

Commutative Algebra with a View Toward Algebraic Geometry

David Eisenbud

May 6, 2021

Contents

1	Elementary Definitions	1
1.1	Rings and Ideals	1
1.2	Unique Factorization	2
1.3	Modules	2
2	Roots of Commutative Algebra	2
2.1	The Basis Theorem	2
2.2	Graded Rings	4
2.3	Algebra and Geometry: The Nullstellensatz	5
2.4	Hilbert Functions and Polynomials	7
2.5	Exercise	8
3	Localization	9
3.1	Fractions	9

1 Elementary Definitions

1.1 Rings and Ideals

If R is a commutative ring, then a **commutative algebra** over R (or **commutative R -algebra**) is a commutative ring S together with a homomorphism $\alpha : R \rightarrow S$ of rings. We usually suppress the homomorphism α from the notation, and write rs in place of $\alpha(r)s$. Any ring is a \mathbb{Z} -ring in a unique way. Polynomial ring $S = R[x_1, \dots, x_n]$ is an R -algebra

1.2 Unique Factorization

1.3 Modules

If M and N are R -modules, then the **direct sum** of M and N is the module $M \oplus N = \{(m, n) \mid m \in M, n \in N\}$ with the module structure $r(m, n) = (rm, rn)$. There are natural inclusion and projections maps $M \subset M \oplus N$ and $M \oplus N \rightarrow M$ given by $m \mapsto (m, 0)$ and $(m, n) \mapsto m$. These maps are enough to identify a direct sum: That is M is a **direct summand** of a module P iff there are homomorphisms $\alpha : M \rightarrow P$ and $\sigma : P \rightarrow M$ whose composition $\sigma\alpha$ is the identity map of M ; then $P \cong M \oplus (\ker \sigma)$

2 Roots of Commutative Algebra

2.1 The Basis Theorem

A ring R is **Noetherian** if every ideal of R is finitely generated, which is equivalent to the **ascending chain condition on ideals of R** , which says that every strictly ascending chain of ideals must terminate

Theorem 2.1 (Hilbert Basis Theorem). *If a ring R is Noetherian, then the polynomial ring $R[x]$ is Noetherian*

If $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in R[x]$ with $a_n \neq 0$, we define the **initial term** of f to be $a_n x^n$, and **initial coefficient** of f to be a_n

Proof. Let $I \subset R[x]$ be an ideal; we shall show that I is finitely generated. Choose a sequence of elements $f_1, f_2, \dots \in I$ as follows: Let f_1 be a nonzero element of least degree in I . For $i \geq 1$, if $(f_1, \dots, f_i) \neq I$, then choose f_{i+1} to be an element of least degree among $I \setminus (f_1, \dots, f_i)$. If $(f_1, \dots, f_i) = I$, stop choosing.

Let a_j be the initial coefficient of f_j . Since R is Noetherian, the ideal $J = (a_1, a_2, \dots)$ of all the a_i produced is finitely generated. We may choose a set of generators from among the a_i themselves. Let m be the first integer s.t. a_1, \dots, a_m generate J . We claim that $I = (f_1, \dots, f_m)$

In the contrary case, our process chose an element f_{m+1} . We may write $a_{m+1} = \sum_{j=1}^m u_j a_j$, for some $u_j \in R$. Since the degree of f_{m+1} is at least as great as the degree of any of the f_1, \dots, f_m , we may define a polynomial $g \in R$

having the same degree and initial term as f_{m+1} by the formula

$$g = \sum_{j=1}^m u_j f_j x^{\deg f_{m+1} - \deg f_j} \in (f_1, \dots, f_m)$$

The difference $f_{m+1} - g \in I$ but not in (f_1, \dots, f_m) , and has degree strictly less than the degree of f_{m+1} . This contradicts the choice of f_{m+1} as having minimal degree \square

Corollary 2.2. *Any homomorphic image of a Noetherian ring is Noetherian. Furthermore, if R_0 is a Noetherian ring, and R is a finitely generated algebra over R_0 , then R is Noetherian*

Proof. Given an ideal I in R/J , with R Noetherian, the preimage of I in R is finitely generated, and the images of its generators generate I

Since R is a finitely generated algebra over R_0 , R is a homomorphic image of $S := R_0[x_1, \dots, x_r]$ for some r . Using Theorem 2.1 and induction on r , we see that S is Noetherian. Since a homomorphic image of a Noetherian ring is Noetherian, we are done. \square

An R -module M is **Noetherian** if every submodule of N is finitely generated

Proposition 2.3. *If R is a Noetherian ring and M is a finitely generated R -module, then M is Noetherian*

Proof. Suppose that M is generated by f_1, \dots, f_t , and let N be a submodule. We shall show that N is finitely generated by induction on t .

If $t = 1$, then the map $R \rightarrow M$ sending 1 to f_1 is surjective. The preimage of N is an ideal, which is finitely generated since R is Noetherian. The images of its generators generate N

Now suppose $t > 1$. The image \bar{N} of N in M/Rf_1 is finitely generated by induction. Let g_1, \dots, g_s be elements of N whose images generate \bar{N} . Since $Rf_1 \subset M$ is generated by one element, its submodule $N \cap Rf_1$ is finitely generated, say by h_1, \dots, h_r ¹.

We shall show that the elements h_1, \dots, h_r and g_1, \dots, g_s together generate N \square

¹StackExchange Let $R_N = \{r \in R \mid rf_1 \in N\}$. Then R_N is an ideal of R . Since R is Noetherian, the ideal R_N of R is finitely generated.

2.2 Graded Rings

A **graded ring** is a ring R together with a direct sum decomposition

$$R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots \quad \text{as abelian groups}$$

s.t.

$$R_i R_j \subset R_{i+j} \quad \text{for } i, j \geq 0$$

A **homogeneous element** of R is an element of one of the groups R_i , and a **homogeneous ideal** of R is an ideal that is generated by homogeneous elements. If $f \in R$, there is a unique expression for f of the form

$$f = f_0 + f_1 + \cdots \quad \text{with } f_i \in R_i \text{ and } f_j = 0 \text{ for } j \gg 0$$

the f_i are called the **homogeneous components** of f .

The ideal consisting of all elements of degree greater than 0 is called the **irrelevant ideal** written as R_+

The simplest example of a graded ring is the ring of polynomials $S = k[x_1, \dots, x_r]$ **graded by degree**: that is, with grading

$$S = S_0 \oplus S_1 \oplus \cdots$$

where S_d is the vector space of homogeneous polynomials (also called forms) of degree d

Definition 2.4. A polynomial is **homogeneous of degree d** if its a linear combination of monomials of degree d

A monomial in n variables is $x_1^{i_1} \dots x_n^{i_n}$, its **degree** is $i_1 + \cdots + i_n$

The space of all homogeneous polynomials of a given degree d in n variables is *finite dimensional*

Proposition 2.5. The number of monomials of degree d in 3 variables is C_{d+2}^2 . And for n variables, the number is C_{d+n-1}^{n-1}

Suppose that I is a homogeneous ideal of a graded ring R , and I is generated by homogeneous elements f_1, \dots, f_s . If $f \in I$ is any homogeneous elements, then we can write $f = \sum g_i f_i$ with each g_i homogeneous of degree $\deg g_i = \deg f - \deg f_i$

2.3 Algebra and Geometry: The Nullstellensatz

Gauss' **fundamental theorem of algebra** establishes the basic link between algebra and geometry: It says that a polynomial in one variable over \mathbb{C} , an algebra object, is determined up to a scalar factor by the set of its roots (with multiplicities), a geometric object

A polynomial $f \in k[x_1, \dots, x_n]$ with coefficients in a field k defines a function $f : k^n \rightarrow k$; the value of f at a point $(a_1, \dots, a_n) \in k^n$ is obtained by substituting the a_i for the x_i in f . The function defined by f is called a **polynomial function** on the n -dimensional vector space k^n over k , with values in k . If k is infinite, then no polynomial function other than 0 can vanish identically (always 0) on k^n . (The case of one variable is the statement that a polynomial in one variable can have only finitely many roots, and follows from Euclid's algorithm for division. In the general case we think of a nonzero polynomial $f(x_1, \dots, x_n)$ in n variables as a polynomial in $n-1$ variables with coefficients that are polynomials in one variable)

It follows that if k is infinite, then distinct polynomials define distinct functions. Thus we may regard the polynomial ring $k[x_1, \dots, x_n]$ as the ring of polynomial functions on k^n . Viewed with its ring of polynomial functions, k^n is usually called **affine n -space** over k , written $\mathbf{A}^n(k)$ or simply \mathbf{A}^n

Given a subset $I \subset k[x_1, \dots, x_n]$, we define a corresponding **algebraic subset** of k^n to be

$$Z(I) = \{(a_1, \dots, a_n) \in k^n \mid f(a_1, \dots, a_n) = 0 \text{ for all } f \in I\}$$

Such algebraic sets are sometimes called an **affine algebraic sets**

If $X = Z(I)$ is an algebraic set, then an **algebraic subset** $Y \subset X$ is a set of the form $Y = Z(J)$ that happens to be contained in X . An algebraic set is called **irreducible** if it is not the union of two smaller algebraic subsets. Irreducible algebraic sets are called **algebraic varieties**

If $k = \mathbb{R}$ or $k = \mathbb{C}$, then k^n is naturally a topological space, and an algebraic subset $X \subset \mathbf{A}^n$ inherits the subspace topology, called the **classical topology**. But there is another, coarser topology on X that is defined over any field. Polynomial functions on X will play the role of continuous functions, even when the fields we are working over have no topology, and by analogy with the continuous case it is natural to think of an algebraic subset Y as a **closed** subset of X . Since we obviously have $\bigcap_i Z(J_i) = Z(\bigcup_i J_i)$. Furthermore, if we define $\prod_{i=1}^n J_i$ to be the set consisting of all products of one function from each J_i , then $\bigcup_{i=1}^n Z(J_i) = Z(\prod_{i=1}^n J_i)$. Thus we may

define a topology on X by taking the closed sets to be the algebraic subsets of X . This topology is called the **Zariski topology**.

Given any set $X \subset k^n$, we define

$$I(X) = \{f \in k[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in X\}$$

It is clear that $I(X)$ is an ideal. A **polynomial function** (or **regular function**) on X is the restriction of a polynomial function on k^n on X . Identifying two polynomial functions if they agree at all the points of X , we get the **coordinate ring** $A(X)$ of X . Clearly we have $A(X) = k[x_1, \dots, x_n]/I(X)$

Not every homomorphic image $A = k[x_1, \dots, x_n]/I$ could be the coordinate ring of a set. For suppose an element $f \in A$ satisfies $f^n = 0$. If f were a function on some set X , we would have $0 = f^d(p) = f(p)^d$; that is, $f(p)$ is **nilpotent** for all $p \in X$. But the values of f are elements of k , a field; so they are all 0, and f itself is the zero element of $A(X)$. In general, a ring is said to be **reduced** if its only nilpotent element is 0; we have just shown that $A(X)$ is reduced

If R is a ring and $I \subset R$ is an ideal, then the set

$$\text{rad } I := \{f \in R \mid f^m \in I \text{ for some integer } m\}$$

is an ideal. It is called the **radical** of I . An ideal I is called a **radical ideal** if $I = \text{rad } I$. It follows that R/I is a reduced ring iff I is a radical ideal. Thus, the ideals $I(X)$ are all radical ideals

Not even every radical ideal in S can occur as $I(X)$: For example, the ideal $I = (x^2 + 1) \subset \mathbb{R}[x]$ is radical because $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ is reduced. But $Z(I) = \emptyset$, so I is not of the form $I(X)$ for any X . If k is algebraically closed, the situation is better. For example, every polynomial in one variable is a product of linear factors, and a polynomial $f \in k[x]$ generates a radical ideal iff it has no multiple roots. In this case if X is the set of roots of f , then $I(X) = (f)$. Hilbert's Nullstellensatz extends this to polynomial rings with many variables

Theorem 2.6 (Nullstellensatz). *Let k be an algebraically closed field. If $I \subset k[x_1, \dots, x_n]$ is an ideal, then*

$$I(Z(I)) = \text{rad } I$$

Thus, the correspondences $I \mapsto Z(I)$ and $X \mapsto I(X)$ induce a bijection between the collection of algebraic subsets of $A_k^n = k^n$ and radical ideals of $k[x_1, \dots, x_n]$

Corollary 2.7. *A system of polynomial equations*

$$\begin{aligned} f_1(x_1, \dots, x_n) &= 0 \\ &\dots \\ f_m(x_1, \dots, x_n) &= 0 \end{aligned}$$

over an algebraically closed field k has no solution in k^n iff 1 can be expressed as a linear combination

$$1 = \sum p_i f_i$$

with polynomial coefficients p_i

Proof. By the Nullstellensatz, if $Z(f_1, \dots, f_m) = \emptyset$, then 1 is in the radical of (f_1, \dots, f_m) \square

Corollary 2.8. *If k is an algebraically closed field and A is a k -algebra, then $A = A(X)$ for some algebraic set X iff A is reduced and finitely generated as a k -algebra*

Proof. If $A = A(X)$ for some $X \subset k^n$, then $A = k[x_1, \dots, x_n]/I(X)$ is generated as a k -algebra by x_1, \dots, x_n . Since $I(X)$ is radical, A is reduced

Conversely, if A is a finitely generated k -algebra, then after choosing generators we may write $A = k[x_1, \dots, x_n]/I$ for some ideal I . Since A is reduced, I is radical. Thus $I = I(Z(I))$ by the Nullstellensatz, and we may take $X = Z(I)$ \square

2.4 Hilbert Functions and Polynomials

Definition 2.9. If $R = R_0 \oplus R_1 \oplus \dots$ is a graded ring, then a **graded module** over R is a module M with a decomposition

$$M = \bigoplus_{i=-\infty}^{+\infty} M_i \quad \text{as abelian groups}$$

s.t. $R_i M_j \subset M_{i+j}$ for all i, j

Definition 2.10. Let M be a finitely generated graded module over $k[x_1, \dots, x_r]$, with grading by degree. The numerical function

$$H_M(s) := \dim_k M_s$$

is called the **Hilbert function of M** (These dimensions are all finite; if M_s were not finite dimensional, then the submodule $\bigoplus_s M_i$ would not be finitely generated, contradicting Proposition 2.3)

Theorem 2.11 (Hilbert). *If M is a finitely generated graded module over $k[x_1, \dots, x_r]$, then $H_M(s)$ agrees, for large s , with a polynomial of degree $\leq r - 1$*

Definition 2.12. This polynomial, denoted $P_M(s)$, is called the **Hilbert polynomial of M**

We define $M(d)$ to be this graded module; more formally, $M(d)$ is isomorphic to M as a module and has grading defined by

$$M(d)_e = M_{d+e}$$

$M(d)$ is sometimes referred to as the **d th twist of M** .

Lemma 2.13. *Let $H(s) \in \mathbb{Z}$ be defined for all for all natural numbers s . If the "first difference" $H'(s) = H(s) - H(s - 1)$ agrees with a polynomial of degree $\leq n - 1$ having rational coefficients for $s \geq s_0$, then $H(s)$ agrees with a polynomial of degree $\leq n$ having rational coefficients for all $s \geq s_0$*

Proof. Suppose that $Q(s)$ is a polynomial of degree $\leq n - 1$ with rational coefficients s.t. $H'(s) = Q(s)$ for $s \geq s_0$. For any integer s set $P(s) = H(s_0) + \sum_{t=s_0+1}^s Q(t)$, where the sum is taken over all integers between $s_0 + 1$ and s whether $s \geq s_0 + 1$ or $s \leq s_0 + 1$. For $s \geq s_0$ we have $P(s) = H(s)$. For all s we have $P(s) - P(s - 1) = Q(s)$. It follows that $P(s)$ is a polynomial of degree $\leq n$ with rational coefficients \square

Proof of Theorem 2.11. We do induction on r . If $r = 0$, then M is simply a finite-dimensional graded vector space. In this case $H_M(s) = 0$ \square

2.5 Exercise

Exercise 2.5.1. Prove that the following conditions on a module M over a commutative ring are equivalent. The case $M = R$ is the case of ideals

1. M is Noetherian
2. Every ascending chain of submodules of M terminates
3. Every set of submodules of M contains elements maximal under inclusion
4. Given any sequence of elements $f_1, f_2, \dots \in M$, there is a number m s.t. for each $n > m$ there is an expression $f_n = \sum_{i=1}^m a_i f_i$ with $a_i \in R$

Proof. $1 \rightarrow 2$ obvious.

$2 \rightarrow 3$ zorn's lemma

$2 \rightarrow 4$. \square

3 Localization

A **local ring** is a ring with just one maximal ideal.

3.1 Fractions

Given a ring R , an R -module M , and a multiplicatively closed subset $U \subset R$, we define the **localization of M at U** , written as $M[U^{-1}]$ or $U^{-1}M$, to be the set of equivalence classes of pair (m, u) with $m \in M$ and $u \in U$ with equivalence relation $(m, u) \sim (m', u')$ if there is an element $v \in U$ s.t. $v(u'm - um') = 0$ in M . The equivalence class of (m, u) is denoted m/u . We make $M[U^{-1}]$ into an R -module by defining

$$\begin{aligned} m/u + m'/u' &= (u'm + um')/uu' \\ r(m/u) &= (rm)/u \end{aligned}$$

for $m, m' \in M, u, u' \in U, r \in R$. Note that $u'm/u'u = m/u$. The localization comes equipped with a natural map of R -modules $M \rightarrow M[U^{-1}]$ carrying m to $m/1$

It is convenient to extend the notation a little further: If $U \subset R$ is an arbitrary set, and $\bar{U} \subset R$ is the multiplicatively closed set of all products of elements in U , then we set $M[U^{-1}] := M[\bar{U}^{-1}]$

If we apply the definition in the case $M = R$, the resulting localization is a ring, with multiplication defined by

$$(r/u)(r'/u') = rr'/uu'$$

and in fact $M[U^{-1}]$ is an $R[U^{-1}]$ -module with action defined by

$$(r/u)(m/u') = rm/uu' \quad \text{for } r \in R, m \in M, u, u' \in U$$

Proposition 3.1. *Let U be a multiplicatively closed set of R , and let M be an R -module. An element $m \in M$ goes to 0 in $M[U^{-1}]$ iff m is annihilated by an element $u \in U$. In particular, if M is finitely generated, then $M[U^{-1}] = 0$ iff M is annihilated by an element of U*

Proof. If generators $m_i \in M$ are annihilated by elements $u_i \in U$, then M is annihilated by the product of the u_i □

The quotient field of an integral domain R , which we shall denote by $K(R)$, is the localization $R[U^{-1}]$ where $U = R - \{0\}$. For an arbitrary ring

R , take U to be the set of nonzerodivisors of R , and define the **total quotient ring** $K(R)$ of R by $K(R) := R[U^{-1}]$. By Proposition 3.1 $K(R)$ is the "biggest" localization of R s.t. the natural map $R \rightarrow R[U^{-1}]$ is an injection

An ideal $P \subset R$ is prime iff $R - P$ is a multiplicatively closed set. If P is a prime ideal and $U = R - P$, then we write R_P for $R[U^{-1}]$. Similarly, for any R -module M , we write M_P for $M[U^{-1}]$. We write $\kappa(P)$ for the ring R_P/P_P , the **residue class field of R at P** .