602: Algebra II

Nir Elber

Spring 2025

Contents

How strange to actually have to see the path of your journey in order to make it.

—Neal Shusterman, [Shu16]

Theme 1
Introduction

1.1 January 30

I missed the first class due to an interview. Hopefully I have some idea of what is going on. This class has a grader, named Chuhuan Huang; his email is `chuaun@jh.edu`.

1.1.1 Algebraic Sets

Today we will continue talking about algebraic sets. Our exposition follows [Lan02, Section 11.2]. We recall the definition.

Definition 1.1 (algebraic)**.** Fix a field k. An *algebraic set* is a subset $A \subseteq k^n$ for which there is an ideal $I \subseteq k[x_1, \dots, x_n]$ for which

$$A = \{x \in k^n : f(x) = 0 \text{ for all } f \in I\}.$$

We may say that A is the zero set $Z(I)$ for the polynomials f.

Remark 1.2. One may replace the ideal I with a general subset $S \subseteq k[x_1, \dots, x_n]$. This does not increase the generality because the subset $Z(S) \subseteq k^n$ of zeroes of S is the same as the subset $Z(I)$ where I is the ideal generated by S.

Algebraic sets form some classical version of algebraic geometry, which encodes a certain communication between geometry and algebra. For example, the affine space $k^n = \mathbb{A}_k^n$ and the algebra $k[x_1, \dots, x_n]$.

Last time, we stated the nullstellensatz. This requires the notion of the radical.

Definition 1.3 (radical)**.** An ideal I of a ring R is *radical* if and only if any $a \in R$ for which there is $n \geq 0$ such that $a^n \in I$ satisfies $a \in I$. Given any ideal I of a ring R, one can define the radical ideal $\sqrt{I}$ as

$$\{a \in R : a^n \in I \text{ for some } n \geq 0\}.$$

Example 1.4. Given an algebraic set $A \subseteq \mathbb{A}_k^n$, one can check that the ideal

$$I(A) \coloneqq \{f \in k[x_1, \dots, x_n] : f(x) = 0 \text{ for all } x \in A\}$$

is a radical ideal.

And here is our statement.

Theorem 1.5 (Nullstellensatz)**.** Fix an algebraically closed field k and a positive integer n. Then there is a bijection between the set of algebraic subsets of an affine space $\mathbb{A}_k^n$ and the radical ideals $I \subseteq k[x_1, \dots, x_n]$. This bijection is given by the constructions $I \mapsto Z(I)$ and $A \mapsto I(A)$.

Proof. This theorem is rather hard, so we will not attempt to prove it now. ■

Remark 1.6. One can check that the bijections in Theorem 1.5 are inclusion-reversing. For example, an inclusion $A \subseteq B$ of algebraic sets induces an inclusion of ideals $I(B) \subseteq I(A)$.

This is remarkable because it will let us play algebraic intuition and geometric intuition off of each other, which each have their own strengths.

As a sort of example of this interplay, we recall the notion of Noetherian.

Definition 1.7 (Noetherian)**.** A ring R is *Noetherian* if and only if any ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq \cdots$$

eventually stabilizes; i.e., there should exist some N such that $I_n = I_m$ for any $n, m > N$.

As such, the bijection of Theorem 1.5 tells us that algebraic sets satisfies some kind of descending chain condition: any descending chain

$$A_1 \supseteq A_2 \supseteq \cdots$$

of algebraic sets must stabilize in the sense there is N for which $A_n = A_m$ whenever $n, m > N$.

As another example, we note that there are natural geometric operations of union and intersection of algebraic sets. Here are the corresponding operations on ideals.

Lemma 1.8. Fix two ideals I and J of a ring R.

(a) The intersection $I \cap J$ is an ideal of R.

(b) The sum $I + J = \{a + b : a \in I \text{ and } b \in J\}$ is an ideal of R.

Proof. Omitted. The idea is to unravel the definition of ideals everywhere. ■

The point is that, for algebraic sets A and B, one can check that $I(A \cup B) = I(A) \cap I(B)$ and $I(A \cap B) = \sqrt{I(A) + I(B)}$. For example, to check that $I(A \cup B) = I(A) \cap I(B)$, we must check that some $f \in k[x_1, \dots, x_n]$ vanishes on $A \cup B$ if and only if it vanishes on both A and B. Similarly, to check $I(A \cap B) = \sqrt{I(A) + I(B)}$, Theorem 1.5 allows us to check that $A \cap B$ is cut out by $I(A) + I(B)$, which can be done after some effort.

1.1.2 Irreducible Algebraic Sets

On the geometric side, one often finds that our algebraic sets can be decomposed into smaller pieces.

Example 1.9. The algebraic set $x_1 x_2 = 0$ inside $\mathbb{A}_k^2$ is the union of the two lines $x_1 = 0$ and $x_2 = 0$.

To prevent this sort of thing from happening, we introduce irreducibility.

Definition 1.10 (irreducible)**.** Fix an algebraically closed field k. An algebraic set $A \subseteq \mathbb{A}_k^n$ is *irreducible* if and only if any decomposition $A = A_1 \cup A_2$ into algebraic subsets has $A = A_1$ or $A = A_2$.

This allows us to define the notion of variety.

Definition 1.11 (variety)**.** Fix an algebraically closed field k. An *affine algebraic variety* over k is an irreducible algebraic set.

Of course, with a notion of irreducibility, we would like to know that we can always break down algebraic sets into irreducible ones.

Proposition 1.12. Fix an algebraically closed field k.

(a) For any algebraic set $A \subseteq \mathbb{A}_k^n$, there are irreducible algebraic subsets $V_1, \dots, V_n$ such that

$$A = V_1 \cup \cdots \cup V_n.$$

(b) The decomposition in (a) is unique up to permutation and inclusions.

(c) Fix irreducible algebraic subsets $W, V_1, \dots, V_n$ such that $W \subseteq V_1 \cup \cdots \cup V_n$. Then $W \subseteq V_i$ for some i.

Proof. Here we go.

(a) This is an example of "Noetherian induction." If A is irreducible, then we are done. Otherwise, we may write A as a union of proper algebraic subsets $A_1 \cup A_2$. If A_1 and A_2 are irreducible, then we are done. Otherwise, we can continue decomposing them. Note that this process must eventually terminate by the descending chain condition described above.

(b) Suppose that we have two equal unions

$$V_1 \cup \cdots \cup V_n = W_1 \cup \cdots \cup W_m$$

of irreducible algebraic sets. It is enough to check that each V_i is included in some W_j, for then one finds that the decompositions must be the same up to permutation and inclusion. This last claim follows from (c), which we prove next (and independently).

(c) Note that

$$W = (W \cap V_1) \cup \cdots \cup (W \cap V_n).$$

Thus, we have decomposed W into a union of algebraic sets, so we must have $W = W \cap V_i$ for some i. The result follows. ∎

Corollary 1.13. Fix an algebraically closed field k. Then an algebraic set $A \subseteq \mathbb{A}_k^n$ is irreducible if and only if $I(A)$ is a prime ideal.

Proof. We show our two implications separately. Set $I \coloneqq I(A)$ for brevity.

- Suppose that I is not prime, and we will show that A is not irreducible. Well, because I is not prime, we are granted $f, g \notin I$ such that $fg \in I$. Then define $A_1 \coloneqq Z(I + (f))$ and $A_2 \coloneqq Z(I + (g))$ so that A_1 and A_2 are proper subsets of A. We finish by claiming that $A = A_1 \cup A_2$. Well, $x \in A$ will have $(fg)(x) = 0$, so $f(x) = 0$ or $g(x) = 0$, so $x \in A_1$ or $x \in A_2$.

- Suppose that A is not irreducible, and we will show that I is not prime. Well, we are granted a decomposition $A = A_1 \cup A_2$ of A into proper algebraic subsets, and write $I_1 = I(A_1)$ and $I_2 = I(A_2)$. Then Theorem 1.5 tells us that there must be $f \in I_1 \setminus I$ and $g \in I_2 \setminus I$. But then fg can be checked to vanish on $A_1 \cup A_2$, so $fg \in I$, and we are done. ∎

1.1.3 Asides

A key benefit of geometry is that one expects to have some topological structure. However, for an arbitrary field k, it is not so obvious how to do this. The solution is the Zariski topology.

Definition 1.14 (Zariski topology)**.** Fix a field k. Then we define the *Zariski topology* on $\mathbb{A}_k^n$ as given by requiring that the closed sets are exactly the algebraic sets.

Remark 1.15. Let's check that the Zariski topology is actually a topology.

- Note that $\varnothing$ is an algebraic set cut out by $k[x_1, \dots, x_n]$, and $\mathbb{A}_k^n$ is an algebraic set cut out by (0).
- For two algebraic sets A and B, the union $A \cup B$ is still algebraic by Lemma 1.8.
- For a collection $\{A_i\}$ of closed sets, the intersection must go down to a finite intersection by the descending chain condition, which is then algebraic by Lemma 1.8.

As a quick aside, let's gesture towards algebraic geometry. For example, there is an irreducible decomposition for general rings, even working for rings which are not radical; this is known as the primary decomposition. For example, the algebraic set cut out by (x^2y) should be expanded as $(x^2) \cap (y)$, and even though (x^2) is not radical! This is the realm of scheme theory.

In our classical language above, we see that closed points of $\mathbb{A}_k^n$ correspond to maximal ideals $\mathfrak{m} \subseteq k[x_1, \dots, x_n]$: simply send $(a_1, \dots, a_n) \in \mathbb{A}_k^n$ to the ideal

$$(x_1 - a_1, \dots, x_n - a_n)$$

which cuts out this point. When moving to scheme theory, maximal ideals will produce points, but we will have other points; maximal ideals will correspond precisely to the closed points.

Remark 1.16. If k fails to be algebraically closed, field, we note that the bijection between n-tuples in $\mathbb{A}_k^n$ and maximal ideals breaks down. For example, if $k = \mathbb{R}$, then the ideal $(x^2 + 1) \subseteq \mathbb{R}[x]$ is maximal, but it cuts out no points in $\mathbb{A}_{\mathbb{R}}^1$; similarly, $(x^2 + y^2 + 1) \subseteq \mathbb{R}[x, y]$ is maximal! We may say that these maximal ideals cut out a closed point "of degree 2" because they are generated by a polynomial of degree 2. It turns out that all closed points in $\mathbb{A}_{\mathbb{R}}^n$ have degree 1 or 2; this boils down to a classification of the maximal ideals in $\mathbb{R}[x_1, \dots, x_n]$.

Remark 1.17 (Pappus)**.** It is possible to detect the commutativity of the field k using geometry. This is a configuration due to Pappus. In short, one considers two pairs of collinear points (P_1, P_5, P_3) and (P_4, P_2, P_6). It turns out that the collinearity of the intersections $\overline{P_1P_2} \cap \overline{P_4P_5}$ and $\overline{P_5P_6} \cap \overline{P_2P_3}$ and $\overline{P_1P_6} \cap \overline{P_3P_4}$ exactly corresponds to an algebraic equation which detects commutativity of k. To be slightly more formal, one can write out what the collinearity means in terms of an algebraic equation in terms of elements of k, and this equation is always satisfied in elements of k if and only if k is commutative.

1.1.4 Kummer Theory

Our exposition follows [Lan02, Theorems IV.8.1–IV.8.2]. Similar to Galois theory, Kummer theory is interested in a duality between fields and groups. However, Kummer theory will work only with abelian extensions and pay special attention to cyclic extensions. In this sense, Kummer theory is more related to class field theory (in number theory) than Galois theory.

For this discussion, we fix a field k (probably not algebraically closed) and a positive integer m, and we assume for simplicity that $\operatorname{char} k \nmid m$. We are interested in Galois extensions K of k with abelian Galois group of exponent m. Intuitively, this means that $\operatorname{Gal}(K/k)$ is sum of cyclic groups whose sizes divide m. The key assumption of Kummer theory is that $\mu_m \subseteq k$, where μ_m means the set of mth roots of unity.

Example 1.18. The extensions of $\mathbb{Q}$ which are Galois with Galois group of exponent 2 are called "multi-quadratic." It turns out that they can also be described as being generated by square roots of elements of $\mathbb{Q}$. This is possible, from the perspective of Kummer theory, because $\mu_2 = \{\pm 1\}$ is contained in $\mathbb{Q}$.

Remark 1.19. Relaxing the condition $\mu_m \subseteq k$ dives into class field theory. Relaxing the condition that our extensions are abelian leads towards the Langlands program.

1.2 February 4

There is a topics list for presentations. They are not required, but they may help improve one's grade. There is a Gradescope for submission with code NG337Y. The homework is 37–38 on page 327, 44 on page 329, and 1, 2, 5–9 on pages 545–546. It is due next week.

1.2.1 More on Kummer Theory

Today we return to Kummer theory. As last time, we assume that k is a field, and m is a positive integer such that $\mu_m \subseteq k$ and that $\operatorname{char} k \nmid m$. (We will touch on $m = p = \operatorname{char} k > 0$ later.)

We begin by classifying cyclic extensions. We begin with a "cohomological" input.

Proposition 1.20 (Hilbert's theorem 90)**.** Fix a cyclic extension K/k of degree m, and choose a generator $\sigma \in \operatorname{Gal}(K/k)$. The following are equivalent for some $\beta \in K^\times$.

(a) $\mathrm{N}_{K/k}(\beta) = 1$.

(b) There is $\alpha \in K^\times$ such that $\beta = \sigma(\alpha)/\alpha$.

Proof. To see that (b) implies (a), we compute

$$\begin{aligned}\mathrm{N}_{K/k}(\beta) &= \prod_{i=0}^{m-1} \sigma^i(\beta) \\ &= \prod_{i=0}^{m-1} \sigma^{i+1}(\alpha) \cdot \prod_{i=0}^{m-1} \sigma^i(\alpha) \\ &= 1,\end{aligned}$$

where the last equality follows by re-indexing the left product.

The main content will be in showing (a) implies (b). The key difficulty lies in the construction of α, which will not be done explicitly. There are a few ways to motivate the following discussion. We will simply say that the above "telescoping" suggests that we would like to choose α of the form

$$\alpha = \theta + \beta\theta^\sigma + \beta^{1+\sigma}\theta^{\sigma^2} + \cdots + \beta^{1+\sigma+\cdots+\sigma^{m-2}}\theta^{\sigma^{m-1}}$$

for some $\theta \in K$, where we are using exponential notation for our Galois action. Indeed, we see that $\sigma(\alpha)\beta = \alpha$, so we will be done as soon as we can find any $\theta \in K$ making the above expression for α nonzero.

More generally, there is a linear independence result for characters: we claim that any distinct characters $\chi_1, \ldots, \chi_n$ of a finite group G are linearly independent as functions $G \to \mathbb{C}$. Indeed, supposing for the sake of contradiction that there is a set of linearly dependent distinct characters, we may assume that our list is minimal. But then a nonzero linear relation $a_1\chi_1 + \cdots + a_n\chi_n = 0$ induces a smaller relation

$$a_1(\sigma_1(y) - \sigma_n(y))\sigma_1 + \cdots + a_n(\sigma_n(y) - \sigma_n(y))\sigma_n = 0$$

for any choice of $y \in G$. (Namely, this relation is smaller because the last coefficient is now zero.) For example, if we choose y so that $\sigma_1(y) \neq \sigma_n(y)$, then the first coefficient is nonzero, so this is indeed a strictly smaller nonzero linear relation, providing the needed contradiction. ■

Corollary 1.21. Fix a cyclic extension K/k of degree m. Suppose that $\operatorname{char} k \nmid m$ and $\mu_m \subseteq k$. Then there is $\alpha \in K$ such that $K = k(\alpha)$ and $\alpha^m \in k$.

Proof. Choose a generator σ of $\mathrm{Gal}(K/k)$. We use Proposition 1.20 to construct the needed α. In particular, choose a generator ζ of μ_m, and then $\zeta \in k$ implies that $\mathrm{N}_{K/k}(\zeta) = \zeta^m = 1$. Thus, there is $\alpha \in K$ such that $\zeta = \sigma(\alpha)/\alpha$, so $\sigma(\alpha) = \zeta\alpha$, and a quick induction shows that $\sigma^i(\alpha) = \zeta^i\alpha$ for all i. Thus, α has m distinct Galois conjugates, so $k(\alpha)$ is a degree m extension of k, so $k(\alpha) = K$ follows for degree reasons. Lastly, we should check that $\alpha^m \in k$, which follows because

$$\sigma^i(\alpha^m) = \zeta^{mi}\alpha^m = \alpha^m$$

for all σ. ■

Here is the main theorem, which extends the example from last class.

Theorem 1.22 (Kummer)**.** Fix a field k and a positive integer m. Suppose that $\operatorname{char} k \nmid m$ and $\mu_m \subseteq k$.

(a) There is a map sending subgroups B between $k^{\times m}$ and $k^\times$ to abelian extensions K/k of exponent m. This map sends B to the extension $K_B \coloneqq k(B^{1/m})$ of k generated by the mth roots of B.

(b) Given some such B, the extension K_B/k is finite if and only if the index $[B : k^{\times m}]$ is finite. In fact, there is an isomorphism
$$\mathrm{Gal}(K_B/k)^\vee \to B/k^{\times m}.$$

(c) The map in (a) is an inclusion-preserving bijection.

Proof. The main input is to define a "Kummer pairing." Motivated by the above discussion, one can describe the pairing $\mathrm{Gal}(K_B/k) \times B \to \mu_m$ by sending a pair (σ, a) to the root of unity $\langle\sigma, a\rangle \in \mu_m$ such that

$$\sigma(\alpha) = \langle\sigma, a\rangle\sigma(\alpha),$$

where α is any root of the polynomial $X^m - a$. Namely, α and $\sigma(\alpha)$ are both roots of the equation $X^m - a$, so there is a unique root of unity $\langle\sigma, a\rangle \in \mu_m$ relating the two. Additionally, one can check that $\langle\sigma, a\rangle$ does not depend on the precise choice of α: any other root of $X^m - a$ takes the form $\zeta\alpha$ for some $\zeta \in \mu_m$, so the fact that $\mu_m \subseteq k$ implies that

$$\frac{\sigma(\zeta\alpha)}{\zeta\alpha} = \frac{\sigma(\alpha)}{\alpha}.$$

We now show our parts in sequence. Everything is rather formal except for the surjectivity check in (c), for which we must use Corollary 1.21.

(a) We must check that K_B/k is an abelian Galois extension of exponent m.

- To see that it is Galois, it is enough to check that it is generated by Galois elements, so it is enough to check that all Galois conjugates of $\alpha \in B^{1/m}$ live in K_B. Well, $a \coloneqq \alpha^m$ is an element of k by construction, so α is the root of the polynomial $X^m - a$. Because $\mu_m \subseteq k$, we see that the set
$$\{\zeta\alpha : \zeta \in \mu_m\}$$
of roots of $X^m - a$ is therefore contained in K_B.

- To see that it is abelian, choose two automorphisms $\sigma, \tau \in \mathrm{Gal}(K_B/k)$. We would like to check that $\sigma\tau = \tau\sigma$. It is enough to check this equality on generating elements of K_B/k, so we once again choose some $\alpha \in B^{1/m}$ and set $a \coloneqq \alpha^m$. Then we see that

$$\sigma\tau(\alpha) = \langle \sigma, a\rangle\langle \tau, a\rangle = \tau\sigma(\alpha).$$

(b) We will show that $\langle \cdot, \cdot \rangle$ descends to a perfect pairing

$$\mathrm{Gal}(K_B/k) \times B/k^{\times m} \to \mu_m.$$

Here are our checks.

- Well-defined: if $a \in B$ and $b \in k$, we must check that $\langle \sigma, a\rangle = \langle \sigma, ab^m\rangle$. Well, this amounts to noting

$$\frac{\sigma(\alpha)}{\alpha} = \frac{\sigma(\alpha b)}{\alpha b}$$

for a chosen root α of $X^m - a$.

- Injective on $\mathrm{Gal}(K_B/k)$: suppose that $\sigma \in \mathrm{Gal}(K_B/k)$ makes $\langle \sigma, \cdot\rangle$ the trivial function, and we must show that σ is trivial. Well, it is enough to show that σ is trivial on $B^{1/m}$, so we choose some $\alpha \in B^{1/m}$ and set $a \coloneqq \alpha^m$. Then

$$\frac{\sigma(\alpha)}{\alpha} = \langle \sigma, a\rangle = 1,$$

so σ is the identity on α.

- Injective on $B/k^{\times m}$: suppose that $a \in B$ makes $\langle \cdot, a\rangle$ is trivial, and we would like to show that $a \in k^{\times m}$. Well, choose a root $\alpha \in K_B$ of $X^m - a$, and we would like to show that $\alpha \in k$. For this, we note that $\langle \sigma, \alpha\rangle = 1$ implies that $\sigma(\alpha) = \alpha$ for all $\sigma \in \mathrm{Gal}(K_B/k)$, so the result follows.

(c) This will require some effort. Here are our checks.

- Inclusion-preserving: if $B_1 \subseteq B_2$, then we see $B_1^{1/m} \subseteq B_2^{1/m}$, so $K_{B_1} \subseteq K_{B_2}$.
- Injective: in light of the previous check, it's enough to see that $K_{B_1} \subseteq K_{B_2}$ implies that $B_1 \subseteq B_2$. For this, we reduce to the finite case. Choose $b \in B_1$, and it is enough to check that $b \in B_2$ given that $K_{\langle b\rangle} \subseteq K_{B_2}$. However, $b \in K_{B_2}$ implies that b can be written as a finite polynomial in terms of finitely many elements in $B_2^{1/m}$, so we may as well replace B_2 by this finite subset to check that $b \in K_{B_2}$. In total, we are reduced to the case where B_1 is generated by b and B_2 is finite.
  Now, define $B_3 \subseteq k^\times$ as being generated by B_2 and b. Because $b \in K_{B_2}$ already, we know $K_{B_2} = K_{B_3}$, so the duality of (b) implies

$$[B_2 : k^{\times m}] = [B_3 : k^{\times m}].$$

Because $B_2/k^{\times m} \subseteq B_3/k^{\times m}$ already, we see that equality must follow, so $b \in B_2$ is forced.

- Surjective: Choose an extension K/k which is abelian of exponent m. It is enough to check that K can be generated by the mth roots of some subset $S \subseteq k^{\times m}$, from which we find $K = K_B$ where B is the multiplicative subgroup generated by S. By writing K as a composite of finite extensions of k, we note that each of these finite extensions must be abelian, so it is enough to generate such a finite abelian extension by mth roots. Well, a finite abelian group can be written as a product of cyclic groups, so we may write a finite abelian extension as a composite of cyclic ones, so it is enough to generate such finite cyclic extensions by mth roots. This is possible by Corollary 1.21. ∎

1.2.2 Artin–Schreier Theory

Fix a field k of positive characteristic $p > 0$. Instead of using the pth power map (which is injective in characteristic $p > 0$ and therefore not very useful), we define a map $\pi\colon k \to k$ by $\pi(x) \coloneqq x^p - x$.

Theorem 1.23 (Artin–Schreier)**.** Fix a field k of positive characteristic $p > 0$. Define the map $\pi\colon k \to k$ by $\pi(x) \coloneqq x^p - x$.

(a) There is a map between subgroups B of k and abelian extensions K/k of exponent p. This map sends B to the extension $K_B \coloneqq k\left(\pi^{-1}B\right)$.

(b) Given some such B, the extension K_B/k is finite if and only if $[B : \pi(k)] < \infty$.

(c) The map in (a) is an inclusion-reversing bijection.

The proofs are similar, but I will omit them (as they were omitted in lecture) due to laziness. Here, the pairing (σ, a) is defined by choosing a root α of $X^p - X - a$ and then setting

$$\langle \sigma, a \rangle \coloneqq \sigma(\alpha) - \alpha.$$

1.2.3 Matrices and Linear Algebra

We now turn to a subject closer to linear algebra. We remark that we will discuss multilinear algebra later in this class.

Notation 1.24. Fix a commutative ring R, and choose nonnegative integers $m, m \geq 0$. Then we let $R^{m\times n}$ denote the R-module of $m \times n$ matrices with entries in R. We may write $M_n(R) \coloneqq R^{n\times n}$, which we note is a ring under matrix multiplication.

Remark 1.25. If $m = 0$ or $n = 0$, then these matrices are generally vacuous. For inductive reasons, it is occasionally helpful to assume that there is exactly one such square 0×0 matrix with determinant 1 and trace 0.

Given a matrix $A \in R^{m\times n}$, we may write out its coefficients as $\{A_{ij}\}$, where the indices implicitly range among $i \in \{1, \dots, m\}$ and $j \in \{1, \dots, n\}$.

Remark 1.26. As usual, we note that there is an explicitly defined matrix multiplication

$$R^{m\times n} \times R^{\ell\times m} \to R^{\ell\times n}.$$

Explicitly, one has

$$(AB)_{ik} \coloneqq \sum_{j=1}^{m} A_{ij}B_{jk}.$$

Remark 1.27. One can consider infinite-dimensional matrices, but we will generally avoid doing so.

Here are the typical operations one can do on matrices.

Definition 1.28 (transpose)**.** Fix a commutative ring R, and choose nonnegative integers $m, n \geq 0$. Given $A \in R^{m\times n}$, we define the *transpose* $A^\intercal \in R^{n\times m}$ as having the coefficients

$$\left(A^\intercal\right)_{ij} \coloneqq A_{ji}$$

for any $i \in \{1, \dots, m\}$ and $j \in \{1, \dots, n\}$.

Remark 1.29. Here are some basic properties of the transpose which can be checked on the level of the coefficients.

- For $A, B \in R^{m\times n}$, we have $(A+B)^\intercal = A^\intercal + B^\intercal$.
- For $A \in R^{m\times n}$ and $B \in R^{\ell\times m}$, we have $(AB)^\intercal = B^\intercal A^\intercal$.

These two points imply that $(\cdot)^\intercal$ induces a homomorphism $M_n(R) \to M_n(R)^{\mathrm{op}}$ of rings.

Remark 1.30. Fix a matrix $A \in R^{m\times n}$, and let $\varphi_A \colon R^n \times R^m$ denote the corresponding linear map. Taking duals (i.e., taking $\mathrm{Hom}_R(-,R)$) and fixing the usual dual basis, one finds that the dual morphism $\varphi_A^\vee \colon R^m \to R^n$ has matrix given by $A^\intercal$.

It will be helpful to change rings in the sequel.

Notation 1.31 (base change)**.** Fix a ring homomorphism $\varphi \colon R \to R'$. Given some matrix $A \in R^{m\times n}$, then we define the matrix $\varphi(A) \in (R')^{m\times n}$ on coefficients by

$$\varphi(A)_{ij} \coloneqq \varphi(A_{ij}).$$

Example 1.32. In linear algebra, the sort of base-changes one typically does is embedding a field k into a larger field such as an algebraic closure. (For example, the embedding $\mathbb{R} \hookrightarrow \mathbb{C}$ is used frequently.) However, we remark that we are also permitting some more exotic morphisms such as the surjection $\mathbb{Z} \twoheadrightarrow \mathbb{F}_p$.

Let's go ahead and define some functions on matrices.

Definition 1.33 (trace)**.** Fix a commutative ring R, and choose nonnegative integers $m, n \geq 0$. Given $A \in R^{m\times n}$, we define the *trace* as

$$\operatorname{tr} A \coloneqq \sum_{i=1}^{\min\{m,n\}} A_{ii}.$$

Remark 1.34. Here are some basic properties that can be checked on coefficients.

- For $A \in R^{m\times n}$ and $B \in R^{n\times m}$, one has $\operatorname{tr}(AB) = \operatorname{tr}(BA)$.
- Specifically, if $A, B \in M_n(R)$ with B invertible, then $\operatorname{tr}\left(B^{-1}AB\right) = \operatorname{tr} A$. We remark that one can show this in a "basis-free" manner by providing a basis-free definition of the trace and then remarking that $A \mapsto B^{-1}AB$ amounts to a change of basis.

Definition 1.35 (rank)**.** Fix a field k, and choose nonnegative integers $m, n \geq 0$. Given $A \in R^{m\times n}$, we define the *rank* as the dimension of the image of the associated linear map $A \colon R^n \to R^m$.

Remark 1.36. By duality arguments, one finds that $\operatorname{rank} A = \operatorname{rank} A^\intercal$. Roughly speaking, one takes $\mathrm{Hom}_k(-,k)$ everywhere. This is an abstracted version of the

Remark 1.37. There is a short exact sequence

$$0 \to \ker A \subseteq k^n \overset{A}{\twoheadrightarrow} \operatorname{im} A \to 0.$$

Taking dimensions, one finds $n = \dim \ker A + \dim \operatorname{im} A$.

Remark 1.38. We quickly remark that there is a method of Gaussian elimination which can be used to compute ranks. In fact, one can show that the "column" and "row" ranks are preserved by the row and column operations (because row and column operations amount to multiplying by the left or on the right by some specified invertible matrices), from which it follows that the column and row ranks are equal after reducing to some row Echelon form.

Remark 1.39. There is a variant of Gaussian elimination when we are not working over a field. The resulting "reduced" matrix is called the Smith normal form.

We would now like a way to work with R-modules of the form R^n without admitting that the module is R^n.

Definition 1.40 (free)**.** Fix a commutative ring R. Then an R-module M is *free of finite rank* if and only if there is a finite subset $B \subseteq M$ such that any $m \in M$ admits a unique tuple $\{a_b\}_{b \in B}$ of elements in R such that

$$m = \sum_{b \in B} a_b b.$$

In this event, we call the subset B a *basis*, and we say that the *rank* of M is $\#B$.

Remark 1.41. There is a generalization removing the finite rank condition, but then we must require that the tuple of coefficients $\{a_b\}$ have $a_b = 0$ for all but finitely many $b \in B$.

Notation 1.42. Fix a commutative ring R, and let E and F be free modules of finite rank with bases $B = \{b_1, \dots, b_m\}$ and $C = \{c_1, \dots, c_n\}$, respectively. Given any $(n \times m)$-matrix A, we define the associated R-module map $A_C^B \colon E \to F$ by

$$A_C^B(b_j) \coloneqq \sum_{i=1}^{n} A_{ij} c_i.$$

For example, if $E = F$, then one can see that the endomorphism ring $\operatorname{End}_R(E)$ is isomorphic to $M_n(R)$, where n is the rank of E.

Remark 1.43. One can check that this construction $A \mapsto A_C^B$ provides a bijection between matrices and linear maps. Instead of writing out the checks, we will remark that the inverse map sends a map $f \colon E \to F$ to the matrix A defined by

$$f(b_j) = \sum_{i=1}^{n} (M_C^B f)_{ij} c_i,$$

where the coefficients are uniquely defined by having a basis.

Remark 1.44. As usual, on coefficients, one can check that $(A + A')_C^B = A_C^B + (A')_C^B$. If there is an additional free R-module G of finite rank and basis D, then one can check on coefficients that

$$(A'A)_D^B = (A')_D^C \circ A_C^B.$$

For example, this gives a clean proof that matrix multiplication should associate because function composition is associative.

1.3 February 6

Today we continue talking about linear algebra.

1.3.1 Determinants

Today, R will be a commutative ring. Given a free R-module E of rank n, we showed last time that there is an isomorphism

$$\mathrm{End}_R(E) \cong M_n(R)$$

of rings. Roughly speaking, this isomorphism is fixed as soon as we choose a basis for E. Restricting to invertible endomorphisms, we produce an isomorphism

$$\mathrm{Aut}_R(E) \cong \mathrm{GL}_n(R)$$

of groups.

Notation 1.45. Fix a commutative ring R. Given a free R-module E, we set $\mathrm{GL}_R(E) \coloneqq \mathrm{Aut}_R(E)$. We may also write $\mathrm{GL}(E)$.

We would like a way to check if an element of $M_n(R)$ is invertible and thus lives in $\mathrm{GL}_n(R)$. This is the role of the determinant.

Definition 1.46 (determinant)**.** Fix a commutative ring R. Then the determinant is the unique function $\det\colon M_n(R) \to R$ which satisfies the following.

(a) $\det$ is R-multilinear in the row and columns: scaling and adding two columns together does similar to the determinant.

(b) $\det$ is alternating in the row and columns: switching two rows or columns switches the sign of $\det$.

(c) $\det I_n = 1$, where I_n is the identity matrix.

Remark 1.47. For characteristic 2 reasons, perhaps one should change (ii) the requirement that the determinant vanishes whenever two columns are equal.

Remark 1.48. One can show using Gaussian elimination that these properties produce at most one function $\det\colon M_n(R) \to R$. Of course, it is not yet obvious that such a function exists at all, but we will explain shortly that it does.

Remark 1.49. These properties can be seen as geometrically intuitive, viewing $\det$ as a signed volume of the parallelepiped generated by the columns of the matrix.

Let's say something about why the determinant exists. This boils down to the following claim.

Proposition 1.50. Fix a commutative ring R and a free module E of rank n. Then there is a unique function $\det\colon E^n \to R$ satisfying the following properties.

(a) $\det$ is R-multilinear: one has $\det(v_1, \dots, v_{i-1}, ax + by, v_{i+1}, \dots, v_n)$ equals

$$a\det(v_1, \dots, v_{i-1}, x, v_{i+1}, \dots, v_n) + b\det(v_1, \dots, v_{i-1}, y, v_{i+1}, \dots, v_n).$$

(b) $\det$ is alternating: one has

$$\det(v_1, \dots, v_n) = 0$$

if $v_i = v_j$ for any distinct pairs (i, j).

(c) $\det(e_1, \dots, e_n) = 1$ for any choice of basis $\{e_1, \dots, e_n\}$.

Remark 1.51. Roughly speaking, this proposition amounts to saying that the nth alternating power $\wedge^n E$ is free over R of rank 1. Then $\det$ makes a basis of this space.

Remark 1.52. One can show that $\det AB = \det A \cdot \det B$ for matrices $A, B \in M_n(R)$. In particular, we see that $\det\colon \mathrm{GL}_n(R) \to R^\times$ is a group homomorphism.

Remark 1.53. Using the previous remark, we see that $A \in \mathrm{GL}_n(R)$ implies that $\det A \in R^\times$. In fact, the converse is also true, but it is not so obvious. Roughly speaking, one should explicitly construct an inverse using something like Kramer's rule or the adjugate matrix, and somewhere in the construction of the inverse one needs to invert a determinant.

1.3.2 Bilinear Forms

Here is our definition.

Definition 1.54 (bilinear)**.** Fix a commutative ring R and two R-modules E and F. Then a *bilinear form* is a function $f\colon E \times F \to R$ satisfying the following.

(a) For any $x \in E$, the function $F \to R$ defined by $y \mapsto f(x, y)$ is R-linear.

(b) For any $y \in F$, the function $E \to R$ defined by $x \mapsto f(x, y)$ is R-linear.

We let $L^2(E, F; R)$ denote the set of bilinear forms $E \times F \to R$.

Remark 1.55. We note that $L^2(E, F; R)$ is an R-module.

One can expand out these conditions in terms of elements. For example, the linearity of $y \mapsto f(x, y)$ amounts to requiring

$$f(x, b_1y_1 + b_2y_2) = b_1f(x, y_1) + b_2f(x, y_2).$$

As in geometry, it will be helpful to have a notion of orthogonality.

Definition 1.56 (orthogonal)**.** Fix a commutative ring R, and let $\langle \cdot, \cdot \rangle\colon E \times F \to R$ be a bilinear form. Then we say that $x \in E$ and $y \in F$ are *orthogonal* if and only if $\langle x, y \rangle = 0$. We write $F^\perp$ for the collection of $x \in E$ such that $\langle x, y \rangle = 0$ for all $y \in R$; we define $E^\perp \subseteq F$ similarly.

Remark 1.57. One can directly check that $F^\perp$ and $E^\perp$ are R-submodules of E and F, respectively.

Definition 1.58. Fix a commutative ring R, and let $\langle \cdot, \cdot \rangle : E \times F \to R$ be a bilinear form.

- $\langle \cdot, \cdot \rangle$ is *non-degenerate on the left* if and only if $F^\perp = 0$.
- $\langle \cdot, \cdot \rangle$ is *non-degenerate on the right* if and only if $E^\perp = 0$.
- $\langle \cdot, \cdot \rangle$ is *non-degenerate* if and only if we have both $E^\perp = 0$ and $F^\perp = 0$.

We take a moment to explain some currying.

Proposition 1.59. Fix a commutative ring R and R-modules E and F. Then there is a canonical isomorphism

$$L^2(E, F; R) \to \mathrm{Hom}_R(E, \mathrm{Hom}_R(F, R)).$$

Proof. The forward map sends some bilinear form $f : E \times F \to R$ to the morphism $\varphi_f : E \to \mathrm{Hom}_R(F, R)$ defined by

$$\varphi_f(x)(y) \coloneqq f(x, y).$$

Here, $\varphi_f(x)$ is a function $F \to R$, which explains the notation $\varphi_f(x)(y)$. The bilinearity conditions on f exactly condition to the needed linearity checks on our forward map $\varphi_\bullet$.

The backward map sends some $\varphi : E \to \mathrm{Hom}_R(F, R)$ to the bilinear form $f : E \times F \to R$ by

$$f(x, y) \coloneqq \varphi(x)(y).$$

Once again, one checks that f is bilinear using the linearity of φ and $\varphi(x)$. One can check that these constructions are mutually inverse, so we have indeed defined some isomorphisms. ∎

This discussion motivates the following definition.

Definition 1.60. Fix a commutative ring R, and let $f : E \times F \to R$ be a bilinear form.

- f is *non-singular on the left* if and only if the corresponding map $F \to \mathrm{Hom}_R(E, R)$ is an isomorphism.
- f is *non-singular on the right* if and only if the corresponding map $E \to \mathrm{Hom}_R(F, R)$ is an isomorphism.

Remark 1.61. It more or less follows from the definitions that being non-singular (on the left/right) implies being non-degenerate (on the left/right, respectively).

Remark 1.62. For finite-dimensional vector spaces over a field, one can see that being non-degenerate is equivalent to being non-singular. However, this is not true in general: it already fails if we pass to infinite-dimensional vector spaces.

Remark 1.63. If f is non-singular, then we note that we have a composite isomorphism

$$L^2(E, F; R) \cong \mathrm{Hom}_R(E, \mathrm{Hom}_R(F, R)) \leftarrow \mathrm{Hom}_R(E, E) = \mathrm{End}_R(E).$$

In general, the backwards map is well-defined: it simply sends $A \in \mathrm{End}_R(E)$ the bilinear map $(x, y) \mapsto f(Ax, y)$.

Definition 1.64 (transpose)**.** Fix a commutative ring R and a non-singular bilinear form $f\colon E \times F \to R$. We describe a construction of the transpose $\operatorname{End}_R(E) \to \operatorname{End}_R(F)$ in the presence of a non-singular bilinear form f. Given $A \in \operatorname{End}_R(E)$, one can define $A^\intercal \in \operatorname{End}_R(F)$ by satisfying the equation

$$\langle Ax, y\rangle = \langle x, A^\intercal y\rangle.$$

In particular, we see that the vector $A^\intercal y$ is uniquely defined by the non-singularity of f. One can check some basic properties such as the fact that $A^\intercal$ is actually linear and satisfies $(A+B)^\intercal = A^\intercal + B^\intercal$ and $(cA)^\intercal = cA^\intercal$.

1.4 February 11

The next homework can be found on pages 567–570; please do exercises 1–6 and 19–22.

1.4.1 More on Bilinear Forms

Euclidean geometry benefits from having access to an orthogonal group. In general, we may be interested in the automorphisms of a particular bilinear form.

Definition 1.65. Fix a bilinear form $f\colon E \times E \to R$ of an R-module E. Then an *automorphism of* f, denoted $A \in \operatorname{Aut} f$, is an automorphism $A \in \operatorname{Aut}_R E$ such that

$$f(Ax, Ay) = f(x, y)$$

for any $x, y \in E$.

Remark 1.66. If E is free of finite rank and f is nonsingular, then we can define the transpose $A^\intercal$ of some A. Then we see that

$$f(Ax, Ay) = f(A^\intercal Ax, y),$$

so we see that $A \in \operatorname{Aut} f$ if and only if $A^\intercal A = \mathrm{id}_E$.

Let's list a few more adjectives for our bilinear forms.

Definition 1.67. Fix a commutative ring R and a free module E of finite rank. Further, fix a matrix M and a bilinear form f on E.

- We say that M is *symmetric* if and only if $M = M^\intercal$. Similarly, M is *alternating* if and only if $M = -M^\intercal$, and the diagonal entries of M vanish.
- We say that f is *symmetric* if and only if $f(x, y) = f(y, x)$ always. Similarly, f is *alternating* if and only if $f(x, x) = 0$ always.

Let's explain the correspondence here. This depends on a map

$$M_n(R) \cong L^2(E),$$

where n is the rank of E. In brief, this depends on a choice of basis $B = \{x_1, \dots, x_n\}$ of E, whereupon we see that we can send a matrix M to the bilinear form

$$\langle x, y\rangle \coloneqq x^\intercal M y,$$

where x and y are realized as elements of R^n via the basis B. Conversely, a bilinear form $f\colon E \times E \to R$ produces a matrix M by letting the coefficient M_{ij} be given by $f(x_i, x_j)$. It is not hard to check that these define inverse maps $M_n(R) \to L^2(E)$ of R-modules.

Proposition 1.68. Fix a free module E of finite rank n over a commutative ring R, and let B be a basis. Under the isomorphism $M_n(R) \cong L^2(E)$, a matrix is symmetric or alternating if and only the corresponding bilinear form is symmetric or alternating, respectively.

Proof. This is direct. For example, one finds that f is symmetric if and only if $f(x_i, x_j) = f(x_j, x_i)$ on a basis, which is equivalent to the corresponding matrix being symmetric. A similar argument works in the alternating case. ■

1.4.2 Representations of Algebras

Let k be a commutative ring (sadly), and let R be a k-algebra.

Definition 1.69 (representation)**.** Fix a k-algebra R. Then a *representation* of R is a homomorphism

$$\rho \colon R \to \operatorname{End}_k(E)$$

of k-algebras, where E is some k-module. Given two representations $\rho_1 \colon R \to \operatorname{End}_k(E_1)$ and $\rho_2 \colon R \to \operatorname{End}_k(E_2)$, a homomorphism $f \colon \rho_1 \to \rho_2$ of representations is a homomorphism $f \colon E_1 \to E_2$ such that

$$f(\rho_1(r)x) = \rho_2(r)f(x)$$

for all $r \in R$ and $x \in E_1$.

Remark 1.70. Given two representations $\rho_1 \colon R \to \operatorname{End}_k(E_1)$ and $\rho_2 \colon R \to \operatorname{End}_k(E_2)$, we remark that there is a direct sum representation $(\rho_1 \oplus \rho_2) \colon R \to \operatorname{End}_k(E_1 \oplus E_2)$.

Example 1.71 (principal representation)**.** Suppose that $I \subseteq R$ is an ideal. Then multiplication in R defines a representation $\rho \colon R \to \operatorname{End}_k(I)$.

Representations are helpful because they allow us to classify (and compute with) k-algebras by placing them inside matrix algebras, and matrix algebras can be studied via the sort of linear algebra we've already discussed.

Remark 1.72. The presence of the homomorphism ρ allows us to view E as a module over R, where the action map $R \to \operatorname{End}(E)$ is given by ρ.

Representation theory may be interested in decomposing E into "subrepresentations." This frequently amounts to finding invariant subspaces, as in the following definition.

Definition 1.73 (invariant submodule)**.** Fix a commutative ring k and a representation $\rho \colon R \to \operatorname{End}_k(E)$. An *invariant submodule* is a submodule $F \subseteq E$ such that $\operatorname{im} \rho(r)|_F \subseteq F$ for all $r \in R$.

Remark 1.74. An invariant submodule $F \subseteq E$ induces an embedding of representations $F \hookrightarrow E$. There is also a way to realize a representation structure on E/F by $\rho(r) \colon (x + F) \mapsto (\rho(r)x + F)$.

Thus, we hope that the building blocks of our representation theory are those with no interesting invariant submodules.

Definition 1.75 (irreducible)**.** Fix a commutative ring k and a representation $\rho \colon R \to \operatorname{End}_k(E)$. Then ρ is *simple* or *irreducible* if and only if E is nonzero, and there are no nonzero proper invariant submodules of E.

Sadly, it is not always case that one can write a representation as a sum of irreducible representations, so we introduce a new word.

Definition 1.76 (semisimple)**.** Fix an algebra R over a commutative ring k. Then a representation $\rho\colon R \to \operatorname{End}_k(E)$ is *semisimple* if and only if E is isomorphic to a direct sum of irreducible representations.

Example 1.77 (Maschke)**.** Fix a finite group G, and consider the $\mathbb{C}$-algebra $\mathbb{C}[G]$. Then it turns out that all representations of $\mathbb{C}[G]$ are semisimple.

1.4.3 Representations of the Polynomial Ring

Fix now a field k, and we will work with the commutative k-algebra $R \coloneqq k[t]$. Then the data of a representation $\rho\colon k[t] \to \operatorname{End}_k(E)$ amounts to dictating $\rho(t)$, from which the rest of the representation is determined uniquely: given $A \coloneqq \rho(t)$, then the rest of the representation is given by

$$\rho\left(\sum_{i=0}^{d} c_i t^i\right) = \sum_{i=0}^{\infty} c_i A^i,$$

and it is not hard to check that this definition produces a well-defined representation ρ no matter how A is chosen. Thus, representations of $k[t]$ have equivalent data to a pair (E, A) of a vector space E over k together with an endomorphism A of E.

This perspective grants a clean definition of the minimal polynomial.

Definition 1.78 (minimal polynomial)**.** Fix a finite-dimensional vector space E over k. For some $A \in \operatorname{End}_k E$, we let $\rho_A\colon k[t] \to \operatorname{End}_k E$ be the representation with $\rho_A(t) = A$. Then the *minimal polynomial* for A is the monic polynomial $q_A \in k[t]$ generating the ideal $\ker \rho_A \subseteq k[t]$.

Example 1.79. Suppose that there is some $v \in E$ such that the vectors $\{A^i v\}_{i \geq 0}$ span E. With $d = \dim E$, then one finds that the vectors $\{v, Av, \dots, A^{d-1}v\}$ should be a basis of E: certainly, there is e large enough so that the vectors $\{v, Av, \dots, A^e v\}$ span E, so one can extract a basis as a subset. Now, expanding $A^d v = \sum_{i=0}^{d-1} -a_i A^i v$, we see that the minimal polynomial is $q_A(t) = t^d + a_{d-1}t^{d-1} + \cdots + a_1 t + a_0$, and A has the matrix form

$$A = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{d-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{d-1} \end{bmatrix}.$$

Additionally, we remark that the map $k[t] \to E$ given by $p(t) \mapsto p(A)v$ is surjective by hypothesis on E, so we see that we have an isomorphism $E \cong k[t]/(q_A(t))$ of $k[t]$-modules.

It turns out that all representations of $k[t]$ look like the above, maybe up to decomposition.

Theorem 1.80. Fix a finite-dimensional vector space E over a field k. Choose $A \in \mathrm{End}_k(E)$. Then is a unique sequence of nonzero, nonconstant, monic polynomials $(q_1, \dots, q_r)$ such that $q_i \mid q_{i+1}$ for each i, and there is an isomorphism of $k[t]$-modules

$$E \cong \bigoplus_{i=1}^{r} \frac{k[t]}{(q_i(t))}.$$

Further, the sequence $(q_1, \dots, q_r)$ is uniquely determined by the pair (E, A).

Proof. This is essentially the theory of the Jordan normal form. Alternatively, one can use the theory of finitely generated modules over a principal ideal domain because $k[t]$ is a principal ideal domain, for which we refer to [Lan02, Theorem III.7.7]. In fact, $k[t]$ is a Euclidean domain, so one is able to give a fairly explicit argument.

Let's take a moment to explain how the classification of finitely generated modules over a principal ideal domain is used: one then knows that we can write E as

$$E \cong \bigoplus_{i=1}^{r} \frac{k[t]}{(q_i(t))}$$

for some monic or zero polynomials $(q_1, \dots, q_r)$ satisfying $q_i \mid q_{i+1}$ for each i. However, E is finite-dimensional, so we are not allowed to have $q_i = 0$ for any i (for then $k[t]$ embeds into E, making $\dim_k E = \infty$). The result follows. ∎

Remark 1.81. It follows from the statement that q_r is the minimal polynomial of A. Indeed, the point is to recognize that $q_1 \mid q_2 \mid \cdots q_{r-1} \mid q_r$.

Definition 1.82 (invariants)**.** Fix a finite-dimensional vector space E over a field k. Choose $A \in \mathrm{End}_k(E)$. The sequence of *invariants* of A is the sequence $(q_1, \dots, q_r)$ constructed in Theorem 1.80.

We will show one the homework that the pair (E, A) is essentially determined by the sequence $(q_1, \dots, q_r)$.

1.5 February 13

Here we go.

1.5.1 More on Invariants

Let's give a few examples of invariants.

Example 1.83. Consider the case where $A \in \mathrm{End}_k(E)$ is the zero operator. Then $E = k \oplus \cdots \oplus k$ as a $k[t]$-representation, where $k[t]$ acts on k by $t \mapsto 0$. We conclude that our sequence of invariants are given by $(q_1, \dots, q_n) = (0, \dots, 0)$.

Let's give a couple applications of these invariants.

Corollary 1.84. Fix a field extension k'/k, and choose some $A \in M_n(k)$. Suppose the invariants of A split into linear polynomials in k. Then the invariants of A as an element of $\mathrm{End}_k(k^n)$ are the same as the invariants of A as an element of $\mathrm{End}_{k'}((k')^n)$.

Proof. The idea is that the isomorphism

$$E \cong \bigoplus_{i=1}^{r} \frac{k[t]}{(q_i(t))}$$

extends to an isomorphism

$$E_{k'} \cong \bigoplus_{i=1}^{r} \frac{k'[t]}{(q_i(t))},$$

from which the result follows. ∎

We now turn to the Jordan decomposition.

Theorem 1.85. Fix a finite-dimensional vector space E over a field k. Suppose that $A \in \mathrm{End}_k(E)$ has sequence of invariants given by the single polynomial $q(t) = (t-\alpha)^e$. Then E admits a basis over k such that A is the matrix

$$J_e(\alpha) = \begin{bmatrix} \alpha & 0 & 0 & \cdots & 0 & 0 \\ 1 & \alpha & 0 & \cdots & 0 & 0 \\ 0 & 1 & \alpha & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha & 0 \\ 0 & 0 & 0 & \cdots & 1 & \alpha \end{bmatrix}.$$

Proof. By hypothesis, we have an isomorphism $E \cong k[t]/\left((t-\alpha)^e\right)$ of $k[t]$-modules. Then we fix such an isomorphism, and we let $v \in E$ be the image of 1 under such an isomorphism. Then we see that

$$\left\{1, (t-\alpha), (t-\alpha)^2, \ldots, (t-\alpha)^{e-1}\right\}$$

is a basis of $k[t]/\left((t-\alpha)^e\right)$ (over k), so

$$\left\{v, (A-\alpha)v, (A-\alpha)^2, \ldots, (A-\alpha)^{e-1}v\right\}$$

is a basis for E. One can now check that this is the required basis; for example, $Av = \alpha v + (A-\alpha)v$ explains the first column of the given matrix. ∎

Notation 1.86. Fix a field k. For $\alpha \in k$ and nonnegative integer $n \geq 0$, we define the *Jordan block* $J_n(\alpha) \in M_n(k)$ as the matrix

$$J_n(\alpha) = \begin{bmatrix} \alpha & 0 & 0 & \cdots & 0 & 0 \\ 1 & \alpha & 0 & \cdots & 0 & 0 \\ 0 & 1 & \alpha & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha & 0 \\ 0 & 0 & 0 & \cdots & 1 & \alpha \end{bmatrix}.$$

Corollary 1.87 (Jordan normal form)**.** Fix a finite-dimensional vector space E over a field k which is algebraically closed. Fix $A \in \mathrm{End}_k(E)$. Then E admits a basis so that A is the block matrix

$$\begin{bmatrix} J_{n_1}(\alpha_1) & & \\ & \ddots & \\ & & J_{n_k}(\alpha_k) \end{bmatrix},$$

where $n_1, \ldots, n_k \geq 0$ are nonnegative, and $\alpha_1, \ldots, \alpha_k \in k$ are some elements.

Proof. Combine Theorem 1.80 with the basis constructed by Theorem 1.85. ∎

1.5.2 The Characteristic Polynomial

We now discuss the characteristic polynomial.

Definition 1.88. Fix a commutative ring k and matrix $M \in M_n(k)$. Then we define the *characteristic polynomial* $P_M(t)$ as the determinant of the matrix

$$tI_n - M \in M_n(k[t]),$$

where I_n is the identity matrix.

Example 1.89. If $M = 0$, then $P_M(t) = \det tI_n = (t-1)^n$.

Remark 1.90. If $N \in M_n(k)$ is invertible, then we claim that $P_{N^{-1}MN}(t) = P_M(t)$. Indeed, the inverse of N in $M_n(k)$ explains that N is still invertible in $M_n(k[t])$, so we see that

$$\det\left(tI_n - N^{-1}MN\right) = \det\left(N^{-1}\right)\det\left(tI_n - M\right)\det(N),$$

from which the result follows.

Remark 1.91. If $\varphi\colon k \to k'$ is a homomorphism of commutative rings, then

$$P_{\varphi(M)}(t) = \varphi(P_M(t)).$$

The previous remark allows us to prove the following theorem cleanly.

Theorem 1.92 (Cayley–Hamilton)**.** Fix a commutative ring k. For matrix $M \in M_n(k)$, one has $P_M(M) = 0$.

Proof. Omitted. This is fairly technical, requiring a discussion of the adjugate matrix. We refer to [Lan02, Theorem XIV.3.1]. ∎

Here is the chief application of the characteristic polynomial.

Definition 1.93 (eigenvalue)**.** Fix a vector space E over a field k and an operator $A \in \operatorname{End}_k(E)$. An *eigenvector* of A is a nonzero element $v \in E$ for which there is an *eigenvalue* $\lambda \in k$ such that $Av = \lambda v$.

Theorem 1.94. Fix a vector space E over a field k and an operator $A \in \operatorname{End}_k(E)$. Then the eigenvectors of A are exactly the roots of $P_A(t)$ in k.

Proof. Note that λ is an eigenvalue if and only if $A - \lambda \operatorname{id}_E$ fails to be invertible, which is equivalent to $\det(A - \lambda\operatorname{id}_E) = 0$, which is equivalent to $P_A(\lambda) = 0$. ∎

While we're here, let's talk a bit more about eigenvectors.

Theorem 1.95. Fix a vector space E over a field k and an operator $A \in \operatorname{End}_k(E)$. For each $\lambda \in k$, let $E_\lambda \subseteq E$ be the (possibly trivial) subspace of eigenvectors of E with eigenvalue λ (together with 0). Then the spaces $\{E_\lambda : \lambda \in k\}$ are linearly independent.

Proof. Suppose these are not linearly independent. Then there is a minimal relation among these eigenspaces, allowing us to produce a minimal collection of distinct eigenvalues $\{\lambda_1, \dots, \lambda_n\}$ together with eigenvectors $\{v_1, \dots, v_n\} \subseteq E$ (with $v_i \in E_{\lambda_i}$ for each i) such that

$$v_1 + \cdots + v_n = 0.$$

Note Applying A to this list, we see that

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0,$$

so we see that

$$(\lambda_n - \lambda_1)v_1 + \cdots + (\lambda_n - \lambda_{n-1})v_{n-1} + \underbrace{(\lambda_n - \lambda_n)}_{0} v = 0.$$

This is a strictly smaller relation, so we are done. ■

Corollary 1.96. Fix a vector space E over a field k and an operator $A \in \mathrm{End}_k(E)$. Suppose that A has $\dim_k E$ distinct eigenvalues in k. Then E admits a basis making A a diagonal matrix.

Proof. By hypothesis, $P_A(t)$ factors into linear factors, so we produce many distinct eigenvectors, which we now know are linearly independent. This is the needed basis. ■

As an aside, we connect the characteristic polynomial with the invariants.

Proposition 1.97. Fix a vector space E over a field k and an operator $A \in \mathrm{End}_k(E)$. Let $(q_1, \dots, q_r)$ be the sequence of invariants of A. Then

$$P_A(t) = q_1(t) \cdots q_r(t).$$

Proof. By decomposing E as a $k[t]$-module, we may assume that $E = k[t]/(q(t))$ for some polynomial $q(t)$. Then the result follows from Example 1.79. ■

Remark 1.98. We can now see that the minimal polynomial $q_r(t)$ and the characteristic polynomial $P_A(t)$ have the same irreducible factors.

Let's check that the characteristic polynomial is functorial.

Proposition 1.99. Fix a commutative ring k, and choose some $f \in k[t]$. For an $n(\times n)$-matrix M, suppose that $P_M(t) = \prod_{i=1}^n (t - \alpha_i)$. Then

$$P_{f(M)}(t) = \prod_{i=1}^n (t - f(\alpha_i)).$$

Proof. Over a field, one can base-change to the algebraic closure and then upper-triangularize M, from which the result follows by a computation. The general case can be reduced to the field case. Roughly speaking, the above statement can be seen as a statement about an equality of two polynomials in n^2 variables in $\mathbb{Z}[a_{00}, \dots, a_{nn}]$ (where we view the entries in M as indeterminate elements), and then the equality can be checked after base-changing to the fraction field, where we know the result. ■

In the sequel, it will be helpful to know something about additivity of the characteristic polynomial. Let's discuss this.

Theorem 1.100. Fix a commutative ring k, and let E', E, E'' be free k-modules. Suppose that we have endomorphisms $A' \in \operatorname{End}_k E'$ and $A \in \operatorname{End}_k E$ and $A'' \in \operatorname{End}_k E''$ fitting into a commutative diagram as follows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E' & \longrightarrow & E & \longrightarrow & E'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle A'} & & \downarrow{\scriptstyle A} & & \downarrow{\scriptstyle A''} & & \\ 0 & \longrightarrow & E' & \longrightarrow & E & \longrightarrow & E'' & \longrightarrow & 0 \end{array}$$

Then $P_A(t) = P_{A'}(t)P_{A''}(t)$.

Proof. Embed E' into E, and we consider E'' as the quotient E/E'. Then one can find a basis

$$\{v_1, \dots, v_{e'}, w_1, \dots, w_{e''}\}$$

of E, where $\{v_1, \dots, v_{e'}\} \subseteq E'$ is a basis, and the projections $\{w_1 + E', \dots, w_{e''} + E'\} \subseteq E/E'$ is a basis. Then one can write down a "block upper-triangular" matrix representation for A by gluing together matrix representations for A' and A'': namely, if M' and M'' are the representations of A' and A'' with respect to the given bases of E' and E'' (respectively), from which we see that A admits a matrix representation

$$\begin{bmatrix} M & * \\ & M' \end{bmatrix},$$

where $*$ denotes some coefficients which do not matter. Subtracting $t \operatorname{id}_E$ and taking the determinant completes the proof. ∎

Remark 1.101. The professor made a big deal about the fact that having a short exact sequence

$$0 \to E' \to E \to E'' \to 0$$

does not necessarily imply that $E \cong E' \oplus E''$. However, this is true for fields k. In general, one needs some hypothesis on our modules; for example, this is also true if E'' is free.

As a last application of the characteristic polynomial, we compute the trace and determinant.

Proposition 1.102. Fix a free module E of finite rank over a ring k. Suppose $A \in \operatorname{End}_k(E)$ has characteristic polynomial

$$P_A(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_1 t + c_0.$$

Then $\operatorname{tr} A = -c_{n-1}$ and $\det A = (-1)^n c_0$.

Proof. For the determinant, one simply has

$$c_0 = P_A(0) = \det(-A) = (-1)^n c_0.$$

For the trace, one needs to expand out the summation form of the determinant to compute $\det(tI_n - A)$. The idea is that not many terms in the big sum will actually contain a factor of t^{n-1}. ∎

Remark 1.103. In the situation of Theorem 1.100, we have $\operatorname{tr}(A')+\operatorname{tr}(A'') = \operatorname{tr}(A)$ and $\det(A')\det(A'') = \det(A)$. This follows by using the above computation of tr and $\det$.

As a last aside, we remark that Theorem 1.100 tells us that the characteristic polynomial $A \mapsto P_A$ is a certain map of categories. Fix a ground ring A. Let's define the categories.

- On one hand, we let $\mathcal{A}$ denote the "Euler–Grothendieck" category of pairs (E, A) where E is a free k-module of finite rank, and $A \in \mathrm{End}_k(E)$. One can think of $\mathcal{A}$ as being made of $k[t]$-modules where the underlying k-module is free of finite rank.
- On the other hand, we consider the multiplicative monoid $k[t]$.

Thus, we see that $(E, A) \mapsto P_A$ provides a map from $\mathcal{A}$ to the multiplicative monoid. We remark that P_A also factors through short exact sequences as described in Theorem 1.100, which one can view in the following sense: let $K(\mathcal{A})$ be the category $\mathcal{A}$ where we take the quotient by isomorphisms $(E', A') \oplus (E'', A'') \cong (E, A)$ whenever there is a diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E' & \longrightarrow & E & \longrightarrow & E'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle A'} & & \downarrow{\scriptstyle A} & & \downarrow{\scriptstyle A''} & & \\ 0 & \longrightarrow & E' & \longrightarrow & E & \longrightarrow & E'' & \longrightarrow & 0 \end{array}$$

which commutes. Of course, we also know that we can do something similar for the trace and determinant.

1.6 February 13

The next homework can be found on pages 596–599. Please do the exercises 2–4, 11–14, and 17–19.

1.6.1 Quadratic Forms

For today, we will focus on symmetric and skew-symmetric bilinear forms. We will also have occasion to consider Hermitian forms, which we go ahead and define.

Definition 1.104 (Hermitian)**.** Fix a ring R admitting an automorphism $a \mapsto \overline{a}$ of order 2. Given a module E, a map $g\colon E \times E \to R$ is *Hermitian* if and only if it satisfies the following.

- The function $a \mapsto g(a, b)$ is R-linear for any $b \in E$.
- Conjugate symmetry: we have $g(a, b) = \overline{g(b, a)}$ for any $a, b \in E$.

Note that the map $b \mapsto g(a, b)$ is not expected to be R-linear due to the conjugate symmetry.

We would like to find good bases for such quadratic forms. For example, when writing out bilinear forms as matrices, it would be nice for these matrices to be block-diagonal with small blocks.

Lemma 1.105. Fix a module E over a ring R. Suppose that $g\colon E \times E \to R$ is symmetric, alternating, or Hermitian. Fix some $a \in E$. Then the following are equivalent for some $a \in E$.

(i) The map $b \mapsto g(a, b)$ is the zero map.

(ii) The map $b \mapsto g(b, a)$ is the zero map.

Proof. Use the ambient symmetry of g. ∎

This motivates the following definition.

Definition 1.106 (kernel)**.** Fix a module E over a ring R. Suppose that $g\colon E \times E \to R$ is symmetric, alternating, or Hermitian. Then the *kernel* of g is

$$\ker g \coloneqq \{a \in E : g(a, b) = g(b, a) = 0 \text{ for all } b \in E\}.$$

We say that g is *non-degenerate* if and only if $\ker g = 0$.

We remark that a non-degenerate bilinear form gives rise to an isomorphism $E \to E^\vee$ while a non-degenerate Hermitian form gives rise to an isomorphism $E \to \overline{E}^\vee$, where $\overline{E}^\vee$ denotes the conjugate dual.

We will decompose our quadratic forms into direct sums. The concrete way to do this is via orthogonal decompositions.

Definition 1.107 (orthogonal)**.** Fix a module E over a ring R. Suppose that $g\colon E \times E \to R$ is symmetric, alternating, or Hermitian. Then two $a, b \in E$ are *orthogonal*, written $a \perp b$ if and only if $g(a, b) = 0$. Two subspaces $F, G \subseteq E$ are *orthogonal* if and only if $a \perp b$ for all $a \in F$ and $b \in G$. In this last situation, we say that E is an orthogonal direct sum $F \oplus F'$ if and only if we also have $F + F' = E$.

Definition 1.108 (orthogonal basis)**.** Fix a free module E of finite rank over a ring R. Suppose that $g\colon E \times E \to R$ is symmetric, alternating, or Hermitian. An *orthogonal basis* is a basis of E in which all elements are pairwise orthogonal.

Remark 1.109. For the professor, all bases come with an order.

Remark 1.110. If E is given an orthogonal basis $\{v_1, \dots, v_n\}$, then the spans of disjoint subsets produce orthogonal subspaces.

We are now ready to define a quadratic function.

Definition 1.111 (quadratic)**.** Fix modules E and F over a ring R. A function $f\colon E \to F$ is *quadratic* if and only if it takes the form

$$f(x) = g(x, x) + h(x)$$

where $g\colon E \times E \to F$ is R-bilinear and $h\colon E \to F$ is R-linear. We say further that f is *homogeneous quadratic* if $h = 0$. Lastly, a quadratic form is a homogeneous quadratic function with target R.

Remark 1.112. If F has no 2-torsion, then the decomposition of f into $g + h$ is unique. Indeed, one can compute that

$$2g(x, y) = f(x + y) - f(x) - f(y),$$

from which we can then read off h as $f - g$.

Remark 1.113. Suppose further that the multiplication-by-2 map $2\colon F \to F$ is an isomorphism. Then for any function $f\colon E \to F$, we find that $2f(x) - \frac{1}{2}f(2x)$ is $\mathbb{Z}$-bilinear; if further $f(2x) = 4f(x)$, then f is homogeneous quadratic. This can be checked by a direct computation.

Let's begin doing some decompositions.

Proposition 1.114. Fix a field k of characteristic not 2. If g is a symmetric bilinear form on a finite-dimensional vector space E over k, then E admits an orthogonal basis.

Proof. If g is zero, there is nothing to do. Then one can construct the basis inductively by choosing some $v \notin \ker g$ to start and then inductively passing to the orthogonal complement. For example, it is possible to do this using the Gram–Schmidt process. A careful proof using the Gram–Schmidt process must deal with $\ker g$. In brief, one can decompose E into a direct sum of $\ker g$ with a subspace $E' \subseteq E$ on which g is non-degenerate. ∎

Over ordered fields, one can add some positivity.

Definition 1.115 (ordered field)**.** An *ordered field* k is a field k together with a collection of positive elements $P \subseteq k$ satisfying the following.

- For each $x \in k$, exactly one of $x \in P$, $x = 0$, or $-x \in P$ is true.
- For each $x, y \in P$, one has $x + y \in P$ and $xy \in P$.

Theorem 1.116 (Sylvester)**.** Fix an ordered field k, and let g be a non-degenerate symmetric bilinear form on a vector space E over k. Then there is $r \geq 0$ such that any orthogonal basis S of E has

$$r = \#\{v \in S : g(v, v) > 0\}.$$

Proof. Choose two orthogonal bases $\{v_1, \dots, v_n\}$ and $\{w_1, \dots, w_n\}$, and set $a_i \coloneqq g(v_i, v_i)$ and $b_i \coloneqq g(w_i, w_i)$ for each i. By reordering, we may assume that

$$\{i : a_i > 0\} = \{1, 2, \dots, r\} \qquad \text{and} \qquad \{i : b_i > 0\} = \{1, 2, \dots, s\}$$

for some $r, s \geq 0$. We would like to show that $r = s$. By symmetry, it's enough to check that $r \leq s$, which is equivalent to checking that $r + (n - s) \leq n$, where $n = \dim E$.

For this, we check that the vectors

$$\{v_1, \dots, v_r\} \sqcup \{w_{s+1}, \dots, w_n\}$$

are linearly independent. Well, suppose that we have some linear relation

$$\sum_{i=1}^{r} x_i v_i = \sum_{j=s+1}^{n} y_j w_j.$$

Taking the norm on both sides, we see that

$$\sum_{i=1}^{r} x_i^2 a_i \geq 0 \geq \sum_{j=s+1}^{n} y_j^2 b_j,$$

with equality in the middle holding if and only if $x_i = 0$ and $y_j = 0$ for all i and j. ∎

Corollary 1.117. Fix an ordered field k such that the positive elements are squares. For any non-degenerate symmetric bilinear form g on a vector space E over k, there is an orthonormal basis $\{v_1, \dots, v_n\}$ with some $r \geq 0$ such that

$$\begin{cases} g(v_i, v_i) = +1 & \text{if } i \leq r, \\ g(v_i, v_i) = -1 & \text{if } i > r. \end{cases}$$

Proof. Simply rescale the given basis by some squares. ∎

These sorts of results motivate us to define some nice bases.

Definition 1.118 (positive-definite)**.** Fix an ordered field k and a non-degenreate symmetric bilinear form g on a vector space E over k.

- Then g is *positive-definite* if and only if $g(v, v) > 0$ for all $v \in E$.
- Then g is *negative-definite* if and only if $g(v, v) < 0$ for all $v \in E$.

Remark 1.119. Theorem 1.116 allows us to decompose any E into an orthogonal direct sum E_+ and E_- so that g restricted to E_+ or E_- is positive-definite or negative-definite, respectively.

BIBLIOGRAPHY

[Lan02] Serge Lang. *Algebra / Serge Lang.* eng. Revised Third Edition. Graduate texts in mathematics ; 211. New York: Springer, 2002. ISBN: 038795385X.

[Shu16] Neal Shusterman. *Scythe*. Arc of a Scythe. Simon & Schuster, 2016.

List of Definitions