250B: Commutative Algebra
Or, Eisenbud With Details

Nir Elber

Spring 2022

Contents

Theme 1: The Nullstellensatz

1.1 February 10

Here we go.

1.1.1 Unique Factorization Domains

We start with the following result; it is due to Gauss.

Theorem 1.1. Fix R a unique factorization domain. Then $R[x]$ is a unique factorization domain.

Proof. The main character is as follows.

Content

Definition 1.2 (Content)**.** Fix $f(x) = a_0 + \cdots + a_n x^n \in R[x]$. Then we define the *content* of f to be the ideal

$$\operatorname{cont}(f) := (a_0, \dots, a_n) \subseteq R.$$

Here is the main claim.

Lemma 1.3. Fix $f, g \in R[x]$. Then $\operatorname{cont}(fg) \subseteq \operatorname{cont}(f)\operatorname{cont}(g) \subseteq \operatorname{rad}\operatorname{cont}(fg)$.

Proof. That $\operatorname{cont}(fg) \subseteq \operatorname{cont}(f)\operatorname{cont}(g)$ follows from expanding out fg. To show the other direction, we recall from **??** that

$$\operatorname{rad}\operatorname{cont}(fg) = \bigcap_{\operatorname{cont}(fg) \subseteq \mathfrak{p}} \mathfrak{p}.$$

Now, for any $\mathfrak{p}$ containing $\operatorname{cont}(fg)$, we have to show that $\operatorname{cont}(f)\operatorname{cont}(g) \subseteq \mathfrak{p}$. But then we note that $\overline{f}, \overline{g} \in (R/\mathfrak{p})[x]$ will have

$$\overline{f} \cdot \overline{g} = 0$$

by definition of $\mathfrak{p}$. Thus, either $\overline{f} \in \mathfrak{p}$ or $\overline{g} \in \mathfrak{p}$, so $\operatorname{cont}(f) \subseteq \mathfrak{p}$ or $\operatorname{cont}(g) \subseteq \mathfrak{p}$. This finishes the other inclusion. ∎

The key to continue is to work with the field of fractions $K := \operatorname{Frac}(R)$, noting that any polynomial $f \in R[x]$ will have a unique factorization in $K[x]$ (because, say, $K[x]$ is Euclidean).

Namely, our next step is to classify irreducibles in $R[x]$.

Lemma 1.4. Fix everything as above. Then f is irreducible in $R[x]$ implies that f is irreducible in $K[x]$.

Proof. We proceed by contraposition. If $f(x)$ is not irreducible (but still not zero and not a unit), then we can write $f = g_0 h_0$ where $\deg g_0, \deg h_0 < \deg f$. Clearing denominators, we can write

$$rf = gh$$

where $g, h \in R[x]$. So now we can talk about the content. If r is a unit, then we see that f is indeed not reducible. If r is not a unit, then for each prime $p \mid f$, we see that $\operatorname{cont}(f)\operatorname{cont}(g) \subseteq \operatorname{rad}\operatorname{cont}(fg) \subseteq (p)$, so either $g \in (p)$ or $h \in (p)$, and then we can cancel out by p. In particular, we can, after enough cancelling, force r to be a unit, thus finishing. ∎

To finish checking that $R[x]$ is a unique factorization domain, we recall that it suffices to show all irreducibles are prime.

Lemma 1.5. Fix everything as above. If f is irreducible, in $R[x]$, then f is prime.

Proof. Well, if f is irreducible in $R[x]$, then it is irreducible and hence prime in $K[x]$. In particular, if $f \mid gh$ for $g, h \in R[x]$, then without loss of generality

$$g = f(q/r)$$

for some $q/r \in K[x]$ so that $q \in K[x]$. In particular, $fq = rg$, so arguing as above we can remove the primes dividing r into q because f will not be divisible by any prime constant. ■

The above lemma finishes the proof. ■

Corollary 1.6. The ring $k[x_1, \dots, x_n]$ is a unique factorization domain.

Proof. Induction on n. ■

Example 1.7. We show that $\left(y^2 - x^3\right) \subseteq k[x, y]$ is prime. It suffices to show that $y^2 - x^3$ is prime in $k[x, y]$, for which it suffices to show that $y^2 - x^3$ is irreducible in $k(x)[y]$. But $y^2 - x^3$ is a quadratic in $k(x)[y]$ and therefore irreducible because it has no roots: there is no $y = f(x)/g(x)$ such that $f(x)^2/g(x)^2 = x^3$.

Example 1.8. We show that $\left(y^2 - x^3\right) \subseteq k[x, y]$ is prime a different way. Indeed, by sending $x \mapsto t^2$ and $y \mapsto t^3$, there is an embedding

$$\frac{k[x, y]}{(y^2 - x^3)} \hookrightarrow k\left[t^2, t^3\right]$$

by a homework problem. So the quotient is a domain, so $\left(y^2 - x^3\right)$ is prime.

1.1.2 The Cayley–Hamilton Theorem

Here is the main result we are going to prove.

Theorem 1.9. Fix R a ring and $A \in R^{n \times n}$ a matrix. Then define $p_A(x) := \det(xI - A) \in R[x]$. Then $p_A(A) = 0 \in R^{n \times n}$.

This statement is usually stated in linear algebra over a field, but it should hold for arbitrary rings.

Proof. We need to pick up the following definition.

Adjugate matrix

Definition 1.10 (Adjugate matrix)**.** Fix $A \in R^{n \times n}$. Then we define the *adjugate matrix* by

$$C_{ij} := (-1)^{ij} \det A_{i,j},$$

where $A_{i,j}$ is the matrix A without the ith row and without the jth column.

Example 1.11. Set

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}.$$

Then

$$C = \begin{bmatrix} a_{22} & -a_{21} \\ -a_{12} & a_{11} \end{bmatrix}.$$

We can verify by hand that $C^\intercal A = (\det A)I$.

The central idea behind the adjugate matrix is that it "almost inverts" A.

Lemma 1.12. Fix $A \in R^{n\times n}$ with adjugate matrix C. Then $C^\intercal A = (\det A)I$.

Proof. Omitted. ■

To show the result, the key is to consider the elements of R as living in $\mathrm{End}_R(R)$, alongside with A. we define

$$A(x) := xI - A,$$

which is a matrix whose entires are in $\mathrm{End}_R(R)$. We can check that this matrix vanishes on each basis vector of R^n when we take $x = A$. Then we see that

$$C^\intercal(x)A(x) = \det(xI - A)I$$

will still vanish upon taking $x = A$. Expanding out $\det(xI - A)$ as a polynomial (with coefficients in $\mathrm{End}_R(R)$) finishes. ■

Our application to commutative algebra is as follows.

Theorem 1.13. Fix M a finitely generated R-module with n generators. Further, fix $\varphi \in \mathrm{End}_R(M)$. Then there exists some monic polynomial

$$p_\varphi = x^n + p_1 x^{n-1} + \cdots + p_n$$

of degree n such that $p_\varphi(\varphi)$ is zero. In fact, if there is an ideal $I \subseteq R$ such that $IM = M$, then $p_k \in I^k$.

Proof. Let $\{m_1, \ldots, m_n\}$ generate M so that we can use the equations

$$\varphi(m_i) = \sum_{k=1}^{n} a_{ij} m_j$$

to give a matrix form for φ. Then we set p_φ to be the characteristic polynomial for φ, which finishes the first part by the Cayley–Hamilton theorem. For the second part, we note that $IM = M$ can force that $a_{ij} \in I$ for each i, j, which upon writing out the coefficients for the characteristic polynomial will finish. ■

Let's now see some applications.

Proposition 1.14. Let M be a finitely generated R-module and $\psi \in \mathrm{End}_R(M)$. Then if ψ is surjective, then ψ is an isomorphism.

Proof. The key trick is to give M an $R[t]$-module structure to M by defining $R[t] \mapsto \operatorname{End}_R M$ by sending $t \mapsto \psi$. In particular, using the above, we get some p_{id} such that $p_{\mathrm{id}}(\mathrm{id}) = 0$. Further, because ψ is surjective, we see that $(t) \cdot M = M$, so when we write out

$$p_{\mathrm{id}}(x) = x^n + p_1 x^{n-1} + \cdots + p_n,$$

we see that $p_i \in \left(t^i\right)$ for each i. In particular, plugging in $x = \mathrm{id}$, we see that

$$0 = \mathrm{id} + t \cdot q(t)$$

for some $q \in R[t]$. In particular, t is invertible with inverse $q(t)$. ■

Remark 1.15. This need not be true even in vector spaces which are not finitely generated. For example, consider

$$V := \bigoplus_{i=1}^{\infty} k v_i$$

for some vectors $\{v_i\}_{i=1}^{\infty}$. Then we have the surjective map defined by $v_1 \mapsto 0$ and $v_i \mapsto v_{i-1}$ for $i > 1$, and this is not an isomorphism.

Remark 1.16. This definitely need not be true for injections giving isomorphisms. For example, $\mathbb{Z} \to 2\mathbb{Z} \hookrightarrow \mathbb{Z}$ is injective but not an isomorphism.

Corollary 1.17. Fix m and n positive integers. Then if $R^n \cong R^m$ is an isomorphism of R-modules. Then $m = n$.

Proof. Without loss of generality take $n \geq m$. Then we can construct a surjective map

$$R^m \cong R^n \twoheadrightarrow R^m,$$

which must be an isomorphism by Proposition 1.14. However, the map $R^n \twoheadrightarrow R^m$ by projection has a kernel whenever $n > m$, so the composite would have a kernel, which is our contradiction. So we must have $n = m$. ■

1.1.3 Nakayama's Lemma

Recall the definition.

Jacobson radical

Definition 1.18 (Jacobson radical)**.** Fix a ring R. Then we define the *Jacobson radical* by

$$\operatorname{rad} R := \bigcap_{\mathfrak{m}} \mathfrak{m}.$$

Observe that $r \in \operatorname{rad} R$ if and only if $1 - r \in R^\times$. In particular, $r \in \operatorname{rad} R$ if and only if $1 - r$ is not in any maximal ideal if and only if $(1 - r) = R$.

We have the following result.

Theorem 1.19 (Nakayama's lemma)**.** Fix $I \subseteq \operatorname{rad} R$ and M a finitely generated R-module. Then if $IM = M$, we have $M = 0$.

Proof. The main idea is in the following lemma.

Lemma 1.20. Fix everything as above. Then $IM = M$ implies that there is some $r \in I$ such that $(1 - r)M = 0$.

Proof. The idea is, as usual, to use Theorem 1.13. We are promised some polynomial

$$p_{\mathrm{id}}(x) := x^n + p_1 x^{n-1} + \cdots + p_n,$$

where $p_k \in I^k$. But plugging in $x = \mathrm{id}$ gives the result after rearranging for $\mathrm{id}^n = \mathrm{id}$. ■

From this lemma the result directly follows because the promised $1 - r$ is a unit. ■

Corollary 1.21. Fix $I \subseteq \operatorname{rad} R$ and M a finitely generated R-module with elements $m_1, \ldots, m_n \in M$. Then if the images $\overline{m_1}, \ldots, \overline{m_n}$ generate M/IM, then the original elements generate M.

Proof. Consider

$$M' := Rm_1 + \cdots + Rm_n.$$

Then because the given elements generate M/IM, we note that $M/M' = I(M/M')$, so $M/M' = 0$, so $M = M'$. ■

Here is an application, to localization.

Proposition 1.22. Fix R a local ring with M and N finitely generated R-modules. Then $M \otimes_R N = 0$ if and only if $M = 0$ or $N = 0$.

Proof. If $M = 0$ or $N = 0$, then of course $M \otimes_R N = 0$.

In the reverse direction, suppose $M \neq 0$. Fix $\mathfrak{m}$ the maximal ideal. Then, because M is finitely generated by some elements, we get a surjective map $M \twoheadrightarrow R/\mathfrak{m}$. Tensoring, we see that

$$M \otimes_R N \to (R/\mathfrak{m}) \otimes_R N \to 0$$

is also surjective, but then $R/\mathfrak{m} \otimes_R N = N/\mathfrak{m}N$. However, $M \otimes_R N = 0$, so $N/\mathfrak{m}N = 0$ for all maximal ideals, so $N = 0$. ■

Corollary 1.23. Fix M and N finitely generated R-modules. Then $M \otimes_R N = 0$ if and only if $\operatorname{Ann} M + \operatorname{Ann} N = R$.

Proof. If $\operatorname{Ann} M + \operatorname{Ann} N = R$, then $M \otimes_R N = 0$ by decomposing $1 = a + b$ where $a \in \operatorname{Ann} M$ and $b \in \operatorname{Ann} N$.

In the other direction, suppose that $I := \operatorname{Ann} M + \operatorname{Ann} N \subsetneq R$. Putting I in some maximal ideal $\mathfrak{m}$, we note that we can localize to $R_{\mathfrak{m}}$ and then reduce to Proposition 1.22. ■

Corollary 1.24. Fix M and N finitely generated R-modules. Then $\operatorname{Supp}(M \otimes_R N) = \operatorname{Supp} M \cap \operatorname{Supp} N$.

Proof. Fix a prime $\mathfrak{p}$. Then we see that

$$(M \otimes_R N)_{\mathfrak{p}} = M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} N_{\mathfrak{p}}$$

will vanish if and only if $M_{\mathfrak{p}} = 0$ or $N_{\mathfrak{p}} = 0$ (in particular, $R_{\mathfrak{p}}$ is local with unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$, so Proposition 1.22 applies), which is precisely the statement after negation. ■

We note that the condition that M and N are finitely generated is crucial.

Non-Example 1.25. We note that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = 0$ because $\mathbb{Q}$ is divisible and $\mathbb{Z}/n\mathbb{Z}$ is torsion. But $\mathbb{Q} \neq 0$ and $\mathbb{Z}/n\mathbb{Z} \neq 0$.

1.1.4 Integrality Preview

We will spend the rest of class on the following theorem.

Proposition 1.26. 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.

Proof. Here we go.

(a) If S is finitely generated as an R-module, we apply Theorem 1.13 with $\varphi = \mu_s : m \mapsto sm$ to finish.

In the other direction, suppose

$$p(x) := x^n + p_1 x^{n-1} + \cdots + p_n$$

is a polynomial in I. Then $\{1, s, s^2, \ldots, s^{n-1}\}$ will generate S over R: indeed, it suffices to check that each s^k can be written as an R-linear combination of the $\{1, s, \ldots, s^{n-1}\}$, but we get this by induction after noting p promises

$$s^{n+\ell} = -\sum_{i=0}^{n-1} p_{n-i} s^{i+\ell}.$$

(b) If S is a free, finitely generated R-module, we got some monic polynomial in I, so we find the nonzero polynomial of least degree. Because the generation is free, using a power basis means we can force this polynomial to be monic, which gives the result.

The other direction is similar to the other direction above. ■

We close with some definitions.

Finite

Definition 1.27 (Finite)**.** Fix S an R-algebra. Then S is *finite* over R if and only if S is finitely geneated over R.

Integral

Definition 1.28 (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.