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 January 30

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.

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