Contents

Chapter 7
Integrality and valuation rings

The notion of integrality is familiar from number theory: it is similar to "algebraic" but with the polynomials involved are required to be monic. In algebraic geometry, integral extensions of rings correspond to correspondingly nice morphisms on the Spec's—when the extension is finitely generated, it turns out that the fibers are finite. That is, there are only finitely many ways to lift a prime ideal to the extension: if $A \to B$ is integral and finitely generated, then $\operatorname{Spec} B \to \operatorname{Spec} A$ has finite fibers.

Integral domains that are *integrally closed* in their quotient field will play an important role for us. Such "normal domains" are, for example, regular in codimension one, which means that the theory of Weil divisors (see **??**) applies to them. It is particularly nice because Weil divisors are sufficient to determine whether a function is regular on a normal variety.

A canonical example of an integrally closed ring is a valuation ring; we shall see in this chapter that any integrally closed ring is an intersection of such.

§1 Integrality

1.1 Fundamentals

As stated in the introduction to the chapter, integrality is a condition on rings parallel to that of algebraicity for field extensions.

Definition 1.1 Let R be a ring, and R' an R-algebra. An element $x \in R'$ is said to be **integral** over R if x satisfies a monic polynomial equation in $R[X]$, say

$$x^n + r_1 x^{n-1} + \cdots + r_n = 0, \quad r_1, \ldots, r_n \in R.$$

We can say that R' is **integral** over R if every $x \in R'$ is integral over R.

Note that in the definition, we are not requiring R to be a *subring* of R'.

Example 1.2 $\frac{1+\sqrt{-3}}{2}$ is integral over $\mathbb{Z}$; it is in fact a sixth root of unity, thus satisfying the equation $X^6 - 1 = 0$. However, $\frac{1+\sqrt{5}}{2}$ is not integral over $\mathbb{Z}$. To explain this, however, we will need to work a bit more (see Proposition 1.5 below).

Example 1.3 Let L/K be a field extension. Then L/K is integral if and only if it is algebraic, since K is a field and we can divide polynomial equations by the leading coefficient to make them monic.

Example 1.4 Let R be a graded ring. Then the subring $R^{(d)} \subset R$ was defined in **??**; recall that this consists of elements of R all of whose nonzero homogeneous components live in degrees that are multiples of d. Then the dth power of any homogeneous element in R is in $R^{(d)}$. As a result, every homogeneous element of R is integral over $R^{(d)}$.

We shall now interpret the condition of integrality in terms of finite generation of certain modules. Suppose R is a ring, and R' an R-algebra. Let $x \in R'$.

Proposition 1.5 *$x \in R'$ is integral over R if and only if the subalgebra $R[x] \subset R'$ (generated by R, x) is a finitely generated R-module.*

This notation is an abuse of notation (usually $R[x]$ refers to a polynomial ring), but it should not cause confusion.

This result for instance lets us show that $\frac{1+\sqrt{-5}}{2}$ is not integral over $\mathbb{Z}$, because when you keep taking powers, you get arbitrarily large denominators: the arbitrarily large denominators imply that it cannot be integral.

Proof. If $x \in R'$ is integral, then x satisfies

$$x^n + r_1 x^{n-1} + \cdots + r_n = 0, \quad r_i \in R.$$

Then $R[x]$ is generated as an R-module by $1, x, \ldots, x^{n-1}$. This is because the submodule of R' generated by $1, x, \ldots, x^{n-1}$ is closed under multiplication by R and by multiplication by x (by the above equation).

Now suppose x generates a subalgebra $R[x] \subset R'$ which is a finitely generated R-module. Then the increasing sequence of R-modules generated by $\{1\}, \{1, x\}, \{1, x, x^2\}, \ldots$ must stabilize, since the union is $R[x]$.[1] It follows that some x^n can be expressed as a linear combination of smaller powers of x. Thus x is integral over R. ▲

So, if R' is an R-module, we can say that an element $x \in R'$ is **integral** over R if either of the following equivalent conditions are satisfied:

1. There is a monic polynomial in $R[X]$ which vanishes on x.
2. $R[x] \subset R'$ is a finitely generated R-module.

Example 1.6 Let F be a field, V a finite-dimensional F-vector space, $T : V \to V$ a linear transformation. Then the ring generated by T and F inside $\mathrm{End}_F(V)$ (which is a noncommutative ring) is finite-dimensional over F. Thus, by similar reasoning, T must satisfy a polynomial equation with coefficients in F (e.g. the characteristic polynomial).

Of course, if R' is integral over R, R' may not be a finitely generated R-module. For instance, $\overline{\mathbb{Q}}$ is not a finitely generated $\mathbb{Q}$-module, although the extension is integral. As we shall see in the next section, this is always the case if R' is a finitely generated *R-algebra*.

We now will add a third equivalent condition to this idea of "integrality," at least in the case where the structure map is an injection.

Proposition 1.7 *Let R be a ring, and suppose R is a subring of R'. $x \in R'$ is integral if and only if there exists a finitely generated faithful R-module $M \subset R'$ such that $R \subset M$ and $xM \subset M$.*

A module M is *faithful* if $xM = 0$ implies $x = 0$. That is, the map from R into the $\mathbb{Z}$-endomorphisms of M is injective. If R is a *subring* of R' (i.e. the structure map $R \to R'$ is injective), then R' for instance is a faithful R-module.

[1] As an easy exercise, one may see that if a finitely generated module M is the union of an increasing sequence of submodules $M_1 \subset M_2 \subset M_3 \subset \ldots$, then $M = M_n$ for some n; we just need to take n large enough such that M_n contains each of the finitely many generators of M.

Proof. It's obvious that the second condition above (equivalent to integrality) implies the condition of this proposition. Indeed, one could just take $M = R[x]$.

Now let us prove that if there exists such an M which is finitely generated, then x is integral. Just because M is finitely generated, the submodule $R[x]$ is not obviously finitely generated. In particular, this implication requires a bit of proof.

We shall prove that the condition of this proposition implies integrality. Suppose $y_1, \ldots, y_k \in M$ generate M as R-module. Then multiplication by x gives an R-module map $M \to M$. In particular, we can write

$$xy_i = \sum a_{ij} y_j$$

where each $a_{ij} \in R$. These $\{a_{ij}\}$ may not be unique, but let us make some choices; we get a k-by-k matrix $A \in M_k(R)$. The claim is that x satisfies the characteristic polynomial of A.

Consider the matrix

$$(x1 - A) \in M_n(R').$$

Note that $(x1 - A)$ annihilates each y_i, by the choice of A. We can consider the adjoint $B = (x1 - A)^{adj}$. Then

$$B(x1 - A) = \det(x1 - A)1.$$

This product of matrices obviously annihilates each vector y_i. It follows that

$$(\det(x1 - A)y_i = 0, \quad \forall i,$$

which implies that $\det(x1 - A)$ kills M. This implies that $\det(x1 - A) = 0$ since M is faithful.

As a result, x satisfies the characteristic polynomial. ▲

EXERCISE 7.1 Let R be a noetherian local domain with maximal ideal $\mathfrak{m}$. As we will define shortly, R is *integrally closed* if every element of the quotient field $K = K(R)$ integral over R belongs to R itself. Then if $x \in K$ and $x\mathfrak{m} \subset \mathfrak{m}$, we have $x \in R$.

EXERCISE 7.2 Let us say that an A-module is *n-generated* if it is generated by at most n elements.

Let A and B be two rings such that $A \subset B$, so that B is an A-module.

Let $n \in \mathbb{N}$. Let $u \in B$. Then, the following four assertions are equivalent:

1. There exists a monic polynomial $P \in A[X]$ with $\deg P = n$ and $P(u) = 0$.
2. There exist a B-module C and an n-generated A-submodule U of C such that $uU \subset U$ and such that every $v \in B$ satisfying $vU = 0$ satisfies $v = 0$. (Here, C is an A-module, since C is a B-module and $A \subset B$.)
3. There exists an n-generated A-submodule U of B such that $1 \in U$ and $uU \subset U$.
4. As an A-module, $A[u]$ is spanned by $1, u, \ldots, u^{n-1}$.

We proved this to show that the set of integral elements is well behaved.

Proposition 1.8 *Let $R \subset R'$. Let $S = \{x \in R' : x \text{ is integral over } R\}$. Then S is a subring of R'. In particular, it is closed under addition and multiplication.*

Proof. Suppose $x, y \in S$. We can consider the finitely generated modules $R[x], R[y] \subset R'$ generated (as algebras) by x over R. By assumption, these are finitely generated R-modules. In particular, the tensor product

$$R[x] \otimes_R R[y]$$

is a finitely generated R-module (by **??**).

We have a ring-homomorphism $R[x] \otimes_R R[y] \to R'$ which comes from the inclusions $R[x], R[y] \hookrightarrow R'$. Let M be the image of $R[x] \otimes_R R[y]$ in R'. Then M is an R-submodule of R', indeed an R-subalgebra containing x, y. Also, M is finitely generated. Since $x + y, xy \in M$ and M is a subalgebra, it follows that

$$(x + y)M \subset M, \quad xyM \subset M.$$

Thus $x + y, xy$ are integral over R. ▲

Let us consider the ring $\mathbb{Z}[\sqrt{-5}]$; this is the canonical example of a ring where unique factorization fails. This is because $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. One might ask: what about $\mathbb{Z}[\sqrt{-3}]$? It turns out that $\mathbb{Z}[\sqrt{-3}]$ lacks unique factorization as well. Indeed, here we have

$$(1 - \sqrt{-3})(1 + \sqrt{-3}) = 4 = 2 \times 2.$$

These elements can be factored no more, and $1 - \sqrt{-3}$ and 2 do not differ by units. So in this ring, we have a failure of unique factorization. Nonetheless, the failure of unique factorization in $\mathbb{Z}[\sqrt{-3}]$ is less noteworthy, because $\mathbb{Z}[\sqrt{-3}]$ is not *integrally closed*. Indeed, it turns out that $\mathbb{Z}[\sqrt{-3}]$ is contained in the larger ring $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, which does have unique factorization, and this larger ring is finite over $\mathbb{Z}[\sqrt{-3}]$.[2] Since being integrally closed is a prerequisite for having unique factorization (see **??** below), the failure in $\mathbb{Z}[\sqrt{-3}]$ is not particularly surprising.

Note that, by contrast, $\mathbb{Z}[\frac{1+\sqrt{-5}}{2}]$ does not contain $\mathbb{Z}[\sqrt{-5}]$ as a finite index subgroup—it cannot be slightly enlarged in the same sense. When one enlarges $\mathbb{Z}[\sqrt{-5}]$, one has to add a lot of stuff. We will see more formally that $\mathbb{Z}[\sqrt{-5}]$ is *integrally closed* in its quotient field, while $\mathbb{Z}[\sqrt{-3}]$ is not. Since unique factorization domains are automatically integrally closed, the failure of $\mathbb{Z}[\sqrt{-5}]$ to be a UFD is much more significant than that of $\mathbb{Z}[\sqrt{-3}]$.

1.2 Le sorite for integral extensions

In commutative algebra and algebraic geometry, there are a lot of standard properties that a *morphism* of rings $\phi : R \to S$ can have: it could be of *finite type* (that is, S is finitely generated over $\phi(R)$), it could be *finite* (that is, S is a finite R-module), or it could be *integral* (which we have defined in Definition 1.1). There are many more examples that we will encounter as we dive deeper into commutative algebra. In algebraic geometry, there are corresponding properties of morphisms of *schemes,* and there are many more interesting ones here.

In these cases, there is usually—for any reasonable property—a standard and familiar list of properties that one proves about them. We will refer to such lists as "sorites," and prove our first one now.

Proposition 1.9 (Le sorite for integral morphisms) *1. For any ring R and any ideal $I \subset R$, the map $R \to R/I$ is integral.*

2. If $\phi : R \to S$ and $\psi : S \to T$ are integral morphisms, then so is $\psi \circ \phi : R \to T$.

3. If $\phi : R \to S$ is an integral morphism and R' is an R-algebra, then the base-change $R' \to R' \otimes_R S$ is integral.

[2] In fact, $\mathbb{Z}[\sqrt{-3}]$ is an index two subgroup of $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, as the ring $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ can be described as the set of elements $a + b\sqrt{-3}$ where a, b are either both integers or both integers plus $\frac{1}{2}$, as is easily seen: this set is closed under addition and multiplication.

Proof. The first property is obvious. For the second, the condition of integrality in a morphism of rings depends on the inclusion of the image in the codomain. So we can suppose that $R \subset S \subset T$. Suppose $t \in T$. By assumption, there is a monic polynomial equation

$$t^n + s_1 t^{n-1} + \cdots + s_n = 0$$

that t satisfies, where each $s_i \in S$.

In particular, we find that t is integral over $R[s_1, \ldots, s_n]$. As a result, the module $R[s_1, \ldots, s_n, t]$ is finitely generated over the ring $R' = R[s_1, \ldots, s_n]$. By the following Proposition 1.10, R' is a finitely generated R-module. In particular, $R[s_1, \ldots, s_n, t]$ is a finitely generated R-module (not just a finitely generated R'-module).

Thus the R-module $R[s_1, \ldots, s_n, t]$ is a faithful R' module, finitely generated over R, which is preserved under multiplication by t. ▲

We now prove a result that can equivalently be phrased as "finite type plus integral implies finite" for a map of rings.

Proposition 1.10 *Let R' be a finitely generated, integral R-algebra. Then R' is a finitely generated R-module: that is, the map $R \to R'$ is finite.*

Proof. Induction on the number of generators of R' as R-algebra. For one generator, this follows from Proposition 1.5. In general, we will have $R' = R[\alpha_1, \ldots, \alpha_n]$ for some $\alpha_i \in R'$. By the inductive hypothesis, $R[\alpha_1, \ldots, \alpha_{n-1}]$ is a finite R-module; by the case of one generator, R' is a finite $R[\alpha_1, \ldots, \alpha_{n-1}]$-module. This establishes the result by the next exercise. ▲

EXERCISE 7.3 Let $R \to S, S \to T$ be morphisms of rings. Suppose S is a finite R-module and T a finite T-module. Then T is a finite R-module.

1.3 Integral closure

Let R, R' be rings.

Definition 1.11 If $R \subset R'$, then the set $S = \{x \in R' : x \text{ is integral}\}$ is called the **integral closure** of R in R'. We say that R is **integrally closed in** R' if $S = R'$.

When R is a domain, and K is the quotient field, we shall simply say that R is **integrally closed** if it is integrally closed in K. Alternatively, some people say that R is **normal** in this case.

Integral closure (in, say, the latter sense) is thus an operation that maps integral domains to integral domains. It is easy to see that the operation is *idempotent:* the integral closure of the integral closure is the integral closure.

Example 1.12 The integers $\mathbb{Z} \subset \mathbb{C}$ have as integral closure (in $\mathbb{C}$) the set of complex numbers satisfying a monic polynomial with integral coefficients. This set is called the set of **algebraic integers**.

For instance, i is an algebraic integer because it satisfies the equation $X^2 + 1 = 0$. $\frac{1-\sqrt{-3}}{2}$ is an algebraic integer, as we talked about last time; it is a sixth root of unity. On the other hand, $\frac{1+\sqrt{-5}}{2}$ is not an algebraic integer.

Example 1.13 Take $\mathbb{Z} \subset \mathbb{Q}$. The claim is that $\mathbb{Z}$ is integrally closed in its quotient field $\mathbb{Q}$, or simply—integrally closed.

Proof. We will build on this proof later. Here is the point. Suppose $\frac{a}{b} \in \mathbb{Q}$ satisfying an equation

$$P(a/b) = 0, \quad P(t) = t^n + c_1 t^{n-1} + \cdots + c_0, \ \forall c_i \in \mathbb{Z}.$$

Assume that a, b have no common factors; we must prove that b has no prime factors, so is ± 1. If b had a prime factor, say q, then we must obtain a contradiction.

We interrupt with a definition.

Definition 1.14 The **valuation at** q (or **q-adic valuation**) is the map $v_q : \mathbb{Q}^* \to \mathbb{Z}$ is the function sending $q^k(a/b)$ to k if $q \nmid a, b$. We extend this to all rational numbers via $v(0) = \infty$.

In general, this just counts the number of factors of q in the expression.

Note the general property that

$$v_q(x+y) \geq \min(v_q(x), v_q(y)). \tag{7.1}$$

If x, y are both divisible by some power of q, so is $x+y$; this is the statement above. We also have the useful property

$$v_q(xy) = v_q(x) + v_q(y). \tag{7.2}$$

Now return to the proof that $\mathbb{Z}$ is normal. We would like to show that $v_q(a/b) \geq 0$. This will prove that b is not divisible by q. When we show this for all q, it will follow that $a/b \in \mathbb{Z}$.

We are assuming that $P(a/b) = 0$. In particular,

$$\left(\frac{a}{b}\right)^n = -c_1 \left(\frac{a}{b}\right)^{n-1} - \cdots - c_0.$$

Apply v_q to both sides:

$$n v_q(a/b) \geq \min_{i>0} v_q(c_i (a/b)^{n-i}).$$

Since the $c_i \in \mathbb{Z}$, their valuations are nonnegative. In particular, the right hand side is at least

$$\min_{i>0} (n-i) v_q(a/b).$$

This cannot happen if $v_q(a/b) < 0$, because $n - i < n$ for each $i > 0$. ▲

This argument applies more generally. If K is a field, and $R \subset K$ is a subring "defined by valuations," such as the v_q, then R is integrally closed in its quotient field. More precisely, note the reasoning of the previous example: the key idea was that $\mathbb{Z} \subset \mathbb{Q}$ was characterized by the rational numbers x such that $v_q(x) \geq 0$ for all primes q. We can abstract this idea as follows. If there exists a family of functions $\mathcal{V}$ from $K^* \to \mathbb{Z}$ (such as $\{v_q : \mathbb{Q}^* \to \mathbb{Z}\}$) satisfying (7.1) and (7.2) above such that R is the set of elements such that $v(x) \geq 0, v \in \mathcal{V}$ (along with 0), then R is integrally closed in K. We will talk more about this, and about valuation rings, below.

Example 1.15 We saw earlier (Example 1.2) that $\mathbb{Z}[\sqrt{-3}]$ is not integrally closed, as $\frac{1+\sqrt{-3}}{2}$ is integral over this ring and in the quotient field, but not in the ring.

We shall give more examples in the next subsection.

1.4 Geometric examples

Let us now describe the geometry of a non-integrally closed ring. Recall that finitely generated (reduced) $\mathbb{C}$-algebras are supposed to correspond to affine algebraic varieties. A *smooth* variety (i.e., one that is a complex manifold) will always correspond to an integrally closed ring (though this relies on a deep result that a regular local ring is a factorization domain, and consequently integrally closed): non-normality is a sign of singularities.

Example 1.16 Here is a ring which is not integrally closed. Take $\mathbb{C}[x,y]/(x^2-y^3)$. Algebraically, this is the subring of the polynomial ring $\mathbb{C}[t]$ generated by t^2 and t^3.

In the complex plane, $\mathbb{C}^2$, this corresponds to the subvariety $C \subset \mathbb{C}^2$ defined by $x^2 = y^3$. In $\mathbb{R}^2$, this can be drawn: it has a singularity at $(x,y) = 0$.

Note that $x^2 = y^3$ if and only if there is a complex number z such that $x = z^3, y = z^2$. This complex number z can be recovered via x/y when $x, y \neq 0$. In particular, there is a map $\mathbb{C} \to C$ which sends $z \to (z^3, z^2)$. At every point other than the origin, the inverse can be recovered using rational functions. But this does not work at the origin.

We can think of $\mathbb{C}[x,y]/(x^2-y^3)$ as the subring R' of $\mathbb{C}[z]$ generated by $\{z^n, n \neq 1\}$. There is a map from $\mathbb{C}[x,y]/(x^2-y^3)$ sending $x \to z^3, y \to z^2$. Since these two domains are isomorphic, and R' is not integrally closed, it follows that $\mathbb{C}[x,y]/(x^2-y^3)$ is not integrally closed. The element z can be thought of as an element of the fraction field of R' or of $\mathbb{C}[x,y]/(x^2-y^3)$. It is integral, though.

The failure of the ring to be integrally closed has to do with the singularity at the origin.

We now give a generalization of the above example.

Example 1.17 This example is outside the scope of the present course. Say that $X \subset \mathbb{C}^n$ is given as the zero locus of some holomorphic functions $\{f_i : \mathbb{C}^n \to \mathbb{C}\}$. We just gave an example when $n = 2$. Assume that $0 \in X$, i.e. each f_i vanishes at the origin.

Let R be the ring of germs of holomorphic functions 0, in other words holomorphic functions from small open neighborhoods of zero. Each of these f_i becomes an element of R. The ring $R/(\{f_i\})$ is called the ring of germs of holomorphic functions on X at zero.

Assume that R is a domain. This assumption, geometrically, means that near the point zero in X, X can't be broken into two smaller closed analytic pieces. The fraction field of R is to be thought of as the ring of germs of meromorphic functions on X at zero.

We state the following without proof:

Theorem 1.18 *Let g/g' be an element of the fraction field, i.e. $g, g' \in R$. Then g/g' is integral over R if and only if g/g' is bounded near zero.*

In the previous example of X defined by $x^2 = y^3$, the function x/y (defined near the origin on the curve) is bounded near the origin, so it is integral over the ring of germs of regular functions. The reason it is not defined near the origin is *not* that it blows up. In fact, it extends continuously, but not holomorphically, to the rest of the variety X.

§2 Lying over and going up

We now interpret integrality in terms of the geometry of Spec. In general, for $R \to S$ a ring-homomorphism, the induced map $\operatorname{Spec} S \to \operatorname{Spec} R$ need not be topologically nice; for instance, even if S is a finitely generated R-algebra, the image of $\operatorname{Spec} S$ in $\operatorname{Spec} R$ need not be either open or closed.[3]

We shall see that under conditions of integrality, more can be said.

2.1 Lying over

In general, given a morphism of algebraic varieties $f : X \to Y$, the image of a closed subset $Z \subset X$ is far from closed. For instance, a regular function $f : X \to \mathbb{C}$ that is a closed map would have to

[3]It is, however, true that if R is *noetherian* (see Chapter 5) and S finitely generated over R, then the image of $\operatorname{Spec} S$ is *constructible,* that is, a finite union of locally closed subsets. **TO BE ADDED:** this result should be added sometime.

be either surjective or constant (if X is connected, say). Nonetheless, under integrality hypotheses, we can say more.

Proposition 2.1 (Lying over) *If $\phi : R \to R'$ is an integral morphism, then the induced map*

$$\operatorname{Spec} R' \to \operatorname{Spec} R$$

is a closed map; it is surjective if ϕ is injective.

Another way to state the last claim, without mentioning $\operatorname{Spec} R'$, is the following. Assume ϕ is injective and integral. Then if $\mathfrak{p} \subset R$ is prime, then there exists $\mathfrak{q} \subset R'$ such that $\mathfrak{p}$ is the inverse image $\phi^{-1}(\mathfrak{q})$.

Proof. First suppose ϕ injective, in which case we must prove the map $\operatorname{Spec} R' \to \operatorname{Spec} R$ surjective. Let us reduce to the case of a local ring. For a prime $\mathfrak{p} \in \operatorname{Spec} R$, we must show that $\mathfrak{p}$ arises as the inverse image of an element of $\operatorname{Spec} R'$. So we replace R with $R_{\mathfrak{p}}$. We get a map

$$\phi_{\mathfrak{p}} : R_{\mathfrak{p}} \to (R - \mathfrak{p})^{-1} R'$$

which is injective if ϕ is, since localization is an exact functor. Here we have localized both R, R' at the multiplicative subset $R - \mathfrak{p}$.

Note that $\phi_{\mathfrak{p}}$ is an integral extension too. This follows because integrality is preserved by base-change. We will now prove the result for $\phi_{\mathfrak{p}}$; in particular, we will show that there is a prime ideal of $(R-\mathfrak{p})^{-1}R'$ that pulls back to $\mathfrak{p}R_{\mathfrak{p}}$. These will imply that if we pull this prime ideal back to R', it will pull back to $\mathfrak{p}$ in R. In detail, we can consider the diagram

$$\begin{array}{ccc} \operatorname{Spec}(R-\mathfrak{p})^{-1}R' & \longrightarrow & \operatorname{Spec} R_{\mathfrak{p}} \\ \downarrow & & \downarrow \\ \operatorname{Spec} R' & \longrightarrow & \operatorname{Spec} R \end{array}$$

which shows that if $\mathfrak{p}R_{\mathfrak{p}}$ appears in the image of the top map, then $\mathfrak{p}$ arises as the image of something in $\operatorname{Spec} R'$. So it is sufficient for the proposition (that is, the case of ϕ injective) to handle the case of R local, and $\mathfrak{p}$ the maximal ideal.

In other words, we need to show that:

> If R is a *local* ring, $\phi : R \hookrightarrow R'$ an injective integral morphism, then the maximal ideal of R is the inverse image of something in $\operatorname{Spec} R'$.

Assume R is local with maximal ideal $\mathfrak{p}$. We want to find a prime ideal $\mathfrak{q} \subset R'$ such that $\mathfrak{p} = \phi^{-1}(\mathfrak{q})$. Since $\mathfrak{p}$ is already maximal, it will suffice to show that $\mathfrak{p} \subset \phi^{-1}(\mathfrak{q})$. In particular, we need to show that there is a prime ideal $\mathfrak{q}$ such that $\mathfrak{p}R' \subset \mathfrak{q}$. The pull-back of this will be $\mathfrak{p}$.

If $\mathfrak{p}R' \neq R'$, then $\mathfrak{q}$ exists, since every proper ideal of a ring is contained in a maximal ideal. We will in fact show

$$\mathfrak{p}R' \neq R', \tag{7.3}$$

or that $\mathfrak{p}$ does not generate the unit ideal in R'. If we prove (7.3), we will thus be able to find our $\mathfrak{q}$, and we will be done.

Suppose the contrary, i.e. $\mathfrak{p}R' = R'$. We will derive a contradiction using Nakayama's lemma (**??**). Right now, we cannot apply Nakayama's lemma directly because R' is not a finite R-module. The idea is that we will "descend" the "evidence" that (7.3) fails to a small subalgebra of R', and then obtain a contradiction. To do this, note that $1 \in \mathfrak{p}R'$, and we can write

$$1 = \sum x_i \phi(y_i)$$

where $x_i \in R', y_i \in \mathfrak{p}$. This is the "evidence" that (7.3) fails, and it involves only a finite amount of data.

Let R'' be the subalgebra of R' generated by $\phi(R)$ and the x_i. Then $R'' \subset R'$ and is finitely generated as an R-algebra, because it is generated by the x_i. However, R'' is integral over R and thus finitely generated as an R-module, by Proposition 1.10. This is where integrality comes in.

So R'' is a finitely generated R-module. Also, the expression $1 = \sum x_i \phi(y_i)$ shows that $\mathfrak{p}R'' = R''$. However, this contradicts Nakayama's lemma. That brings the contradiction, showing that $\mathfrak{p}$ cannot generate (1) in R', and proving the surjectivity part of lying over theorem.

Finally, we need to show that if $\phi : R \to R'$ is *any* integral morphism, then $\operatorname{Spec} R' \to \operatorname{Spec} R$ is a closed map. Let $X = V(I)$ be a closed subset of $\operatorname{Spec} R'$. Then the image of X in $\operatorname{Spec} R$ is the image of the map

$$\operatorname{Spec} R'/I \to \operatorname{Spec} R$$

obtained from the morphism $R \to R' \to R'/I$, which is integral; thus we are reduced to showing that any integral morphism ϕ has closed image on the Spec. Thus we are reduced to $X = \operatorname{Spec} R'$, if we throw out R' and replace it by R'/I.

In other words, we must prove the following statement. Let $\phi : R \to R'$ be an integral morphism; then the image of $\operatorname{Spec} R'$ in $\operatorname{Spec} R$ is closed. But, quotienting by $\ker \phi$ and taking the map $R/\ker \phi \to R'$, we may reduce to the case of ϕ injective; however, then this follows from the surjectivity result already proved. ▲

In general, there will be *many* lifts of a given prime ideal. Consider for instance the inclusion $\mathbb{Z} \subset \mathbb{Z}[i]$. Then the prime ideal $(5) \in \operatorname{Spec} \mathbb{Z}$ can be lifted either to $(2+i) \in \operatorname{Spec} \mathbb{Z}[i]$ or $(2-i) \in \operatorname{Spec} \mathbb{Z}[i]$. These are distinct prime ideals: $\frac{2+i}{2-i} \notin \mathbb{Z}[i]$. But note that any element of $\mathbb{Z}$ divisible by $2+i$ is automatically divisible by its conjugate $2-i$, and consequently by their product 5 (because $\mathbb{Z}[i]$ is a UFD, being a euclidean domain).

Nonetheless, the different lifts are incomparable.

Proposition 2.2 *Let $\phi : R \to R'$ be an integral morphism. Then given $\mathfrak{p} \in \operatorname{Spec} R$, there are no inclusions among the elements $\mathfrak{q} \in \operatorname{Spec} R'$ lifting $\mathfrak{p}$.*

In other words, if $\mathfrak{q}, \mathfrak{q}' \in \operatorname{Spec} R'$ lift $\mathfrak{p}$, then $\mathfrak{q} \not\subset \mathfrak{q}'$.

Proof. We will give a "slick" proof by various reductions. Note that the operations of localization and quotienting only shrink the Spec's: they do not "merge" heretofore distinct prime ideals into one. Thus, by quotienting R by $\mathfrak{p}$, we may assume R is a *domain* and that $\mathfrak{p} = 0$. Suppose we had two primes $\mathfrak{q} \subsetneq \mathfrak{q}'$ of R' lifting $(0) \in \operatorname{Spec} R$. Quotienting R' by $\mathfrak{q}$, we may assume that $\mathfrak{q} = 0$. We could even assume $R \subset R'$, by quotienting by the kernel of ϕ. The next lemma thus completes the proof, because it shows that $\mathfrak{q}' = 0$, contradiction. ▲

Lemma 2.3 *Let $R \subset R'$ be an inclusion of integral domains, which is an integral morphism. If $\mathfrak{q} \in \operatorname{Spec} R'$ is a nonzero prime ideal, then $\mathfrak{q} \cap R$ is nonzero.*

Proof. Let $x \in \mathfrak{q}'$ be nonzero. There is an equation

$$x^n + r_1 x^{n-1} + \cdots + r_n = 0, \quad r_i \in R,$$ ▲

that x satisfies, by assumption. Here we can assume $r_n \neq 0$; then $r_n \in \mathfrak{q}' \cap R$ by inspection, though. So this intersection is nonzero.

Corollary 2.4 *Let $R \subset R'$ be an inclusion of integral domains, such that R' is integral over R. Then if one of R, R' is a field, so is the other.*

Proof. Indeed, $\operatorname{Spec} R' \to \operatorname{Spec} R$ is surjective by Proposition 2.1: so if $\operatorname{Spec} R'$ has one element (i.e., R' is a field), the same holds for $\operatorname{Spec} R$ (i.e., R is a field). Conversely, suppose R a field. Then any two prime ideals in $\operatorname{Spec} R'$ pull back to the same element of $\operatorname{Spec} R$. So, by Proposition 2.2, there can be no inclusions among the prime ideals of $\operatorname{Spec} R'$. But R' is a domain, so it must then be a field. ▲

EXERCISE 7.4 Let k be a field. Show that $k[\mathbb{Q}_{\geq 0}]$ is integral over the polynomial ring $k[T]$. Although this is a *huge* extension, the prime ideal (T) lifts in only one way to $\operatorname{Spec} k[\mathbb{Q}_{\geq 0}]$.

EXERCISE 7.5 Suppose $A \subset B$ is an inclusion of rings over a field of characteristic p. Suppose $B^p \subset A$, so that B/A is integral in a very strong sense. Show that the map $\operatorname{Spec} B \to \operatorname{Spec} A$ is a *homeomorphism.*

2.2 Going up

Let $R \subset R'$ be an inclusion of rings with R' integral over R. We saw in the lying over theorem (Proposition 2.1) that any prime $\mathfrak{p} \in \operatorname{Spec} R$ has a prime $\mathfrak{q} \in \operatorname{Spec} R'$ "lying over" $\mathfrak{p}$, i.e. such that $R \cap \mathfrak{q} = \mathfrak{p}$. We now want to show that we can lift finite *inclusions* of primes to R'.

Proposition 2.5 (Going up) *Let $R \subset R'$ be an integral inclusion of rings. Suppose $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_n \subset R$ is a finite ascending chain of prime ideals in R. Then there is an ascending chain $\mathfrak{q}_1 \subset \mathfrak{q}_2 \subset \cdots \subset \mathfrak{q}_n$ in $\operatorname{Spec} R'$ lifting this chain.*

Moreover, $\mathfrak{q}_1$ can be chosen arbitrarily so as to lift $\mathfrak{p}_1$.

Proof. By induction and lying over (Proposition 2.1), it suffices to show:

> Let $\mathfrak{p}_1 \subset \mathfrak{p}_2$ be an inclusion of primes in $\operatorname{Spec} R$. Let $\mathfrak{q}_1 \in \operatorname{Spec} R'$ lift $\mathfrak{p}_1$. Then there is $\mathfrak{q}_2 \in \operatorname{Spec} R'$, which satisfies the dual conditions of lifting $\mathfrak{p}_2$ and containing $\mathfrak{q}_1$.

To show that this is true, we apply Proposition 2.1 to the inclusion $R/\mathfrak{p}_1 \hookrightarrow R'/\mathfrak{q}_1$. There is an element of $\operatorname{Spec} R'/\mathfrak{q}_1$ lifting $\mathfrak{p}_2/\mathfrak{p}_1$; the corresponding element of $\operatorname{Spec} R'$ will do for $\mathfrak{q}_2$. ▲

§3 Valuation rings

A valuation ring is a special type of local ring. Its distinguishing characteristic is that divisibility is a "total preorder." That is, two elements of the quotient field are never incompatible under divisibility. We shall see in this section that integrality can be detected using valuation rings only.

Geometrically, the valuation ring is something like a local piece of a smooth curve. In fact, in algebraic geometry, a more compelling reason to study valuation rings is provided by the valuative criteria for separatedness and properness (cf. [GD] or [Har77]). One key observation about valuation rings that leads the last results is that any local domain can be "dominated" by a valuation ring with the same quotient field (i.e. mapped into a valuation ring via local homomorphism), but valuation rings are the maximal elements in this relation of domination.

3.1 Definition

Definition 3.1 A **valuation ring** is a domain R such that for every pair of elements $a, b \in R$, either $a \mid b$ or $b \mid a$.

Example 3.2 $\mathbb{Z}$ is not a valuation ring. It is neither true that 2 divides 3 nor that 3 divides 2.

Example 3.3 $\mathbb{Z}_{(p)}$, which is the set of all fractions of the form $a/b \in \mathbb{Q}$ where $p \nmid b$, is a valuation ring. To check whether a/b divides a'/b' or vice versa, one just has to check which is divisible by the larger power of p.

Proposition 3.4 *Let R be a domain with quotient field K. Then R is a valuation ring if and only if for every $x \in K$, either x or x^{-1} lies in R.*

Proof. Indeed, if $x = a/b,\ a, b \in R$, then either $a \mid b$ or $b \mid a$, so either x or $x^{-1} \in R$. This condition is equivalent to R's being a valuation ring. ▲

3.2 Valuations

The reason for the name "valuation ring" is provided by the next definition. As we shall see, any valuation ring comes from a "valuation."

By definition, an *ordered abelian group* is an abelian group A together with a set of *positive elements* $A_+ \subset A$. This set is required to be closed under addition and satisfy the property that if $x \in A$, then precisely one of the following is true: $x \in A_+$, $-x \in A_+$, and $x = 0$. This allows one to define an ordering $<$ on A by writing $x < y$ if $y - x \in A_+$. Given A, we often formally adjoin an element ∞ which is bigger than every element in A.

Definition 3.5 Let K be a field. A **valuation** on K is a map $v : K \to A \cup \{\infty\}$ for some ordered abelian group A satisfying:

1. $v(0) = \infty$ and $v(K^*) \subset A$.
2. For $x, y \in K^*$, $v(xy) = v(x) + v(y)$. That is, $v|_{K^*}$ is a homomorphism.
3. For $x, y \in K$, $v(x + y) \geq \min(v(x), v(y))$.

Suppose that K is a field and $v : K \to A \cup \{\infty\}$ is a valuation (i.e. $v(0) = \infty$). Define $R = \{x \in K : v(x) \geq 0\}$.

Proposition 3.6 *R as just defined is a valuation ring.*

Proof. First, we prove that R is a ring. R is closed under addition and multiplication by the two conditions

$$v(xy) = v(x) + v(y)$$

and

$$v(x + y) \geq \min v(x), v(y),$$

so if $x, y \in R$, then $x + y, xy$ have nonnegative valuations.

Note that $0 \in R$ because $v(0) = \infty$. Also $v(1) = 0$ since $v : K^* \to A$ is a homomorphism. So $1 \in R$ too. Finally, $-1 \in R$ because $v(-1) = 0$ since A is totally ordered. It follows that R is also a group.

Let us now show that R is a valuation ring. If $x \in K^*$, either $v(x) \geq 0$ or $v(x^{-1}) \geq 0$ since A is totally ordered.[4] So either $x, x^{-1} \in R$. ▲

In particular, the set of elements with nonnegative valuation is a valuation ring. The converse also holds. Whenever you have a valuation ring, it comes about in this manner.

Proposition 3.7 *Let R be a valuation ring with quotient field K. There is an ordered abelian group A and a valuation $v : K^* \to A$ such that R is the set of elements with nonnegative valuation.*

[4] Otherwise $0 = v(x) + v(x^{-1}) < 0$, contradiction.

Proof. First, we construct A. In fact, it is the quotient of K^* by the subgroup of units R^* of R. We define an ordering by saying that $x \leq y$ if $y/x \in R$—this doesn't depend on the representatives in K^* chosen. Note that either $x \leq y$ or $y \leq x$ must hold, since R is a valuation ring. The combination of $x \leq y$ and $y \leq x$ implies that x, y are equivalent classes. The nonnegative elements in this group are those whose representatives in K^* belong to R.

It is easy to see that K^*/R^* in this way is a totally ordered abelian group with the image of 1 as the unit. The reduction map $K^* \to K^*/R^*$ defines a valuation whose corresponding ring is just R. We have omitted some details; for instance, it should be checked that the valuation of $x + y$ is at least the minimum of $v(x), v(y)$. ▲

To summarize:

> Every valuation ring R determines a valuation v from the fraction field of R into $A \cup \{\infty\}$ for A a totally ordered abelian group such that R is just the set of elements of K with nonnegative valuation. As long as we require that $v : K^* \to A$ is surjective, then A is uniquely determined as well.

Definition 3.8 A valuation ring R is **discrete** if we can choose A to be $\mathbb{Z}$.

Example 3.9 $\mathbb{Z}_{(p)}$ is a discrete valuation ring.

The notion of a valuation ring is a useful one.

3.3 General remarks

Let R be a commutative ring. Then $\operatorname{Spec} R$ is the set of primes of R, equipped with a certain topology. The space $\operatorname{Spec} R$ is almost never Hausdorff. It is almost always a bad idea to apply the familiar ideas from elementary topology (e.g. the fundamental group) to $\operatorname{Spec} R$. Nonetheless, it has some other nice features that substitute for its non-Hausdorffness.

For instance, if $R = \mathbb{C}[x, y]$, then $\operatorname{Spec} R$ corresponds to $\mathbb{C}^2$ with some additional nonclosed points. The injection of $\mathbb{C}^2$ with its usual topology into $\operatorname{Spec} R$ is continuous. While in $\operatorname{Spec} R$ you don't want to think of continuous paths, you can in $\mathbb{C}^2$.

Suppose you had two points $x, y \in \mathbb{C}^2$ and their images in $\operatorname{Spec} R$. Algebraically, you can still think about algebraic curves passing through x, y. This is a subset of x, y defined by a single polynomial equation. This curve will have what's called a "generic point," since the ideal generated by this curve will be a prime ideal. The closure of this generic point will be precisely this algebraic curve—including x, y.

Remark If $\mathfrak{p}, \mathfrak{p}' \in \operatorname{Spec} R$, then

$$\mathfrak{p}' \in \overline{\{\mathfrak{p}\}}$$

iff

$$\mathfrak{p}' \supset \mathfrak{p}.$$

Why is this? Well, the closure of $\{\mathfrak{p}\}$ is just $V(\mathfrak{p})$, since this is the smallest closed subset of $\operatorname{Spec} R$ containing $\mathfrak{p}$.

The point of this discussion is that instead of paths, one can transmit information from point to point in $\operatorname{Spec} R$ by having one point be in a closure of another. However, we will show that this relation is contained by the theory of valuation rings.

Theorem 3.10 *Let R be a domain containing a prime ideal $\mathfrak{p}$. Let K be the fraction field of R. Then there is a valuation v on K defining a valuation ring $R' \subset K$ such that*

1. *$R \subset R'$.*

2. $\mathfrak{p} = \{x \in R : v(x) > 0\}$.

Let us motivate this by the remark:

Remark A valuation ring is automatically a local ring. A local ring is a ring where either $x, 1-x$ is invertible for all x in the ring. Let us show that this is true for a valuation ring.

If x belongs to a valuation ring R with valuation v, it is invertible if $v(x) = 0$. So if $x, 1-x$ were both noninvertible, then both would have positive valuation. However, that would imply that $v(1) \geq \min v(x), v(1-x)$ is positive, contradiction.

> If R' is any valuation ring (say defined by a valuation v), then R' is local with maximal ideal consisting of elements with positive valuation.

The theorem above says that there's a good supply of valuation rings. In particular, if R is any domain, $\mathfrak{p} \subset R$ a prime ideal, then we can choose a valuation ring $R' \supset R$ such that $\mathfrak{p}$ is the intersection of the maximal ideal of R' intersected with R. So the map $\operatorname{Spec} R' \to \operatorname{Spec} R$ contains $\mathfrak{p}$.

Proof. Without loss of generality, replace R by $R_{\mathfrak{p}}$, which is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. The maximal ideal intersects R only in $\mathfrak{p}$.

So, we can assume without loss of generality that

1. R is local.
2. $\mathfrak{p}$ is maximal.

Let P be the collection of all subrings $R' \subset K$ such that $R' \supset R$ but $\mathfrak{p}R' \neq R'$. Then P is a poset under inclusion. The poset is nonempty, since $R \in P$. Every totally ordered chain in P has an upper bound. If you have a totally ordered subring of elements in P, then you can take the union. We invoke:

Lemma 3.11 *Let R_α be a chain in P and $R' = \bigcup R_\alpha$. Then $R' \in P$.*

Proof. Indeed, it is easy to see that this is a subalgebra of K containing R. The thing to observe is that

$$\mathfrak{p}R' = \bigcup_\alpha \mathfrak{p}R_\alpha;$$

since by assumption, $1 \notin \mathfrak{p}R_\alpha$ (because each $R_\alpha \in P$), $1 \notin \mathfrak{p}R'$. In particular, $R' \notin P$. ▲

By the lemma, Zorn's lemma to the poset P. In particular, P has a maximal element R'. By construction, R' is some subalgebra of K and $\mathfrak{p}R' \neq R'$. Also, R' is maximal with respect to these properties.

We show first that R' is local, with maximal ideal $\mathfrak{m}$ satisfying

$$\mathfrak{m} \cap R = \mathfrak{p}.$$ ▲

The second part is evident from locality of R', since $\mathfrak{m}$ must contain the proper ideal $\mathfrak{p}R'$, and $\mathfrak{p} \subset R$ is a maximal ideal.

Suppose that $x \in R'$; we show that either $x, 1-x$ belongs to R'^* (i.e. is invertible). Take the ring $R'[x^{-1}]$. If x is noninvertible, this properly contains R'. By maximality, it follows that $\mathfrak{p}R'[x^{-1}] = R'[x^{-1}]$.

And we're out of time. We'll pick this up on Monday.

Let us set a goal.

First, recall the notion introduced last time. A **valuation ring** is a domain R where for all x in the fraction field of R, either x or x^{-1} lies in R. We saw that if R is a valuation ring, then R is local. That is, there is a unique maximal ideal $\mathfrak{m} \subset R$, automatically prime. Moreover, the zero ideal (0) is prime, as R is a domain. So if you look at the spectrum $\operatorname{Spec} R$ of a valuation ring R, there is a unique closed point $\mathfrak{m}$, and a unique generic point (0). There might be some other prime ideals in $\operatorname{Spec} R$; this depends on where the additional valuation lives.

Example 3.12 Suppose the valuation defining the valuation ring R takes values in $\mathbb{R}$. Then the only primes are $\mathfrak{m}$ and zero.

Let R now be any ring, with $\operatorname{Spec} R$ containing prime ideals $\mathfrak{p} \subset \mathfrak{q}$. In particular, $\mathfrak{q}$ lies in the closure of $\mathfrak{p}$. As we will see, this implies that there is a map

$$\phi : R \to R'$$

such that $\mathfrak{p} = \phi^{-1}(0)$ and $\mathfrak{q} = \phi^{-1}(\mathfrak{m})$, where $\mathfrak{m}$ is the maximal ideal of R'. This statement says that the relation of closure in $\operatorname{Spec} R$ is always controlled by valuation rings. In yet another phrasing, in the map

$$\operatorname{Spec} R' \to \operatorname{Spec} R$$

the closed point goes to $\mathfrak{q}$ and the generic point to $\mathfrak{p}$. This is our eventual goal.

To carry out this goal, we need some more elementary facts. Let us discuss things that don't have any obvious relation to it.

3.4 Back to the goal

Now we return to the goal of the lecture. Again, R was any ring, and we had primes $\mathfrak{p} \subset \mathfrak{q} \subset R$. We wanted a valuation ring R' and a map $\phi : R \to R'$ such that zero pulled back to $\mathfrak{p}$ and the maximal ideal pulled back to $\mathfrak{q}$.

What does it mean for $\mathfrak{p}$ to be the inverse image of $(0) \subset R'$? This means that $\mathfrak{p} = \ker \phi$. So we get an injection

$$R/\mathfrak{p} \rightarrowtail R'.$$

We will let R' be a subring of the quotient field K of the domain $R/\mathfrak{p}$. Of course, this subring will contain $R/\mathfrak{p}$.

In this case, we will get a map $R \to R'$ such that the pull-back of zero is $\mathfrak{p}$. What we want, further, to be true is that R' is a valuation ring and the pull-back of the maximal ideal is $\mathfrak{q}$.

This is starting to look at the problem we discussed last time. Namely, let's throw out R, and replace it with $R/\mathfrak{p}$. Moreover, we can replace R with $R_{\mathfrak{q}}$ and assume that R is local with maximal ideal $\mathfrak{q}$. What we need to show is that a valuation ring R' contained in the fraction field of R, containing R, such that the intersection of the maximal ideal of R' with R is equal to $\mathfrak{q} \subset R$. If we do this, then we will have accomplished our goal.

Lemma 3.13 *Let R be a local domain. Then there is a valuation subring R' of the quotient field of R that* dominates *R, i.e .the map $R \to R'$ is a* local *homomorphism.*

Let's find R' now.

Choose R' maximal such that $\mathfrak{q}R' \neq R'$. Such a ring exists, by Zorn's lemma. We gave this argument at the end last time.

Lemma 3.14 *R' as described is local.*

Proof. Look at $\mathfrak{q}R' \subset R'$; it is a proper subset, too, by assumption. In particular, $\mathfrak{q}R'$ is contained in some maximal ideal $\mathfrak{m} \subset R'$. Replace R' by $R'' = R'_{\mathfrak{m}}$. Note that

$$R' \subset R''$$

and

$$\mathfrak{q}R'' \neq R''$$

because $\mathfrak{m}R'' \neq R''$. But R' is maximal, so $R' = R''$, and R'' is a local ring. So R' is a local ring.▲

Let $\mathfrak{m}$ be the maximal ideal of R'. Then $\mathfrak{m} \supset \mathfrak{q}R$, so $\mathfrak{m} \cap R = \mathfrak{q}$. All that is left to prove now is that R' is a valuation ring.

Lemma 3.15 *R' is integrally closed.*

Proof. Let R'' be its integral closure. Then $\mathfrak{m}R'' \neq R''$ by lying over, since $\mathfrak{m}$ (the maximal ideal of R') lifts up to R''. So R'' satisfies

$$\mathfrak{q}R'' \neq R''$$

and by maximality, we have $R'' = R'$. ▲

To summarize, we know that R' is a local, integrally closed subring of the quotient field of R, such that the maximal ideal of R' pulls back to $\mathfrak{q}$ in R. All we now need is:

Lemma 3.16 *R' is a valuation ring.*

Proof. Let x lie in the fraction field. We must show that either x or $x^{-1} \in R'$. Say $x \notin R'$. This means by maximality of R' that $R'' = R'[x]$ satisfies

$$\mathfrak{q}R'' = R''.$$

In particular, we can write

$$1 = \sum q_i x^i, \quad q_i \in \mathfrak{q}R' \subset R'.$$

This implies that

$$(1 - q_0) + \sum_{i>0} -q_i x^i = 0.$$

But $1 - q_0$ is invertible in R', since R' is local. We can divide by the highest power of x:

$$x^{-N} + \sum_{i>0} \frac{-q_i}{1 - q_0} x^{-N+i} = 0.$$

In particular, $1/x$ is integral over R'; this implies that $1/x \in R'$ since R' is integrally closed and q_0 is a nonunit. So R' is a valuation ring. ▲

We can state the result formally.

Theorem 3.17 *Let R be a ring, $\mathfrak{p} \subset \mathfrak{q}$ prime ideals. Then there is a homomorphism $\phi : R \to R'$ into a valuation ring R' with maximal ideal $\mathfrak{m}$ such that*

$$\phi^{-1}(0) = \mathfrak{p}$$

and

$$\phi^{-1}(\mathfrak{m}) = \mathfrak{q}.$$

There is a related fact which we now state.

Theorem 3.18 *Let R be any domain. Then the integral closure of R in the quotient field K is the intersection*

$$\bigcap R_\alpha$$

of all valuation rings $R_\alpha \subset K$ containing R.

So an element of the quotient field is integral over R if and only if its valuation is nonnegative at every valuation which is nonnegative on R.

Proof. The $\subset$ argument is easy, because one can check that a valuation ring is integrally closed. (Exercise.) The interesting direction is to assume that $v(x) \geq 0$ for all v nonnegative on R.

Let us suppose x is nonintegral. Suppose $R' = R[1/x]$ and I be the ideal $(x^{-1}) \subset R'$. There are two cases:

1. $I = R'$. Then in the ring R', x^{-1} is invertible. In particular, $x^{-1}P(x^{-1}) = 1$. Multiplying by a high power of x shows that x is integral over R. Contradiction.
2. Suppose $I \subsetneq R'$. Then I is contained in a maximal ideal $\mathfrak{q} \subset R'$. There is a valuation subring $R'' \subset K$, containing R', such that the corresponding valuation is positive on $\mathfrak{q}$. In particular, this valuation is positive on x^{-1}, so it is negative on x, contradiction. ▲

So the integral closure has this nice characterization via valuation rings. In some sense, the proof that $\mathbb{Z}$ is integrally closed has the property that every integrally closed ring is integrally closed for that reason: it's the common nonnegative locus for some valuations.

§4 The Hilbert Nullstellensatz

The Nullstellensatz is the basic algebraic fact, which we have invoked in the past to justify various examples, that connects the idea of the Spec of a ring to classical algebraic geometry.

4.1 Statement and initial proof of the Nullstellensatz

There are several ways in which the Nullstellensatz can be stated. Let us start with the following very concrete version.

Theorem 4.1 *All maximal ideals in the polynomial ring $R = \mathbb{C}[x_1, \dots, x_n]$ come from points in $\mathbb{C}^n$. In other words, if $\mathfrak{m} \subset R$ is maximal, then there exist $a_1, \dots, a_n \in \mathbb{C}$ such that $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$.*

The maximal spectrum of $R = \mathbb{C}[x_1, \dots, x_n]$ is thus identified with $\mathbb{C}^n$.

We shall now reduce Theorem 4.1 to an easier claim. Let $\mathfrak{m} \subset R$ be a maximal ideal. Then there is a map

$$\mathbb{C} \to R \to R/\mathfrak{m}$$

where $R/\mathfrak{m}$ is thus a finitely generated $\mathbb{C}$-algebra, as R is. The ring $R/\mathfrak{m}$ is also a field by maximality.

We would like to show that $R/\mathfrak{m}$ is a finitely generated $\mathbb{C}$-vector space. This would imply that $R/\mathfrak{m}$ is integral over $\mathbb{C}$, and there are no proper algebraic extensions of $\mathbb{C}$. Thus, if we prove this, it will follow that the map $\mathbb{C} \to R/\mathfrak{m}$ is an isomorphism. If $a_i \in \mathbb{C}$ $(1 \leq i \leq n)$ is the image of x_i in $R/\mathfrak{m} = \mathbb{C}$, it will follow that $(x_1 - a_1, \dots, x_n - a_n) \subset \mathfrak{m}$, so $(x_1 - a_1, \dots, x_n - a_n) = \mathfrak{m}$.

Consequently, the Nullstellensatz in this form would follow from the next claim:

Proposition 4.2 *Let k be a field, L/k an extension of fields. Suppose L is a finitely generated k-algebra. Then L is a finite k-vector space.*

This is what we will prove.

We start with an easy proof in the special case:

Lemma 4.3 *Assume k is uncountable (e.g. $\mathbb{C}$, the original case of interest). Then the above proposition is true.*

Proof. Since L is a finitely generated k-algebra, it suffices to show that L/k is algebraic. If not, there exists $x \in L$ which isn't algebraic over k. So x satisfies no nontrivial polynomials. I claim now that the uncountably many elements $\frac{1}{x-\lambda}, \lambda \in K$ are linearly independent over K. This will be a contradiction as L is a finitely generated k-algebra, hence at most countably dimensional over k. (Note that the polynomial ring is countably dimensional over k, and L is a quotient.)

So let's prove this. Suppose not. Then there is a nontrivial linear dependence

$$\sum \frac{c_i}{x - \lambda_i} = 0, \quad c_i, \lambda_i \in K.$$

Here the λ_j are all distinct to make this nontrivial. Clearing denominators, we find

$$\sum_i c_i \prod_{j \neq i} (x - \lambda_j) = 0.$$

Without loss of generality, $c_1 \neq 0$. This equality was in the field L. But x is transcendental over k. So we can think of this as a polynomial ring relation. Since we can think of this as a relation in the polynomial ring, we see that doing so, all but the $i = 1$ term in the sum is divisible by $x - \lambda_1$ as a polynomial. It follows that, as polynomials in the indeterminate x,

$$x - \lambda_1 \mid c_1 \prod_{j \neq 1} (x - \lambda_j).$$

This is a contradiction since all the λ_i are distinct. ▲

This is kind of a strange proof, as it exploits the fact that $\mathbb{C}$ is uncountable. This shouldn't be relevant.

4.2 The normalization lemma

Let's now give a more algebraic proof. We shall exploit the following highly useful fact in commutative algebra:

Theorem 4.4 (Noether normalization lemma) *Let k be a field, and $R = k[x_1, \dots, x_n]/\mathfrak{p}$ be a finitely generated domain over k (where $\mathfrak{p}$ is a prime ideal in the polynomial ring).*

Then there exists a polynomial subalgebra $k[y_1, \dots, y_m] \subset R$ such that R is integral over $k[y_1, \dots, y_m]$.

Later we will see that m is the *dimension* of R.

There is a geometric picture here. Then $\operatorname{Spec} R$ is some irreducible algebraic variety in k^n (plus some additional points), with a smaller dimension than n if $\mathfrak{p} \neq 0$. Then there exists a *finite map* to k^m. In particular, we can map surjectively $\operatorname{Spec} R \to k^m$ which is integral. The fibers are in fact finite, because integrality implies finite fibers. (We have not actually proved this yet.)

How do we actually find such a finite projection? In fact, in characteristic zero, we just take a vector space projection $\mathbb{C}^n \to \mathbb{C}^m$. For a "generic" projection onto a subspace of the appropriate dimension, the projection will will do as our finite map. In characteristic p, this may not work.

Proof. First, note that m is uniquely determined as the transcendence degree of the quotient field of R over k.

Among the variables $x_1, \dots, x_n \in R$ (which we think of as in R by an abuse of notation), choose a maximal subset which is algebraically independent. This subset has no nontrivial polynomial relations. In particular, the ring generated by that subset is just the polynomial ring on that subset. We can permute these variables and assume that

$$\{x_1, \dots, x_m\}$$

is the maximal subset. In particular, R contains the *polynomial ring* $k[x_1, \dots, x_m]$ and is generated by the rest of the variables. The rest of the variables are not adjoined freely though.

The strategy is as follows. We will implement finitely many changes of variable so that R becomes integral over $k[x_1, \dots, x_m]$.

The essential case is where $m = n - 1$. Let us handle this. So we have

$$R_0 = k[x_1, \dots, x_m] \subset R = R_0[x_n]/\mathfrak{p}.$$

Since x_n is not algebraically independent, there is a nonzero polynomial $f(x_1, \dots, x_m, x_n) \in \mathfrak{p}$.

We want f to be monic in x_n. This will buy us integrality. A priori, this might not be true. We will modify the coordinate system to arrange that, though. Choose $N \gg 0$. Define for $1 \leq i \leq m$,

$$x_i' = x_i + x_n^{N^i}.$$

Then the equation becomes:

$$0 = f(x_1, \dots, x_m, x_n) = f(\left\{x_i' - x_n^{N^i}\right\}, x_n).$$

Now $f(x_1, \dots, x_n, x_{n+1})$ looks like some sum

$$\sum \lambda_{a_1 \dots b} x_1^{a_1} \dots x_m^{a_m} x_n^b, \quad \lambda_{a_1 \dots b} \in k.$$

But N is really really big. Let us expand this expression in the x_i' and pay attention to the largest power of x_n we see. We find that

$$f(\left\{x_i' - x_n^{N_i}\right\}, x_n)$$

has the largest power of x_n precisely where, in the expression for f, a_m is maximized first, then a_{m-1}, and so on. The largest exponent would have the form

$$x_n^{a_m N^m + a_{m-1} N^{m-1} + \dots + b}.$$

We can't, however, get any exponents of x_n in the expression $f(\left\{x_i' - x_n^{N_i}\right\}, x_n)$ other than these. If N is super large, then all these exponents will be different from each other. In particular, each power of x_n appears precisely once in the expansion of f. We see in particular that x_n is integral over $x_1', \dots, x_n'$. Thus each x_i is as well.

So we find

R is integral over $k[x_1', \dots, x_m']$.

We have thus proved the normalization lemma in the codimension one case. What about the general case? We repeat this. Say we have

$$k[x_1, \dots, x_m] \subset R.$$

Let R' be the subring of R generated by $x_1, \ldots, x_m, x_{m+1}$. The argument we just gave implies that we can choose $x_1', \ldots, x_m'$ such that R' is integral over $k[x_1', \ldots, x_m']$, and the x_i' are algebraically independent. We know in fact that $R' = k[x_1', \ldots, x_m', x_{m+1}]$.

Let us try repeating the argument while thinking about x_{m+2}. Let $R'' = k[x_1', \ldots, x_m', x_{m+2}]$ modulo whatever relations that x_{m+2} has to satisfy. So this is a subring of R. The same argument shows that we can change variables such that $x_1'', \ldots, x_m''$ are algebraically independent and R'' is integral over $k[x_1'', \ldots, x_m'']$. We have furthermore that $k[x_1'', \ldots, x_m'', x_{m+2}] = R''$.

Having done this, let us give the argument where $m = n - 2$. You will then see how to do the general case. Then I claim that:

R is integral over $k[x_1'', \ldots, x_m'']$.

For this, we need to check that x_{m+1}, x_{m+2} are integral (because these together with the x_i'' generate $R''[x_{m+2}][x_{m+2}] = R$. But x_{m+2} is integral over this by construction. The integral closure of $k[x_1'', \ldots, x_m'']$ in R thus contains

$$k[x_1'', \ldots, x_m'', x_{m+2}] = R''. \qquad \blacktriangle$$

However, R'' contains the elements $x_1', \ldots, x_m'$. But by construction, x_{m+1} is integral over the $x_1', \ldots, x_m'$. The integral closure of $k[x_1'', \ldots, x_m'']$ must contain x_{m+2}. This completes the proof in the case $m = n - 2$. The general case is similar; we just make several changes of variables, successively.

4.3 Back to the Nullstellensatz

Consider a finitely generated k-algebra R which is a field. We need to show that R is a finite k-module. This will prove the proposition. Well, note that R is integral over a polynomial ring $k[x_1, \ldots, x_m]$ for some m. If $m > 0$, then this polynomial ring has more than one prime. For instance, (0) and $(x_1, \ldots, x_m)$. But these must lift to primes in R. Indeed, we have seen that whenever you have an integral extension, the induced map on spectra is surjective. So

$$\operatorname{Spec} R \to \operatorname{Spec} k[x_1, \ldots, x_m]$$

is surjective. If R is a field, this means $\operatorname{Spec} k[x_1, \ldots, x_m]$ has one point and $m = 0$. So R is integral over k, thus algebraic. This implies that R is finite as it is finitely generated. This proves one version of the Nullstellensatz.

Another version of the Nullstellensatz, which is more precise, says:

Theorem 4.5 *Let $I \subset \mathbb{C}[x_1, \ldots, x_n]$. Let $V \subset \mathbb{C}^n$ be the subset of $\mathbb{C}^n$ defined by the ideal I (i.e. the zero locus of I).*

Then $\operatorname{Rad}(I)$ *is precisely the collection of f such that $f|_V = 0$. In particular,*

$$\operatorname{Rad}(I) = \bigcap_{\mathfrak{m} \supset I, \mathfrak{m} \text{ maximal}} \mathfrak{m}.$$

In particular, there is a bijection between radical ideals and algebraic subsets of $\mathbb{C}^n$.

The last form of the theorem, which follows from the expression of maximal ideals in the polynomial ring, is very similar to the result

$$\operatorname{Rad}(I) = \bigcap_{\mathfrak{p} \supset I, \mathfrak{p} \text{ prime}} \mathfrak{p},$$

true in any commutative ring. However, this general result is not necessarily true.

Example 4.6 The intersection of all primes in a DVR is zero, but the intersection of all maximals is nonzero.

Proof (Proof of Theorem 4.5). It now suffices to show that for every $\mathfrak{p} \subset \mathbb{C}[x_1, \ldots, x_n]$ prime, we have

$$\mathfrak{p} = \bigcap_{\mathfrak{m} \supset I \text{ maximal}} \mathfrak{m}$$

since every radical ideal is an intersection of primes.

Let $R = \mathbb{C}[x_1, \ldots, x_n]/\mathfrak{p}$. This is a domain finitely generated over $\mathbb{C}$. We want to show that the intersection of maximal ideals in R is zero. This is equivalent to the above displayed equality.

So fix $f \in R - \{0\}$. Let R' be the localization $R' = R_f$. Then R' is also an integral domain, finitely generated over $\mathbb{C}$. R' has a maximal ideal $\mathfrak{m}$ (which a priori could be zero). If we look at the map $R' \to R'/\mathfrak{m}$, we get a map into a field finitely generated over $\mathbb{C}$, which is thus $\mathbb{C}$. The composite map

$$R \to R' \to R'/\mathfrak{m}$$

is just given by an n-tuple of complex numbers, i.e. to a point in $\mathbb{C}^n$ which is even in V as it is a map out of R. This corresponds to a maximal ideal in R. This maximal ideal does not contain f by construction. ▲

Exercise 7.6 Prove the following result, known as "Zariski's lemma" (which easily implies the Nullstellensatz): if k is a field, k' a field extension of k which is a finitely generated k-*algebra*, then k' is finite algebraic over k. Use the following argument of McCabe (in [McC76]):

1. k' contains a subring S of the form $S = k[x_1, \ldots, x_t]$ where the $x_1, \ldots, x_t$ are algebraically independent over k, and k' is algebraic over the quotient field of S (which is a polynomial ring).
2. If k' is not algebraic over k, then $S \neq k$ is not a field.
3. Show that there is $y \in S$ such that k' is integral over S_y. Deduce that S_y is a field.
4. Since $\operatorname{Spec}(S_y) = \{0\}$, argue that y lies in every non-zero prime ideal of $\operatorname{Spec} S$. Conclude that $1 + y \in k$, and S is a field—contradiction.

4.4 A little affine algebraic geometry

In what follows, let k be algebraically closed, and let A be a finitely generated k-algebra. Recall that $\operatorname{Specm} A$ denotes the set of maximal ideals in A. Consider the natural k-algebra structure on $\operatorname{Funct}(\operatorname{Specm} A, k)$. We have a map

$$A \to \operatorname{Funct}(\operatorname{Specm} A, k)$$

which comes from the Weak Nullstellensatz as follows. Maximal ideals $\mathfrak{m} \subset A$ are in bijection with maps $\varphi_{\mathfrak{m}} : A \to k$ where $\ker(\varphi_{\mathfrak{m}}) = \mathfrak{m}$, so we define $a \longmapsto [\mathfrak{m} \longmapsto \varphi_{\mathfrak{m}}(a)]$. If A is reduced, then this map is injective because if $a \in A$ maps to the zero function, then $a \in \cap \mathfrak{m} \to a$ is nilpotent $\to a = 0$.

Definition 4.7 A function $f \in \operatorname{Funct}(\operatorname{Specm} A, k)$ is called **algebraic** if it is in the image of A under the above map. (Alternate words for this are **polynomial** and **regular**.)

Let A and B be finitely generated k-algebras and $\phi : A \to B$ a homomorphism. This yields a map $\Phi : \operatorname{Specm} B \to \operatorname{Specm} A$ given by taking pre-images.

Definition 4.8 A map $\Phi : \operatorname{Specm} B \to \operatorname{Specm} A$ is called **algebraic** if it comes from a homomorphism ϕ as above.

To demonstrate how these definitions relate to one another we have the following proposition.

Proposition 4.9 *A map $\Phi : \operatorname{Specm} B \to \operatorname{Specm} A$ is algebraic if and only if for any algebraic function $f \in \operatorname{Funct}(\operatorname{Specm} A, k)$, the pullback $f \circ \Phi \in \operatorname{Funct}(\operatorname{Specm} B, k)$ is algebraic.*

Proof. Suppose that Φ is algebraic. It suffices to check that the following diagram is commutative:

$$\begin{array}{ccc} \operatorname{Funct}(\operatorname{Specm} A, k) & \xrightarrow{-\circ\Phi} & \operatorname{Funct}(\operatorname{Specm} B, k) \\ \uparrow & & \uparrow \\ A & \xrightarrow[\phi]{} & B \end{array}$$

where $\phi : A \to B$ is the map that gives rise to Φ.

[$\Leftarrow$] Suppose that for all algebraic functions $f \in \operatorname{Funct}(\operatorname{Specm} A, k)$, the pull-back $f \circ \Phi$ is algebraic. Then we have an induced map, obtained by chasing the diagram counter-clockwise:

$$\begin{array}{ccc} \operatorname{Funct}(\operatorname{Specm} A, k) & \xrightarrow{-\circ\Phi} & \operatorname{Funct}(\operatorname{Specm} B, k) \\ \uparrow & & \uparrow \\ A & \overset{\phi}{\dashrightarrow} & B \end{array}$$

From ϕ, we can construct the map $\Phi' : \operatorname{Specm} B \to \operatorname{Specm} A$ given by $\Phi'(\mathfrak{m}) = \phi^{-1}(\mathfrak{m})$. I claim that $\Phi = \Phi'$. If not, then for some $\mathfrak{m} \in \operatorname{Specm} B$ we have $\Phi(\mathfrak{m}) \neq \Phi'(\mathfrak{m})$. By definition, for all algebraic functions $f \in \operatorname{Funct}(\operatorname{Specm} A, k)$, $f \circ \Phi = f \circ \Phi'$ so to arrive at a contradiction we show the following lemma:
Given any two distinct points in $\operatorname{Specm} A = V(I) \subset k^n$, there exists some algebraic f that separates them. This is trivial when we realize that any polynomial function is algebraic, and such polynomials separate points. ▲

§5 Serre's criterion and its variants

We are going to now prove a useful criterion for a noetherian ring to be a product of normal domains, due to Serre: it states that a (noetherian) ring is normal if and only if most of the localizations at prime ideals are discrete valuation rings (this corresponds to the ring being *regular* in codimension one, though we have not defined regularity yet) and a more technical condition that we will later interpret in terms of *depth.* One advantage of this criterion is that it does *not* require the ring to be a product of domains a priori.

5.1 Reducedness

There is a "baby" version of Serre's criterion for testing whether a ring is reduced, which we star with.

Recall:

Definition 5.1 A ring R is **reduced** if it has no nonzero nilpotents.

Proposition 5.2 *If R is noetherian, then R is reduced if and only if it satisfies the following conditions:*

1. *Every associated prime of R is minimal (no embedded primes).*
2. *If $\mathfrak{p}$ is minimal, then $R_{\mathfrak{p}}$ is a field.*

Proof. First, assume R reduced. What can we say? Say $\mathfrak{p}$ is a minimal prime; then $R_{\mathfrak{p}}$ has precisely one prime ideal (namely, $\mathfrak{m} = \mathfrak{p}R_{\mathfrak{p}}$). It is in fact a local artinian ring, though we don't need that fact. The radical of $R_{\mathfrak{p}}$ is just $\mathfrak{m}$. But R was reduced, so $R_{\mathfrak{p}}$ was reduced; it's an easy argument that localization preserves reducedness. So $\mathfrak{m} = 0$. The fact that 0 is a maximal ideal in $R_{\mathfrak{p}}$ says that it is a field.

On the other hand, we still have to do part 1. R is reduced, so $\mathrm{Rad}(R) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}\, R} \mathfrak{p} = 0$. In particular,

$$\bigcap_{\mathfrak{p} \text{ minimal}} \mathfrak{p} = 0.$$

The map

$$R \to \prod_{\mathfrak{p} \text{ minimal}} R/\mathfrak{p}$$

is injective. The associated primes of the product, however, are just the minimal primes. So $\mathrm{Ass}(R)$ can contain only minimal primes.

That's one direction of the proposition. Let us prove the converse now. Assume R satisfies the two conditions listed. In other words, $\mathrm{Ass}(R)$ consists of minimal primes, and each $R_{\mathfrak{p}}$ for $\mathfrak{p} \in \mathrm{Ass}(R)$ is a field. We would like to show that R is reduced. Primary decomposition tells us that there is an injection

$$R \hookrightarrow \prod_{\mathfrak{p}_i \text{ minimal}} M_i, \quad M_i \ \ \mathfrak{p}_i - \text{primary}.$$

In this case, each M_i is primary with respect to a minimal prime. We have a map

$$R \hookrightarrow \prod M_i \to \prod (M_i)_{\mathfrak{p}_i},$$

which is injective, because when you localize a primary module at its associated prime, you don't kill anything by definition of primariness. Since we can draw a diagram

$$\begin{array}{ccc} R & \longrightarrow & \prod M_i \\ \downarrow & & \downarrow \\ \prod R_{\mathfrak{p}_i} & \longrightarrow & \prod (M_i)_{\mathfrak{p}_i} \end{array}$$

and the map $R \to \prod (M_i)_{\mathfrak{p}_i}$ is injective, the downward arrow on the right injective. Thus R can be embedded in a product of the fields $\prod R_{\mathfrak{p}_i}$, so is reduced. ▲

This proof actually shows:

Proposition 5.3 (Scholism) *A noetherian ring R is reduced iff it injects into a product of fields. We can take the fields to be the localizations at the minimal primes.*

Example 5.4 Let $R = k[X]$ be the coordinate ring of a variety X in $\mathbb{C}^n$. Assume X is reduced. Then MaxSpec$R$ is a union of irreducible components X_i, which are the closures of the minimal primes of R. The fields you get by localizing at minimal primes depend only on the irreducible components, and in fact are the rings of meromorphic functions on X_i. Indeed, we have a map

$$k[X] \to \prod k[X_i] \to \prod k(X_i).$$

If we don't assume that R is radical, this is **not** true.

There is a stronger condition than being reduced we could impose. We could say:

Proposition 5.5 *If R is a noetherian ring, then R is a domain iff*

1. *R is reduced.*

2. *R has a unique minimal prime.*

Proof. One direction is obvious. A domain is reduced and (0) is the minimal prime.

The other direction is proved as follows. Assume 1 and 2. Let $\mathfrak{p}$ be the unique minimal prime of R. Then $\mathrm{Rad}(R) = 0 = \mathfrak{p}$ as every prime ideal contains $\mathfrak{p}$. As (0) is a prime ideal, R is a domain.▲

We close by making some remarks about this embedding of R into a product of fields.

Definition 5.6 Let R be any ring, not necessarily a domain. Let $K(R)$ be the localized ring $S^{-1}R$ where S is the multiplicatively closed set of nonzerodivisors in R. $K(R)$ is called the **total ring of fractions** of R.

When R is a field, this is the quotient field.

First, to get a feeling for this, we show:

Proposition 5.7 *Let R be noetherian. The set of nonzerodivisors S can be described by $S = R - \bigcup_{\mathfrak{p} \in \mathrm{Ass}(R)} \mathfrak{p}$.*

Proof. If $x \in \mathfrak{p} \in \mathrm{Ass}(R)$, then x must kill something in R as it is in an associated prime. So x is a zerodivisor.

Conversely, suppose x is a zerodivisor, say $xy = 0$ for some $y \in R - \{0\}$. In particular, $x \in \mathrm{Ann}(y)$. We have an injection $R/\mathrm{Ann}(y) \hookrightarrow R$ sending 1 to y. But $R/\mathrm{Ann}(y)$ is nonzero, so it has an associated prime $\mathfrak{p}$ of $R/\mathrm{Ann}(y)$, which contains $\mathrm{Ann}(y)$ and thus x. But $\mathrm{Ass}(R/\mathrm{Ann}(y)) \subset \mathrm{Ass}(R)$. So x is contained in a prime in $\mathrm{Ass}(R)$. ▲

Assume now that R is reduced. Then $K(R) = S^{-1}R$ where S is the complement of the union of the minimal primes. At least, we can claim:

Proposition 5.8 *Let R be reduced and noetherian. Then $K(R) = \prod_{\mathfrak{p}_i \text{ minimal}} R_{\mathfrak{p}_i}$.*

So $K(R)$ is the product of fields into which R embeds.

We now continue the discussion begun last time. Let R be noetherian and M a finitely generated R-module. We would like to understand very rough features of M. We can embed M into a larger R-module. Here are two possible approaches.

1. $S^{-1}M$, where S is a large multiplicatively closed subset of M. Let us take S to be the set of all $a \in R$ such that $M \xrightarrow{a} M$ is injective, i.e. a is not a zerodivisor on M. Then the map

$$M \to S^{-1}M$$

   is an injection. Note that S is the complement of the union of $\mathrm{Ass}(R)$.

2. Another approach would be to use a *primary decomposition*

$$M \hookrightarrow \prod M_i,$$

where each M_i is $\mathfrak{p}_i$-primary for some prime $\mathfrak{p}_i$ (and these primes range over $\mathrm{Ass}(M)$). In this case, it is clear that anything not in each $\mathfrak{p}_i$ acts injectively. So we can draw a commutative diagram

$$\begin{array}{ccc} M & \longrightarrow & \prod M_i \\ \downarrow & & \downarrow \\ \prod M_{\mathfrak{p}_i} & \longrightarrow & \prod (M_i)_{\mathfrak{p}_i} \end{array} .$$

The map going right and down is injective. It follows that M injects into the product of its localizations at associated primes.

The claim is that these constructions agree if M has no embedded primes. I.e., if there are no nontrivial containments among the associated primes of M, then $S^{-1}M$ (for $S = R - \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$) is just $\prod M_{\mathfrak{p}}$. To see this, note that any element of S must act invertibly on $\prod M_{\mathfrak{p}}$. We thus see that there is always a map

$$S^{-1}M \to \prod_{\mathfrak{p} \in \mathrm{Ass}(M)} M_{\mathfrak{p}}.$$

Proposition 5.9 *This is an isomorphism if M has no embedded primes.*

Proof. Let us go through a series of reductions. Let $I = \mathrm{Ann}(M) = \{a : aM = 0\}$. Without loss of generality, we can replace R by R/I. This plays nice with the associated primes.

The assumption is now that $\mathrm{Ass}(M)$ consists of the minimal primes of R.

Without loss of generality, we can next replace R by $S^{-1}R$ and M by $S^{-1}M$, because that doesn't affect the conclusion; localization plays nice with associated primes.

Now, however, R is artinian: i.e., all primes of R are minimal (or maximal). Why is this? Let R be *any* noetherian ring and $S = R - \bigcup_{\mathfrak{p} \text{ minimal}} \mathfrak{p}$. Then I claim that $S^{-1}R$ is artinian. We'll prove this in a moment.

So R is artinian, hence a product $\prod R_i$ where each R_i is local artinian. Without loss of generality, we can replace R by R_i by taking products. The condition we are trying to prove is now that

$$S^{-1}M \to M_{\mathfrak{m}}$$

for $\mathfrak{m} \subset R$ the maximal ideal. But S is the complement of the union of the minimal primes, so it is $R - \mathfrak{m}$ as R has one minimal (and maximal) ideal. This is obviously an isomorphism: indeed, both are M. ▲

TO BE ADDED: proof of artianness

Corollary 5.10 *Let R be a noetherian ring with no embedded primes (i.e. $\mathrm{Ass}(R)$ consists of minimal primes). Then $K(R) = \prod_{\mathfrak{p}_i \text{ minimal}} R_{\mathfrak{p}_i}$.*

If R is reduced, we get the statement made last time: there are no embedded primes, and $K(R)$ is a product of fields.

5.2 The image of $M \to S^{-1}M$

Let's ask now the following question. Let R be a noetherian ring, M a finitely generated R-module, and S the set of nonzerodivisors on M, i.e. $R - \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$. We have seen that there is an imbedding

$$\phi : M \hookrightarrow S^{-1}M.$$

What is the image? Given $x \in S^{-1}M$, when does it belong to the imbedding above.

To answer such a question, it suffices to check locally. In particular:

Proposition 5.11 *x belongs to the image of M in $S^{-1}M$ iff for every $\mathfrak{p} \in \operatorname{Spec} R$, the image of x in $(S^{-1}M)_{\mathfrak{p}}$ lies inside $M_{\mathfrak{p}}$.*

This isn't all that interesting. However, it turns out that you can check this at a smaller set of primes.

Proposition 5.12 *In fact, it suffices to show that x is in the image of $\phi_{\mathfrak{p}}$ for every $\mathfrak{p} \in \operatorname{Ass}(M/sM)$ where $s \in S$.*

This is a little opaque; soon we'll see what it actually means. The proof is very simple.

Proof. Remember that $x \in S^{-1}M$. In particular, we can write $x = y/s$ where $y \in M, s \in S$. What we'd like to prove that $x \in M$, or equivalently that $y \in sM$.[5] In particular, we want to know that y maps to zero in M/sM. If not, there exists an associated prime $\mathfrak{p} \in \operatorname{Ass}(M/sM)$ such that y does not get killed in $(M/sM)_{\mathfrak{p}}$. We have assumed, however, for every associated prime $\mathfrak{p} \in \operatorname{Ass}(M)$, $x \in (S^{-1}M)_{\mathfrak{p}}$ lies in the image of $M_{\mathfrak{p}}$. This states that the image of y in this quotient $(M/sM)_{\mathfrak{p}}$ is zero, or that y is divisible by s in this localization. ▲

The case we actually care about is the following:

Take R as a noetherian domain and $M = R$. Then $S = R - \{0\}$ and $S^{-1}M$ is just the fraction field $K(R)$. The goal is to describe R as a subset of $K(R)$. What we have proven is that R is the intersection in the fraction field

$$\boxed{R = \bigcap_{\mathfrak{p} \in \operatorname{Ass}(R/s), s \in R-0} R_{\mathfrak{p}}.}$$

So to check that something belongs to R, we just have to check that in a *certain set of localizations.*

Let us state this as a result:

Theorem 5.13 *If R is a noetherian domain*

$$R = \bigcap_{\mathfrak{p} \in \operatorname{Ass}(R/s), s \in R-0} R_{\mathfrak{p}}$$

5.3 Serre's criterion

We can now state a result.

Theorem 5.14 (Serre) *Let R be a noetherian domain. Then R is integrally closed iff it satisfies*

1. *For any $\mathfrak{p} \subset R$ of height one, $R_{\mathfrak{p}}$ is a DVR.*
2. *For any $s \neq 0$, R/s has no embedded primes (i.e. all the associated primes of R/s are height one).*

Here is the non-preliminary version of the Krull theorem.

Theorem 5.15 (Algebraic Hartogs) *Let R be a noetherian integrally closed ring. Then*

$$R = \bigcap_{\mathfrak{p} \text{ height one}} R_{\mathfrak{p}},$$

where each $R_{\mathfrak{p}}$ is a DVR.

[5] In general, this would be equivalent to $ty \in tsM$ for some $t \in S$; but S consists of nonzerodivisors on M.

Proof. Now evident from the earlier result Theorem 5.13 and Serre's criterion. ▲

Earlier in the class, we proved that a domain was integrally closed if and only if it could be described as an intersection of valuation rings. We have now shown that when R is noetherian, we can take *discrete* valuation rings.

Remark In algebraic geometry, say $R = \mathbb{C}[x_1, \dots, x_n]/I$. Its maximal spectrum is a subset of $\mathbb{C}^n$. If I is prime, and R a domain, this variety is irreducible. We are trying to describe R inside its field of fractions.

The field of fractions are like the "meromorphic functions"; R is like the holomorphic functions. Geometrically, this states to check that a meromorphic function is holomorphic, you can just check this by computing the "poleness" along each codimension one subvariety. If the function doesn't blow up on each of the codimension one subvarieties, and R is normal, then you can extend it globally.

This is an algebraic version of Hartog's theorem: this states that a holomorphic function on $\mathbb{C}^2 - (0,0)$ extends over the origin, because this has codimension > 1.

All the obstructions of extending a function to all of $\operatorname{Spec} R$ are in codimension one.

Now, we prove Serre's criterion.

Proof. Let us first prove that R is integrally closed if 1 and 2 occur. We know that

$$R = \bigcap_{\mathfrak{p} \in \operatorname{Ass}(R/x), x \neq 0} R_{\mathfrak{p}};$$

by condition 1, each such $\mathfrak{p}$ is of height one, and $R_{\mathfrak{p}}$ is a DVR. So R is the intersection of DVRs and thus integrally closed.

The hard part is going in the other direction. Assume R is integrally closed. We want to prove the two conditions. In R, consider the following conditions on a prime ideal $\mathfrak{p}$:

1. $\mathfrak{p}$ is an associated prime of R/x for some $x \neq 0$.
2. $\mathfrak{p}$ is height one.
3. $\mathfrak{p}_{\mathfrak{p}}$ is principal in $R_{\mathfrak{p}}$.

First, 3 implies 2 implies 1. 3 implies that $\mathfrak{p}$ contains an element x which generates $\mathfrak{p}$ after localizing. It follows that there can be no prime between (x) and $\mathfrak{p}$ because that would be preserved under localization. Similarly, 2 implies 1 is easy. If $\mathfrak{p}$ is minimal over (x), then $\mathfrak{p} \in \operatorname{Ass} R/(x)$ since the minimal primes in the support are always associated.

We are trying to prove the inverse implications. In that case, the claims of the theorem will be proved. We have to show that 1 implies 3. This is an argument we really saw last time, but let's see it again. Say $\mathfrak{p} \in \operatorname{Ass}(R/x)$. We can replace R by $R_{\mathfrak{p}}$ so that we can assume that $\mathfrak{p}$ is maximal. We want to show that $\mathfrak{p}$ is generated by one element.

What does the condition $\mathfrak{p} \in \operatorname{Ass}(R/x)$ buy us? It tells us that there is $\overline{y} \in R/x$ such that $\operatorname{Ann}(\overline{y}) = \mathfrak{p}$. In particular, there is $y \in R$ such that $\mathfrak{p}y \subset (x)$ and $y \notin (x)$. We have the element $y/x \in K(R)$ which sends $\mathfrak{p}$ into R. That is,

$$(y/x)\mathfrak{p} \subset R.$$

There are two cases to consider, as in last time:

1. $(y/x)\mathfrak{p} = R$. Then $\mathfrak{p} = R(x/y)$ so $\mathfrak{p}$ is principal.
2. $(y/x)\mathfrak{p} \neq R$. In particular, $(y/x)\mathfrak{p} \subset \mathfrak{p}$. Then since $\mathfrak{p}$ is finitely generated, we find that y/x is integral over R, hence in R. This is a contradiction as $y \notin (x)$.

Only the first case is now possible. So $\mathfrak{p}$ is in fact principal. ▲

CRing Project contents

CRing Project bibliography

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[BBD82] A. A. Beĭlinson, J. Bernstein, and P. Deligne. Faisceaux pervers. In *Analysis and topology on singular spaces, I (Luminy, 1981)*, volume 100 of *Astérisque*, pages 5–171. Soc. Math. France, Paris, 1982.

[Bou98] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[Cam88] Oscar Campoli. A principal ideal domain that is not a euclidean domain. *American Mathematical Monthly*, 95(9):868–871, 1988.

[CF86] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*, London, 1986. Academic Press Inc. [Harcourt Brace Jovanovich Publishers]. Reprint of the 1967 original.

[Cla11] Pete L. Clark. Factorization in euclidean domains. 2011. Available at `http://math.uga.edu/~pete/factorization2010.pdf`.

[dJea10] Aise Johan de Jong et al. *Stacks Project*. Open source project, available at `http://www.math.columbia.edu/algebraic_geometry/stacks-git/`, 2010.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[For91] Otto Forster. *Lectures on Riemann surfaces*, volume 81 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. Translated from the 1977 German original by Bruce Gilligan, Reprint of the 1981 English translation.

[GD] Alexander Grothendieck and Jean Dieudonné. *Élements de géometrie algébrique*. Publications Mathématiques de l'IHÉS.

[Ger] Anton Geraschenko (mathoverflow.net/users/1). Is there an example of a formally smooth morphism which is not smooth? MathOverflow. `http://mathoverflow.net/questions/200` (version: 2009-10-08).

[Gil70] Robert Gilmer. An existence theorem for non-Noetherian rings. *The American Mathematical Monthly*, 77(6):621–623, 1970.

[Gre97] John Greene. Principal ideal domains are almost euclidean. *The American Mathematical Monthly*, 104(2):154–156, 1997.

[Gro57] Alexander Grothendieck. Sur quelques points d'algèbre homologique. *Tôhoku Math. J. (2)*, 9:119–221, 1957.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Hat02] Allen Hatcher. *Algebraic topology*. Cambridge University Press, Cambridge, 2002. Available at `http://www.math.cornell.edu/~hatcher/AT/AT.pdf`.

[Hov07] Mark Hovey. *Model Categories*. American Mathematical Society, 2007.

[KS06] Masaki Kashiwara and Pierre Schapira. *Categories and sheaves*, volume 332 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2006.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[LR08] T. Y. Lam and Manuel L. Reyes. A prime ideal principle in commutative algebra. *J. Algebra*, 319(7):3006–3027, 2008.

[Mar02] David Marker. *Model theory*, volume 217 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002. An introduction.

[Mat80] Hideyuki Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series*. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980.

[McC76] John McCabe. A note on Zariski's lemma. *The American Mathematical Monthly*, 83(7):560–561, 1976.

[Mil80] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[ML98] Saunders Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1998.

[Per04] Hervé Perdry. An elementary proof of Krull's intersection theorem. *The American Mathematical Monthly*, 111(4):356–357, 2004.

[Qui] Daniel Quillen. Homology of commutative rings. Mimeographed notes.

[Ray70] Michel Raynaud. *Anneaux locaux henséliens*. Lecture Notes in Mathematics, Vol. 169. Springer-Verlag, Berlin, 1970.

[RG71] Michel Raynaud and Laurent Gruson. Critères de platitude et de projectivité. Techniques de "platification" d'un module. *Invent. Math.*, 13:1–89, 1971.

[Ser65] Jean-Pierre Serre. *Algèbre locale. Multiplicités*, volume 11 of *Cours au Collège de France, 1957–1958, rédigé par Pierre Gabriel. Seconde édition, 1965. Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1965.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[Ser09] Jean-Pierre Serre. How to use finite fields for problems concerning infinite fields. 2009. arXiv:0903.0517v2.

[SGA72] *Théorie des topos et cohomologie étale des schémas. Tome 1: Théorie des topos*. Lecture Notes in Mathematics, Vol. 269. Springer-Verlag, Berlin, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck, et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat.

[SGA03] *Revêtements étales et groupe fondamental (SGA 1)*. Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3. Société Mathématique de France, Paris, 2003. Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)].

[Tam94] Günter Tamme. *Introduction to étale cohomology*. Universitext. Springer-Verlag, Berlin, 1994. Translated from the German by Manfred Kolster.

[Vis08] Angelo Vistoli. Notes on Grothendieck topologies, fibered categories, and descent theory. *Published in* FGA Explained, 2008. arXiv:math/0412512v4.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.