Chapter 2 AFFINE ALGEBRAIC GEOMETRY

2.1 Ideals, review

idealreview

Let R be a (commutative) ring. An *ideal* I of R is a nonempty subset that is closed under linear combinations: If $a_1, ..., a_n$ are in I and $r_1, ..., r_n$ are in R, then $r_1a_1 + \cdots + r_na_n$ is in I.

The *zero ideal* of R consists of the zero element alone, and the *unit ideal* is the whole ring R. An ideal I is the unit ideal if and only if it contains the element 1 of the ring, and this is true if and only if it contains a *unit*, an invertible element of R. A field is a ring that contains precisely two ideals, the zero ideal and the unit ideal.

Let $z_1, ..., z_k$ be elements of R. The ideal I *generated by* $z_1, ..., z_k$ consists of all combinations $r_1z_1 + \cdots + r_kz_k$ with coefficients r_i in R. Other notations for this ideal are $(z_1, ..., z_k)$ and (z). The Hilbert Basis Theorem, which we review in Section 2.4, asserts that every ideal of the polynomial algebra $\mathbb{C}[x_1, ..., x_n]$ can be generated by some finite set.

Let $A \subset B$ be rings. The *extension* of an ideal I of A is the ideal IB of B generated by I. Its elements are finite sums $\sum_i z_ib_i$ with z_i in I and b_i in B. The *contraction* of an ideal J of B is the ideal $J \cap A$ of A.

If I and J are ideals of R, the *product ideal* IJ is the ideal whose elements are finite sums of products $\sum a_\nu b_\nu$ with a_ν in I and b_ν in J.

A *prime ideal* of R is an ideal P such that the quotient ring R/P is a *domain*, a nonzero ring with no zero divisors. The unit ideal is not a prime ideal.

defprime **2.1.1. Proposition.** *Let P be an ideal, of a ring R, not the unit ideal. The following conditions on P are equivalent.*
(i) *P is a prime ideal.*
(ii) *If a and b are elements of R and if $ab \in P$, then $a \in P$ or $b \in P$.*
(iii) *If A and B are ideals of R, and if $AB \subset P$, then $A \subset P$ or $B \subset P$.*
(iv) *If A and B are ideals of R that contain P, and if $AB \subset P$, then $A = P$ or $B = P$.* □

Because $AB \subset A \cap B$, one may replace AB by $A \cap B$ in parts **(iii)** and **(iv)**.

Two ideals I and J of a R are *comaximal* if $I + J = R$.

comax **2.1.2. Chinese Remainder Theorem.** *Let I and J be comaximal ideals of R.*
(i) *The product ideal IJ is equal to the intersection $I \cap J$.*
(ii) *The map $R \to R/I \times R/J$ that sends an element a of R to its pair of residues is surjective. Its kernel is $I \cap J$.* □

affvar

2.2 Affine Varieties

As before, the affine space $\mathbb{A}^n$ is the space of n-tuples of complex numbers.

We consider finite sets of polynomial equations in n variables $x_1, \dots, x_n$:

equations (2.2.1) $$f_1 = 0\,,\ \dots,\ f_k = 0.$$

If it seems unlikely to cause confusion, we may abbreviate the notation for a finite indexed set such as $x_1, \dots, x_n$ by the single letter x. The polynomial algebra may be denoted in abbreviated form by $\mathbb{C}[x]$, and the system of equations by $f = 0$.

- The *affine scheme* $V(f)$ is the subset of affine space $\mathbb{A}^n$ of points $(a_1, \dots, a_n)$ at which the polynomials f_i vanish, the points that solve the equations (2.2.1). We refer to those points as the *zeros* of the polynomials f. The affine schemes are the closed sets in the Zariski topology of $\mathbb{A}^n$.

We use analogous notation for infinite sets. If S is any set of polynomials, $V(S)$ denotes the set of points of affine space at which all elements of S vanish.

If I is the ideal generated by some polynomials $f_1, ..., .f_k$, the affine scheme $V(f)$ is equal to $V(I)$. All elements of the ideal I vanish there.

An *algebra* A is a ring that contains the field $\mathbb{C}$ of complex numbers as subring. A *homomorphism of algebras* is a ring homomorphism that restricts to the identity on $\mathbb{C}$.

- The *coordinate algebra* $A(f)$ of the affine scheme $V(f)$ is the quotient $\mathbb{C}[x]/(f)$ of the polynomial algebra.

When properly defined, an affine scheme remembers its coordinate algebra as well as its point set, so our definition of affine scheme is imprecise. Let's not worry about this here.

- An *affine variety* is the affine scheme $V(P)$ defined by a prime ideal P.

Thus the coordinate algebra $\mathbb{C}[x]/P$ of the affine variety $V(P)$ is a domain. The coordinate algebra of affine space $\mathbb{A}^n$ itself is the polynomial algebra $\mathbb{C}[x]$. Geometric properties of an affine variety are reflected in algebraic properties of its coordinate algebra, and conversely. Algebraic geometry studies this relationship.

A few examples of varieties:

- The point $p = (a_1, \dots, a_n)$ of $\mathbb{A}^n$ is the affine variety defined by the n equations $x_i - a_i = 0$, $i = 1, \dots, n$. It is a variety because the polynomials $x_i - a_i$ generate a maximal ideal of the polynomial algebra, and a maximal ideal is a prime ideal.

The maximal ideal that corresponds to a point p will be denoted by $\mathfrak{m}_p$. It is the kernel of the substitution homomorphism $\mathbb{C}[x] \xrightarrow{\pi_p} \mathbb{C}$ that sends a polynomial $g(x)$ to $g(p) = g(a_1, ..., a_n)$.

The coordinate algebra $\mathbb{C}[x]/\mathfrak{m}_p$ of the point p is the *residue field* at p. It will be denoted by $k(p)$. As a field, $k(p)$ is isomorphic to the field $\mathbb{C}$ of complex numbers, but it has the additional structure that comes from its description as a particular quotient of the polynomial ring.

- The varieties in the affine line $\mathbb{A}^1$ are the points of $\mathbb{A}^1$, and the line $\mathbb{A}^1$ itself.

- The set X of solutions of a single irreducible polynomial equation $f_1(x_1, ..., x_n) = 0$ is an *affine hypersurface*. An affine hypersurface is a variety because an irreducible element generates a prime ideal in the unique factorization domain $\mathbb{C}[x]$.

The *special linear group* SL_2, the group of complex 2×2 matrices with determinant 1, is an affine hypersurface, the locus of zeros of the irreducible polynomial $xw - yz - 1$ in $\mathbb{A}^4$.

- A hypersurface in the affine plane $\mathbb{A}^2$ is an *affine plane curve*.

As before, a *line* in the affine plane is a locus defined by a linear equation $ax + by = c$. Its coordinate algebra is isomorphic to a polynomial ring in one variable.

- Let $p = (a_1, \dots, a_n)$ and $q = (b_1, \dots, b_n)$ be distinct points of $\mathbb{A}^n$. The *point pair* $\{p, q\}$ is the affine scheme defined by the system of n^2 equations $(x_i - a_i)(x_j - b_j) = 0$ with $1 \le i, j \le n$. A point pair isn't called a variety because the ideal generated by the polynomials $(x_i - a_i)(x_j - b_j)$ isn't a prime ideal, and its coordinate algebra isn't a domain.

pointpair **2.2.2. Proposition.** *The coordinate algebra of a point pair is isomorphic to the product algebra* $\mathbb{C} \times \mathbb{C}$.

proof. This follows from the Chinese Remainder Theorem. We inspect the homomorphism

$$\mathbb{C}[x] \xrightarrow{\varphi} k(p) \times k(q) \approx \mathbb{C} \times \mathbb{C}$$

that sends f to the pair of values $(f(p), f(q))$. Its kernel is the intersection $\mathfrak{m}_p \cap \mathfrak{m}_q$ of the maximal ideals $\mathfrak{m}_p$ and $\mathfrak{m}_q$. Distinct maximal ideals are comaximal, so $\mathfrak{m}_p \cap \mathfrak{m}_q = \mathfrak{m}_p \mathfrak{m}_q$, and φ is surjective. Since the elements $x_i - a_i$ generate $\mathfrak{m}_p$ and $x_j - b_j$ generate $\mathfrak{m}_q$, their products generate the product ideal, which is the kernel of φ. So the coordinate algebra of the point pair, the quotient of the polynomial algebra by $\mathfrak{m}_p \mathfrak{m}_q$, is isomorphic to the image $k(x) \times k(y)$. □

Here is another consequence of the Chinese Remainder Theorem:

findimalg **2.2.3. Proposition.** *An algebra A that is a complex vector space of dimension d has at most d maximal ideals.*

proof. We show that if $\mathfrak{m}_1, ..., \mathfrak{m}_n$ are maximal ideals of A and $k_i = A/\mathfrak{m}_i$, the homomorphism $A \to k_1 \times \cdots \times k_n$ is surjective. Therefore $n \le d$. By induction on n, we may assume that the map $A \to k_1 \times \cdots \times k_{n-1}$ is surjective, and that its kernel is the product ideal $J = \mathfrak{m}_1 \cdots \mathfrak{m}_{n-1}$. So $k_1 \times \cdots \times k_{n-1} \approx A/J$. Because $\mathfrak{m}_n$ is a prime ideal that doesn't contain any of the ideals $\mathfrak{m}_i$ for $i < n$, $\mathfrak{m}_n$ doesn't contain J. Since $\mathfrak{m}_1$ is a maximal ideal, $\mathfrak{m}_1$ and J are comaximal, the map $A \to A/J \times k_n$ is surjective, and its kernel is $\mathfrak{m}_1 \cdots \mathfrak{m}_n$. □

corrthmsec ## 2.3 The Correspondence Theorem

corrthm **2.3.1. Correspondence Theorem.** *Let $R \xrightarrow{\varphi} S$ be a surjective ring homomorphism with kernel K. For example, φ might be the canonical map from R to R/K. There is a bijective correspondence*

$$\{\textit{ideals of } R \textit{ that contain } K\} \quad \longleftrightarrow \quad \{\textit{ideals of } S\}$$

This correspondence associates an ideal I of R that contains K with its image $\varphi(I)$ in S and it associates an ideal J of S with its inverse image $\varphi^{-1}(J)$ in R.

If an ideal I of R that contains K corresponds to the ideal J of S, then φ induces an isomorphism of quotient rings $R/I \to S/J$. So if one of the ideals, I or J, is prime or maximal, they both are. □

mapprop **2.3.2. Theorem. Mapping Property of quotient rings.** *Let R and S be rings, let K be an ideal of a ring R, and let $R \xrightarrow{\pi} \overline{R}$ denote the canonical map from R to the quotient ring $\overline{R} = R/K$. Homomorphisms $R \xrightarrow{\varphi} S$ whose kernels contain K correspond bijectively to homomorphisms $\overline{R} \xrightarrow{\overline{\varphi}} S$, by $\varphi = \overline{\varphi} \circ \pi$.*

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle\pi}\downarrow & & \| \\ \overline{R} & \xrightarrow{\overline{\varphi}} & S \end{array}$$

□

commutative-diagram **2.3.3. Note.** In the above diagram, the maps $\overline{\varphi} \circ \pi$ and φ are equal. This is referred to by saying that the diagram is *commutative*. A *commutative diagram* is one in which the maps that can be obtained by composing the arrows shown depend only on the domain and range. In these notes, all diagrams of maps are commutative, and we won't mention commutativity again. □

hilb

2.4 Using the Hilbert Basis Theorem

A module M over a ring R is a *finite module* if it is generated by a finite set $\{m_1, ..., m_k\}$ of elements – if every element of M can be obtained as a combination $r_1m_1 + \cdots + r_km_k$ with coefficients r_i in R.

An ideal I of a ring R is *finitely generated* if it can be generated by a finite set of elements, which means that, when regarded as an R-module, I is a finite module. A ring is *noetherian* if all of its ideals are finitely generated. The ring of integers and fields are examples of notherian rings.

basisthm **2.4.1. Hilbert Basis Theorem.** *If R is a noetherian ring, the polynomial ring $R[x_1, ..., x_n]$ in finitely many variables over R is noetherian.* □

A set of elements $\{\alpha_1, ..., \alpha_n\}$ *generates* an algebra A if every element of A can be expressed, usually not uniquely, as a *polynomial* in these elements, with complex coefficients. Or, $\alpha_1, ..., \alpha_n$ generate A if the homomorphism $\mathbb{C}[x_1, ..., x_n] \to A$ that sends $x_i \rightsquigarrow \alpha_i$ is surjective. If so, then A will be isomorphic to the quotient $\mathbb{C}[x]/I$, where I is the kernel of that homomorphism. A *finite-type algebra* is one that is generated by a finite set of elements.

qnoeth **2.4.2. Lemma.** *The quotient R/K of a noetherian ring R modulo an ideal K is noetherian.*

proof. If an ideal J of R/K is the image of an ideal I of R, the images of a finite set of generators for I will generate J. □

ftypenoeth **2.4.3. Corollary.** *Every finite-type algebra is noetherian.* □

If (f) is the ideal generated by some polynomials $f_1, ..., f_k$, an isomorphism $\mathbb{C}[x]/(f) \approx A$ is called a *presentation* of the algebra A. Working with a finite-type algebra without a chosen presentation is analogous to working with a vector space without a chosen basis. One can choose a presentation when needed. However, it is often difficult to work explicitly with the quotient modulo an ideal.

Ralgebra **2.4.4. Note.** If $R \to A$ is any ring homomorphism, the ring A may be called an *R-algebra*. A *finite-type* R-algebra is one that is generated, as R-algebra, by a finite set of elements, which means that A is isomorphic to a quotient of a polynomial algebra $R[x]$ in finitely many variables. The Hilbert Basis Theorem implies that, when R is a noetherian ring, every finite-type R-algebra is noetherian. □

It is important not to confuse the concept of a finite-type algebra with that of a finite module. A finite-type R-algebra A is an algebra such that every element can be written as a polynomial in some finite set of elements $\alpha_1, ..., \alpha_k$, with coefficients in R. A finite R-module M is a module such that every element can be written as a linear combination of some finite set of elements $m_1, ..., m_k$, with coefficients in R. □

ascchcond **(2.4.5) the ascending chain condition**

The condition that a ring R be noetherian can be rewritten in several ways that we explain here.

Our convention is that if S and S' are sets, the notation $S \subset S'$ means that S is a subset of S', while $S < S'$ means that S is a subset of S' and not the whole set S'. A *proper* subset of a set S' is a nonempty subset different from S'. So S is a proper subset of S' if $\emptyset < S < S'$.

A sequence $S_1, S_2, ...$, finite or infinite, of subsets of a set Z forms an *increasing chain* if $S_n \subset S_{n+1}$ for all n, equality $S_n = S_{n+1}$ being permitted. If $S_n < S_{n+1}$ for all n, the chain is *strictly increasing*.

unionisideal **2.4.6. Lemma.** *Let $I_1 \subset I_2 \subset \cdots$ be an increasing chain of ideals of a ring R. The union $J = \bigcup I_\nu$ is an ideal.*

proof. We must show that if a and b are elements of J and r is an element of R, then $a + b$ and ra are in J. Since a is in J, it is in I_ν for some ν, and then, because the chain is increasing, a is in I_n for any $n \geq \nu$. Similarly, there is an index μ such that b is in I_n for $n \geq \mu$. If n is sufficiently large, I_n will contain both a and b. Then because I_n is an ideal, $a + b$ and ra will be in I_n, and therefore they will be in J. □

Let $\mathcal{S}$ be a set whose members are subsets of a set Z. A member M of $\mathcal{S}$ is *maximal* if there is no M' in $\mathcal{S}$ such that $M < M'$. For instance, the set of proper subsets of a set of five elements contains five maximal members, the subsets of order four. The set of finite subsets of the integers contains no maximal member. An ideal is a maximal ideal if it is a maximal member of the set of ideals different from the unit ideal.

noetherconds **2.4.7. Proposition.** *The following conditions on a ring R are equivalent:*

(i) *R is noetherian: Every ideal of R is finitely generated.*

(ii) *The ascending chain condition: Every strictly increasing chain $I_1 < I_2 < \cdots$ of ideals of R is finite.*

(iii) *Every nonempty set of ideals of R contains a maximal member.*

proof. **(i) $\Longrightarrow$ (ii)**: Suppose that R is noetherian, and that we are given an infinite increasing chain of ideals $I_1 \subset I_2 \subset \cdots$. We show that the sequence cannot be strictly increasing. Let J denote the ideal $\bigcup I_\nu$. Because R is noetherian, J is finitely generated, say $J = (\alpha_1, ..., \alpha_k)$. Because the chain is increasing, all of the elements α_i will be in I_n if n is large enough. Then $J \subset I_n \subset I_{n+1} \subset J$. All of these inclusions are equalities, and $I_n = I_{n+1}$.

(ii) $\Longrightarrow$ (iii): We assume **(ii)**. Let $\mathcal{S}$ be a nonempty set of ideals of R. Since it is nonempty, $\mathcal{S}$ contains an ideal, say I_1. If I_1 is a maximal member of $\mathcal{S}$, we stop. If not, there is a member I_2 of $\mathcal{S}$ with $I_1 < I_2$. Continuing in this way, we construct a strictly increasing chain of members of $\mathcal{S}$. This chain must be finite, and the ideal at the end will be a maximal member of $\mathcal{S}$.

(iii) $\Longrightarrow$ (i): We assume **(iii)**. Let J be an ideal of R, and let $\mathcal{S}$ be the set of finitely generated ideals that are contained in J. This set isn't empty because it contains the zero ideal. Therefore it contains a maximal member, say I, and I is generated by a finite set $\alpha_1, ..., \alpha_k$ of elements of J. Since I is maximal, it must be equal to J. Otherwise, adding an element of J not in I to the generating set $\alpha_1, ..., \alpha_k$ would produce a larger finitely generated ideal contained in J. So $I = J$, and therefore J is finitely generated. □

fingenlemma **2.4.8. Lemma.** *Let R be a ring and let $0 \to N_1 \xrightarrow{\alpha} N_2 \xrightarrow{\beta} N_3 \to 0$ be a short exact sequence of R-modules.*

(i) *If N_2 is finitely generated, so is N_3.*

(ii) *If N_1 and N_3 are finitely generated, so is N_2.*

proof. The fact that the map α is injective allows us to regard N_1 as a subset of N_2. Let $u = \{u_1, ..., u_\ell\}$ be a subset of N_1, let $v = \{v_1, ..., v_k\}$ be a subset of N_2, and let $w = \{w_1, ..., w_k\}$ denote the set of images $w_i = \beta(v_i)$ of v in N_3.

(i) Suppose that N_2 is finitely generated. So there is a finite set v that generates N_2. We show that the image set w generates N_3, and therefore that N_3 is finitely generated. Let x be an arbitrary element of N_3, and let y be an element of N_2 whose image $\beta(y)$ is x. Since v generates N_2, y can be written as a combination $\sum r_i v_i$. Applying β, $x = \beta(y) = \sum r_i \beta(v_i) = \sum r_i w_i$. So x is a combination of the elements w. Therefore w generates N_3.

(ii) Let u and v and w be as above. We show that if w generates N_3 and u generates N_1, then the union $u \cup v$ generates N_2. We start with an arbitrary element y of N_2. Its image x in N_3 will be a combination $x = \sum r_i w_i$ of w. We look at the corresponding combination $\sum r_i v_i$ of v, and we call it y'. The image of y' in N_3 is $\sum r_i w_i = x$, the same as the image of y. Therefore $z = y - y'$ is in the kernel of β, which is N_1. So we can write z as a combination, $\sum s_k u_k$ of the set u. Then $y = y' + z = \sum r_i v_i + \sum s_k u_k$. Therefore the set $u \cup v$ generates N_2. □

noetherian-module **2.4.9. Proposition.** *Let R be a noetherian ring, and let M be a finite R-module.*

(i) *Every submodule of M is a finite module.*

(ii) *The set of submodules of M satisfies the ascending chain condition.*

(iii) *Every nonempty set of submodules of M contains a maximal member.*

proof. **(i)** Let N be a submodule of M. Since M is finitely generated, there is a surjective map of modules $R^k \to M$. The Correspondence Theorem tells us that N is the image of a submodule N' of R^k. Lemma 2.4.8 shows that if N' is finitely generated, so is N. So it is enough to prove the assertion when M is the module R^k.

We use the short exact sequence $0 \to R \xrightarrow{i} R^k \xrightarrow{\pi} R^{k-1} \to 0$, where $i(a) = (0, ..., 0, a)$ and $\pi(a_1, ..., a_k) = (a_1, ..., a_{k-1})$. Let N be a submodule of R^k, let I be its inverse image $i^{-1}N$, which is a submodule, and therefore an ideal, of R, and let $\overline{N}$ be its image πN, a submodule of R^{k-1}. The sequence $0 \to I \to N \to \overline{N} \to 0$ is exact, I is finitely generated because R is noetherian, and induction on k allows us to assume that $\overline{N}$ is finitely generated. Lemma 2.4.8 tells us that N is finitely generated.

The proofs of **(ii)** and **(iii)** are analogous to the proofs of parts **(ii)** and **(iii)** of Proposition 2.4.7. □

All versions of the noetherian property are useful. Here is a simple application of the third one.

idealinmaximal **2.4.10. Corollary.** *Let R be a nonzero noetherian ring.*
(i) *Every ideal I of R that is not the unit ideal is contained in a maximal ideal.*
(ii) *R contains at least one maximal ideal.*
(iii) *An element of R that isn't contained in any maximal ideal is a unit.*

proof. We derive this from the noetherian property though, using Zorn's Lemma, it can be proved without the noetherian hypothesis.

(i) Let $\mathcal{S}$ be the set consisting of the ideals J that contain I and are not equal to the unit ideal: $I \subset J < R$. The ideal I is an element of $\mathcal{S}$. Therefore $\mathcal{S}$ isn't empty, so it contains a maximal member. That element will be a maximal ideal.

(ii) This follows by applying **(i)** to the zero ideal.

(iii) If an element α is not in any maximal ideal, **(i)** shows that the principal ideal (α) must be the unit ideal. □

powersgenerate **2.4.11. Corollary.** *Let $s_1, ..., s_k$ be elements of a noetherian ring R that generate the unit ideal of R. For any positive integer n, The powers $s_1^n, ..., s_k^n$ also generate the unit ideal.*

proof. The ideal generated by a set of elements $s_1, ..., s_k$ is the unit ideal if and only if it isn't contained in any maximal ideal, and since a maximal ideal is a prime ideal, it will contain s_i if and only if it contains s_i^n. □

null

2.5 The Nullstellensatz

nullone **2.5.1. Nullstellensatz (version 1).** *Let $\mathbb{C}[x]$ be the polynomial algebra in the variables $x_1, \dots, x_n$. There are bijective correspondences between the following sets:*

- *points p of the affine space $\mathbb{A}^n$,*
- *algebra homomorphisms $\pi_p : \mathbb{C}[x] \to \mathbb{C}$,*
- *maximal ideals $\mathfrak{m}_p$ of $\mathbb{C}[x]$.*

The homomorphism π_p that corresponds to the point $p = (a_1, \dots, a_n)$ of $\mathbb{A}^n$ evaluates a polynomial at p: $\pi_p(g) = g(a_1, ..., a_n)$. The maximal ideal $\mathfrak{m}_p$ that corresponds to p is the kernel of π_p. It is the ideal generated by the linear polynomials $x_1 - a_1, \dots, x_n - a_n$.

It is obvious that every algebra homomorphism $\mathbb{C}[x] \to \mathbb{C}$ is surjective, so its kernel is a maximal ideal. It isn't obvious that every maximal ideal of $\mathbb{C}[x]$ is the kernel of such a homomorphism. For a proof, see for instance [Algebra, 11.8.6]. □

The Correspondence Theorem and the Mapping Property of quotient Rings extend the Nullstellensatz to finite-type algebras.

nulltwo **2.5.2. Nullstellensatz (version 2).** *Let A be a finite-type algebra. There are bijective correspondences between*

- *algebra homomorphisms $\overline{\pi} : A \to \mathbb{C}$, and*
- *maximal ideals $\overline{\mathfrak{m}}$ of A.*

The maximal ideal $\overline{\mathfrak{m}}$ that corresponds to a homomorphism $\overline{\pi}$ is the kernel of $\overline{\pi}$.

If A is presented as a quotient of a polynomial ring, say $A = \mathbb{C}[x_1, ..., x_n]/I$, then these sets also correspond bijectively to points p of the affine scheme $V(I)$ of zeros of I in $\mathbb{A}^n$.

proof. Choosing a presentation for A allows us to assume that A is a quotient of a polynomial ring, say $\mathbb{C}[x]/I$. The Correspondence Theorem tells us that maximal ideals of A correspond to maximal ideals of $\mathbb{C}[x]$ that contain I. These maximal ideals correspond to points of $V(I)$ (see Section 2.2). The Mapping Property,

applied to the canonical homomorphism $\mathbb{C}[x] \xrightarrow{\varphi} A$, tells us that homomorphisms $A \xrightarrow{\overline{\pi}} \mathbb{C}$ correspond to homomorphisms $\mathbb{C}[x] \xrightarrow{\pi} \mathbb{C}$ whose kernels contain I:

polyringtoA (2.5.3)

$$\begin{array}{ccc} \mathbb{C}[x] & \xrightarrow{\pi} & \mathbb{C} \\ {\scriptstyle\varphi}\downarrow & & \| \\ A & \xrightarrow{\overline{\pi}} & \mathbb{C} \end{array}$$

These are the homomorphisms that correspond to points of $V(I)$. □

We will see two more versions of the Nullstellensatz.

spectrumalg **(2.5.4) the spectrum of a finite-type algebra**

The Nullstellensatz allows us to define an affine scheme associated to a finite-type algebra A without reference to a presentation. To do this, we replace the scheme $V(I)$ of zeros of I in $\mathbb{A}^n$, which depends on a presentation, by an abstract set of points, the *spectrum* of A, that we denote by $\operatorname{Spec} A$. We put one point into the spectrum for every maximal ideal of A, and we denote by $\overline{\mathfrak{m}}_p$ the maximal ideal that corresponds to a point p. Points of the spectrum also correspond bijectively to algebra homomorphisms $\overline{\pi}_p : A \to \mathbb{C}$. When we present A as a quotient $\mathbb{C}[x]/I$ of a polynomial algebra, the points of $\operatorname{Spec} A$ correspond to points of the affine scheme $V(I)$.

To work with $\operatorname{Spec} A$, we may interpret its points as maximal ideals or as homomorphisms to $\mathbb{C}$, whichever is most convenient, and if we have chosen a presentation $A \approx \mathbb{C}[x]/I$, we may interpret its points as the points of $V(I)$.

The ring A is the *coordinate algebra* of the scheme $\operatorname{Spec} A$, and if the coordinate algebra A is a domain, $\operatorname{Spec} A$ is called a *variety*.

empty **2.5.5. Corollary.**

(i) *Let I be an ideal of the polynomial ring $\mathbb{C}[x]$. The affine scheme $V(I)$ is the empty set if and only if its coordinate algebra $A = \mathbb{C}[x]/I$ is the zero ring, which happens if and only if I is the unit ideal.*

(ii) *If A is a finite-type algebra, and if $\operatorname{Spec} A$ is empty, then A is the zero ring.*

proof. See Corollary 2.4.10. □

Note. We have used the symbol $\overline{\pi}$ above, to distinguish homomorphisms $A \to \mathbb{C}$ from homomorphisms $\mathbb{C}[x_1, \dots, x_n] \to \mathbb{C}$, and the notation $\overline{\mathfrak{m}}$ is used for an analogous reason. In the future, we will put bars over the letters only when there is danger of confusion. Most often, we will denote the maximal ideal of A and the homomorphism $A \to \mathbb{C}$ that correspond to a point p by $\mathfrak{m}_p$ and π_p, respectively. □

strongnull **2.5.6. Nullstellensatz (version 3): Strong Nullstellensatz.**

(i) *Let I be an ideal of the polynomial algebra $\mathbb{C}[x_1, \dots, x_n]$, and let V be the affine scheme $V(I)$ in $\mathbb{A}^n$. If a polynomial g vanishes at every point of V, then I contains a power of g.*

(ii) *Let A be a finite-type algebra. An element α that is in every maximal ideal of A is nilpotent.*

An element α of a ring A is *nilpotent* if some power α^k is zero.

eltzero **2.5.7. Corollary. (i)** *Let P be a prime ideal of the polynomial ring $\mathbb{C}[x_1, \dots, x_n]$. If a polynomial g vanishes at every point of $V(P)$, then g is an element of P. If P is the principal ideal generated by an irreducible polynomial f and if g vanishes on $V(f)$, then f divides g.*

(ii) *Let A be a finite-type domain. The zero element is the only element of A that is in every maximal ideal of A.* □

proof of the Strong Nullstellensatz **(i)** This beautiful proof is due to Rainich, who published it in 1929, under the pseudonym of Rabinowitsch.

Let $g(x)$ be a polynomial that vanishes identically on V. Since the assertion is trivial when g is zero, we may assume that g isn't zero. The Hilbert Basis Theorem tells us that I is a finitely generated ideal; Let $f = f_1, \dots, f_k$ be a set of generators. In the $n+1$-dimensional affine space with coordinates $(x_1, \dots, x_n, y)$, let W be the locus

fgy (2.5.8) $$f_1(x) = \cdots = f_k(x) = 0 \quad \text{and} \quad g(x)y - 1 = 0.$$

Points of W correspond bijectively to maximal ideals of the polynomial algebra $\mathbb{C}[x_1, ..., x_n, y]$ that contain the ideal $J = (f_1, ..., f_k, gy - 1)$.

Here is the point: Suppose that we have a solution $(x_1, ..., x_n) = (a_1, ..., a_n)$ of the equations $f(x) = 0$. By hypothesis, $g(x) = 0$ at every point at which $f(x) = 0$. So from $f(a) = 0$, it follows that $g(a) = 0$. Then there can be no b such that $g(a)b = 1$. This means that there is no point $(a_1, ..., a_n, b)$ that solves the equations (2.5.8). The locus W is empty, and therefore J is the unit ideal of $\mathbb{C}[x, y]$ (2.4.10). There are polynomials $p_1(x, y), \dots, p_k(x, y)$ and $q(x, y)$ such that

rabinowitz (2.5.9) $$p_1 f_1 + \cdots + p_k f_k + q(gy - 1) = 1.$$

Let B denote the algebra $\mathbb{C}[x, y]/(gy - 1)$. This is the ring obtained by adjoining an inverse y of $g(x)$ to $\mathbb{C}[x]$. Working in B, we substitute g^{-1} for y into (2.5.9). The equation becomes

$$p_1(x, g^{-1})f_1(x) + \cdots + p_k(x, g^{-1})f_k(x) = 1.$$

We multiply both sides by a large power g^N of g to clear denominators. Say that $g^N p_i(x, g^{-1})$ is the polynomial $h_i(x)$. Then

$$h_1(x)f_1(x) + \cdots + h_k(x)f_k(x) = g^N(x)$$

is true in B and in its subring $\mathbb{C}[x]$. This equation shows that g^N is in the ideal I.

Part **(ii)** follows from **(i)**. Say that A is presented as $\mathbb{C}[x]/I$, and let $g(x)$ be a polynomial whose residue in A is α. Then α is in every maximal ideal of A if and only if $g = 0$ at all points of $V(I)$. This is version 2 of the Nullstellensatz. If $g = 0$ at all points of $V(I)$, then some power g^n is in I, and then $\alpha^n = 0$. □

radicalofideal **(2.5.10) the radical of an ideal**

When do two ideals define the same affine scheme? The Strong Nullstellensatz answers this question.

Let I be an ideal of a ring R. The *radical* $\operatorname{rad} I$ of I is the set of all elements α such that some power α^r is in I.

raddef **(2.5.11)** $$\operatorname{rad} I = \{\alpha \in R \,|\, \alpha^r \in I \text{ for some } r > 0\}.$$

The radical is an ideal. An ideal that is equal to its radical is a *radical ideal*.

If n is a positive integer, J^n stands for the product of n copies of the ideal J, the ideal generated by products of length n of elements of J. Its elements are sums of such products.

radpower **2.5.12. Lemma.** *Let I be an ideal of a ring R. Then $I \subset \operatorname{rad} I$. If R is noetherian, then $(\operatorname{rad} I)^n \subset I$ when n is sufficiently large.*

proof. It is obvious that $I \subset \operatorname{rad} I$. If R is noetherian, then $\operatorname{rad} I$ is generated by a finite set of elements, say by $\alpha = \{\alpha_1, ..., \alpha_k\}$, and for large r, $\alpha_i^r \in I$. We can use the same large integer r for every i. Let $n = rk$. If $e_1, ..., e_k$ are integers such that $e_1 + \cdots + e_k \geq n$, then $e_i \geq r$ for at least one i. So any monomial $\beta = \alpha_1^{e_1} \cdots \alpha_k^{e_k}$ of degree n in α will be divisible by at least one α_i. Therefore those monomials are in I. The monomials of degree n generate $(\operatorname{rad} I)^n$, so $(\operatorname{rad} I)^n \subset I$. □

The next corollary follows from the Strong Nullstellensatz.

zeroonV **2.5.13. Corollary.** *Let I and J be ideals in the polynomial algebra $\mathbb{C}[x_1, \dots, x_n]$.*
(i) *A polynomial g vanishes at every point of $V(I)$ if and only if it is an element of the radical* $\operatorname{rad} I$.
(ii) *$V(I) \subset V(J)$ if and only if $\operatorname{rad} I \supset \operatorname{rad} J$, and $V(I) = V(J)$ if and only if $\operatorname{rad} I = \operatorname{rad} J$.* □

Thus there is a bijective correspondence between radical ideals in the polynomial ring $\mathbb{C}[x_1, ..., x_n]$ and affine schemes in $\mathbb{A}^n$.

vofi (2.5.14)
$$V(I) = \{p \,|\, f(p) = 0 \text{ if } f \in I\}$$
$$\operatorname{rad} I = \{f \,|\, f(p) = 0 \text{ if } p \in V(I)\}.$$

strongnullex **2.5.15. Examples. (i)** In the affine line $\mathbb{A}^1 = \operatorname{Spec}\mathbb{C}[x]$, the two polynomials $x^3(x-1)$ and $x(x-1)^2$ have the same zero set: the point pair $\{0, 1\}$, but the principal ideals they generate aren't equal. The radicals of the principal ideals they generate are equal to the principal ideal generated by $x(x-1)$.

(ii) Let I be the ideal of the polynomial algebra $\mathbb{C}[x, y]$ in two variables generated by y^5 and $y^2 - x^3$. The origin $x = y = 0$ is their only common zero, and the polynomial x also vanishes at the origin. The Strong Nullstellensatz predicts that a power of x is in I. This is verified by the following equation:

$$yy^5 - (y^4 + y^2x^3 + x^6)(y^2 - x^3) \;=\; x^9.$$

(iii) We may regard the set of pairs A, B of $n \times n$ matrices as points of an affine space $\mathbb{A}^{2n^2}$ with coordinates a_{ij}, b_{ij}, $1 \le i, j \le n$. The pairs of *commuting* matrices, $AB = BA$, form an affine scheme in $\mathbb{A}^{2n^2}$, the locus of common zeros of the n^2 polynomials p_{ij} that compute the entries of the matrix $AB - BA$:

commmateq (**2.5.16**)
$$p_{ij}(a, b) = \sum_\nu a_{i\nu}b_{\nu j} - b_{i\nu}a_{\nu j}.$$

If I denotes the ideal of the polynomial algebra $\mathbb{C}[a, b]$ generated by the polynomials p_{ij}, $V(I)$ identifies with the set of pairs of commuting complex matrices. The Strong Nullstellensatz asserts that if a polynomial $g(a, b)$ vanishes on every pair of commuting matrices, then some power of g is in I. Is g itself in I? It is a famous conjecture that I is a prime ideal, and that therefore this is true. Proving this conjecture would establish your reputation as a mathematician, but I don't recommend spending very much time on it right now. □

thenilradical (**2.5.17**) **the nilradical**

A ideal I of a ring R is *nilpotent* if some power I^k is the zero ideal. The *nilradical* N of a ring R is the set of nilpotent elements of R, the set of elements z such that some power z^n is zero. The nilradical is the radical of the zero ideal.

intersect-primes **2.5.18. Proposition.** *Let N be the nilradical of a noetherian ring R.*
(i) *N is nilpotent.*
(ii) *N is the intersection of the prime ideals of R.*

proof. See Lemma 2.5.12 for **(i)**. We prove **(ii)**. Let x be a nilpotent element of R. Then some power of x is zero. Since the zero element is in every prime ideal, x is in every prime ideal. We show that if an element x isn't nilpotent, there is a prime ideal that doesn't contain it. Let $\mathcal{S}$ be the set of ideals of R that don't contain a power of x. The zero ideal is one such ideal, so $\mathcal{S}$ isn't empty. Therefore $\mathcal{S}$ contains a maximal member I. We claim that I is a prime ideal, and to show this, we show that if J and K are ideals strictly larger than I, then JK is not contained in I. Since I is a maximal member of $\mathcal{S}$, J and K aren't members of $\mathcal{S}$. They contain powers of x, say $x^k \in J$ and $x^\ell \in K$. Then $x^{k+\ell}$ is in JK but not in I. Therefore $JK \not\subset I$. □

powerzero **2.5.19. Corollary.** *If a noetherian ring contains just one prime ideal, then that ideal is nilpotent.* □

Note. Using Zorn's Lemma, one can prove that the nilradical is the intersection of the prime ideals without the assumption that R be noetherian.

vsinplane

2.6 Varieties in the Affine Plane

In this section, R denotes the polynomial ring $\mathbb{C}[x, y]$ in two variables.

primetwovar **2.6.1. Theorem. (i)** *The varieties in the affine plane $\mathbb{A}^2$ are: the affine plane $\mathbb{A}^2$ itself, the affine plane curves, and the points.*
(ii) *The prime ideals of R are: the zero ideal, the principal ideals generated by irreducible polynomials, and the maximal ideals.*

For the proof, we embed the one-variable polynomial ring $\mathbb{C}[x]$ into its field of fractions $F = \mathbb{C}(x)$, the field of rational functions in x, and we study R as a subring of the one-variable polynomial ring $F[y]$. This is a useful method because $F[y]$ is a principal ideal domain. Its algebra is simpler.

We call a nonzero polynomial $f(x, y)$, an element of $\mathbb{C}[x, y]$, *primitive* if it has no factor that is a polynomial in x alone. Every nonzero element of $F[y]$ can be written as $r(x)h(x, y)$, where $r(x)$ is an element of F and $h(x, y)$ is a primitive polynomial. This expression is unique up to scalar factor. Let's agree that when we say that two nonzero polynomials f and g have *no common factor*, we mean that they have no common factor except constants.

nocommon-factor **2.6.2. Lemma.** *Let $f(x, y)$ and $g(x, y)$ be nonzero elements of R with no common factor. Then their only common divisors in $F[y]$ are elements of F.*

proof. Suppose given an irreducible element q of $F[y]$ which divides both f and g in $F[y]$. An irreducible element isn't allowed to be a unit. Since nonzero elements of F are units in $F[y]$, we may assume that q is a primitive polynomial. Since q is irreducible in $F[y]$, it is also irreducible in R, and therefore it is a prime element of the unique factorization domain R. Since q divides f in $F[y]$, there is a polynomial $r(x)$ in $\mathbb{C}[x]$ such that q divides rf in R. Since q is irreducible and r is a unit in $F[y]$, q doesn't divide r in $F[y]$ or in in R. So q divides f. Similarly, q divides g. So f and g have a common factor. □

quotfindim **2.6.3. Lemma.** *Let f and g be nonzero elements of R with no common factor. The quotient algebra $R/(f, g)$ is a finite-dimensional complex vector space.*

proof. If f and g have no common factor, the previous lemma shows that their greatest common divisor in $F[y]$ is 1. Since $F[y]$ is a principal ideal domain, we can write $1 = p_0 f + q_0 g$ for some p_0 and q_0 in $F[y]$. The coefficients of p_0 and q_0 have denominators that are polynomials in x. Clearing those denominators gives us a relation of the form $u(x) = pf + qg$ with u in $\mathbb{C}[x]$ and p, q in R.

Similarly, by studying the embedding of R into the ring $F'[x]$, where F' is the field of rational functions in y, we obtain a relation of the form $v(y) = p'f + q'g$. Then both $u(x)$ and $v(x)$ are in the ideal (f, g), and by the mapping property of quotients, there is a surjective homomorphism $R/(u, v) \to R/(f, g)$:

$$\begin{array}{ccc} R & \longrightarrow & R/(f,g) \\ \downarrow & & \| \\ R/(u,v) & \longrightarrow & R/(f,g) \end{array}$$

If $u(x)$ and $v(y)$ have degrees r and s, respectively, the residues of the monomials $x^i y^j$ with $i < r$ and $j < s$ form a basis of $R/(u, v)$. So $R/(u, v)$ is finite-dimensional. Since $R/(u, v)$ maps surjectively to $R/(f, g)$, that ring is also finite-dimensional. □

proof Theorem 2.6.1 **(ii)** The zero ideal is prime because R is a domain, an irreducible polynomial generates a prime ideal because R is a unique factorization domain, and a maximal ideal is a prime ideal.

Let P be a nonzero prime ideal of R, and let h be a nonzero element of P. Since P is a prime ideal, it contains an irreducible factor f of h. Then P contains the principal ideal (f). If $P = (f)$ we are done. Otherwise let g be an element of P that is not in (f). Since f is irreducible and doesn't divide g, f and g have no common factor. Lemma 2.6.3 shows that $R/(f, g)$ is a finite-dimensional algebra that maps surjectively to R/P. Therefore R/P is a finite-dimensional domain. A domain that is a finite-dimensional complex vector space is a field, so P is a maximal ideal, and because $\mathbb{C}$ is algebraically closed, $R/P \approx \mathbb{C}$.

Part **(i)** is the translation of **(ii)** to varieties. □

zar

2.7 The Zariski Topology II

Review. Let X be a topological space. The *complement* of a subset S of X is the set of elements of X not in S. The *closure* $\overline{S}$ of S is the smallest closed subset of X that contains S. A subset of X whose closure is equal to X is a *dense* subset.

A subset X of a topological space S is usually made into a topological space by giving it the *induced topology*. The open (or closed) subsets in this topology are the intersections of X with open (or closed) subsets of S. A subset, with its induced topology, is called a *subspace* of X.

In Chapter 1, we defined the Zariski topology on affine space. The closed subsets of $\mathbb{A}^n$ are the affine schemes. The *Zariski topology* on a closed subvariety X of $\mathbb{A}^n$ is the topology induced from the Zariski topology on $\mathbb{A}^n$. Since a closed subvariety X is a closed subset of $\mathbb{A}^n$, a subset Y of X will be closed if and only if it is closed in $\mathbb{A}^n$. So X is a *closed subspace* of $\mathbb{A}^n$.

ztopdimone **2.7.1. Example.** *(The Zariski topology on a plane affine curve.)* The proper closed subsets of a plane affine curve X are its nonempty finite subsets. For, say that $X = \operatorname{Spec} A$, where $A = \mathbb{C}[x,y]/(f)$ and f is an irreducible polynomial. If Z is a proper closed subset of X, there must be a polynomial g not divisible by f that vanishes on Z. The equations $f = g = 0$ in $\mathbb{A}^2$ have finitely many common solutions (Lemma 2.6.3 and Proposition 2.2.3). □

One can define the Zariski topology on an affine variety $X = \operatorname{Spec} A$ also when A is a finite-type domain without a chosen presentation. We denote the maximal ideal of A that corresponds to a point p of X by $\mathfrak{m}_p$, as usual. Then a subset V is *closed* in X if there is an ideal J of A such that V is the set

defineVofJ (2.7.2) $$V_X(J) = \{p \in X \mid J \subset \mathfrak{m}_p\}$$

If A is presented as $\mathbb{C}[x]/I$ and J' denotes the inverse image of J in $\mathbb{C}[x]$, the set $V_X(J)$ is equal to the set $V_{\mathbb{A}^n}(J')$, which we have been denoting by $V(J')$, of $\mathbb{A}^n$.

The next corollary follows from the Strong Nullstellensatz:

subsofspecA **2.7.3. Corollary.** *Let J_1 and J_2 be ideals of a finite-type domain A, and let $X = \operatorname{Spec} A$. Then $V_X(J_1) \subset V_X(J_2)$ if and only if $\operatorname{rad} J_1 \supset \operatorname{rad} J_2$, and $V_X(J_1) = V_X(J_2)$ if and only if $\operatorname{rad} J_1 = \operatorname{rad} J_2$.* □

A topological space X is said to have the *descending chain condition* on closed subsets if every strictly descending, chain $C_1 > C_2 > \cdots$ of closed sets is finite. A space with th descending chain condition on closed subsets is called a *noetherian space*. The descending chain condition on closed sets is equivalent with the ascending chain condition on open sets.

dccquasi-compact **2.7.4. Corollary.** *A noetherian topological space is quasicompact: Every open covering has a finite subcovering.* □

deschain **2.7.5. Proposition.** *If A is a finite-type domain, its spectrum $X = \operatorname{Spec} A$ is a noetherian space.*

This follows from the ascending chain condition for ideals of the noetherian ring A. □

The use of the descending chain condition for closed subvarieties is analogous to the use of the ascending chain condition for ideals. Every nonempty set of closed subsets of a noetherian space has a minimal member.

irrclosed (**2.7.6**) **irreducible closed sets**

irredlemma **2.7.7. Lemma.** *The following conditions on a nonempty closed subset Z of a topological space X are equivalent.*

(i) *Z is not the union of proper closed subsets: If C and D are closed subsets of Z, then $Z = C$ or $Z = D$.*

(ii) *If C and D are closed subsets of X and if $Z \subset C \cup D$, then $Z \subset C$ or $Z \subset D$.*

(iii) *The intersection $U \cap V$ of nonempty open subsets U and V of Z is nonempty.*

(iv) *Every nonempty open subset of Z is dense.* □

defirred **2.7.8. Definition.** A nonempty subset Z of a topological space X that satisfies these conditions is an *irreducible* subset.

This concept is useful primarily for noetherian topological spaces. The only irreducible subsets of a Hausdorff space are the points.

closureirred **2.7.9. Corollary.** *The closure $\overline{Z}$ of an irreducible subset Z of a topological space is irreducible.*

proof. Suppose that $\overline{Z}$ is the union $C \cup D$ of closed sets C and D. Then Z is the union of the sets $C \cap Z$ and $D \cap Z$, which are closed in Z. Therefore Z is one of the two. Say that $Z = C \cap Z$. Then $Z \subset C$, and since C is closed, $\overline{Z} \subset C$, and since $C \subset \overline{Z}$ as well, $C = \overline{Z}$. □

unionirred **2.7.10. Proposition.** *In a noetherian topological space, every closed subset is the union of finitely many irreducible closed subsets.*

proof. Suppose that a closed subset C_0 of a noetherian space X isn't the union of finitely many irreducible closed sets. Then C_0 isn't irreducible, so it is a union $C_1 \cup D_1$, where C_1 and D_1 are proper closed subsets of C_0. Since C_0 isn't a finite union of irreducible closed sets, C_1 and D_1 cannot both be finite unions of irreducible closed sets. Say that C_1 isn't such a union. We replace C_0 by C_1 and repeat the argument, to construct an infinite, strictly descending chain $C_0 > C_1 > \cdots$. This contradicts the hypothesis that X is noetherian. □

irredprime **2.7.11. Lemma.** *The irreducible closed subsets of an affine variety $X = \operatorname{Spec} A$ are those of the form $V_X(P)$, where P is a prime ideal of A. They are the closed subvarieties of X.*

proof. Let Y be a closed subset of X, say $Y = V_X(J)$. We may assume that J is a radical ideal of A (2.7.3). If J is not a prime ideal, there will be ideals K_1, K_2 such that $J < K_i$, but $J = K_1 \cap K_2$. Since J is a radical ideal, and since the radical of $K_1 \cap K_2$ is $\operatorname{rad} K_1 \cap \operatorname{rad} K_2$, we may assume that K_i are radical ideals. Then $V_X(J) > V_X(K_i)$, but $V_X(J) = V_X(K_1) \cup V_X(K_2)$. Therefore Y is not irreducible. Conversely, if J is a prime ideal, such ideals K_i do not exist, and therefore Y is irreducible. □

Note: In a primitive sense, the geometry of an affine scheme $X = \operatorname{Spec} A$ can be thought of as given by closed sets and incidence relations, the inclusion of one closed subset into another, as when a point lies on a line in plane geometry. A finer study of the geometry takes into account things such as tangency and singularity. But it is reasonable to begin by studying incidences $C' \subset C$ among closed subvarieties. Proposition 2.7.11 translates such incidences into inclusions $P' \supset P$ in the opposite direction among prime ideals of the coordinate algebra A. This is one reason that prime ideals are important. □

regfn

2.8 Regular Functions on Affine Varieties

A complex polynomial defines a complex valued function on the affine space $\mathbb{A}^n$, and distinct polynomials define distinct functions. So when the scalars are complex numbers, there is no need to be careful about the distinction between a formal polynomial and the polynomial function it defines.

Let A be a finite-type domain and let $X = \operatorname{Spec} A$. The elements of A define functions on X called *regular functions*. We denote an element of A and the function it defines by the same letter. To define the function associated to an element α, we let $\overline{\pi}_p : A \to \mathbb{C}$ be the homomorphism to $\mathbb{C}$ that corresponds to a point p of X. By definition, the value at p of the function α is $\overline{\pi}_p(\alpha)$:

pipaap (2.8.1) $$\alpha(p) = \overline{\pi}_p(\alpha).$$

The relation between regular functions and polynomial functions is explained as follows. First, the coordinate ring of affine space $\mathbb{A}^n$ is the polynomial ring $\mathbb{C}[x_1, ..., x_n]$. A regular function is a function defined by a polynomial $g(x)$. The homomorphism $\pi_p : \mathbb{C}[x] \to \mathbb{C}$ that corresponds to a point $p = (a_1, ..., a_n)$ is evaluation at that point. So $g(p) = g(a_1, ..., a_n) = \pi_p(g)$, which agrees with (2.8.1).

Next, suppose that A is presented as $\mathbb{C}[x]/I$. The element α will be the residue of a polynomial g (that isn't uniquely determined). We can restrict the function g on $\mathbb{A}^n$ to the subset X, to obtain the function α on

X. A point p of X determines homomorphisms $\pi_p : \mathbb{C}[x] \to \mathbb{C}$ and $\overline{\pi}_p : A \to \mathbb{C}$, and $\overline{\pi}_p(\alpha) = \pi_p(g)$ (see Diagram 2.5.3). So for p in X,

redefinefn (2.8.2) $$\alpha(p) \stackrel{defn}{=} \overline{\pi}_p(\alpha) = \pi_p(g) \stackrel{defn}{=} g(p).$$

The regular functions on a closed subvariety X of the affine space $\mathbb{A}^n$ are the restrictions of polynomial functions.

describemax **2.8.3. Corollary.** *Let A be a finite-type domain, and let p be a point of* $\operatorname{Spec} A$*. An element α of A is in the maximal ideal $\overline{\mathfrak{m}}_p$ if and only if $\alpha(p) = 0$.* □

scheme-function **2.8.4. Note.** One can use formula (2.8.1) to define the function associated to an element α of a finite-type algebra A, whether or not A is a domain. However the function may not determine the algebra. For instance, if A is the quotient $\mathbb{C}[x]/(x^2)$ of a polynomial algebra in one variable, elements of A have the form $\alpha = a_0 + a_1 x$, with $a_i \in \mathbb{C}$. Here $\operatorname{Spec} A$ consists of a single point p, and $\overline{\pi}_p(a_0 + a_1 x) = a_0$. □

morphism

2.9 Morphisms of Affine Varieties

The word "morphism" is used to describe the allowed maps between affine varieties. Those maps are the ones that can be defined using regular functions.

If $Y \stackrel{u}{\longrightarrow} X$ is a map of sets and g is a function on X, composition with u produces a function $g \circ u$ on Y:

defpullback (2.9.1)
$$\begin{array}{ccc} Y & \xrightarrow{g\circ u} & \mathbb{C} \\ {\scriptstyle u}\downarrow & & \| \\ X & \xrightarrow{g} & \mathbb{C} \end{array}$$

The composition with u defines a homomorphism from the algebra of functions on X to the algebra of functions on Y that is often denoted by u^* and is called a *pullback*:

$$Functions(Y) \stackrel{u^*}{\longleftarrow} Functions(X)$$

(see 2.9.1). Thus by definition, $u^* g = g \circ u$. (An asterisk in the superscript position is often used to indicate that the direction of an arrow has been reversed.)

defmorphism **2.9.2. Definition.** Let X and Y be affine varieties. A *morphism* $Y \stackrel{u}{\longrightarrow} X$ is a map such that the pullback of every regular function on X is a regular function on Y.

morphhomo **2.9.3. Proposition.** *Let A and B be the coordinate algebras of the affine varieties X and Y, respectively. Morphisms $Y \stackrel{u}{\longrightarrow} X$ correspond bijectively to algebra homomorphisms in the opposite direction $B \stackrel{\varphi}{\longleftarrow} A$.*

For example, an embedding of an affine variety $X = \operatorname{Spec} A$ into affine space, $X \subset \mathbb{A}^n$, corresponds to a surjective homomorphism $A \leftarrow \mathbb{C}[x_1, ..., x_n]$. The affine blowup $\mathbb{A}^2_{x,z} \to \mathbb{A}^2_{x,y}$ that sends $(x, z) \rightsquigarrow (x, y) = (x, xz)$ described in (**1.10.4**) corresponds to the ring homomorphism $\mathbb{C}[x, z] \stackrel{\varphi}{\longleftarrow} \mathbb{C}[x, y]$ defined by $\varphi(x) = x$, $\varphi(y) = xz$.

As this proposition shows, there is little difference between the theory of affine varieties and the theory of commutative rings. But the fact that the arrows $Y \stackrel{u}{\longrightarrow} X$ and $B \stackrel{\varphi}{\longleftarrow} A$ are in opposite directions can be confusing.

proof of Proposition 2.9.3. We drop some parentheses to minimize clutter. Given a morphism $X \stackrel{u}{\longleftarrow} Y$, we define a homomorphism $A \stackrel{\varphi}{\longrightarrow} B$. If α is an element of A, a regular function on X, we define $\varphi\alpha = \alpha \circ u$. Since u is a morphism, $\varphi\alpha$ is a regular function on Y, an element of B. The map φ thus defined is a homomorphism, and it satisfies the rule

phialpha (2.9.4) $$[\varphi\alpha](y) = \alpha(uy).$$

In the other direction, we suppose given a homomorphism $A \xrightarrow{\varphi} B$, and we define a morphism $X \xleftarrow{u} Y$. Let y be a point of Y. Evaluation of functions at y gives us a homomorphism $\pi_y : B \to \mathbb{C}$. The composed map $\pi_y\varphi$ is a homomorphism $A \to \mathbb{C}$. According to the Nullstellensatz, this homomorphism is evaluation of functions at a point x of X, and that point is defined to be the image of y: $uy = x$ Thus π_x is a homomorphism $A \to \mathbb{C}$, and u is defined by the relation $\pi_x = \pi_y\varphi$. Then if α is an element of A and if we evaluate its image $\varphi\alpha$ in B at y (2.8.1), we get formula (2.9.4) again:

$$[\varphi\alpha](y) = \pi_y(\varphi\alpha) = \pi_x\alpha = \alpha(x)$$

By definition, $[u^*\alpha](y) = \alpha \circ u(y) = \alpha(x)$. So $u^*\alpha = \varphi\alpha$ is an element of B, a regular function on Y, and u is a morphism.

morphmax **2.9.5. Corollary.** *Let $Y \xrightarrow{u} X$ be the morphism of affine varieties that corresponds to an algebra homomorphism $A \xrightarrow{\varphi} B$. Let y be a point of Y and let $x = uy$ be its image in X. Then $\pi_x = \pi_y \circ \varphi$, and $\mathfrak{m}_x = \varphi^{-1}\mathfrak{m}_y$.* □

morphcontin **2.9.6. Proposition.** *A morphism $Y \xrightarrow{u} X$ of affine varieties is a continuous map in the Zariski topology.*

proof. Say that $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$. The morphism u corresponds to an algebra homomorphism $A \to B$. Let C be the closed subset $V_X(J)$ of X, and let J' be the extended ideal JB of B. Then $u^{-1}C$ is the closed set $V_Y(JB)$. To prove this, one verifies that the following conditions on a point y are equivalent:

$$uy \in C, \quad J \subset \mathfrak{m}_{uy} = (\mathfrak{m}_y \cap A), \quad JB \subset \mathfrak{m}_y, \quad y \in V_Y(JB)$$

□

The next proposition spells the definition of morphism out in terms of equations.

mapbtoa **2.9.7. Proposition.** *Let $(f_1, \dots, f_r)$ be an ideal of the polynomial algebra $\mathbb{C}[x_1, \dots, x_k]$, and let $A = \mathbb{C}[x]/(f)$. Homomorphisms from A to an arbitrary algebra B correspond bijectively to sets of elements $\beta_1, \dots, \beta_k$ of B such that*

$$f_1(\beta) = \cdots = f_r(\beta) = 0.$$

This is an important principle:

- *To map the algebra $A = \mathbb{C}[x]/(f)$ to an algebra B means to solve the equations $f = 0$ in B.*

proof. We compose a map $A \xrightarrow{\varphi} B$ with the canonical map $\mathbb{C}[x] \xrightarrow{\tau} A$, obtaining a map $\Phi : \mathbb{C}[x] \to B$.

$$\begin{array}{ccc} \mathbb{C}[x] & \xrightarrow{\Phi} & B \\ {\scriptstyle\tau}\downarrow & & \| \\ A & \xrightarrow{\varphi} & B \end{array}$$

The map Φ is obtained by substituting some elements β_j of B for the variables x_j. Since the polynomials $f_1, ..., f_r$ are in the kernel of τ, they are in the kernel of Φ too, which means that $f_i(\beta) = 0$. Conversely, if Φ is a map $\mathbb{C}[x] \to B$ whose kernel contains $f_1, \dots, f_r$, the Mapping Property of quotients shows that it has the form $\varphi\tau$. □

cuspnormx **2.9.8. Example.** *(resolving a cusp curve)* The equation $y^2 = x^3$ defines a plane curve $C = \operatorname{Spec} A$ with a cusp at the origin, where $A = \mathbb{C}[x, y]/(y^2 - x^3)$. The homomorphism $A \xrightarrow{\varphi} \mathbb{C}[t]$ that sends $x \rightsquigarrow t^2$ and $y \rightsquigarrow t^3$ defines a morphism $C \xleftarrow{u} \mathbb{A}^1_t$ that sends a point t of $\mathbb{A}^1$ to the point $(x, y) = (t^2, t^3)$ of C. This morphism is a bijective map whose inverse function v sends a point $(x, y) \neq (0, 0)$ of C to the point $t = y/x$, and sends $(x, y) = (0, 0)$ to the point $t = 0$. Both u and v are continuous, and therefore are homeomorphisms in the Zariski topology (and in the classical topology). However, φ isn't an algebra isomorphism because y/x isn't an element of A. There is no inverse homomorphism $\mathbb{C}[t] \to A$. Therefore v isn't a morphism, and u isn't an isomorphism.

boldloc (**2.9.9**) **localization**

deflocaliz **2.9.10. Definition.** If s is a nonzero element of a domain A, the ring $A[s^{-1}]$ obtained by adjoining an inverse of s to A will be called a *simple localization*, or just a *localization* of A. and will often be denoted by A_s. If A is a finite-type algebra then $X_s = \operatorname{Spec} A_s$ is a *simple localization*, or a *localization* of $X = \operatorname{Spec} A$.

specAs **2.9.11. Lemma. (i)** *The homomorphism $A \to A_s$ defines an injective morphism $X \xleftarrow{u} X_s$, whose image is the open set of points of X at which the function s isn't zero.*

(ii) *When X_s is identified with its image in X, the Zariski topology on X_s is the induced topology from X, so X_s becomes an open subspace of X.*

This lemma gives us a way to construct non-affine varieties by identifying common localizations. For example, the projective line $\mathbb{P}^1$ can be constructed from two affine lines $U^0 = \operatorname{Spec} \mathbb{C}[t]$ and $U^1 = \operatorname{Spec} \mathbb{C}[u]$ by identifying the open subsets $U^0_t = \mathbb{C}[t, t^{-1}]$ and $U^1_u \mathbb{C}[u, u^{-1}]$ of U^0 and U^1, respectively, using the rule $u = t^{-1}$.

However, one must be careful when doing this. One could also identify those localizations using the rule $t = u$, but 'forgetting' to identify $t = 0$ with $u = 0$. The result of this would be an affine line in which the origin is replaced by a pair of points. We'll come back to this example later.

$$figure$$

proof.*of Lemma 2.9.11.* **(i)** Let p be a point of X, and let $A \xrightarrow{\pi_p} \mathbb{C}$ be the corresponding homomorphism. If the image $\pi_p(s)$ isn't zero, π_p extends uniquely to a homomorphism $A_s \to \mathbb{C}$ that sends $s^{-1} \rightsquigarrow \pi_p(s)^{-1}$. This gives us a point of X_s whose image via the morphism $X_s \xrightarrow{u} X$ is p. On the other hand, if $\pi_p(s) = 0$, then π_p does not extend. So

$$X_s \approx X - V_X(s).$$

The effect of adjoining the inverse of an element s is to throw out the points of X at which s vanishes.

(ii) If C is closed in X, then $C \cap X_s$ is closed in X_s. Conversely, let C' be a closed subset of X_s. We must show that C' is the intersection $C \cap X_s$ where C is closed in X. Say that $C' = V_{X_s}(I')$ for some ideal I' of A_s. The intersection $I = I' \cap A$ is an ideal of A. Let $C = V_X(I)$, let p be a point of C', and let $\mathfrak{m}_p$ and $\mathfrak{m}'_p$ denote the maximal ideals of p in A and A_s, respectively. Then $\mathfrak{m}_p = \mathfrak{m}'_p \cap A$. Since p is in $C' = V_{X_s}(I')$, $I' \subset \mathfrak{m}'_p$, and therefore $I \subset \mathfrak{m}_p$. So $p \in C$, and therefore $C' = C \cap X_s$. □

punctline **2.9.12. Example.** *(the punctured line as a variety)* The punctured affine line $\mathbb{A}^1 - \{0\}$ corresponds bijectively to the spectrum of the *Laurent polynomial ring* $\mathbb{C}[t, t^{-1}]$. □

Recapitulating, *morphisms* $\operatorname{Spec} B \xrightarrow{u} \operatorname{Spec} A$ of affine schemes correspond to algebra homomorphisms $A \xrightarrow{\varphi} B$. A morphism is an *isomorphism* if and only if there is an inverse morphism, which is true if and only if φ is an isomorphism of algebras. An *automorphism* of a variety X is an isomorphism $X \to X$.

grpi

2.10 Finite group actions

Let G be a finite group of automorphisms of a finite-type domain B. An element of B is *invariant* if it is fixed by all σ in G. The invariant elements form a subalgebra of B that is often denoted by B^G. We will show that B^G is a finite-type algebra, and we describe the morphism $\operatorname{Spec} B = Y \to X = \operatorname{Spec} B^G$ defined by the inclusion $B^G \subset B$.

actonplaneex **2.10.1. Example.** Let B be the polynomial ring $\mathbb{C}[y_1, y_2]$, let σ be the automorphism defined by $\sigma y_1 = \zeta y_1$ and $\sigma y_2 = \zeta^{-1} y_2$, with $\zeta = e^{2\pi i/n}$, and let G be the cyclic group of order n generated by σ. A monomial $m = y_1^i y_2^j$ is invariant if and only if n divides $i - j$, and an invariant polynomial is a linear combination of

invariant monomials. The ring $A = B^G$ of invariant polynomials is generated by three elements $u_1 = y_1^n$, $u_2 = y_2^n$, and $w = y_1y_2$, and that A is isomorphic to the quotient of the polynomial ring $\mathbb{C}[u_1, u_2, w]$, modulo the principal ideal generated by $h = w^n - u_1u_2$. You will be able to show this.

Let Y denote the affine plane $\operatorname{Spec} B$, and let $X = \operatorname{Spec} A$. The group G operates on Y, and except for the origin, which is a fixed point, the orbit of a point (y_1, y_2) of Y consists of the n points $(\zeta^i y_1, \zeta^{-i} y_2)$, $i = 0, \dots, n-1$. In all cases, the points of X correspond bijectively to G-orbits in Y. To verify this, we fix complex numbers u_1, u_2, w with $w^n = u_1u_2$. If $u_1 \neq 0$, the equation $u_1 = y_1^n$ has n solutions for y_1, and then y_2 is determined by the equation $w = y_1y_2$. Similarly, there are n points in the fibre if $u_2 \neq 0$. If $u_1 = u_2 = 0$, then $w = y_1 = y_2 = 0$. □

The next theorem shows that the description of X as the set of G-orbits in Y is true for any finite group operation.

groupoperone **2.10.2. Theorem.** *Let B be a finite-type domain, let G be a finite group of automorphisms of B, and let A be the subalgebra B^G of invariant elements of B. Let $Y = \operatorname{Spec} B$ and $X = \operatorname{Spec} A$.*

(i) *A is a finite-type domain and B is a finite A-module.*

(ii) *G operates on Y.*

(iii) *The morphism $Y \to X$ defined by the inclusion $A \subset B$ is surjective, and its fibres are the G-orbits of points of Y.*

Thus if we denote the set of G-orbits in Y by Y/G, there is a bijective map $Y/G \approx X$.

proof. **(i)** The structure of the proof is interesting. One constructs a finite-type algebra R, with $R \subset A \subset B$, such that B is a finite R-module. Using this, one shows that A is a finite-type algebra.

Let $\{z_1, \dots, z_k\}$ be the G-orbit of an element $z = z_1$ of B. The coefficients s_i of the polynomial

spoly **(2.10.3)** $$f(t) \;=\; (t - z_1) \cdots (t - z_k) \;=\; t^k - s_1 t^{k-1} + \cdots \pm s_k$$

are the elementary symmetric functions in the orbit $\{z_1, ..., z_k\}$. They are invariant, so $f(t)$ has coefficients in A, and it has z as a root. The equation $f(z) = 0$ allows us to write any power of z as a polynomial in z with coefficients in A, of degree less than k.

We choose a finite set of generators $y = \{y_1, \dots, y_r\}$ for the algebra B. If the order of the orbit of y_j is k_j, y_j will be the root of a monic polynomial f_j of degree k_j with coefficients in A. Let R denote the finite-type algebra generated by the coefficients of all of the polynomials f_j. The equation $f_j(y_j) = 0$ allows us to write a power y_j^n of y_j as a polynomial $p(y_j)$ in y_j with coefficients in R, such that the degree of p is less than k_j. Using these polynomials, we can write every monomial $y_1^{e_1} \cdots y_r^{e_r}$ as a polynomial $p(y_1, ..., y_r)$ with coefficients in R whose degree in y_j is $\leq k_j$. Since y generates B, we can write every element of B as such a polynomial. So the finite set of monomials $y_1^{e_1} \cdots y_r^{e_r}$ with $e_j < k_j$ spans B as an R-module. Therefore B is a finite R-module. The invariant algebra A is a subalgebra of B that contains R. So when regarded as an R-module, A is a submodule of the finite module B. Since R is a finite-type algebra, it is noetherian. Therefore A is also a finite R-module. When we put a finite set of algebra generators for R together with a finite set of R-module generators for A, we obtain a finite set of algebra generators for A. So A is of finite type. And since B is a finite R-module, B is also a finite A-module.

(ii) A group element σ is an automorphism $B \to B$ that defines an automorphism $Y \longleftarrow Y$. We denote the automorphism of Y by σ too. This gives the operation of G on Y. However, there is a point that should be mentioned.

Let's say that we write the operation of G on B on the left, so that σ maps an element b to σb. Then if σ and τ are two group elements, $\sigma\tau b$ means first operate by τ: $\quad(\sigma\tau)b = \sigma(\tau b)$. We interpret a point y of $Y = \operatorname{Spec} B$ as a homomorphism $B \xrightarrow{\pi_p} \mathbb{C}$. The operation of σ on homomorphisms to $\mathbb{C}$ is composition with σ. It sends π_y to $\pi_y \circ \sigma$ (see (2.9.5)). The operation on homomorphisms is on the right. For operations on the right, $\sigma\tau$ acts as first operate by σ: $\quad\pi_y(\sigma\tau) = (\pi_y\sigma)\tau$.

- *If G operates on the left on B, it operates on the right on* $\operatorname{Spec} B$.

(iii) The diagram of algebra homomorphisms

actonB (2.10.4)
$$\begin{array}{ccc} B & \xrightarrow{\sigma} & B \\ \cup\uparrow & & \cup\uparrow \\ A & = & A \end{array}$$

gives us a diagram of morphisms

actonX (2.10.5)
$$\begin{array}{ccc} Y & \xleftarrow{\sigma} & Y \\ \downarrow & & \downarrow \\ X & = & X \end{array}$$

which shows that the elements of Y forming a G-orbit have the same image in X, and therefore that Y/G maps to X. We show that this map is bijective. To show that the map $Y/G \to X$ is injective, we use the following lemma.

arbvals **2.10.6. Lemma.** **(i)** *Let $p_1, \dots, p_k$ be a finite set of distinct points of affine space $\mathbb{A}^n$, and let $c_1, \dots, c_k$ be complex numbers. There is a polynomial $f(x_1, \dots, x_n)$ such that $f(p_i) = c_i$ for $i = 1, \dots, n$.*
(ii) *Let B be a finite-type algebra, let $q_1, \dots, q_k$ be points of $\operatorname{Spec} B$, and let $c_1, \dots, c_k$ be complex numbers. There is an element β in B such that $\beta(q_i) = c_i$ for $i = 1, \dots, k$.* □

Note that if b is an element of B, the product and the sum of the elements σb,

invarelts (2.10.7)
$$\prod_{\sigma\in G} \sigma b \quad \text{and} \quad \sum_{\sigma\in G} \sigma b$$

are invariant elements.

Let O_1 and O_2 be distinct orbits. There is an element b of B such that at every point of O_1 its value is 0, and at every point of O_2 its value is 1. Then the invariant element $\beta = \prod_\sigma \sigma b$ also evaluates to 0 at every point of O_1 and to 1 on every point of O_2. If p_i denotes the image in X of the orbit O_i, then β is in the maximal ideal $\mathfrak{m}_{p_1}$, but not in $\mathfrak{m}_{p_2}$. The images of the two orbits are distinct. Therefore the map $Y/G \to X$ is injective.

To show that the map $Y/G \to X$ is surjective, it suffices to show that the map $Y \to X$ is surjective, and for this we use the next lemma.

extideal **2.10.8. Lemma.** *If I is an ideal of the invariant ring A, and if the extended ideal IB is the unit ideal of B, then I is the unit ideal of A.*

As before, the extended ideal IB is the ideal of B generated by I.

proof of Lemma 2.10.8. If $IB = B$, there will be an equation $\sum_i z_i b_i = 1$, with z_i in I and b_i in B. The sum $\alpha_i = \sum_\sigma \sigma b_i$ is invariant, so it is an element of A, as are the elements z_i. Then

$$\sum_\sigma 1 = \sum_\sigma \sigma(1) = \sum_{\sigma,i} \sigma(z_i b_i) = \sum_{i,\sigma} z_i \sigma b_i = \sum_i z_i \sum_\sigma \sigma b_i = \sum_i z_i \alpha_i$$

Because the elements z_i are in I, the right side $\sum_i z_i\alpha_i$ is in I, and the left side $\sum_\sigma 1$ is the order of the group, which an invertible element of A. So I is the unit ideal. □

We prove surjectivity of the map $Y \to X$ now. Let p be a point of X. The extended ideal $\mathfrak{m}_p B$ is not the unit ideal. So it is contained in a maximal ideal $\mathfrak{m}_q$ of B, where q is a point of Y. Then

mpinmqcapA (2.10.9)
$$\mathfrak{m}_p \ \subset\ (\mathfrak{m}_p B) \cap A \ \subset\ \mathfrak{m}_q \cap A.$$

Here $\mathfrak{m}_q \cap A$ is an ideal of A, and it isn't the unit ideal because 1 isn't in $\mathfrak{m}_q$. Since $\mathfrak{m}_p$ is a maximal ideal, $\mathfrak{m}_p = \mathfrak{m}_q \cap A$. This means that the point q maps to p in X (2.9.5). So the map $Y \to X$ is surjective. □

2.11 Tensor Products

tensprod

We have collected the facts about tensor products that we will use in subsequent chapters here. We apologize for the fact that this material is rather dry.

Let U and V be modules over a ring R. The *tensor product* $U \otimes_R V$ of U and V is an R-module generated by elements $u \otimes v$ called tensors, with u in U and v in V. Its elements are combinations of tensors with coefficients in R. Since we can absorb a coefficient from R into one of the factors of a tensor, every element of $U \otimes_R V$ can be written as a finite sum $\sum u_i \otimes v_i$.

The module of relations among the tensors is generated by the following *bilinear relations*:

bilinrels (2.11.1)
$$(u_1 + u_2) \otimes v = u_1 \otimes v + u_2 \otimes v\,, \quad u \otimes (v_1 + v_2) = u \otimes v_1 + u \otimes v_2$$

and
$$ur \otimes v = u \otimes rv$$

for all u in U, v in V, and r in R. The tensor symbol $\otimes$ is used as a reminder that the elements $u \otimes v$ are manipulated using these relations.

There are a few remarks to be made.

(1) The last of the bilinear relations states that scalars move through the tensor symbol. This is why we write the term on the right of that relation as $ur \otimes v$ instead of as $ru \otimes v$. As written, the relations define the tensor product of a *right module* U, a module in which scalars act on the right, and a *left module* V. Since we are working with commutative rings, right modules can be made into left modules simply by setting $ru = ur$. Let's agree that unless stated otherwise, scalar multiplication on the two sides supposed to be equal:

$$ru = ur$$

One can't do this when the ring is noncommutative, and there are situations in which a right R-module is also a left module over a different commutative ring.

(2) The tensor product $U \otimes V$ is made into a left R-module on using the structure of U as left module:

tensormodule (2.11.2)
$$r(u \otimes v) = (ru) \otimes v$$

If there was no left module structure on U, the tensor product wouldn't be a left module.

(3) There is no close relation between the tensor product $U \otimes_R V$ and the *product* module $U \times V$ whose elements are pairs (u, v), with componentwise addition and scalar multiplication. For instance, if U and V are free modules of ranks r and s, then $U \otimes_R V$ is free of rank is rs, while $U \times V$ is free of rank $r + s$.

(4) On the other hand,

there is an obvious map $U \times V \xrightarrow{\beta} U \otimes_R V$ from the product *set* to the tensor product that sends (u, v) to $u \otimes v$. The fact that the relations among tensors are the bilinear relations shows that this map is bilinear. In fact, it is a universal bilinear map: Any R-bilinear map $U \times V \xrightarrow{f} M$ to a module M can be obtained from a module homomorphism $U \otimes_R V \xrightarrow{\widetilde{f}} M$ by composition, $f = \widetilde{f} \circ \beta$: $\quad U \times V \xrightarrow{\beta} U \otimes_R V \xrightarrow{\widetilde{f}} M$. □

canonisom **2.11.3. Proposition.** *There are canonical isomorphisms*

- $U \otimes_R R \approx U, \quad u \otimes r \leftrightsquigarrow ur$
- $(U \oplus U') \otimes_R V \approx (U \otimes_R V) \oplus (U' \otimes_R V), \quad (u_1 + u_2) \otimes v \leftrightsquigarrow u_1 \otimes v + u_2 \otimes v$

and if R is commutative, then

- $U \otimes_R V \approx V \otimes_R U, \quad u \otimes v \leftrightsquigarrow v \otimes u$
- $(U \otimes_R V) \otimes_R W \approx U \otimes_R (V \otimes_R W), \quad (u \otimes v) \otimes w \leftrightsquigarrow u \otimes (v \otimes w)$

The proofs are very simple. We verify the "distributive law" $(U \otimes_R V) \oplus (U' \otimes_R V) \approx (U \oplus U') \otimes_R V$ as an example. The left side is generated by tensors $u \otimes v$ and $u' \otimes v$, and the relations are the bilinear relations in the two summands. The right side is generated by tensors $x \otimes v$, where $x = u + u'$, with the bilinear relations

$$(x_1 + x_2) \otimes v = x_1 \otimes v + x_2 \otimes v, \quad x \otimes (v_1 + v_2) = x \otimes v_1 + x \otimes v_2, \quad xr \otimes v = x \otimes rv)$$

The relations defining the right side hold on the left side, and setting $x = u + 0$ and $x = 0 + u'$ shows that the relations defining the left side hold in the right side. □

prodbasis **2.11.4. Corollary.** *If U and V are free R-modules with bases $\{u_i\}$ and $\{v_j\}$, respectively, then $U \otimes_R V$ is a free R-module with basis $\{u_i \otimes v_j\}$.* □

rexacttensor **2.11.5. Proposition.** *The tensor product operation is right exact. If*

$$U \xrightarrow{f} U' \xrightarrow{g} U'' \to 0$$

is an exact sequence of R-modules, then for any R-module V, the sequence

$$U \otimes_R V \xrightarrow{f\otimes id} U' \otimes_R V \xrightarrow{g\otimes id} U'' \otimes_R V \to 0$$

is exact.

proof. Let Z be the image of $f \otimes id$, and let $W = (U' \otimes_R V)/Z$. The composed map $(g \otimes id)(f \otimes id)$ is zero, so there is an induced map $W \to U'' \otimes V$. We must show that this map is invertible. To define its inverse, we define a bilinear map $U'' \times V \to W$. Given a tensor $u'' \otimes v$ in $U'' \otimes_R V$, we choose u' in U' such that $g(u') = u''$, and we map $u'' \otimes v$ to the residue of $u' \otimes v$ in W. This is well-defined because if u'_1 and u'_2 are elements of U' such that $g(u'_1) = g(u'_2)$, then $u'_1 - u'_2$ is in the image of f, and $(u'_1 - u'_2) \otimes v$ is in Z. The bilinear relations hold in W because they hold in $U' \otimes_R V$, so this map corresponds to a module homomorphism $U'' \otimes_R V \to W$ that inverts $g \otimes id$. □

tensorrels **2.11.6. Corollary.** **(i)** *Let U, V be R-modules, and suppose that U is presented as R^m/AR^n by an exact sequence*

$$R^n \xrightarrow{A} R^m \to U \to 0$$

Then $U \otimes_R V \approx V^m/AV^n$.

(ii) *With notation as in* **(i)**, *suppose that V is presented as R^k/BR^ℓ by an exact sequence*

$$R^\ell \xrightarrow{B} R^k \to V \to 0$$

Then the map $R^m \otimes_R R^k \to U \otimes_R V$ is surjective. Its kernel is generated by the images of the two maps

$$R^n \otimes_R R^k \xrightarrow{A\otimes I} R^m \otimes R^k \quad \text{and} \quad R^m \otimes_R R^\ell \xrightarrow{I\otimes B} R^m \otimes R^k.$$

proof. **(ii)** We form a diagram with exact rows and columns:

$$\begin{array}{ccccccc}
R^n \otimes R^\ell & \longrightarrow & R^m \otimes R^\ell & \longrightarrow & U \otimes R^\ell & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
R^n \otimes R^k & \longrightarrow & R^m \otimes R^k & \longrightarrow & U \otimes R^k & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
R^n \otimes V & \longrightarrow & R^m \otimes V & \longrightarrow & U \otimes V & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
0 & & 0 & & 0 & &
\end{array}$$

Then the assertion follows from a general fact. For any diagram

$$\begin{array}{ccccccc}
A & \longrightarrow & A' & \longrightarrow & A'' & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
B & \longrightarrow & B' & \longrightarrow & B'' & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
C & \longrightarrow & C' & \longrightarrow & C'' & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
0 & & 0 & & 0 & &
\end{array}$$

whose rows and columns are exact, the composed map $B' \to C''$ is surjective, and its kernel is the sum of the images of A' and B in B'. The verification is a diagram chase. □

tensornotexact **Example.** This example shows that the tensor product operation isn't exact. Let $R = \mathbb{C}[x]$, and let $\mathbb{C}$ denote the R-module R/xR. When we tensor the exact sequence $0 \to R \xrightarrow{x} R \to \mathbb{C} \to 0$ with $\mathbb{C}$, the result is the non-exact sequence $0 \to \mathbb{C} \xrightarrow{0} \mathbb{C} \to \mathbb{C} \to 0$ □

extendscalars **(2.11.7) extension of scalars in a module**

Let $R \xrightarrow{\rho} S$ be a ring homomorphism. An S-module N can be made into an R-module, in which scalar multiplication by an element a of R is defined to be multiplication by its image in S:

restrscalar (2.11.8) $$ax \overset{def}{=} \rho(a)x$$

This operation is called *restriction of scalars*.

For example, let ρ be the map $\mathbb{C}[t] \to \mathbb{C}$ that evaluates a polynomial p at 0. Restriction of scalars makes a complex vector space V into a $\mathbb{C}[t]$-module in which scalar multiplication is defined by $p(t)v = p(0)v$. This example is trivial, as are all examples of the simple operation of restriction of scalars.

An R, S-*bimodule* is an abelian group that is a left R-module and a right S-module, and such that left and right multiplications commute:

leftright-commute (2.11.9) $$r(ms) = (rm)s$$

For example, if we are given a homomorphism $R \to S$, the ring S becomes an R, S-bimodule in which the left operation of R is by restriction of scalars. Then, given a right R-module M, the tensor product $M' = M \otimes_R S$ becomes a right S-module, multiplication by $s \in S$ being $(m \otimes a)s = m \otimes (as)$. This gives a functor

$$R\text{−}modules \xrightarrow{\otimes S} S\text{−}modules$$

that is called *extension of scalars*.

locistensor **2.11.10. Corollary.** *Let U and V be modules over a domain R and let s be a nonzero element of R. Let R_s, U_s, V_s be the (simple) localizations of R, U, V, respectively (see 2.9.10).*
(i) *There is a canonical isomorphism $U_s \approx U \otimes_R R_s$.*
(ii) *Localization is compatible with tensor product: $U_s \otimes_{R_s} V_s \approx (U \otimes_R V)_s$* □

fibremodule **(2.11.11) fibres of a module**

Let I be an ideal of a finite-type domain A, and let $\overline{A} = A/I$. Also, let U be an A-module, and let UI be the submodule generated by products $u\alpha$ with u in U and α in I. Tensor product with U givews us a diagram

$$\begin{array}{ccccccccc} & & U \otimes_A I & \longrightarrow & U \otimes_A A & \longrightarrow & U \otimes_A \overline{A} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \approx & & \downarrow \approx & & \\ 0 & \longrightarrow & UI & \longrightarrow & U & \longrightarrow & U/UI & \longrightarrow & 0 \end{array}$$

in which the left vertical arrow is surjective.

If I is the maximal ideal $\mathfrak{m}_p$ at a point p of $X = \operatorname{Spec} A$, then $\overline{A}$ is the residue field $k(p)$ at p, and $U \otimes_A k(p)$ is the $k(p)$-module obtained from U by extension of scalars. We call this $k(p)$-module the *fibre* of U at p, and we denote it by $U(p)$. Then there is an exact sequence

Utensorktwo (2.11.12) $$0 \to U\mathfrak{m}_p \to U \to U(p) \to 0$$

that we use to identify the fibre $U(p)$ as $U/U\mathfrak{m}_p = U \otimes_A k(p)$.

The *support* of a finite A-module U is the set of points p such that the fibre $U(p)$ at p isn't zero. The support of a finite module is a closed subset of $X = \operatorname{Spec} A$.

tensoralgebras **(2.11.13) tensor product algebras**

If A and B are algebras over a ring R, the tensor product module $A \otimes_R B$ is made into an R-algebra with multiplication law

$$(\alpha_1 \otimes \beta_1) \cdot (\alpha_2 \otimes \beta_2) = (\alpha_1\alpha_2) \otimes (\beta_1\beta_2)$$

and its multiplicative identity is $1 \otimes 1$. One must show compatibility of multiplication with the bilinear relations. Since this is easy, we'll do one verification as an example. We know that $(\alpha_1 + \alpha_1') \otimes \beta_1 = \alpha_1 \otimes \beta_1 + \alpha_1' \otimes \beta_1$, so we must show that

$$\big((\alpha_1 + \alpha_1') \otimes \beta_1\big) \cdot \big(\alpha_2 \otimes \beta_2\big) \;=\; \big(\alpha_1 \otimes \beta_1\big) \cdot \big(\alpha_2 \otimes \beta_2\big) + \big(\alpha_1' \otimes \beta_1\big) \cdot \big(\alpha_2 \otimes \beta_2\big)$$

Using the definition of multiplication, what is to be shown is that $(\alpha_1 + \alpha_1')\alpha_2 \otimes \beta_1\beta_2 = \alpha_1\alpha_2 \otimes \beta_1\beta_2 + \alpha_1'\alpha_2 \otimes \beta_1\beta_2$, which is true.

tensorproperty **2.11.14. Proposition.** *(mapping property of tensor product algebras) Let A, B, and S be R-algebras. Algebra homomorphisms from $A \otimes_R B$ to S correspond bijectively to pairs of algebra homomorphisms from A and B to S:*

$$\operatorname{Hom}_R(A \otimes_R B, S) \approx \operatorname{Hom}_R(A, S) \times \operatorname{Hom}_R(B, S).$$

proof. We note first that sending $\alpha \rightsquigarrow \alpha \otimes 1$ defines an R-algebra homomorphism $A \to A \otimes_R B$. This is pretty clear: $(\alpha + \alpha') \otimes 1 = \alpha \otimes 1 + \alpha' \otimes 1$, $(\alpha\alpha') \otimes 1 = (\alpha \otimes 1)(\alpha' \otimes 1)$, and $(r\alpha) \otimes 1 = r(\alpha \otimes 1)$. Similarly, $\beta \rightsquigarrow 1 \otimes \beta$ defines an R-algebra homomorphism $B \to A \otimes_R B$. This being so, an R-algebra homomorphism $A \otimes_R B \to S$ gives us homomorphisms $A \to S$ and $B \to S$ by composition. Conversely, let algebra homomorphisms $A \xrightarrow{f} S$ and $B \xrightarrow{g} S$ be given. We define $A \otimes_R B \xrightarrow{\varphi} S$ by $\varphi(\alpha \otimes \beta) = f(\alpha)g(\beta)$. To show that φ is well-defined, one must verify the bilinear relations. We verify one as example:

$$\varphi(a \otimes b) + \varphi(a' \otimes b) \;=\; f(a)g(b) + f(a')g(b) \;=\; f(a + a')g(b) \;=\; \varphi((a + a') \otimes b)$$

Then φ is a homomorphism because

$$\varphi(a_1 \otimes b_1)\varphi(a_2 \otimes b_2) \;=\; f(a_1)g(b_1)f(a_2)g(b_2) \;=\; f(a_1a_2)g(b_1b_2) \;=\; \varphi(a_1a_2 \otimes b_1b_2) \qquad \square$$

prodaffvar **(2.11.15) products of affine varieties**

Let $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$ be affine varieties, and say that the coordinate rings are presented as $A = \mathbb{C}[x_1, ..., x_m]/(f_1, ..., f_k)$ and $B = \mathbb{C}[y_1, ..., y_n]/(g_1, ..., g_\ell)$. So X and Y are subvarieties of $\mathbb{A}^m$ and $\mathbb{A}^n$, respectively. In the product space $\mathbb{A}^{m+n}$ with coordinates x, y, the product $X \times Y$ of the two varieties is the locus

$$f_1(x) = \cdots = f_k(x) = g_1(y) = \cdots = g_\ell(y) = 0.$$

It is an affine variety whose coordinate ring is $\mathbb{C}[x.y]/(f(x), g(y))$. The algebra $\mathbb{C}[x, y]/\big((f(x), g(y)\big)$ is isomorphic to the tensor product $A \otimes_{\mathbb{C}} B$.

tensorfg **2.11.16. Corollary.** *Let $A = \mathbb{C}[x]/(f)$ and $B = \mathbb{C}[y]/(g)$. Then the product variety $\operatorname{Spec} A \times \operatorname{Spec} B$ is isomorphic to the affine variety $\operatorname{Spec} A \otimes_{\mathbb{C}} B$.* $\square$