250B: Commutative Algebra
Or, Eisenbud With Details

Nir Elber

Spring 2022

Contents

Theme 1: The Nullstellensatz

1.1 February 15

Here we go.

Warning 1.1. For today's lecture, an S-algebra R should be thought of as providing an embedding $R \hookrightarrow S$. We will even think $R \subseteq S$.

1.1.1 More on Integrality

Last time we introduced the following proposition.

Proposition 1.2. Fix R a ring and an R-algebra $S := R[s]/I$ for some ideal I. We have the following.

(a) S is finitely generated as an R-module if and only if I contains a monic polynomial (i.e., there is some monic $p(x) \in R[x]$ such that $p(s) = 0$).

(b) S is a free, finitely generated R-module if $I = (p)$ for some monic polynomial p.

This gave rise to the following definitinon.

Integral **Definition 1.3** (Integral)**.** Fix S an R-algebra. Then $s \in S$ is *integral over* R if and only if s is a root of some monic polynomial over R. If all elements $s \in S$ are integral over R, then we say S is *integral over* R.

Being integral is intended to be a generalization of having a finite extension of fields. Along these lines, we get the following definition.

Finite **Definition 1.4** (Finite)**.** Fix S an R-algebra. Then S is *finite* over R if and only if S is finitely geneated over R (as an R-module).

As with fields, we know that any finite field extension must be algebraic, so we might hope that an integral extension is also finite.

Lemma 1.5. Every finite R-algebra S is integral.

Proof. We use the Cayley–Hamilton theorem. Namely, take our endomorphism φ to be multiplication by one of the generators of S as an R-module and then stitch these together. ■

In fact, we can provide a converse.

Lemma 1.6. Fix S an R-algebra. Then S is finite if and only if it is finitely generated as an R-algebra, where the generators are integral.

Proof. We have two directions.

- In one direction, suppose that $S = R[s_1, \ldots, s_n]$, and we consider the chain

$$R \subseteq R[s_1] \subseteq R[s_1, s_2] \subseteq \cdots \subseteq R[s_1, \ldots, s_n].$$

  Each extension is finite because the generators are integral, and we can build a finite set of generators by multiplying the sets together.

- In the other direction, take S a finite R-algebra. Then all elements are integral over R, but we are only permitted finitely many generators, so we can just keep choosing until we are done. ■

Sometimes we aren't integral, but we can always make one.

Integral closure

Definition 1.7 (Integral closure)**.** Fix S an R-algebra. Then the *integral closure* S' is the set of all elements of S which are integral over R.

Remark 1.8. The integral closure depends on the choie of S.

Proposition 1.9. Fix S an R-algebra. Then the integral closure of S is an R-subalgebra of S.

Proof. The main idea is to use Lemma 1.6. We emulate the proof that the set of algebraic elements is a field extension. Namely, for any elements s_1 and s_2 which are integral over R, Lemma 1.6 tells us that

$$R[s_1, s_2]$$

is a finite R-algebra, so all of its elements are integral. Thus, $s_1 s_1$ and $s_1 + s_2$ are integral, showing that S is closed under addition and multiplication. We are also closed under the R-action because elements $r \in R$ in S are integral by the monic polynomial $(x - r) \in R[x]$. ■

We close our discussion by quickly discussing localization: localization commutes with the integral closure.

Proposition 1.10. Fix S an R-algebra with integral closure S'; further take $U \subseteq R$ a multiplicative subset. Then $S'\left[U^{-1}\right]$ is the integral closure of $R\left[U^{-1}\right]$ in $S\left[U^{-1}\right]$.

Proof. The directino that all elements of $S'\left[U^{-1}\right]$ are integral over $R\left[U^{-1}\right]$ is not hard because multiplication by units will not affect integrality.

In the other direction, fix some $\frac{s}{u} \in S\left[U^{-1}\right]$ is integral over $R\left[U^{-1}\right]$ so that we hvae some polynomial

$$\left(\frac{s}{u}\right)^n + \frac{r_1}{u_1}\left(\frac{s}{u}\right)^{n-1} + \cdots + \frac{r_n}{u_n} = 0.$$

Multiplying through by $s(u_1 \cdots u_n u)^n$ will show that $s(u_1 \cdots u_n)$ is integral over R and hence lives in S', which finishes. ■

1.1.2 Normality

We have the following defintions.

Normal

Definition 1.11 (Normal)**.** Fix R a domain with field of fractions $K(R)$. Then R is *normal* if and only if R is integrally closed in $K(R)$.

Normalization

Definition 1.12 (Normalization)**.** Fix R a domain with field of fractions $K(R)$. We can define the *normalization* of R to be the integral closure of R in $K(R)$.

Let's see some examples.

Exercise 1.13. Consider $R = \mathbb{Z}$ with $K(R) = \mathbb{Q}$. Then we show that the integral closure of $\mathbb{Z}$ is $\mathbb{Z}$. In particular, $\mathbb{Z}$ is normal.

Proof. Of course elements of $\mathbb{Z}$ are integral over $\mathbb{Z}$. Suppose that $\frac{p}{q} \in \mathbb{Q}$ is integral; without loss of generality, we may assume $\gcd(p, q) = 1$. Now, we are promised some monic polynomial such that

$$(p/q)^n + a_1(p/q)^{n-1} + \cdots + a_n = 0$$

so that all of the coefficients are in $\mathbb{Z}$. However, multiplying by q^n, we see that

$$p^n = -\left(a_1 p^{n-1} q + \cdots + a_n q^n\right).$$

In particular, q divides the right-hand side, so q divides p^n, so $1 = \gcd(p^n, q) = |q|$. In particular, ■

Essentially the same proof will work for any unique factorization domain.

Proposition 1.14. Any unique factorization domain is normal.

Proof. Copy the proof of Exercise 1.13. ■

And here are more examples.

Example 1.15. The ring $\mathbb{Z}[i]$ is normal and hence integrally closed in $\mathbb{Q}(i)$.

Non-Example 1.16. The ring $\mathbb{Z}\left[\sqrt{5}\right]$ is not normal. Note that the field of fractions is $\mathbb{Q}(\sqrt{5})$, so we note $\frac{1+\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$ is the root of the polynomial

$$x^2 - x - 1$$

by the quadratic formula. However, the integral closure is $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, so this is essentially the only exception.

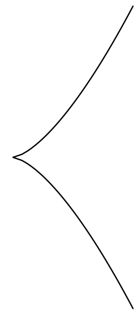
Example 1.17. The integral closure $\overline{\mathbb{Z}}$ of $\mathbb{Z}$ in $\mathbb{C}$ is the ring of all the roots of monic polynomials; these are called the algebraic integers. For example, $\overline{\mathbb{Z}} \subseteq \overline{\mathbb{Q}}$.

1.1.3 Normality via Geometry

There is also a context for normality in algebraic geometry.

Exercise 1.18. We compute the integral closure of the ring $R = k[x, y]/\left(y^2 - x^3\right)$.

Proof. Here is our image.



Note that, working in the fraction field, $\left(\frac{y}{x}\right)^2 = x$ because $y^2 = x^3$, so R is not normal because it does not include $\frac{y}{x}$.

To compute our integral closure, we create a map $R \to k[t]$ by $y \mapsto t^3$ and $x \mapsto t^2$ (so that $t = y/x$), and we find R embeds into $k[t]$. But because $k[t]$ is now integrally closed (it's a unique factorization domain), we see that the pull-back $R[y/x]$ will in fact be integrally closed, so this is our integral closure. ■

Example 1.19. Consider the ring $R = k[x,y]/\left(y^2 - x^2(x+1)\right)$. Then $\left(\frac{y}{x}\right)^2 = x+1$, so R is not normal because it does not include $\frac{y}{x}$.

More generally, suppose that we have affine algebraic sets X and Y with an embedding $A(X) \to A(Y)$. This corresponds to a map $Y \to X$. Normality then means that the image of Y in X is "Zariski dense" so that there is no proper closed subset of X which contains Y.

Speaking with more geometry, a map $Y \to X$ of affine varieties is proper (over $\mathbb{C}$, say) essentially gives us the result that the pre-image of a compact set is compact.

Remark 1.20. I did not follow the above discussin.

We have the following proposition.

Proposition 1.21. Fix S an R-algebra with a monic polynomial $f \in R[x]$. If we can factor $f = gh$ for $g, h \in S[x]$. Then the coefficients of g and h are integral over R.

Proof. Imagine adding some root α_1 of g to S to get a bigger R-algebra named $R[\alpha_1]$. So, writing $g(x) = (x-\alpha_1)g_1(x)$, we see that we can divide out to get

$$\frac{f(x)}{(x-\alpha_1)} = g_1(x)h(x).$$

Inductively removing all roots $\alpha_1, \ldots, \alpha_m$ of g and $\beta_1, \ldots, \beta_n$ of h, we see that

$$f(x) = (x-\alpha_1)\cdots(x-\alpha_m)(x-\beta_1)\cdots(x-\beta_n).$$

Here the leading coefficients match, so we do not inherit a leading term. However, upon expansion, we see that the coefficients of g and h will be elementary symmetric functions of the $\alpha_\bullet$ and $\beta_\bullet$, so in particular they will all be contained in the finite extension $R[\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n]$ and hence be integral. ■

Corollary 1.22. Fix R a normal domain and $f(x) \in R[x]$ some monic polynomial. Then, if $f(x)$ is irreducible, then $f(x)$ is prime.

Proof. Fix $f(x) \in R[x]$. Then f will remain irreducible in $K(R)$, which comes from the above proposition. In particular, we are promised an embedding

$$\frac{R[x]}{(f(x))} \hookrightarrow \frac{K[x]}{(f(x))},$$

so $R[x]/(f(x))$ is a subring of a field and hence an integral domain. ■

Remark 1.23. This generalizes the result that, if R is a unique factorization domain, then $R[x]$ is also a unique factorization domain.

1.1.4 Lifting Primes

Speaking generally for a moment, suppose we have an S-algebra R. Then, if $\varphi : R \to S$ is our promised map, we note that we have a map $\operatorname{Spec} S \to \operatorname{Spec} R$ by φ^{-1}. In particular, when φ^{-1} is an embeding $R \subseteq S$, we get that primes $\mathfrak{q}$ of S go to $\mathfrak{q} \cap R$.

When we have integral extensions, we get some more control.

Proposition 1.24. Fix $R \subseteq S$ an integral extension of rings. For any $\mathfrak{p} \in \operatorname{Spec} R$, there exists $\mathfrak{q} \in \operatorname{Spec} S$ such that $\mathfrak{q} \cap R = \mathfrak{p}$.

Proof. Set $U := R \setminus \mathfrak{p}$, and we will localize at U. Because localization preserves embeddings, we get an embedding $R_\mathfrak{p} = R\left[U^{-1}\right] \subseteq S\left[U^{-1}\right]$. It will suffice to show the statement for the localization because then we can pre-image back to the original statement.

Now, by how primes work in localization, we know that

$$\mathfrak{p}S\left[U^{-1}\right] \cap R_\mathfrak{p} = \mathfrak{p}.$$

Thus, because $\mathfrak{p}$ is the unique maximal ideal of $R_\mathfrak{p}$, it suffices to put $\mathfrak{p}S\left[U^{-1}\right]$ in any larger ideal and then pull-back, as long as we don't get the full ring $R\left[U^{-1}\right]$.

Well, any maximal ideal containing $\mathfrak{p}S\left[U^{-1}\right]$ will do, so we have to show $\mathfrak{p}S\left[U^{-1}\right] \cap R_\mathfrak{p} = R_\mathfrak{p}$. Well, suppose for the sake of contradiction this is true so that

$$1 = p_1 s_1 + \cdots + p_n s_n$$

for some $p_1, \ldots, p_n \in \mathfrak{p}$ and $s_1, \ldots, s_n \in S$. But then $M = R[s_1, \ldots, s_n]$ is a finitely generated R-module (by integrality) where $\mathfrak{p}M = M$ (because of the above equation), which forces $M = 0$ by Nakayama's lemma, which is a contradiction. ■

In fact, we have the following.

Corollary 1.25. Fix $R \subseteq S$ an integral extension. Further, if $I \subseteq R$ is an ideal with $SI \subseteq R \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Spec} R$, then we can choose $\mathfrak{q}$ with $\mathfrak{q} \cap R = \mathfrak{p}$ which contains I.

Proof. One can work in the integral extension $R/I \subseteq S/SI$ and then use the previous proposition. ■

In the case of domains, we have some communication with the field extensions.

Lemma 1.26. Fix $R \subseteq S$ an integral extension of domains. Then $K(S)$ is algebraic over $K(R)$.

Proof. This follows from simply choosing finitely many integral generators of S over R. ■

This gives us the following lack of "avoidance" in integral domains.

Proposition 1.27. Fix $R \subseteq S$ an integral extension of domains and $I \neq 0$ a nonzero ideal of S. Then $I \cap R \neq 0$.

Proof. Suppose $b \in I$. By writing out the polynomial for b over $K(R)$ and then multiplying out by all the denominators, we get some equation in R of the form

$$a_n b^n + \cdots + a_0 = 0.$$

By forcing n minimal, we get $a_0 \neq 0$ (here we use that these are domains), but then $a_0 \in Sb \subseteq I$ as well as $a_0 \in R$. This finishes. ∎

Proposition 1.28. Fix $R \subseteq S$ an extension of integral domains. Then, R is a field if and only if S is a field.

Proof. In one direction, if R is a field, then take any $s \in S$ and write out its equation

$$s^n + a_1 s^{n-1} + \cdots + a_0 = 0.$$

Again, we can force $a_0 \neq 0$, so $a_0 \in R$ is a unit. By factoring out s from the first n terms, we get $s(\text{stuff}) = -a_0 \in R^\times$, so s is a unit.

In the oother direction, suppose for the sake of contradiction that S is a field while S is not. Then R has some nonzero maximal ideal $\mathfrak{p}$ which lifts to a nonzero maximal ideal $\mathfrak{P}$ up in S. But the only ideals of S are (0) or S, neither of which can be the lift of $\mathfrak{P}$. ∎