satisfies the same polynomial, with the coefficients replaced by their images in $V^{-1}R$.

Now suppose that $R \subseteq S$ so that $W = V$. Localization at W preserves the injectivity of maps of R-modules, and hence of R-algebras. $V^{-1}T$ is integral over $V^{-1}R$ by the result of the first paragraph. Now suppose that s/v is integral over $V^{-1}R$. We must show that $s/v \in V^{-1}T$. Consider the monic polynomial satisfied by s/v over $V^{-1}R$. We may multiply

by an element of V to clear denominators, yielding a polynomial $v_0 s^n + r'_{n-1}s^{n-1} + \cdots + r'_0$ in s over R whose image in $V^{-1}S$ is 0. We may multiply by one element of V to get a polynomial $v_1 s^n + r_{n-1}s^{n-1} + \cdots + r_0$ in s over R that really is 0. It is no longer monic, but the leading coefficient is in V. Multiply through by v_1^{n-1} and rewrite the result as $(v_1 s)^n + r_{n-1}(v_1 s)^{n-1} + \cdots + r_1 v_1^{n-2}(v_1 s) + r_0 v_1^{n-1} = 0$. This shows that $v_1 s$ is integral over R. Hence, $v_1 s \in T$, and $s/v = v_1 s/(v_1 v) \in V^{-1}T$. $\square$

If $R \subseteq S$ are rings, a prime Q of S that contracts to a prime P of R is said to *lie over* P.

Lemma. *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. Consider an equation of integral dependence for s on R of degree n. Since $s \neq 0$, we must have that one of the lower coefficients r_i is not 0: let h be the least value of i such that $r_h \neq 0$, so that $r_i = 0$ for $i < h < n$. Then the equation can be rewritten as $s^h(s^{n-h} + \cdots + r_{h+1}s + r_h) = 0$. Since $s \neq 0$ and S is a domain, we have that $s^{n-h} + \cdots + r_{h+1}s + r_h = 0$, so that $r_h = s(-s^{n-h_1} - \cdots - r_{h+1})$, which shows that r_h is a nonzero multiple of s in R. $\square$

Theorem. *Let S be an integral extension of R, $I \subseteq R$ an ideal, and $u \in IS$. Then u satisfies a monic polynomial equation $u^n + i_1 u^{n-1} + \cdots + i_{n-1}u + i_n = 0$ 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 the $s_t \in S$ and the $i_t \in I$. We may therefore replace S by the smaller ring generated over R by u and the elements s_t. This ring is module-finite over R. Thus, there is no loss of generality in assuming that S is module-finite over R, with generators $s_1, \ldots, s_n$, and, as earlier, we may enlarge the set of generators so that we may assume that $s_1 = 1$. It is easy to see that $IS = Is_1 + \cdots + Is_n$, the set of linear combinations of $s_1, \ldots, s_n$ with coefficients in I: each element is for $i \in I$ and $s \in S$ has this form because each element of S is an R-linear combination of $s_1, \ldots, s_n$. If $u \in IS$, then every us_j is in IS, and so there are n equations

$$us_j = \sum_{t=1}^{n} i_{jk} s_k.$$

Let V be the $n \times 1$ column matrix with entries $s_1, \ldots, s_n$ and let B be the $n \times n$ matrix (i_{jk}). Then the same argument that we gave earlier shows that u satisfies the characteristic polynomial of B, which has the form

$$x^n + i_1 x^{n-1} + i_2 x^{n-2} + \cdots + i_n$$

where i_t is in $I^t \subseteq R$ for every t, $1 \leq t \leq n$. $\square$

Lying over theorem. *Let S be an integral extension of R. Then for every prime P of R, there are primes of S that contract to P, and they are mutually incomparable. In particular, the map* $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ *is onto. For every ideal I of R, the contraction of IS to R is contained in* $\operatorname{Rad} I$*, and so if I is radical, $IS \cap R = I$.*

Proof. We prove the last statement first. Let $u \in IS \cap R$, Consider the monic equation that u satisfies given by the preceding theorem. After we substitute u for x, the leftmost term of the equation is u^n while the other terms are in I. This implies that $u^n \in I$ and so $u \in \operatorname{Rad} I$, as required.

In particular, if $I = P$ is prime then $R - P$ is a multiplicative system in $R \subseteq S$, and PS does not meet it, since $PS \cap R = P$. Therefore there is a prime ideal Q of S that contains PS and is disjoint from $R - P$. Since $P \subseteq PS$, we see that $Q \cap R = P$.

It remains only to show that two primes lying over $P \subseteq R$ cannot be comparable. Suppose to the contrary that $Q_0 \subset Q$ both lie over P in R. The trick here is to pass to $R/P \subseteq S/Q_0$. This extension is still integral: given $s \in S$, it satisfies a monic equation over R, and $s + Q$ satisfies the same equation with coefficients considered mod P. Now the nonzero prime ideal Q/Q_0 lies over the prime ideal (0) in R/P. Thus, it suffices to show that if $R \subseteq S$ are domains, then a nonzero prime ideal Q of S cannot lie over (0) in R. This is immediate from the preceding Lemma: any nonzero element of Q has a nonzero multiple in R. $\square$

Example. The ring of functions from an infinite set X to $\mathbb{Z}/2\mathbb{Z}$ is integral over $\mathbb{Z}/2\mathbb{Z}$: every element satisfies $x^2 - x = 0$. It has uncountably minimal primes, mutually incomparable and all lying over (0) in $\mathbb{Z}/2\mathbb{Z}$.

We give another proof of the lying over theorem that does not involve the eigenvalue trick. Suppose that $R \subseteq S$ is integral and that $P \in \operatorname{Spec}(R)$. By Supplementary Problem Set #2, **1.** and **2.**, $R_P \subseteq (R - P)^{-1}S = S_1$ and the extension is still integral. If Q_1 is a prime of S_1 lying over PR_P, then the contraction Q of Q_1 to S will lie over P, since PR_P lies over P. Thus, we have reduced to the case where R is quasi-local with maximal ideal P. It now suffices to show that $PS \neq S$, for then any maximal ideal of S containing PS will be prime, and its contraction to R will contain the maximal ideal P but not 1, forcing the contraction to be P. Consider the family of ideals of R contained in P whose expansion to S is not all of S. This family contains (0), and the union of a chain in the family is again in the family: if $1 \in S$ is a linear combination of finitely many elements from the union, these elements will come from just finitely many of the ideals in the family, and will all lie in the largest of them. Therefore this family has a maximal element I. Consider $IS \cap R = J$. Then $I \subseteq J$, and we must have $J = I$ or else $JS \subseteq IS \neq S$ contradicts the maximality of I. Then $R/I \to S/IS$ is injective and still integral, and R/I is quasi-local. Therefore we may replace $R \subseteq S$ by $R/I \subseteq S/IS$. If $P = (0)$ we are done. If not, then choose $a \in P - \{0\}$. Then the maximality of I implies that $aS = S$ (or else we could have enlarged $I \subseteq R$ using a preimage of a). This means that there is an element b of S such that $ab = 1$. But b is integral over R, so that there is an equation

$$b^n = r_{n-1}b^{n-1} + r_{n-2}b^{n-2} + \cdots + r_1 b + r_0$$

Since $b = a^{-1}$, when we multiply both sides by a^{n-1} we get that

$$b = r_{n-1} + r_{n-2}a + \cdots + r_1 a^{n-2} + r_0 a^{n-1}$$

which shows that $a^{-1} = b \in R$. Thus, a has an inverse in R, contradicting the assumption that $a \in P - \{0\}$. $\square$

Corollary (Going up theorem). *Let $R \hookrightarrow S$ be an integral extension and let*

$$P_0 \subset P_1 \subset \cdots \subset P_d$$

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

$$Q_0 \subset Q_1 \subset \cdots \subset Q_d$$

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

Proof. It suffices to construct $Q_1 \supseteq Q_0$ lying over Q_1: the result then follows by a straightforward induction on d. Consider $R/P_0 \subseteq S/Q_0$. This is an integral extension, and P_1/P_0 is a prime ideal of R/P_0, so there is a prime ideal of S/Q_0 that lies over it: it will have the form Q_1/Q_0 for some prime ideal Q_1 of S. It is clear that $Q_0 \subset Q_1$, and it is easy to verify that that Q_1 lies over P_1 in R. $\square$

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

Proof. Let $Q_0 \subset \cdots \subset Q_d$ be a chain of prime ideals of S. Their contractions will give a chain of prime ideals of the same length in R: they will be distinct, because comparable primes cannot contract to the same prime ideal. This shows that $\dim S \leq \dim R$.

On the other hand, given a finite chain of primes in R, the going up theorem implies the existence of a chain of prime ideals of S of the same length, so that $\dim S \geq \dim R$. $\square$

Let $f : R \to S$ be a ring homomorphism, and let $f^* = \operatorname{Spec}(f) : \operatorname{Spec}(S) \to \operatorname{Spec}(R)$ be the usual map given by contraction. Let $Y = \operatorname{Spec}(S)$ and $X = \operatorname{Spec}(R)$. Given a map of sets $g : Y \to X$, and a point $x \in X$, the set $g^{-1}(x)$ is called the *fiber* of g over x: it is simply the set of points of Y that map to x. Thus, the fiber of the function $f^* = \operatorname{Spec}(f)$ over $P \in \operatorname{Spec}(R)$ is precisely the set of primes of S lying over P in R. This set of primes is homeomorphic with Spec of

$$(R - P)^{-1}S/P^{\mathrm{e}} \cong (\overline{R - P})^{-1}(S/PS),$$

where $\overline{R - P}$ is the image of $R - P$ in S/PS. The ring $(R - P)^{-1}S/P^{\mathrm{e}}$ is called the *fiber* of $R \to S$ over P. (This is really terminology from the theory of schemes, and the term *scheme-theoretic fiber* is also used.) Alternatively, it may be defined as the canonically isomorphic ring $(\overline{R - P})^{-1}(S/PS)$. Note that it is an S-algebra. Its primes correspond exactly to primes of S that contain PS and are disjoint from $R - P$, which is exactly the condition for them to lie over P in R. $(R - P)^{-1}S/P^{\mathrm{e}}$ is also an algebra over R_P/PR_P (which may be identified with fraction field of the domain R/P).

If $R \to S$ is integral (respectively, module-finite), then $R_P/PR_P \to (R - P)^{-1}S/P^{\mathrm{e}}$ is also integral (respectively, module-finite). Up to multiplication by elements coming from units of R, every element of the $(R - P)^{-1}S/P^{\mathrm{e}}$ comes from S, and for the image of an element of S we may use the same equation of integral dependence that it satisfied over R, taking the images of the coefficients in R_P/PR_P. In the case where S is spanned over R by $s_1, \ldots, s_n$, the images of $s_1, \ldots, s_n$ span $(R - P)^{-1}S/P^{\mathrm{e}}$ over R_P/PR_P.

We want to obtain a bound for the number of primes lying over P in the case of a module-finite extension.

We first prove two preliminary results.

Two ideals I, J of a ring R are called *comaximal* if $I + J = R$. Ideals $I_1, \ldots, I_n$ of R are called *pairwise comaximal* if for all $j \neq k$, $I_j + I_k = R$. Note that if $m_1, \ldots, m_n$ are mutually distinct maximal ideals of R, then they are pairwise comaximal.

We recall that the *product ideal* IJ is the ideal generated by all the elements ij for $i \in I$ and $j \in J$. Each element of IJ is a sum of the form $i_1j_1 + \cdots + i_kj_k$ for some positive integer k and elements $i_1, \ldots, i_k \in I$ and $j_1, \ldots, j_k \in J$.

Lemma (Chinese remainder theorem). *If $I_1, \ldots, I_n$ are pairwise comaximal in the ring R, then*

$$I_1 \cdots I_n = I_1 \cap \cdots \cap I_n.$$

Let $J = I_1 \cdots I_n$. The ideals

$$I_1I_2,\ I_3,\ \ldots,\ I_n$$

are also pairwise comaximal. Moreover, the map

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

that sends $r + J$ to $(r + I_1, \ldots, r + I_n)$ is a ring isomorphism.

Proof. First consider the case where $n = 2$. Choose $i_1 \in I_1$ and $i_2 \in I_2$ such that $i_1+i_2 = 1$. If $u \in I \cap J$ then $u = u \cdot 1 = u(i_1 + i_2) = ui_1 + ui_2$. But $ui_1 \in I_1I_2$ because $u \in I_2$, and $ui_2 \in I_1I_2$ because $u \in I_1$. Thus, $u \in I_1I_2$. The map $R \to R/I_1 \times R/I_2$ that sends r to $(r + I_1, r + I_2)$ is a ring homomorphism that clearly has kernel $I_1 \cap I_2 = I_1I_2$. It therefore induces an injection $R/I_1I_2 \hookrightarrow R/I_1 \times R_2$. To see that this map is surjective, let $(r_1 + I_1, r_2 + I_2)$ in the image be given. Then $r_1i_2 + r_2i_1$ maps to this element: mod I_1, $r_1i_2 + r_2i_1 \equiv r_1 \cdot 1 + r_2 \cdot 0 \equiv r_1$, and the calculation mod I_2 is exactly similar.

To prove the second statement, it clearly suffices to show that I_1I_2 is comaximal with I_j for $j \geq 3$. Choose $i_1 \in I_1$ and $u \in I_j$ such $i_1 + u = 1$, and choose $i_2 \in I_2$ and $v \in I_j$ such that $i_2 + v = 1$. Multiply these equations. Then $i_1i_2 + i_1v + ui_2 + uv = 1$, and $i_1i_2 \in I_1I_2$ while $i_1v + ui_2 + uv \in I_j$.

The general case of the ring isomorphism now follows by induction on n. By the induction hypothesis,

$$R/J = R/\big((I_1I_2)I_3 \cdots I_n\big) \cong \big(R/(I_1I_2)\big) \times R/I_3 \times \cdots \times R/I_n$$

and $R/(I_1I_2) \cong R/I_1 \times R/I_2$ by the case $n = 2$ already established. $\square$

If $R = \mathbb{Z}$, the principal ideals $a_1\mathbb{Z}, \ldots\ a_n\mathbb{Z}$ are pairwise comaximal if and only if the integers $a_1, \ldots, a_n$ are relatively prime in pairs, and we get the classical Chinese remainder theorem.

Theorem. *Let R be a reduced K-algebra that is module-finite over the field K. This simply means that R is a finite-dimensional vector space over K. Then R is a product of finite algebraic field extensions $L_1 \times \cdots \times L_n$ of K. R has n maximal ideals, the kernels of the n product projections $R \twoheadrightarrow L_i$, $1 \leq i \leq n$, and n, the number of maximal ideals, is at most the dimension of R as K-vector space.*

Proof. Since K has dimension 0 and R is integral over K, R has dimension 0. Thus, every prime ideal is maximal. Let $m_1, \ldots, m_h$ be any subset of the maximal ideals of R. By the Chinese remainder theorem, $R/(m_1 \cdots m_h) \cong R/m_1 \times \cdots \times R/m_h$. Let $L_i = R/m_i$. L_i is a field and finite-dimensional as a K-vector space, and so it is a finite algebraic extension of K. As a K-vector space, $R/m_1 \times \cdots \times R/m_h$ is the direct sum over K of the L_i, which shows that h is at most the K-vector space dimension of $R/(m_1 \cdots m_h)$, and therefore is also at most the K-vector space dimension of R. This means that the number of maximal ideals of R is at most the K-vector space dimension of R. Now suppose that $m_1, \ldots, m_n$ are all the maximal ideals of R. Since R is reduced, the intersection of the m_i is (0). Thus, $R \cong R/(0) \cong R/m_1 \times \cdots \times R/m_n$. $\square$

Corollary. *Let S be module-finite over R with n generators. The number of prime ideals of S lying over a prime P of R is at most n.*

Proof. By our earlier remarks, we may replace $R \to S$ by $R_P/PR_P \to (R_P)^{-1}S/P^{\mathrm{e}}$, and n does not increase. But now $R = K$ is a field, and S is a finite-dimensional K-vector space of dimension at most n. Passing to S_{red} can only decrease its K-vector space dimension, while the number of prime ideals (which are all maximal) does not change, and now we may apply the preceding result. $\square$

Note that the solution given for problem **4.** in Supplementary Problem Set #1 establishes a bijection between the natural transformations from h_X toh_Y and the morphisms from Y to X, and it easy to check that it is compatible with composition, so that an isomorphism of h_X and h_Y implies an isomorphism of Y with X. A useful consequence is that the object representing a functor is unique, up to isomorphism. This establishes literally hundreds of isomorphisms. For example, if S is a multiplicative system in R with image $\overline{S}$ in R/I, the isomorphism $S^{-1}R/IS^{-1}R \cong \overline{S}^{\,-1}(R/I)$ is a consequence of the fact that both represent, in the category of rings, the functor that assigns to the ring T all homomorphisms from $R \to T$ such that I maps to 0 in T and S maps into the units of T.

If P is a prime ideal of R, by the *height* of P we mean the supremum of lengths of finite strictly ascending chains of primes contained in P. It is immediate that the height of P is the same as the Krull dimension of the quasilocal ring R_P. It should be clear that the dimension of R is the same as the supremum of heights of all prime ideals, and that this will be the same as the supremum of heights of all maximal ideals.

Corollary. *If $R \subseteq S$ is an integral extension and Q is a prime ideal of S lying over a prime P in R, then the height of P is bigger than or equal to the height of Q.*

Proof. A chain of distinct primes contained in Q will contract to a chain of distinct primes contained in P. $\square$

A much harder problem is this: suppose that S is integral over R and we are given a chain

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

of primes in R, and a prime Q_n of S lying over P_n. Can we find a chain

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

of S such that Q_i lies over P_i for every i? This turns out to need additional hypotheses even when R is a domain. In order to formulate the correct hypothesis on R needed here, we must discuss the notion of an integrally closed domain.

The set of elements of $S \supseteq R$ that are integral over R was shown earlier to be a ring. This ring is called the *integral closure of R in S*.

We shall say that a domain R is *integrally closed* or *normal* if every element of the fraction field of R that is integral over R is in R. The integral closure of a domain R in its fraction field is called the *the integral closure* or *normalization* of R.

A unique factorization domain is normal. To see this, suppose that a/b is a fraction integral over R but not in R. We may assume that it has been written in lowest terms, so that a and b have no common divisor other than units, and b is not a unit. If it satisfies the equation

$$(a/b)^d + r_{n-1}(a/b)^{d-1} + \cdots + r_0 = 0$$

with the $r_i \in R$ we may multiply through by b^d to get the equation

$$a^d + r_{n-1}a^{d-1}b + \cdots + r_0 b^d = 0.$$

Every term other than the leftmost is divisible by b, and so $b \mid a^d$. Any prime factor of b must divide a^d and therefore a, a contradiction, since a/b is in lowest terms. $\square$

In particular, any principal ideal domain, as well as any polynomial ring over a field or a principal ideal domain, is normal.

If K is a field, $R = K[x^2, x^3]$ is not normal. $x = x^3/x^2$ is in the fraction field, and is integral over $K[x^2, x^3]$, since $z = x$ is a root of $z^2 - x^2 = 0$. The integral closure of R is $K[x]$.

The ring $\mathbb{Z}[\sqrt{5}]$ is not integrally closed. The element $\tau = \dfrac{1+\sqrt{5}}{2}$ is in the fraction field, and is integral, since it is a root of $x^2 - x - 1 = 0$. It is not obvious but not difficult to show that $\mathbb{Z} + \mathbb{Z}\tau$ is integrally closed, and is the integral closure of $\mathbb{Z}[\sqrt{5}]$. (Suppose that $a + b\sqrt{5}$ is integral over $\mathbb{Z}[\sqrt{5}]$ and hence over $\mathbb{Z}$, where a, $b \in \mathbb{Q}$. It follows that $a - b\sqrt{5}$ will satisfy the same monic polynomial over $\mathbb{Z}$ that $a + b\sqrt{5}$ does, and so is also integral over $\mathbb{Z}$. Adding, we find that $a + b\sqrt{5} + a - b\sqrt{5} = 2a$ is integral over $\mathbb{Z}$, and therefore in $\mathbb{Z}$. Thus, a is either k or $k + 1/2$, where k is an integer. By subtracting a suitable integer linear combination of $\sqrt{5}$ and τ, we get an element of the form $c\sqrt{5}$, integral over $\mathbb{Z}$, such that c is an rational. It will therefore suffice to show that if c is rational and $c\sqrt{5}$ is integral

over $\mathbb{Z}$, then c is an integer. Write $c = m/n$ in lowest terms. Then $5c^2$ is rational and is integral over $\mathbb{Z}$ and therefore is an integer, i.e., $n^2 \mid 5m^2$. If $5 \mid n$ then it does not divide m, and this is impossible. If 5 does not divide n, then $n^2 \mid m^2$, so that c is a rational number whose square is an integer, and it follows that c is an integer. $\square$)

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. For Suppose that $a, b \in R$, $b \neq 0$, but that a/b is integral over R. Then it is integral over S, and therefore $a/b = s \in S$, i.e., $a = bs$. But there is an R-linear map f from $S = R \oplus_R W$ (where W is an R-submodule of S) that kills W and is the identity on R. It follows that $a = f(a) = f(bs) = bf(s)$, and so $a/b = f(s) \in R$.

Let K be a field. Then the ring R generated over K by all monomials of degree d in $S = K[x_1, \ldots, x_n]$ is integrally closed: we shall show that it is a direct summand of $K[x_1, \ldots, x_n]$. Note that every monomial of degree divisible by d, say degree dk, is the product of k monomials of degree d. Let W be the K-span of all monomials whose degree is not divisible by d. The product of an element of R and an element of W is in W: when we multiply and distribute in all possible ways, we get a sum of terms each of which is the product of a monomial of degree divisible by d and a monomial of degree not divisible by d, and that product is in W. Thus, $S = R \oplus_R W$. If the number of variables is greater than one and $d > 1$, these rings are not unique factorization domains. For example, if $n = 2$ and $d = 2$, $S = K[x_1, x_2]$ and $R = K[x_1^2, x_1x_2, x_2^2]$. The fact that $(x_1x_2)^2 = (x_1^2)(x_2^2)$ shows that R is not a UFD.

We can now state the result we aim to prove:

Theorem (Going down theorem). *Let R be a normal integral 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*

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

be a chain of primes in R, and let Q_n be a prime ideal of S lying over P_n. Then there is a chain of primes

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

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

We need some preliminaries before we can prove this.

Proposition. *Let A be a ring and $A[x]$ the polynomial ring in one variable over A.*

(a) *If f and g are nonzero polynomials of $A[x]$ with degrees n and d and leading coefficients a and b respectively, then if either a or b is not a zerodivisor in A, the degree of fg is $d + n$ and its leading coefficient is ab. In particular, the conclusion holds if f or g is monic.*

(b) **(Division algorithm)** *Let g be any polynomial and f a monic polynomial in $R[x]$ of degree d. Then one can write $g = qf + r$, where $q, r \in A[x]$ and either $r = 0$ or the degree of r is $< d$. This representation is unique.*

(c) *Let $R \subseteq S$ be a ring extension and let f, g be as in (b), with f monic. Then g is a multiple of f in $R[x]$ if and only if it is a multiple of f in $S[x]$.*

Proof. It is clear that fg has at most one term of degree $d+n$, namely abx^{d+n}, with all other terms of lower degree, and that it has such a term provided that $ab \neq 0$, which is true if either a or b is not a zerodivisor. This proves part (a).

To prove existence in part (b), we perform long division in the usual way. To make this precise, first note that if $g = 0$ or has degree $< d$, we may take $q = 0$ and $r = g$. Otherwise, let ax^n be the highest degree term in g, where $a \neq 0$ is in R. Then $g_1 = g - ax^{n-d}g$ has smaller degree than f, and so can be written in the form $q_1 g + r$ by induction on the degree of f. But then $f = (ax^{n-d} + q_1)g + r$, as required.

It remains to prove uniqueness. But if $qf + r = q'f + r'$ both satisfy the condition, then $(q - q')f = r' - r$ is 0 or has degree smaller than that of f, which is impossible from part (a) unless $q - q' = 0$, in which case $r' - r = 0$ as well.

To prove part (c), note that we can perform the division algorithm thinking in $R[x]$ or in $S[x]$. By uniqueness, the result is the same. If g is a multiple of f in $S[x]$ the remainder must be zero, and then the same holds in $R[x]$. $\square$

Note in connection with part (a) that if $A = \mathbb{Z}/(4)$ and $\overline{2}$ denotes the image of 2 in A, then $(\overline{2}x + 1)(\overline{2}x + 1) = 1$ in $A[x]$.

Proposition. *Let R be an integrally closed domain with fraction field K and 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 over K. Then $f(x) \in R[x]$, and for any polynomial $g(x) \in R[x]$ such that $g(s) = 0$, $f(x) \mid g(x)$ in $R[x]$.*

Proof. Choose an algebraically closed field L that contains the fraction field of S. Thus, $K \subseteq L$ as well. s satisfies some monic polynomial $h(x)$ with coefficients in R. It follows that $g(x) \mid h(x)$ in $K[x]$. Therefore, every root of g in L is a root of $h(x)$. It follows that all the roots of g are integral over R. The coefficients of g are elementary symmetric functions of the roots of g. Therefore, the coefficients of g are elements of K that are integral over R. Since R is normal, they are in R. Now suppose that $g(x)$ is any polynomial of $R[x]$ such that $g(s) = 0$. We know that $f(x) \mid g(x)$ in $K[x]$. The fact that $f(x) \mid g(x)$ in $R[x]$ follows from part (c) of the preceding proposition. $\square$

We are now ready for:

Proof of the going down theorem. We have an integrally closed domain $R \subseteq S$ where S is integral over R and the nonzero elements of R are not zerodivisors in S. We are given a prime Q of S lying over P in R, and a prime P_0 of R with $P_0 \subset P$. We want to show that there is a prime $Q_0 \subset Q$ such that Q_0 lies over P_0. The general case of the going down theorem then follows by a straightforward induction.

We begin by showing that there is a prime ideal $q \subseteq S$ such that $q \subset Q$ and q lies over the prime ideal (0) in R. To see this, consider the multipicative system $W = (R - \{0\})(S - Q)$ in S. Because the elements of $R - \{0\}$ are not zerodivisors in S and the elements of $S - Q$ are not zero, the multiplicative system W does not contain 0. This means that there is a prime ideal q of S disjoint from W. In particular, since $R - \{0\} \subseteq W$, we must have that $q \cap R = (0)$, and since $S - Q \subseteq W$, we must have that $q \subseteq Q$. Since Q lies over P and

$P_0 \subset P$, $P \neq (0)$, and this means that $q \subset Q$. We now replace S by S/q. Since q does not meet R, we still have an injection $R \hookrightarrow S/q$, and we may replace R by its image in S/q and so assume that $R \subseteq S/q$. This extension is obviously still integral: the monic equation over R satisfied by $s \in S$ is also satisfied by its image in S/q. We replace Q by Q/q, which still lies over P. If we can find a prime of S/q contained in Q/q that lies over P_0, it will have the form Q_0/q for some prime Q_0 of S with $Q_0 \subseteq Q$. Then Q_0 will lie over P_0 in R and we will also have $Q_0 \subseteq Q$. Since $P_0 \subset P$, we actually have that $Q_0 \subset Q$.

Therefore, we may assume without loss of generality that $R \subseteq S$ is an extension of domains and that S is integral over R. This stronger condition replaces the assumption that nonzero elements of R are not zerodivisors in S. Let $A = R - P_0$ and $B = S - Q$. 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 $AB \supseteq A \cup B$, so that $P_0 \subseteq Q_0$ and Q_0 meets neither $R - P_0$ nor $S - Q$. But this means that Q_0 lies over P_0 and is contained in Q, as required.

Suppose that $a \in A$ and $b \in B$ are such that $ab \in P_0S$. The argument used in the proof of the lying over theorem (see the lecture notes from September 24) shows that ab satisfies a monic polynomial equation $g_1(x)$ in one variable x such that all coefficients of the equation except the leading coefficient are in P_0 (not just in P_0S).

This means that b is a root of the polynomial $g(x) = g_1(ax)$ over b. Note that the leading coefficient of $g(x)$ is a power of a, and that all other coefficients are in P_0.

Think of $K = \mathrm{frac}\,(R)$ as contained in $\mathrm{frac}\,(S) = L$. Since b satisfies the algebraic equation $g(b) = 0$, it is algebraic over K, and has a monic minimal polynomial $f(x)$ with coefficients in K that is irreducible in $K[x]$. By the preceding Lemma, this polynomial has coefficients in R, since R is normal. It divides $g(x)$ in $K[x]$, because $g(x)$ has coefficients in $R \subseteq K$, and $f(x)$ is the minimal polynomial of b.

Since $f(x)$ is monic, our result on the division algorithm implies that $f(x)$ divides $g(x)$ in $R[x]$ as well: let us say that $g(x) = f(x)q(x)$, where all three have coefficients in R. We now consider coefficients mod P_0, which means, in effect , that we are working in $\overline{R}[x]$, where $\overline{R} = R/P_0$. Let $\overline{a}$ be the image of a in $\overline{R}$: since $a \in R - P$, $\overline{a} \neq 0$ in R/P. Then, mod P_0, $g(x)$ has the form $\overline{a}^d x^d$, since all lower coefficents are in P_0. This implies that the monic polynomial f must become x^k mod P_0, where k is its degree. This means, thinking over R, that $f(x)$ is monic of degree k with all lower coefficients in P_0: say $f(x) = x^k + p_{k-1}x^{k-1} + \cdots + p_0$, where the $p_j \in P_0$.

Since b is a root of $f(x)$, we have that $b^k = -p_{k-1}b^{k-1} - \cdots - p_0 \in P_0S \subseteq Q$, and so $b \in Q$, which is a contradiction! Thus, AB does not meet P_0S, and we are done. $\square$

Corollary. *Let R be an integrally closed domain, S an integral extension of R that is torsion free over R, and Q a prime ideal of S that lies over P in R. Then the height of Q is equal to the height of P.*

Proof. We have already seen that the height of Q is at most the height of P. Conversely, given a chain of primes contained in P we may use the going down theorem, starting with the largest prime in the chain, to construct a chain of primes in S that lies over it and

is contained in Q, and this shows that the height of Q is at least as big as the height of P. $\square$

Let's look at two examples. Consider $R = K[x] \subseteq K[x, y]/(y^2 - y, xy) = S$. This is integral, since y satisfies a monic equation. It is an extension: we can map this larger algebra back to $K[x]$ by sending $x \mapsto x$ and $y \mapsto 0$, and the composition is the identity on $K[x]$. The element $1 - y$ generates a minimal prime Q of the larger ring containing x and not y: we can see that it is minimal, because a smaller prime cannot contain $(1 - y)$ and cannot contain y either (or else Q would contain both y and $1 - y$), while $y(1 - y) = 0$ in the quotient. But $(1 - y)S$ contracts to $xK[x]$, which has height one. The problem here is that x is a zerodivisor in S, which shows that one cannot omit the hypothesis that S be torsion-free over R in the statement of the going down theorem.

In the example above, R is normal. We next consider an example where both rings are domains but R is not normal: in fact, S is the integral closure of R. Let K be a field, let $S = K[x, y]$, and let

$$R = K[x(1 - x), x^2(1 - x), y, xy] \subseteq S.$$

S is integral over R since it is generated over $K[y] \subseteq R$ by x, and $z = x$ satisfies the monic polynomial $z^2 - z - x(1 - x) = 0$, which has coefficients in R. x is in the fraction field of R, since it is equal to xy/y or $x^2(1 - x)/\big(x(1 - x)\big)$. Let $Q = (1 - x, y)S$, which is easily seen to lie over

$$P = \big(x(1 - x), x^2(1 - x), y, xy\big)R,$$

a maximal ideal of R, and let P_0 be the contraction of xS to R. Then

$$P_0 = \big(x(1 - x), x^2(1 - x), xy\big)R.$$

We claim that no prime Q_0 contained in Q lies over P_0. For any prime of S contained in Q cannot contain x, for $x \notin Q$. But since Q_0 must contain both $x(1 - x)$ and xy (these elements are in P_0) and it does not contain x, it must contain both $1 - x$ and y, which forces it to be equal to Q. But then it lies over P, not P_0. This shows that one cannot omit the hypothesis that R be normal in the statement of the going down theorem.