Lecture 2

Basic Computational Problems and Their Solution

Our basic geometric objects of study are sets of solutions of polynomial equations in affine or projective space and are called affine or projective algebraic sets. In this lecture, we introduce the geometry-algebra dictionary which relates algebraic sets to ideals of polynomial rings, translating geometric statements into algebraic statements and vice versa. We pay particular attention to computational problems arising from basic geometric questions. And, we begin to explore how Gröbner bases can be used to solve the problems.

2.1 Computational Problems Arising from the Geometry-Algebra Dictionary

Let K be a field, and let $\mathbb{A}^n(K)$ be the **affine n-space** over K,

$$\mathbb{A}^n(K) := \left\{(a_1, \ldots, a_n) \,\middle|\, a_1, \ldots, a_n \in K\right\}.$$

Each polynomial $f \in K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ defines a function

$$f : \mathbb{A}^n(K) \to K\,,\ (a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n);$$

the value $f(a_1, \ldots, a_n)$ is obtained by substituting the a_i for the x_i in f and evaluating the corresponding expression in K. This allows us to talk about the vanishing locus of f in $\mathbb{A}^n(K)$, namely $\mathrm{V}(f) := \{p \in \mathbb{A}^n(K) \mid f(p) = 0\}$. If f is nonconstant, we call $\mathrm{V}(f)$ a **hypersurface** in $\mathbb{A}^n(K)$.

Example 2.1. We visualize the hypersurface $\mathrm{V}\big(y^4 + z^2 - y^2(1-x^2)\big) \subset \mathbb{A}^3(\mathbb{R})$ using `SURF`:

□

A subset $A \subset \mathbb{A}^n(K)$ is an **(affine) algebraic set** if it is the common vanishing locus of finitely many polynomials $f_1, \ldots, f_r \in K[\boldsymbol{x}]$:

$$A = \mathrm{V}(f_1, \ldots, f_r) := \{p \in \mathbb{A}^n(K) \mid f_1(p) = \cdots = f_r(p) = 0\}.$$

We then call $f_1 = 0, \ldots, f_r = 0$ a set of **defining equations** for A. Note that every $K[\boldsymbol{x}]$-linear combination $f = \sum_{i=1}^r g_i f_i$ vanishes on A, too. We may, thus, as well say that A is the vanishing locus $\mathrm{V}(I)$ of the ideal $I = \langle f_1, \ldots, f_r \rangle$ formed by all these combinations:

$$A = \mathrm{V}(I) := \{p \in \mathbb{A}^n(K) \mid f(p) = 0 \text{ for all } f \in I\}.$$

By Hilbert's basis theorem, every ideal I of $K[\boldsymbol{x}]$ is of type $I = \langle f_1, \ldots, f_r \rangle$ for some $f_1, \ldots, f_r \in K[\boldsymbol{x}]$. Its vanishing locus $\mathrm{V}(I) \subset \mathbb{A}^n(K)$ is, thus, an algebraic set (in fact, the vanishing locus of any given subset of $K[\boldsymbol{x}]$ is defined as above and is an algebraic set). We have $\mathrm{V}(0) = \mathbb{A}^n(K)$, $\mathrm{V}(1) = \emptyset$, $\mathrm{V}(I) \cup \mathrm{V}(J) = \mathrm{V}(I \cap J)$, and $\bigcap_\lambda \mathrm{V}(I_\lambda) = \mathrm{V}(\sum_\lambda I_\lambda)$. In particular, the algebraic subsets of $\mathbb{A}^n(K)$ satisfy the axioms for the closed sets of a topology on $\mathbb{A}^n(K)$. This topology is called the **Zariski topology**. If $X \subset \mathbb{A}^n(K)$ is any subset, then $\overline{X}$ will denote its closure in the Zariski topology.

Having associated an algebraic subset of $\mathbb{A}^n(K)$ to each ideal of $K[\boldsymbol{x}]$, we now proceed in the other direction. Namely, if $A \subset \mathbb{A}^n(K)$ is an algebraic set, we define the **vanishing ideal** of A to be

$$\mathrm{I}(A) = \{f \in K[\boldsymbol{x}] \mid f(p) = 0 \text{ for all } p \in A\}.$$

Vanishing ideals have a property not shared by all ideals: they are radical ideals. Here, if I is an ideal of a ring R, its **radical** is the ideal

$$\sqrt{I} := \{f \in R \mid f^m \in I \text{ for some } m \geq 1\},$$

and we call I a **radical ideal** if $I = \sqrt{I}$.

Example 2.2. If $f = c \cdot f_1^{m_1} \cdots f_s^{m_s}$ is the factorization of a nonconstant polynomial $f \in K[\boldsymbol{x}]$ into its irreducible coprime factors $f_i \in K[\boldsymbol{x}]$, then

$$\sqrt{\langle f \rangle} = \langle f_1 \cdots f_s \rangle.$$

The product $f_1 \cdots f_s$ is uniquely determined by f up to nonzero scalars and is called the **square-free part** of f. If all m_i are 1, we say that f is **square-free**. In this case, $\langle f \rangle$ is a radical ideal. □

The correspondence between algebraic sets and ideals is made precise by Hilbert's Nullstellensatz which is fundamental to the geometry-algebra dictionary:

Theorem 2.3 (Hilbert's Nullstellensatz). *Let $A \subset \mathbb{A}^n(K)$ be an algebraic set, and let $I \subset K[\boldsymbol{x}]$ be an ideal. If K is algebraically closed, then*

$$A = \mathrm{V}(I) \implies \mathrm{I}(A) = \sqrt{I}.$$

Corollary 2.4. *If K is algebraically closed, then* I *and* V *define a one-to-one correspondence*

$$\{\textit{algebraic subsets of } \mathbb{A}^n(K)\} \underset{\mathrm{V}}{\overset{\mathrm{I}}{\rightleftarrows}} \{\textit{radical ideals of } K[\boldsymbol{x}]\}.$$

Under this correspondence, the points of $\mathbb{A}^n(K)$ correspond to the maximal ideals of $K[\boldsymbol{x}]$.

See, for instance, Decker and Schreyer (2006) for proofs.

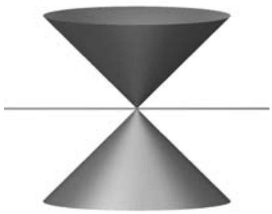
Properties of an ideal I of a ring R can be expressed in terms of the quotient ring R/I. For instance, I is a maximal ideal iff R/I is a field. More generally, I is a prime ideal iff R/I is an integral domain. Finally, I is a radical ideal iff R/I is **reduced** (that is, the only nilpotent element of R/I is zero).

If K is any field, and if $A \subset \mathbb{A}^n(K)$ is an algebraic set, the **coordinate ring** of A is the reduced ring $K[A] := K[\boldsymbol{x}]/\mathrm{I}(A)$. An element of $K[A]$ is, thus, the residue class $\overline{f} = f + \mathrm{I}(A)$ of a polynomial $f \in K[\boldsymbol{x}]$. We may also think of it as a **polynomial function** on A, namely $A \to K$, $p \mapsto f(p)$. The ring $K[A]$ is an integral domain iff A is **irreducible**, that is, iff A cannot be written as the union of two algebraic sets properly contained in A (otherwise, A is **reducible**). If A is irreducible, it is also called an **(affine) variety**. The empty set is not considered to be irreducible.

Example 2.5. (1) The algebraic subset of $\mathbb{A}^3(\mathbb{R})$ with defining equations $x^2z + y^2z - z^3 = x^3 + xy^2 - xz^2 = 0$ is reducible since it decomposes into a cone and a line:

$$\mathrm{V}(x^2z + y^2z - z^3, x^3 + xy^2 - xz^2) = \mathrm{V}(x^2 + y^2 - z^2) \cup \mathrm{V}(x, z)\,.$$

We draw a picture using `SURF`:



(2) The real algebraic set in Example 2.1 is irreducible (even if the picture displayed seems to suggest that it is the union of a surface and a line). See Exercise 2.34 and Lecture 7, Example 7.2. □

If K is any field, and if $I \subset K[\boldsymbol{x}]$ is any ideal, we refer to $K[\boldsymbol{x}]/I$ as an **affine *K*-algebra**, or simply as an **affine ring**. If I is a prime ideal, we refer to $K[\boldsymbol{x}]/I$ as an **affine domain**. Note that every finitely generated K-algebra

S arises as an affine ring. Indeed, choose finitely many generators $s_1, \ldots, s_m$ for S, and represent S as the homomorphic image of the polynomial ring $K[y_1, \ldots, y_m]$ by considering the map $\phi : K[y_1, \ldots, y_m] \twoheadrightarrow S$, $y_i \mapsto s_i$. Then $S \cong K[y_1, \ldots, y_m]/\ker\phi$. If K is algebraically closed, and if S is reduced, then S can be thought of as the coordinate ring of an affine algebraic set. Indeed, if S is reduced, $I := \ker\phi$ is a radical ideal. Hence, $\mathrm{I}(\mathrm{V}(I)) = I$ by the Nullstellensatz, and we may take the algebraic set $\mathrm{V}(I) \subset \mathbb{A}^m(K)$.

Just as affine algebraic sets are given by polynomials, the natural maps between them are also given by polynomials: if $A \subset \mathbb{A}^n(K)$ and $B \subset \mathbb{A}^m(K)$ are algebraic sets, a map $\varphi : A \to B$ is called a **morphism**, or a **polynomial map**, if there exist polynomials $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ such that $\varphi(p) = (f_1(p), \ldots, f_m(p))$ for all $p \in A$. In this case, φ has an algebraic counterpart, namely the K-algebra homomorphism

$$\varphi^* : K[B] \longrightarrow K[A], \;\; y_i + \mathrm{I}(B) \longmapsto f_i + \mathrm{I}(A)\,,$$

where $y_1, \ldots, y_m$ are the coordinates on $\mathbb{A}^m(K)$. If we think of the elements of $K[A]$ and $K[B]$ as polynomial functions on A and on B, then φ^* is obtained by composing a polynomial function on B with φ to obtain a polynomial function on A:

$$\begin{array}{ccc} A & \xrightarrow{\;\;\varphi\;\;} & B \\ & \searrow \quad \swarrow & \\ & K\,. & \end{array}$$

We are now ready to present a list of basic geometric questions and the algebraic problems arising from them. In formulating the problems, we suppose that I and J are ideals of $K[\boldsymbol{x}]$, each given by a finite set of generators. Our basic reference for the results behind our translation from geometry to algebra and vice versa is Decker and Schreyer (2006).

We begin by recalling that $\mathrm{V}(I) \cap \mathrm{V}(J) = \mathrm{V}(I + J)$. Thus, computing the intersection $\mathrm{V}(I) \cap \mathrm{V}(J)$ just amounts to concatenating the given sets of generators for I and J. It is not immediately clear, however, how to deal with the union of algebraic sets.

- Compute the union $\mathrm{V}(I) \cup \mathrm{V}(J)$. Algebraically, find generators for the intersection $I \cap J$.

The Noetherian property of $K[\boldsymbol{x}]$ implies that every (nonempty) algebraic set can be uniquely written as a finite union $A = V_1 \cup \cdots \cup V_s$ of varieties V_i such that $V_i \not\subset V_j$ for $i \neq j$. The V_i are called the **irreducible components** of A.

- Compute the irreducible components of $\mathrm{V}(I)$. Algebraically, compute the minimal associated primes of I.[1] More generally, compute a primary decomposition of I. More specially, compute the radical of I.

[1] The algebraic problem and the geometric problem described here are only equivalent if K is algebraically closed. See Silhol (1978) for a statement that holds over arbitrary fields.

Remark 2.6 (Primary Decomposition). A proper ideal Q of a ring R is said to be **primary** if $f, g \in R$, $fg \in Q$ and $f \notin Q$ implies $g \in \sqrt{Q}$. In this case, $P = \sqrt{Q}$ is a prime ideal, and Q is also said to be a $\boldsymbol{P}$**-primary ideal**. Given any ideal I of R, a **primary decomposition** of I is an expression of I as an intersection of finitely many primary ideals.

Suppose now that R is Noetherian. Then every proper ideal I of R has a primary decomposition. We can always achieve that such a decomposition $I = \bigcap_{i=1}^{r} Q_i$ is **minimal**. That is, the prime ideals $P_i = \sqrt{Q_i}$ are all distinct and none of the Q_i can be left out. In this case, the P_i are uniquely determined by I and are referred to as the **associated primes** of I. If P_i is minimal among $P_1, \dots, P_r$ with respect to inclusion, it is called a **minimal associated prime** of I. The minimal associated primes of I are precisely the minimal prime ideals containing I. Their intersection is equal to $\sqrt{I}$. Every primary ideal occuring in a minimal primary decomposition of I is called a **primary component** of I. The component is said to be **isolated** if its radical is a minimal associated prime of I. Otherwise, it is said to be **embedded**. The isolated components are uniquely determined by I, the others are far from being unique. See Atiyah and MacDonald (1969) for details and proofs. □

Example 2.7. If $f = c \cdot f_1^{m_1} \cdots f_s^{m_s}$ is the factorization of a nonconstant polynomial $f \in K[\boldsymbol{x}]$ into its irreducible coprime factors $f_i \in K[\boldsymbol{x}]$, then

$$\langle f \rangle = \langle f_1^{m_1} \rangle \cap \ldots \cap \langle f_s^{m_s} \rangle$$

is the (unique) minimal primary decomposition. □

The names isolated and embedded come from geometry. If K is algebraically closed, and if I is an ideal of $R = K[\boldsymbol{x}]$, the minimal associated primes of I correspond to the irreducible components of $\mathrm{V}(I)$, while the other associated primes correspond to irreducible algebraic sets contained (or "embedded") in the irreducible components. A more thorough geometric interpretation of primary decomposition requires the language of schemes (see Eisenbud and Harris (2000) for an introduction to schemes). For instance:

Example 2.8. Let $I = \langle xy, y^2 \rangle \subset K[x, y]$. Then the minimal primary decomposition $I = \langle y \rangle \cap \langle x, y^2 \rangle$ exhibits the affine scheme $X = \mathrm{Spec}(K[x, y]/I)$ as the union of the x-axis and an embedded multiple point at the origin. Observe that there are many different ways of writing X as such a union. For instance, $I = \langle y \rangle \cap \langle x, y \rangle^2$ is a minimal primary decomposition as well. □

In these notes, we will, essentially, avoid to talk about schemes.

Remark 2.9 (The Role of the Coefficient Field). Because of Hilbert's Nullstellensatz, algebraic sets are usually studied over an algebraically closed field such as the field of complex numbers. To visualize geometric objects, however, the field of real numbers is chosen. And, to compute examples with exact computer algebra methods, one typically works over a finite field, the field of rational numbers, or a number field (that is, a finite extension of $\mathbb{Q}$ such as $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[t]/\langle t^2-2\rangle$). See also Remark 4.12 in Lecture 4.

In this context, note that if $K \subset L$ is a field extension, and if I is an ideal of $L[\boldsymbol{x}]$ generated by polynomials $f_1, \ldots, f_r$ with coefficients in K, then Buchberger's algorithm applied to $f_1, \ldots, f_r$ yields Gröbner basis elements for I which are also defined over K. For almost all geometric questions discussed in this lecture, this allows us to study the vanishing locus of I in $\mathbb{A}^n(L)$ by computations over K.

Note, however, that a prime ideal of $K[\boldsymbol{x}]$ needs not generate a prime ideal of $L[\boldsymbol{x}]$. From a computational point of view, this is reflected by the fact that for computing a primary decomposition, algorithms for polynomial factorization are needed in addition to Gröbner basis techniques (see Lecture 7). In contrast to Buchberger's algorithm, the algorithms for polynomial factorization and their results are highly sensitive to the ground field.

With respect to dimension (see Remark 2.10 below), we point out that if Q is a primary ideal of $K[\boldsymbol{x}]$ with radical P, then the associated primes of $QL[\boldsymbol{x}]$ are precisely the prime ideals of $L[\boldsymbol{x}]$ intersecting $K[\boldsymbol{x}]$ in P and having the same dimension as P (see Zariski and Samuel (1975–1976), Vol II, Chapter VII, §11). See also Section 6.1.1 in Lecture 6.

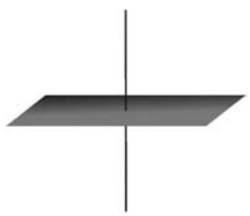
With respect to radicals, note that if K is a perfect field, and if $I \subset K[\boldsymbol{x}]$ is a radical ideal, then also $IL[\boldsymbol{x}]$ is a radical ideal (see again Zariski and Samuel (1975–1976), Vol II, Chapter VII, §11). Recall that finite fields, fields of characteristic zero, and algebraically closed fields are perfect. □

In continuing our problem list, we now present problems for which the geometric interpretation of the algebraic operations under consideration relies on Hilbert's Nullstellensatz. To emphasize this point, we mark such a problem by the square ■ instead of the bullet •.

Convention. *For each problem marked by a square, let* $\overline{K}$ *be an algebraically closed extension field of* K. *If* $I \subset K[\boldsymbol{x}]$ *is an ideal, redefine* $\mathrm{V}(I)$ *to be the vanishing locus of* I *in* $\mathbb{A}^n := \mathbb{A}^n(\overline{K})$. *If* $A = \mathrm{V}(I) \subset \mathbb{A}^n$, *then* $\mathrm{I}(A)$ *is the vanishing ideal of* A *in* $\overline{K}[\boldsymbol{x}]$ *and* $\overline{K}[A] = \overline{K}[\boldsymbol{x}]/\mathrm{I}(A)$ *is its coordinate ring.* □

In what follows, if not otherwise mentioned, I and J are again ideals of $K[\boldsymbol{x}]$, each given by a finite set of generators.

The difference $\mathrm{V}(I) \setminus \mathrm{V}(J)$ need not be an algebraic set. That is, it may not be Zariski closed. As an example, consider the punctured plane obtained by removing the z-axis from the union of the xy-plane and the z-axis.



- Compute the Zariski closure of $\mathrm{V}(I) \setminus \mathrm{V}(J)$. That is, compute the union of those irreducible components of $\mathrm{V}(I)$ which are not contained in $\mathrm{V}(J)$. Algebraically, if I is radical, find generators for the **ideal quotient** of I by J which is defined to be the ideal

$$I : J = \left\{ f \in K[\boldsymbol{x}] \;\middle|\; fJ \subset I \right\}.$$

  If I is not necessarily radical, find generators for the **saturation** of I with respect to J, that is, for the ideal

$$\begin{aligned} I : J^\infty &= \left\{ f \in R \;\middle|\; fJ^m \subset I \text{ for some } m \geq 1 \right\} \\ &= \bigcup_{m=1}^{\infty} (I : J^m). \end{aligned}$$

- **Solvability and ideal membership.** Decide whether $\mathrm{V}(I)$ is empty. Algebraically, decide whether $1 \in I$. More generally, given any polynomial $f \in K[\boldsymbol{x}]$, decide whether $f \in I$.
- **Radical membership.** Decide whether a given polynomial $f \in K[\boldsymbol{x}]$ vanishes on $\mathrm{V}(I)$. Algebraically, decide whether f is contained in $\sqrt{I}$.
- Compute the **dimension** of $\mathrm{V}(I)$. Algebraically, compute the Krull dimension of the affine ring $K[\boldsymbol{x}]/I$.[2]

The definition of the Krull dimension of a ring is somewhat reminiscent of the fact that the dimension of a vector space over a field is the length of the longest chain of proper subspaces:

Remark 2.10 (Dimension and Codimension). The **Krull dimension** (or simply the **dimension**) of a ring R, denoted $\dim R$, is the supremum of the lengths d of chains

$$P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_d$$

of prime ideals of R. If $I \subsetneq R$ is a proper ideal, its **dimension**, written $\dim I$, is defined to be $\dim R/I$. The **codimension** of I, written $\operatorname{codim} I$, is defined as follows. If I is a prime ideal, $\operatorname{codim} I$ is the supremum of lengths of chains of prime ideals with largest ideal $P_d = I$. If I is not necessarily prime, $\operatorname{codim} I$ is the minimum of the codimensions of the prime ideals containing I.

It follows from the definitions that $\dim I + \operatorname{codim} I \leq \dim R$. In general, the inequality may well be strict (see Lecture 9, Example 9.31). Equality holds if R is an affine domain over a field K. In fact, in this case, $\dim R$ equals the transcendence degree of the quotient field of R over K, and this number is the common length of all maximal chains of prime ideals of R (a chain of prime ideals of R is maximal if it cannot be extended to a chain of greater length by inserting a further prime ideal). In particular, $\dim \mathbb{A}^n = \dim K[\boldsymbol{x}] = n$.

[2] The **dimension** of $A = \mathrm{V}(I) \subset \mathbb{A}^n$, written $\dim A$, is defined to be the Krull dimension of the coordinate ring $\overline{K}[A]$. It follows from what we said in Remark 2.9 that $\overline{K}[A]$ and $K[\boldsymbol{x}]/I$ have the same Krull dimension.

An important result in dimension theory, proved using Nakayama's lemma, is **Krull's principal ideal theorem** which asserts that if $I = \langle f \rangle \subsetneq R$ is a principal ideal of a Noetherian ring R and P is a minimal associated prime of I, then $\operatorname{codim} P \leq 1$. If f is a nonzerodivisor of R, each minimal associated prime of $\langle f \rangle$ has precisely codimension 1. In particular, $\dim K[\boldsymbol{x}]/\langle f \rangle = n - 1$ for each nonconstant $f \in K[\boldsymbol{x}]$. In geometric terms, the dimension (of each irreducible component) of a hypersurface $\mathrm{V}(f) \subset \mathbb{A}^n$ is $n - 1$.

If $I \subsetneq K[\boldsymbol{x}]$ is any proper ideal, then according to the definition of dimension, $\dim K[\boldsymbol{x}]/I$ is the maximum dimension of a minimal associated prime of I. Geometrically, the dimension of $\mathrm{V}(I)$ in $\mathbb{A}^n$ is the maximum dimension of an irreducible component of $\mathrm{V}(I)$.

See Eisenbud (1995) for details and proofs. □

- Compute the Zariski closure of the image of $\mathrm{V}(I)$ under the projection $\mathbb{A}^n \to \mathbb{A}^{n-k}$ which sends $(a_1, \dots, a_n)$ to $(a_{k+1}, \dots, a_n)$. Algebraically, eliminate the first k variables from I, that is, compute the ***k*th elimination ideal** $I_k = I \cap K[x_{k+1}, \dots, x_n]$.

- More generally, compute the Zariski closure of the image of $\mathrm{V}(I)$ under an arbitrary morphism $\varphi : \mathrm{V}(I) \to \mathbb{A}^m$. Algebraically, if φ is given by polynomials $f_1, \dots, f_m \in K[x_1, \dots, x_n]$, and if $y_1, \dots, y_m$ are the coordinates on $\mathbb{A}^m$, consider the ideal

$$J = IK[\boldsymbol{x}, \boldsymbol{y}] + \big\langle f_1 - y_1, \dots, f_m - y_m \big\rangle \subset K[\boldsymbol{x}, \boldsymbol{y}]\,.$$

Then J defines the graph of φ in $\mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$, and

$$\overline{\varphi(\mathrm{V}(I))} = \mathrm{V}(J \cap K[\boldsymbol{y}])\,.$$

Remark 2.11. If K is not algebraically closed, and if V_K refers to taking vanishing loci in $\mathbb{A}^n(K)$ and $\mathbb{A}^m(K)$, the Zariski closure of $\varphi(\mathrm{V}_K(I))$ in $\mathbb{A}^m(K)$ may be strictly contained in $\mathrm{V}_K(J \cap K[\boldsymbol{y}])$. Equality holds, however, if $\mathrm{V}_K(I)$ is Zariski dense in the vanishing locus of I in the affine n-space over the algebraic closure of K. Note that if K is infinite, then this condition is fulfilled for $\mathbb{A}^n(K) = \mathrm{V}_K(0)$. Thus, the above applies, in particular, to polynomial parametrizations over infinite fields. Here, a **polynomial parametrization** of an algebraic set $B \subset \mathbb{A}^m(K)$ is a morphism $\varphi : \mathbb{A}^n(K) \to B$ such that $\overline{\varphi(\mathbb{A}^n(K))} = B$. See Decker and Schreyer (2006) for rational parametrizations (and for proofs). □

If a parametrization $\varphi : \mathbb{A}^n(K) \to B$ exists, it allows one to study B in terms of a simpler variety (namely $\mathbb{A}^n(K)$). A more general concept in this direction is normalization. In these notes, we briefly discuss normalization from a computational point of view, addressing the more experienced reader.

- Find the normalization $\widetilde{\mathrm{V}(I)} \to \mathrm{V}(I)$. Algebraically, if I is a radical ideal, find for each (minimal) associated prime P of I the **normalization** of the affine domain $K[\boldsymbol{x}]/P$. That is, find the integral closure of $K[\boldsymbol{x}]/P$ in the quotient field of $K[\boldsymbol{x}]/P$. More precisely, represent the integral closure as an affine domain. As we will see in Lecture 7, this is possible due to a finiteness result of Emmy Noether.

- Check whether $\mathrm{V}(I)$ is smooth. If not, study the behavior of $\mathrm{V}(I)$ at its singular points.

Remark 2.12 (Smooth and Singular Points). Let $A \subset \mathbb{A}^n = \mathbb{A}^n(\overline{K})$ be an algebraic set, and let $p = (a_1, \dots, a_n) \in A$ be a point. We say that A is **smooth** (or **nonsingular**) **at p** if the tangent space $\mathrm{T}_p A$ to A at p has the expected dimension, that is, if

$$\dim \mathrm{T}_p A = \dim_p A\,.$$

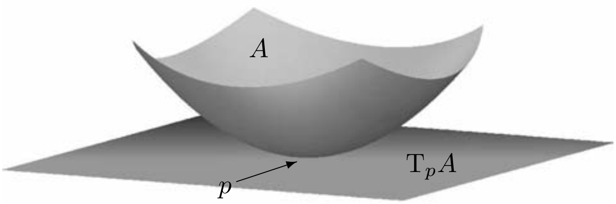
Here, $\dim_p A$ denotes the **dimension of A at p**, which is defined to be the maximum dimension of the irreducible components of A through p. Further, the **tangent space to A at p** is the linear variety

$$\mathrm{T}_p A = \mathrm{V}(d_p f \mid f \in \mathrm{I}(A)) \subset \mathbb{A}^n\,,$$

where for each $f \in \overline{K}[\boldsymbol{x}]$, we set

$$d_p f = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(p)(x_i - a_i) \in \overline{K}[\boldsymbol{x}]\,.$$

This definition extends the concept of tangent spaces from calculus (the partial derivatives are defined in a purely formal way, mimicking the usual rules of differentiation). Note that $\mathrm{T}_p A$ is the union of all lines $L = \{p + tv \mid t \in \overline{K}\}$, $v \in \mathbb{A}^n$, such that all polynomials $f(p + tv) \in \overline{K}[t]$, $f \in \mathrm{I}(A)$, vanish with multiplicity ≥ 2 at 0.



If we regard $\mathrm{T}_p\mathbb{A}^n = \mathbb{A}^n$ as an abstract vector space with origin at p and coordinates $X_j = x_j - a_j$, then $\mathrm{T}_p A$ is a linear subspace of $\mathrm{T}_p\mathbb{A}^n$. In fact, if $\mathrm{I}(A) = \langle f_1, \dots, f_r \rangle \subset \overline{K}[\boldsymbol{x}]$, then $\mathrm{T}_p A$ is the kernel of the linear map $\mathbb{A}^n \to \mathbb{A}^r$ defined by the **Jacobian matrix** at p,

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1}(p) & \dots & \frac{\partial f_1}{\partial x_n}(p) \\ \vdots & & \vdots \\ \frac{\partial f_r}{\partial x_1}(p) & \dots & \frac{\partial f_r}{\partial x_n}(p) \end{pmatrix}.$$

Note that the definition given above treats T_pA externally, that is, in terms of the ambient space $\mathbb{A}^n$. For an intrinsic definition, consider the **local ring of A at p**,

$$\mathcal{O}_{A,p} = \left\{ \frac{f}{g} \;\middle|\; f, g \in \overline{K}[A],\; g(p) \neq 0 \right\}$$

(formally, this is the localization of $\overline{K}[A]$ at the maximal ideal of all polynomial functions on A vanishing at p). Then $\overline{K}[A] \ni \overline{f} = f + \mathrm{I}(A) \mapsto \mathrm{d}_p f|_{\mathrm{T}_pA}$ induces a natural isomorphism of $\overline{K}$-vector spaces

$$\mathfrak{m}_{A,p}/\mathfrak{m}_{A,p}^2 \xrightarrow{\cong} (\mathrm{T}_pA)^* = \mathrm{Hom}_{\overline{K}}\big(\mathrm{T}_pA, \overline{K}\big)\,,$$

where $\mathfrak{m}_{A,p}$ denotes the unique maximal ideal of $\mathcal{O}_{A,p}$,

$$\mathfrak{m}_{A,p} = \left\{ \frac{f}{g} \;\middle|\; f, g \in \overline{K}[A],\; g(p) \neq 0,\; f(p) = 0 \right\}.$$

On the other hand, making use of the fact that every maximal chain of prime ideals of an affine domain R has length $\dim R$, one can show that

$$\dim_p A = \dim \mathcal{O}_{A,p}\,,$$

and the condition on A to be smooth at p may be expressed intrinsically as

$$\dim_{\overline{K}} \mathfrak{m}_{A,p}/\mathfrak{m}_{A,p}^2 = \dim \mathcal{O}_{A,p}\,.$$

If this holds, we refer to $\mathcal{O}_{A,p}$ as a **regular local ring** (it follows from Krull's principal ideal theorem that we always have $\dim_{\overline{K}} \mathfrak{m}_{A,p}/\mathfrak{m}_{A,p}^2 \geq \dim \mathcal{O}_{A,p}$).

If A is smooth at p, we also say that p is a **smooth** (or **nonsingular**) **point** of A. Otherwise, we say that A is **singular at** p, or that p is a **singular point** of A, or that p is a **singularity** of A. We refer to the set A_{sing} of all singular points of A as the **singular locus** of A. If $A = V_1 \cup \cdots \cup V_s$ is the decomposition of A into its irreducible components, then

$$A_{\mathrm{sing}} = \bigcup_{i \neq j} (V_i \cap V_j) \cup \bigcup_i (V_i)_{\mathrm{sing}}.$$

Starting from this formula, one can show that A_{sing} is an algebraic subset of A such that A and A_{sing} have no irreducible component in common. If A_{sing} is empty, then A is **smooth**. Otherwise, A is **singular**.

See, for instance, Decker and Schreyer (2006) for details and proofs. □

How to compute the singular locus will be discussed in Section 2.2 later in this lecture.

Remark 2.13 (Local Properties). Smoothness of A at p is a **local property** in the sense that it remains unchanged if we replace A by any neighborhood of p in A. Algebraically, this is reflected by the fact that smoothness at

p is expressed in terms of the local ring $\mathcal{O}_{A,p}$. If p is the origin, we may write $\mathcal{O}_{A,p}$ as the quotient $\overline{K}[\boldsymbol{x}]_{\langle \boldsymbol{x}\rangle}/\mathrm{I}(A)\cdot \overline{K}[\boldsymbol{x}]_{\langle \boldsymbol{x}\rangle}$. Here, if K is any field, we set

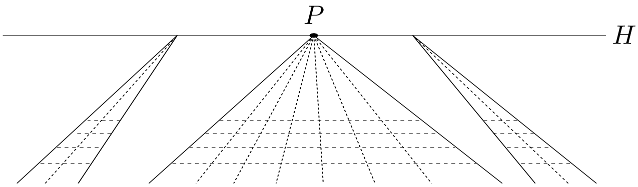
$$K[\boldsymbol{x}]_{\langle \boldsymbol{x}\rangle} = \left\{ \frac{f}{g} \;\middle|\; f,g \in K[\boldsymbol{x}],\ g \notin \langle \boldsymbol{x}\rangle \right\}.$$

From a computational point of view, we may formulate problems analogous to those discussed so far in this lecture for ideals of $K[\boldsymbol{x}]_{\langle \boldsymbol{x}\rangle}$ instead of $K[\boldsymbol{x}]$. In Lecture 9, we will give examples of how to interpret these problems geometrically. □

We now turn from the affine to the projective case.

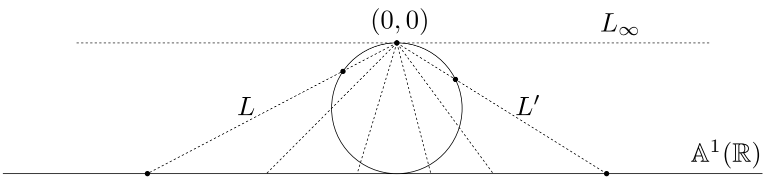
In the affine plane, two lines either meet in a point, or are parallel. In contrast, the projective plane is constructed such that two lines always meet in a point. This is one example of how geometric statements become simpler if we pass from affine to projective geometry.

Historically, the idea of the projective plane goes back to renaissance painters who introduced vanishing points on the horizon to allow for perspective drawing:



We think of a vanishing point (or "point at infinity") as the meeting point of a class of parallel lines in the affine plane $\mathbb{A}^2(\mathbb{R})$*. The projective plane* $\mathbb{P}^2(\mathbb{R})$ *is obtained from* $\mathbb{A}^2(\mathbb{R})$ *by adding one point at infinity for each such class. A projective line in* $\mathbb{P}^2(\mathbb{R})$ *is a line* $L \subset \mathbb{A}^2(\mathbb{R})$ *together with the point at infinity in which the lines parallel to* L *meet. Further, the horizon, that is, the set of all points at infinity, is a projective line in* $\mathbb{P}^2(\mathbb{R})$*, the* **line at infinity**.

To formalize the idea of the projective plane, we observe that each class of parallel lines in $\mathbb{A}^2(\mathbb{R})$ *is represented by a unique line through the origin of* $\mathbb{A}^2(\mathbb{R})$*. This fits nicely with stereographic projection which allows one to identify the set of lines through the projection center with the real line together with a point at infinity:*



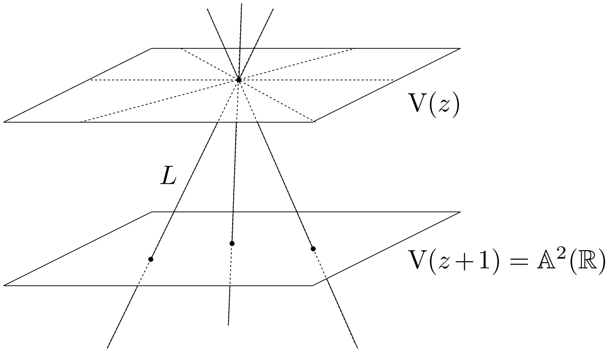
If we define the abstract **projective line** *to be the set*

$$\mathbb{P}^1(\mathbb{R}) = \{\textit{lines through the origin in } \mathbb{A}^2(\mathbb{R})\}$$

and think of it as the line at infinity, we may write

$$\mathbb{P}^2(\mathbb{R}) = \mathbb{A}^2(\mathbb{R}) \cup \mathbb{P}^1(\mathbb{R}).$$

Formally, the definition of $\mathbb{P}^2(\mathbb{R})$ *is completely analogous to the definition of* $\mathbb{P}^1(\mathbb{R})$*. To see this, we identify* $\mathbb{A}^2(\mathbb{R})$ *with the plane* $\mathrm{V}(z+1) \subset \mathbb{A}^3(\mathbb{R})$ *and* $\mathbb{P}^1(\mathbb{R})$ *with the set of lines in the xy-plane* $\mathrm{V}(z)$ *through the origin. Then we may regard* $\mathbb{P}^2(\mathbb{R})$ *as the set of all lines in* $\mathbb{A}^3(\mathbb{R})$ *through the origin:*



Definition 2.14. *If* K *is any field, the* **projective n-space over K** *is defined to be the set*

$$\mathbb{P}^n(K) = \{\textit{lines through the origin in } \mathbb{A}^{n+1}(K)\}. \qquad \square$$

Each line L through the origin $\mathbf{0} \in \mathbb{A}^{n+1}(K)$ may be represented by a point $(a_0, \dots, a_n) \in L \setminus \{\mathbf{0}\}$. We write $(a_0 : \dots : a_n)$ for the corresponding point of $\mathbb{P}^n(K)$ and call $a_0, \dots, a_n$ a set of **homogeneous coordinates** for this point. Here, the colons indicate that $(a_0, \dots, a_n)$ is determined up to a nonzero scalar multiple only. This representation allows us to think of $\mathbb{P}^n(K)$ as the quotient of $\mathbb{A}^{n+1}(K) \setminus \{\mathbf{0}\}$ modulo the equivalence relation defined by $(a_0, \dots, a_n) \sim (b_0, \dots, b_n)$ iff $(a_0, \dots, a_n) = \lambda(b_0, \dots, b_n)$ for some nonzero scalar λ.

Given a polynomial $f \in K[x_0, \dots, x_n]$, the value $f(a_0, \dots, a_n)$ depends on the choice of representative of the point $p = (a_0 : \dots : a_n) \in \mathbb{P}^n(K)$ and can therefore not be called the value of f at p. Note, however, that if f is **homogeneous**, then $f(\lambda x_0, \dots, \lambda x_n) = \lambda^{\deg(f)} f(x_0, \dots, x_n)$ for all nonzero scalars λ and, thus,

$$f(a_0, \dots, a_n) = 0 \iff \forall\, \lambda \in K \setminus \{0\} : \ f(\lambda a_0, \dots, \lambda a_n) = 0.$$

As a consequence, f has a well-defined vanishing locus $\mathrm{V}(f)$ in $\mathbb{P}^n(K)$. If f is nonconstant, we refer to $\mathrm{V}(f)$ as a **hypersurface** in $\mathbb{P}^n(K)$.

A subset $A \subset \mathbb{P}^n(K)$ is a **(projective) algebraic set** if it is the common vanishing locus of finitely many homogeneous polynomials $f_1, \dots, f_r \in K[x_0, \dots, x_n]$:

$$A = \mathrm{V}(f_1, \dots, f_r) := \left\{ p \in \mathbb{A}^n(K) \;\middle|\; f_1(p) = \dots = f_r(p) = 0 \right\}.$$

We then call $f_1 = 0, \dots, f_r = 0$ a set of **defining equations** for A.

If f is a homogeneous linear polynomial, we may identify the algebraic set $\mathrm{V}(f) \subset \mathbb{P}^n(K)$ with $\mathbb{P}^{n-1}(K)$ and its complement $\mathbb{P}^n(K) \setminus \mathrm{V}(f)$ with $\mathbb{A}^n(K)$:

$$\mathbb{P}^n(K) = \mathbb{A}^n(K) \cup \mathbb{P}^{n-1}(K).$$

We refer to $\mathbb{P}^n(K) \setminus \mathrm{V}(f)$ as an **affine chart** of $\mathbb{P}^n$ and to $\mathbb{P}^{n-1}(K)$ as the corresponding **hyperplane at infinity**. For instance, if $f = x_i$, we identify

$$(a_0 : \dots : a_n) \longleftrightarrow \begin{cases} \left(\frac{a_0}{a_i}, \dots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \dots \frac{a_n}{a_i}\right) \in \mathbb{A}^n(K), & \text{if } a_i \neq 0, \\ (a_0 : \ldots : a_{i-1} : a_{i+1} : \ldots : a_n) \in \mathbb{P}^{n-1}(K), & \text{if } a_i = 0. \end{cases}$$

Remark 2.15 (The Projective Geometry-Algebra Dictionary). The geometry-algebra dictionary relates projective algebraic subsets of projective n-space $\mathbb{P}^n(K)$ to homogeneous ideals of $K[x_0, \dots, x_n]$ via maps I and V essentially defined as in the affine case. If K is algebraically closed, the projective version of the Nullstellensatz implies that there is a one-to-one correspondence

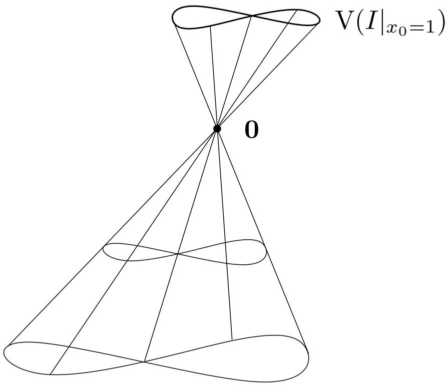
$$\left\{ \begin{array}{c} \text{projective algebraic} \\ \text{subsets of } \mathbb{P}^n(K) \end{array} \right\} \begin{array}{c} \xrightarrow{\ \mathrm{I}\ } \\ \xleftarrow[\ \mathrm{V}\ ]{} \end{array} \left\{ \begin{array}{c} \text{homogeneous radical ideals} \\ \text{of } K[x_0, \dots, x_n] \\ \text{not equal to } \langle x_0, \dots, x_n \rangle \end{array} \right\}.$$

Since $\langle x_0, \dots, x_n \rangle$ does not appear in this correspondence, it is called the **irrelevant ideal**.

The **homogeneous coordinate ring** of a projective algebraic subset $A \subset \mathbb{P}^n(K)$ is the reduced graded K-algebra

$$K[A] := K[x_0, \dots, x_n]/\mathrm{I}(A).$$

In terms of affine algebraic sets, this is the coordinate ring of the affine cone over A. Here, if $A \subset \mathbb{P}^n(K)$ is the vanishing locus of a homogeneous ideal $I \subset K[x_0, \dots, x_n]$, the **affine cone** over A is the vanishing locus of I in $\mathbb{A}^{n+1}(K)$:



In the projective case, we may ask questions analogous to those formulated in the affine case. For most of these questions, we consider as in the affine case an algebraically closed extension field $\overline{K}$ of K and redefine $V(I)$ to be the vanishing locus of I in $\mathbb{P}^n := \mathbb{P}^n(\overline{K})$. Further, if $A = V(I) \subset \mathbb{P}^n$, then $I(A)$ is the vanishing ideal of A in $\overline{K}[x_0, \ldots, x_n]$ and $\overline{K}[x_0, \ldots, x_n]/I(A)$ its homogeneous coordinate ring. The computational answers given to our questions in what follows are valid in the projective case as well. Indeed, Buchberger's algorithm applied to homogeneous polynomials yields Gröbner basis elements which are homogeneous, too.

The ideals we are concerned with in explicit computations are often not radical. For instance, if $A = V(I) \subset \mathbb{P}^n(K)$ is a (nonempty) projective algebraic set, given by a homogeneous ideal $I \subset K[x_0, \ldots, x_n]$, then I might have an embedded $\langle x_0, \ldots, x_n \rangle$-primary component (which depends on the choice of a primary decomposition of I). Such a component defines a multiple structure on the vertex of the affine cone over A; it does not contribute to defining A itself. Computing the saturation $I : \langle x_0, \ldots, x_n \rangle^\infty$, we get a simpler ideal defining A. This may not yet be a radical ideal, but at least it does not have an $\langle x_0, \ldots, x_n \rangle$-primary component.

Though we will not need this in what follows, let us mention that there is a one-to-one correspondence between homogeneous ideals I of $K[x_0, \ldots, x_n]$ satisfying $I = I : \langle x_0, \ldots, x_n \rangle^\infty$ and closed subschemes of $\mathbb{P}^n(K)$ (see Hartshorne (1977), Chapter II, Exercise 5.10). □

One further problem arises from adding points at infinity to affine algebraic sets. To describe this problem, we identify $\mathbb{A}^n(K)$ with the affine chart $\mathbb{P}^n(K) \setminus V(x_0)$ of $\mathbb{P}^n(K)$, referring to its complement $V(x_0)$ in $\mathbb{P}^n(K)$ as the **hyperplane at infinity**. Given an affine algebraic set $A \subset \mathbb{A}^n(K)$, we are interested in the **projective closure** of A, which is defined to be the smallest projective algebraic subset of $\mathbb{P}^n(K)$ containing A.

- Given generators for an ideal I of $K[x_1,\ldots,x_n]$, compute the projective closure of the affine algebraic set defined by I. Algebraically, compute the **homogenization** I^{hom} of I with respect to the slack variable x_0.

Here, $I^{\mathrm{hom}} \subset K[x_0,\ldots,x_n]$ is the ideal generated by the elements

$$f^{\mathrm{hom}} := x_0^{\deg f} \cdot f\left(\frac{x_1}{x_0},\ldots,\frac{x_n}{x_0}\right),$$

$f \in I$ (we refer to f^{hom} as the **homogenization of f** with respect to x_0).

2.2 Basic Applications of Gröbner Bases

All problems posed in the preceeding section can be settled using Gröbner basis techniques (for radicals and primary decomposition, additional techniques are needed). How to compute in the local ring $K[\boldsymbol{x}]_{\langle \boldsymbol{x}\rangle}$, for instance, will be explained in Lecture 9. For radicals and primary decomposition, we refer to Lecture 7. In the same lecture, we will discuss normalization. Solutions to the other problems will be provided in this section (see Lecture 3, Section 3.6 for a detailed discussion of the corresponding `SINGULAR` commands).

To begin with, observe that Remark 1.40 settles the **ideal membership problem**. More generally, it settles the submodule membership problem:

Problem 2.16 (Submodule Membership). Given a free $K[\boldsymbol{x}]$-module F with a fixed basis and nonzero elements $f,\ f_1,\ldots,f_r \in F$, decide whether

$$f \in I := \langle f_1,\ldots,f_r\rangle \subset F.$$

[If so, express f as a $K[\boldsymbol{x}]$-linear combination $f = g_1f_1 + \ldots + g_rf_r$.]

Solution. Compute a Gröbner basis $f_1,\ldots,f_r,f_{r+1},\ldots,f_{r'}$ for I using Buchberger's algorithm and a standard expression for f in terms of $f_1,\ldots,f_{r'}$ with remainder h. If $h = 0$, then $f \in I$. [In this case, for $k = r',\ldots,r+1$, successively do the following: in the standard expression, replace f_k by the expression for f_k in terms of $f_1,\ldots,f_{k-1}$ given by the syzygy leading to f_k in Buchberger's test (this requires the relevant syzygies to be stored during Buchberger's test).] □

Example 2.17. Consider the lexicographic Gröbner basis

$$f_1 = xy - y,\quad f_2 = -x + y^2,\quad f_3 = y^3 - y$$

for the ideal $I = \langle f_1, f_2\rangle$ of $K[x,y]$ computed in Lecture 1, Example 1.46. Let

$$f = x^2y - xy + y^3 - y.$$

Then $f = x \cdot f_1 + 1 \cdot f_3$ is a standard expression for f in terms of f_1, f_2, f_3 with remainder 0, so $f \in I$. Reconsidering the computation in Example 1.46, we see that we have to substitute $y \cdot f_2 + 1 \cdot f_1$ for f_3 in the standard expression. This gives

$$f = (x+1) \cdot f_1 + y \cdot f_2. \qquad \square$$

As already explained, **solvability** can be decided via ideal membership. Similarly for **radical membership**: if an ideal $I \subset K[\boldsymbol{x}]$ and a polynomial $f \in K[\boldsymbol{x}]$ are given, then

$$f \in \sqrt{I} \iff 1 \in \langle I, tf - 1 \rangle \subset K[\boldsymbol{x}, t]\,,$$

where t is a slack variable.

One way of computing **intersections of ideals** and **ideal quotients** also asks for involving rings with extra variables (see Cox, Little, and O'Shea (1997)). Alternatively, proceed as follows. Given ideals $I = \langle f_1, \dots, f_r \rangle$ and $J = \langle g_1, \dots, g_s \rangle$ of $K[\boldsymbol{x}]$, compute the syzygies on the columns of the matrix

$$\begin{pmatrix} 1 & f_1 & \dots & f_r & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 & g_1 & \dots & g_s \end{pmatrix}.$$

The entries of the first row of the resulting syzygy matrix generate $I \cap J$. In the same way, we obtain a generating set for the ideal quotient

$$I : J = \big\{ f \in K[\boldsymbol{x}] \,\big|\, fJ \subset I \big\}$$

from the matrix

$$\begin{pmatrix} g_1 & f_1 & \dots & f_r & 0 & \dots & & & \dots & 0 \\ g_2 & 0 & \dots & 0 & f_1 & \dots & f_r & 0 & \dots & 0 \\ \vdots & & & & & \ddots & & & & \\ g_s & 0 & \dots & & & \dots & 0 & f_1 & \dots & f_r \end{pmatrix}.$$

Note that the **intersection of** two **submodules** I, J of a free $K[\boldsymbol{x}]$-module F and their **submodule quotient** $I : J = \big\{ f \in K[\boldsymbol{x}] \,\big|\, fJ \subset I \big\} \subset K[\boldsymbol{x}]$ are obtained by similar recipes.

Since $I : J^m = (I : J^{m-1}) : J$, the **saturation**

$$I : J^\infty = \bigcup_{m=1}^{\infty} (I : J^m)$$

can be computed by iteration. Indeed, the ascending chain

$$I : J \subset I : J^2 \subset \dots \subset I : J^m \subset \dots$$

is eventually stationary since $K[\boldsymbol{x}]$ is Noetherian.

If $K[\boldsymbol{x}]/I$ is a graded affine ring, we already know that its **Hilbert series** $H_{K[\boldsymbol{x}]/I}(t)$ and its **Hilbert polynomial** $P_{K[\boldsymbol{x}]/I}$ can be computed via Gröbner bases (see Macaulay's Theorem 1.35 and Remark 1.36 in Lecture 1). This gives us one way of computing the dimension of homogeneous ideals. Indeed,

$$\dim K[\boldsymbol{x}]/I = \deg P_{K[\boldsymbol{x}]/I} + 1 \tag{2.1}$$

(see Bruns and Herzog (1993) or Eisenbud (1995)).

Remark-Definition 2.18. In algebraic geometry, we make use of the Hilbert polynomial to define or rediscover **numerical invariants** of a projective algebraic set and its embedding. For this purpose, if $A \subset \mathbb{P}^n$ is a projective algebraic set with homogeneous coordinate ring $\overline{K}[A] = \overline{K}[x_0, \dots, x_n]/\mathrm{I}(A)$, we define the **Hilbert polynomial of** $\boldsymbol{A}$ to be the polynomial $P_A(t) = P_{\overline{K}[A]}(t)$. If d is the degree of $P_A(t)$, the Krull dimension of $\overline{K}[A]$ equals $d+1$ (see equation (2.1) above). In geometric terms, the dimension of the affine cone over A is $d+1$. The **dimension** of A itself is defined to be $\dim A = d$. The **degree** of A is defined to be $d!$ times the leading coefficient of $P_A(t)$. Geometrically, the degree of A is the number of points in which A meets a sufficiently general linear subspace of $\mathbb{P}^n$ of complementary dimension $n-d$ (see, for instance, Decker and Schreyer (2006)). Further, the **arithmetic genus** of A is defined to be $p_a(A) = (-1)^d\big(P_A(0) - 1\big)$. □

Example 2.19. The Hilbert polynomial of the twisted cubic curve $C \subset \mathbb{P}^3$ is $P_C(t) = 3t + 1$ (see Lecture 1, Example 1.25). In particular, C has dimension 1 and degree 3. This justifies the name cubic curve. Moreover, C has arithmetic genus 0. □

In Lecture 6, Section 6.1.1, we will discuss an alternative way of computing dimension which applies to nonhomogeneous ideals, too. As for the Hilbert polynomial, Gröbner bases are used to reduce the general problem to a problem concerning monomial ideals. The `SINGULAR` command `dim` is based on this approach.

We now turn to the computation of the singular locus of an algebraic set. For this, we need the following notation. If $I \subsetneq K[\boldsymbol{x}]$ is a proper ideal, we say that I has **pure codimension** c if all its minimal associated primes have codimension c. Also, I is called **unmixed** if it has no embedded components. In many cases of interest, the following criterion allows one to compute the singular locus (and to check that the given ideal is radical):

Theorem 2.20 (Jacobian Criterion). *Let K be a field with algebraically closed extension field $\overline{K}$, let $I = \langle f_1, \dots, f_r \rangle \subsetneq K[\boldsymbol{x}]$ be an ideal of pure codimension c, and let $A = \mathrm{V}(I)$ be the vanishing locus of I in $\mathbb{A}^n = \mathbb{A}^n(\overline{K})$. If $J \subset K[\boldsymbol{x}]$ is the ideal generated by the $c \times c$ minors of the Jacobian matrix*

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_r}{\partial x_1} & \cdots & \frac{\partial f_r}{\partial x_n} \end{pmatrix},$$

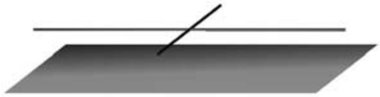
then:

(1) *The vanishing locus of $J + I$ in $\mathbb{A}^n$ contains the singular locus A_{sing}.*
(2) *If $1 \in J + I$, then A is smooth and $I\,\overline{K}[\boldsymbol{x}] = \mathrm{I}(A)$.*
(3) *If $1 \notin J + I$, suppose in addition that I is unmixed (altogether, we ask that all associated primes of I are minimal and of codimension c). If $\mathrm{codim}(J+I) > \mathrm{codim}\, I$, then $\mathrm{V}(J+I) = A_{\mathrm{sing}}$ and $I\,\overline{K}[\boldsymbol{x}] = \mathrm{I}(A)$.*

See Decker and Schreyer (2006), Chapter 4 for a proof and Eisenbud (1995), Section 16.6 and Exercise 11.10 for an algebraic version of the criterion.

The following examples show that the assumptions made in the Jacobian criterion are really needed (in each example, J denotes the respective ideal defined in the criterion).

Example 2.21. (1) Let $I \subset K[x,y,z]$ be the ideal generated by $f_1 = z^2 - z$ and $f_2 = xyz$. Then $I = \langle z\rangle \cap \langle z-1, x\rangle \cap \langle z-1, y\rangle$ has codimension 1, but is not of pure codimension. We have $1 = (2z-1)\frac{\partial f_1}{\partial z} - 4f_1 \in J + I$. However, $A = \mathrm{V}(I) \subset \mathbb{A}^3$ is not smooth. In fact, A is the union of a plane and a pair of lines intersecting in a point which is necessarily a singular point of A:



(2) Applying the Jacobian criterion to the mixed ideal $I = \langle xy, y^2\rangle$, we get $J + I = \langle x, y\rangle$. In contrast, the x-axis $\mathrm{V}(I) \subset \mathbb{A}^2$ is smooth.

(3) The ideal $I = \langle xy^2\rangle \subset K[x,y]$ is unmixed and of pure codimension 1. Its vanishing locus $A = \mathrm{V}(I) \subset \mathbb{A}^2$ is the union of the coordinate axes. Thus, A is singular precisely at the origin. In contrast, the algebraic set defined by the ideal $J + I = \langle xy, y^2\rangle$ in $\mathbb{A}^2$ is the whole x-axis (note that $\operatorname{codim}(J+I) = \operatorname{codim} I = 1$). Scheme-theoretically, I defines the y-axis together with the x-axis doubled. □

Remark 2.22. If $I \subsetneq K[\boldsymbol{x}]$ is any proper ideal, the singular points of $\mathrm{V}(I) \subset \mathbb{A}^n$ arise as the singular points of each irreducible component of $\mathrm{V}(I)$ together with the points of intersection of any two of the components (see Remark 2.12). Thus, if the Jacobian criterion does not apply directly to I, we can combine it with some of the more expensive decomposition techniques discussed in Lecture 7. Indeed, since the Jacobian criterion applies (in particular) to prime ideals, and since we already know how to compute the sum and intersection of ideals, the computation of the singular locus of $\mathrm{V}(I)$ can be reduced to the computation of the minimal associated primes of I. Alternatively, compute an equidimensional decomposition of the radical of I first. □

Remark 2.23 (Jacobian Criterion in the Projective Case). Let I be a proper homogeneous ideal of $K[x_0, \ldots, x_n]$, and let $A = \mathrm{V}(I)$ be the vanishing locus of I in $\mathbb{P}^n = \mathbb{P}^n(\overline{K})$. Suppose that I is of pure codimension c and let J be the corresponding ideal of minors as in Theorem 2.20. Further, suppose that $1 \notin J + I$ (otherwise, A is a linear subspace of $\mathbb{P}^n$). Applying Theorem 2.20 to the affine cone over A, we get:

(1) If $\operatorname{codim}(J+I) = n+1$, then A is smooth.

(2) If all associated primes of I are minimal and of codimension c, and if $\operatorname{codim}(J+I) > \operatorname{codim} I$, then $J + I$ defines the singular locus of A.

Remark 2.22 applies accordingly. □

Determinantal ideals of "expected" codimension provide interesting examples of ideals which are unmixed and pure codimensional (for instance, consider the ideal defining the twisted cubic curve). To state a precise result, let M be a $p \times q$ matrix with entries in $K[\boldsymbol{x}]$, and let $I_k(M) \subset K[\boldsymbol{x}]$ be the ideal generated by the $k \times k$ minors of M, for some p, q, k. Suppose that $I_k(M)$ is a proper ideal of $K[\boldsymbol{x}]$.

Proposition 2.24. *The codimension of every minimal associated prime of $I_k(M)$ and, thus, of $I_k(M)$ itself is at most $(p-k+1)(q-k+1)$.*

Theorem 2.25. *If the codimension of $I_k(M)$ is exactly $(p-k+1)(q-k+1)$, then $K[\boldsymbol{x}]/I_k(M)$ is a Cohen-Macaulay ring.*

We will study Cohen-Macaulay rings in Lecture 5. In this section, we need the corollary below which follows from Theorem 2.25 by applying Theorem 5.41 to the zero ideal of $K[\boldsymbol{x}]/I_k(M)$.

Corollary 2.26 (Unmixedness Theorem). *If the codimension of $I_k(M)$ is exactly $(p-k+1)(q-k+1)$, then all associated primes of $I_k(M)$ are minimal and have this codimension.*

We refer to Eisenbud (1995), Section 18.5 and the references cited there for details and proofs. See also Arbarello et al (1985), Chapter II.

Example 2.27. For the following computation in `SINGULAR`, we choose $K = \mathbb{Q}$ as our coefficient field. In our geometric interpretation, however, we deal with curves in $\mathbb{P}^3 = \mathbb{P}^3(\mathbb{C})$.

To begin with, we define a ring `R` implementing $\mathbb{Q}[x_0, \ldots, x_3]$ and a 4×1 matrix `A` with entries in `R`:

```
> ring R = 0, x(0..3), dp;
> matrix A[4][1] = x(0),x(1),0,0;
```

Next, we randomly create a 4×2 matrix of linear forms in `R`. For this, we load the `SINGULAR` library `random.lib` and use its command `randommat` (see Lecture 3 for libraries):

```
> LIB "random.lib";  // loads other libraries incl. matrix.lib
>                    // and elim.lib, too
> matrix B = randommat(4,2,maxideal(1),100);
```

(note that `maxideal(k)` returns the monomial generators for the k-th power of the homogeneous maximal ideal of the ring `R`). Concatenating the matrices `B` and `A`, we get a 4×3 matrix `M` of linear forms:

```
> matrix M = concat(B,A);  // from matrix.lib
> print(M);
10*x(0)+62*x(1)-33*x(2)+26*x(3), 42*x(0)-12*x(1)-26*x(2)-65*x(3), x(0),
98*x(0)+71*x(1)+36*x(2)+79*x(3), 22*x(0)+84*x(1)-8*x(2)-55*x(3),  x(1),
-82*x(0)-8*x(1)+33*x(2)+56*x(3), -29*x(0)+43*x(1)+46*x(2)+57*x(3),0,
-60*x(0)+60*x(1)-90*x(2)-78*x(3),37*x(0)+93*x(1)+100*x(2)-50*x(3),0
```

We create the ideal `I` which is generated by the maximal minors of `M` and compute its codimension (applied to a ring `R`, the SINGULAR command `nvars` returns the number of variables in `R`):

```
> ideal I = minor(M,3);
> ideal GI = groebner(I);
> int codimI = nvars(R) - dim(GI); codimI;
2
```

So `I` has the expected codimension $2 = (4 - 3 + 1)(3 - 3 + 1)$. It is, thus, unmixed and of pure codimension 2 by Corollary 2.26. We check that the assumption on the codimension in the Jacobian criterion is satisfied:

```
> ideal singI = groebner(minor(jacob(GI),codimI) + I);
> nvars(R) - dim(singI);
3
```

Applying the Jacobian criterion and summing up, we see that the vanishing locus C of `I` in $\mathbb{P}^3$ is a curve, that `I` generates the vanishing ideal of C in $\mathbb{C}[x_0, \ldots, x_3]$, and that `singI` defines the singular locus of C. We visualize the number of generators of `singI` and their degrees by displaying the Betti diagram of `singI` (see Remarks 1.20 and 3.34 for the `betti` command):

```
> print(betti(singI,0),"betti");
           0     1
------------------
    0:     1     -
    1:     -     -
    2:     -     4
    3:     -    20
------------------
total:     1    24
```

As it turns out, `singI` comes with an $\langle x_0, \ldots, x_3\rangle$-primary component. We get rid of this component by saturating `singI` with respect to $\langle x_0, \ldots, x_3\rangle$:

```
> ideal singI_sat = sat(singI,maxideal(1))[1]; // from elim.lib
> print(betti(singI_sat,0),"betti");
           0     1
------------------
    0:     1     2
    1:     -     1
------------------
total:     1     3
> singI_sat;
singI_sat[1]=x(1)
singI_sat[2]=x(0)
singI_sat[3]=3297*x(2)^2-2680*x(2)*x(3)-5023*x(3)^2
```

We read from the output that C has two singular points which lie on the line $L = \mathrm{V}(x_0, x_1)$. In fact, L is a component of C. We check this via ideal membership (see Problem 2.16 and Lecture 3, Section 3.6.1):

```
> ideal IL = x(0),x(1);
> reduce(I,groebner(IL),1);
_[1]=0
_[2]=0
_[3]=0
_[4]=0
```

By saturating with respect to `IL`, we get an ideal defining the components of C other than L (in fact, since `I` is radical, this amounts to just one ideal quotient computation):

```
> ideal I' = sat(I,IL)[1];  // result is a Groebner basis
> degree(GI);
// dimension (proj.)  = 1
// degree (proj.)    = 6
> degree(I');
// dimension (proj.)  = 1
// degree (proj.)    = 5
```

Since `I` is a radical ideal of pure codimension 2, the same holds for `I'` (in fact, `I'` is the intersection of the (minimal) associated primes of `I` other than $\langle x_0, x_1 \rangle$). We may, thus, use the Jacobian criterion to check that C' is smooth:

```
> int codimI' = nvars(R)-dim(I');
> ideal singI' = minor(jacob(I'),codimI') + I';
> nvars(R) - dim(groebner(singI'));
4
```

Since C' and L are smooth, the two singular points of $C = C' \cup L$ must arise as intersection points of C' and L. Thus, L is a secant line to C'. □

Buchberger's algorithm requires the choice of a global monomial order. Its performance and the resulting Gröbner basis depend on the chosen order. For the type of computations done so far in these lectures, in principle any Gröbner basis and, thus, any global monomial order will do. *With respect to efficiency, however, the degree reverse lexicographic order is usually preferable* (see Bayer and Stillman (1987) for some remarks in this direction).

The applications discussed next rely on Gröbner bases whose computation requires the choice of special monomial orders.

Elimination. Let $\boldsymbol{s} \subset \boldsymbol{x} = \{x_1, \ldots, x_n\}$ be a subset of variables, and let I be an ideal of $K[\boldsymbol{x}]$. We explain how to eliminate the variables in $\boldsymbol{s}$ from I, that is, how to compute the **elimination ideal** $I \cap K[\boldsymbol{x} \setminus \boldsymbol{s}]$.

Definition 2.28. A monomial order $>$ on $K[\boldsymbol{x}]$ is called an **elimination order** with respect to $\boldsymbol{s}$ (the variables in $\boldsymbol{s}$) if the following implication holds for all $f \in K[\boldsymbol{x}]$:

$$\mathrm{L}(f) \in K[\boldsymbol{x} \setminus \boldsymbol{s}] \implies f \in K[\boldsymbol{x} \setminus \boldsymbol{s}]\,.$$

In this case, we also say that $>$ has the **elimination property** with respect to $\boldsymbol{s}$ (the variables in $\boldsymbol{s}$). □

Example 2.29. Let $\boldsymbol{s} \subset \boldsymbol{x}$, and let $\boldsymbol{t} := \boldsymbol{x} \setminus \boldsymbol{s}$. Moreover, let $>_{\boldsymbol{s}}$ on $K[\boldsymbol{s}]$ and $>_{\boldsymbol{t}}$ on $K[\boldsymbol{t}]$ be monomial orders. The **product order** (or **block order**) $> = (>_{\boldsymbol{s}}, >_{\boldsymbol{t}})$ on $K[\boldsymbol{x}]$ is defined by

$$\boldsymbol{s}^\alpha \boldsymbol{t}^\gamma > \boldsymbol{s}^\beta \boldsymbol{t}^\delta \;:\Longleftrightarrow\; \boldsymbol{s}^\alpha >_{\boldsymbol{s}} \boldsymbol{s}^\beta \;\text{ or }\; (\boldsymbol{s}^\alpha = \boldsymbol{s}^\beta \;\text{ and }\; \boldsymbol{t}^\gamma >_{\boldsymbol{t}} \boldsymbol{t}^\delta).$$

It is a monomial order which has the elimination property with respect to $\boldsymbol{s}$ iff $>_{\boldsymbol{s}}$ is global, and which is global iff $>_{\boldsymbol{s}}$ and $>_{\boldsymbol{t}}$ are global. A particular example of a product order is the lexicographic order on $K[\boldsymbol{x}]$ which is an elimination order with respect to *each initial set of variables* $\boldsymbol{s} = \{x_1, \ldots, x_k\}$, $k = 1, \ldots, n$. □

Proposition 2.30. *Let $>$ be a global elimination order on $K[\boldsymbol{x}]$ with respect to $\boldsymbol{s} \subset \boldsymbol{x}$, and let $\mathcal{G}$ be a Gröbner basis for I with respect to $>$. Then $\mathcal{G} \cap K[\boldsymbol{x} \setminus \boldsymbol{s}]$ is a Gröbner basis for $I \cap K[\boldsymbol{x} \setminus \boldsymbol{s}]$ with respect to the restriction of $>$ to $K[\boldsymbol{x} \setminus \boldsymbol{s}]$.*

Given a K-algebra homomorphism

$$\phi : K[\boldsymbol{y}] = K[y_1, \ldots, y_m] \longrightarrow K[\boldsymbol{x}]/I\,,\; y_i \longmapsto \overline{f}_i := f_i + I,$$

its kernel can be computed via elimination:

Proposition 2.31 (Kernel of a Ring Map). *Let J be the ideal*

$$J = IK[\boldsymbol{x}, \boldsymbol{y}] + \big\langle f_1 - y_1, \ldots, f_m - y_m \big\rangle \subset K[\boldsymbol{x}, \boldsymbol{y}].$$

Then

$$\ker \phi = J \cap K[\boldsymbol{y}].$$

Computing $\ker \phi$ means to compute the K-algebra relations on $\overline{f}_1, \ldots, \overline{f}_m$ and, thus, to represent the subalgebra $K\big[\overline{f}_1, \ldots, \overline{f}_m\big]$ of $K[\boldsymbol{x}]/I$ as an affine ring: $K\big[\overline{f}_1, \ldots, \overline{f}_m\big] \cong K[\boldsymbol{y}]/\ker \phi$. Geometrically, as already pointed out, computing kernels of ring maps means to compute the **Zariski closure of the image of an algebraic set under a morphism**. Note that in contrast to the case of affine algebraic sets, the image of a projective algebraic set under a morphism is always Zariski closed.

Example 2.32. We use `SINGULAR` to compute defining equations for the twisted cubic curve $C \subset \mathbb{P}^3(\mathbb{R})$ via its parametrization. Algebraically, this amounts to computing the kernel of the ring map

$$\mathbb{Q}[w,x,y,z] \to \mathbb{Q}[s,t], \;\; w \mapsto s^3, \; x \mapsto s^2t, \; y \mapsto st^2, \; z \mapsto t^3\,,$$

and, thus, to eliminate the variables s, t from the ideal

$$\langle w - s^3, x - s^2t, y - st^2, z - t^3\rangle \subset \mathbb{Q}[s,t,w,x,y,z]\,.$$

For this, we set up a ring with a block order having the desired elimination property (see Lecture 3 for more on implementing monomial orders):

```
> ring P1P3 = 0, (s,t,w,x,y,z), (dp(2),dp(4));
> ideal J = w-s3, x-s2t, y-st2, z-t3;
> J = groebner(J);
> J;
J[1]=y2-xz
J[2]=xy-wz
J[3]=x2-wy
J[4]=sz-ty
[...]
J[10]=s3-w
```

The first three Gröbner basis elements do not depend on s and t, they define C. To compute these elements, we may alternatively use the built-in command `preimage` which, hiding the elimination step, computes the desired kernel for us (see Lecture 3, Section 3.6.3):

```
> ring P1 = 0, (s,t), dp;
> ideal ZERO;
> ideal PARA = s3, s2t, st2, t3;
> ring P3 = 0, (w,x,y,z), dp;
> ideal IC = preimage(P1,PARA,ZERO);
> print(IC);
y2-xz,
xy-wz,
x2-wy
```

The point $p = (1:0:1:0) \in \mathbb{P}^3(\mathbb{R})$ does not lie on C:

```
> ideal P = w-y, x, z;
> size(reduce(IC,groebner(P),1));  // ideal membership test
2
```

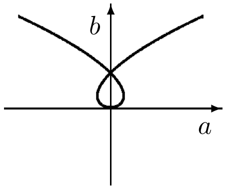
By projecting C from p, we obtain, thus, a morphism $\pi : C \to \mathbb{P}^2(\mathbb{R})$. This morphism is defined by the linear forms $w-y$, x, z defining p. We compute the image $\pi(C)$, that is, the kernel of the ring map

$$\mathbb{Q}[a,b,c] \to \mathbb{Q}[w,x,y,z]/\langle y^2 - xz, xy - wz, x^2 - wy\rangle,$$
$$a \mapsto \overline{w} - \overline{y}, \quad b \mapsto \overline{x}, \quad c \mapsto \overline{z}\,,$$

where a, b, c are the homogenous coordinates on $\mathbb{P}^2(\mathbb{R})$:

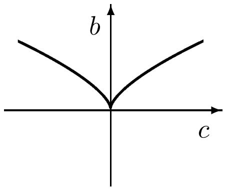
```
> ring P2 = 0, (a,b,c), dp;
> ideal PIC = preimage(P3,P,IC);
> PIC;
PIC[1]=b3-a2c-2b2c+bc2
```

The projected curve is a nodal cubic curve which we visualize in the affine chart $\mathbb{A}^2(\mathbb{R}) \cong \mathbb{P}^2(\mathbb{R}) \setminus V(c)$. For this, we use SURF:



Proceeding similarly for the point $q = (0:1:0:0)$, we get a cuspidal cubic curve (see Lecture 3 for the `setring` command used below):

```
> setring P3;
> ideal Q = w, y, z;
> size(reduce(IC,groebner(Q),1));    // check: Q not on C
1
> setring P2;
> ideal QIC = preimage(P3,Q,IC);
> QIC;
QIC[1]=b3-ac2
```



□

Example 2.33. Consider the map

$$S^2 \longrightarrow \mathbb{A}^3(\mathbb{R}), \quad (x_1, x_2, x_3) \longmapsto (x_1x_2, x_1x_3, x_2x_3),$$

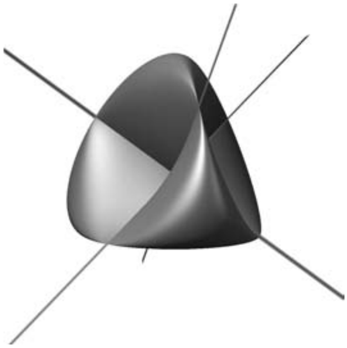
from the real 2-sphere

$$S^2 = V(x_1^2 + x_2^2 + x_3^2 - 1) \subset \mathbb{A}^3(\mathbb{R})$$

to the real 3-space. We refer to (the closure of) its image as the **Steiner Roman surface**. Using the `preimage` command, we compute a defining equation for this surface:

```
> ring S2 = 0, x(1..3), dp;
> ideal SPHERE = x(1)^2+x(2)^2+x(3)^2-1;
> ideal MAP = x(1)*x(2), x(1)*x(3), x(2)*x(3);
> ring R3 = 0, y(1..3), dp;
> ideal ST = preimage(S2, MAP, SPHERE);
> print(ST);
y(1)^2*y(2)^2+y(1)^2*y(3)^2+y(2)^2*y(3)^2-y(1)*y(2)*y(3)
```

To visualize the Steiner Roman surface, we again use `SURF`:



Note that the Steiner Roman surface is irreducible since S^2 is irreducible. What points in the picture are not in the image of S^2? $\square$

Exercise 2.34. Show that the real algebraic set in Example 2.1 is the closure of the image of the map $S^2 \to \mathbb{A}^3(\mathbb{R})$, $(x_1, x_2, x_3) \mapsto (x_1, x_2, x_2 x_3)$. Conclude that this algebraic set is irreducible. $\square$

Finally, we explain how to compute the homogenization of an ideal with respect to an extra variable (in general, as we will see in Exercise 2.2, it is *not* enough to just homogenize the given generators).

Proposition 2.35. *Let I be an ideal of $K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$. Pick a global monomial order $>$ on $K[\boldsymbol{x}]$ which is* **degree compatible**, *that is, which satisfies* $(\deg \boldsymbol{x}^\alpha > \deg \boldsymbol{x}^\beta \implies \boldsymbol{x}^\alpha > \boldsymbol{x}^\beta)$. *If x_0 is an extra variable, set*

$$\boldsymbol{x}^\alpha x_0^d >_{\text{hom}} \boldsymbol{x}^\beta x_0^e \;:\Longleftrightarrow\; \boldsymbol{x}^\alpha > \boldsymbol{x}^\beta \;\text{ or }\; (\boldsymbol{x}^\alpha = \boldsymbol{x}^\beta \text{ and } d > e).$$

Then $>_{\text{hom}}$ is a global monomial order on $K[x_0, x_1, \ldots, x_n]$ (in fact, it is a product order combining two global monomial orders). Further, the following holds if we homogenize with respect to x_0: if $f_1, \ldots, f_r$ form a Gröbner basis for I with respect to $>$, the homogenized polynomials $f_1^{\text{hom}}, \ldots, f_r^{\text{hom}}$ form a Gröbner basis for the homogenized ideal I^{hom} with respect to $>_{\text{hom}}$.

Remark 2.36 (Further Reading). For more details and proofs of the results presented in this lecture, see Cox, Little, and O'Shea (1997), Decker and Schreyer (2006), Eisenbud (1995), Greuel and Pfister (2002), and Matsumura (1986).