Chapter 1

The Geometry-Algebra Dictionary

Algebraic geometers use algebraic means to investigate geometric objects which arise as sets of solutions of polynomial equations defined over a field $\Bbbk$. A fundamental tool is a dictionary which translates geometric statements into algebraic statements and vice versa.

In this chapter, we start developing the dictionary. Our basic geometric objects of study are subsets of some $\Bbbk^n$, called algebraic subsets, which can be described as the locus $\mathrm{V}(f_1, \dots, f_r)$ of common zeros of finitely many polynomials $f_1, \dots, f_r \in \Bbbk[x_1, \dots, x_n]$. If $I \subset \Bbbk[x_1, \dots, x_n]$ is the ideal generated by $f_1, \dots, f_r$, then $\mathrm{V}(f_1, \dots, f_r)$ coincides with the locus $\mathrm{V}(I)$ of common zeros of all the elements of I. Consequently, every algebraic subset of $\Bbbk^n$ has the form $\mathrm{V}(I)$, where $I \subset \Bbbk[x_1, \dots, x_n]$ is an ideal. On the other hand, according to Hilbert's basis theorem, every ideal in $\Bbbk[x_1, \dots, x_n]$ is finitely generated. Hence every ideal in $\Bbbk[x_1, \dots, x_n]$ defines an algebraic subset of $\Bbbk^n$. Ideals in $\Bbbk[x_1, \dots, x_n]$ are our basic algebraic objects of study.

It turns out that distinct ideals may represent the same algebraic set. If an algebraic set $A \subset \Bbbk^n$ is given, the largest ideal I with $A = \mathrm{V}(I)$ is the ideal $\mathrm{I}(A)$ of all polynomials vanishing on A. This ideal has a special algebraic property: it is a radical ideal. Thus I and V define a correspondence between algebraic subsets of $\Bbbk^n$ and radical ideals in $\Bbbk[x_1, \dots, x_n]$. According to Hilbert's Nullstellensatz, this correspondence is one-to-one if $\Bbbk$ is algebraically closed.

On the algebraic side, besides $\mathrm{I}(A)$, we also have the quotient ring $\Bbbk[A] =$

$\mathbb{k}[x_1, \dots, x_n]/\mathrm{I}(A)$ which can be viewed as the ring of polynomial functions on A. The natural maps from an algebraic set $A \subset \mathbb{k}^n$ to an algebraic set $B \subset \mathbb{k}^m$ are the maps $\alpha : A \to B$ whose components are polynomial functions on A. Such maps are called polynomial maps (or morphisms). Every morphism $\alpha : A \to B$ induces a $\mathbb{k}$-algebra homomorphism

$$\alpha^* : \mathbb{k}[B] \to \mathbb{k}[A],\ \psi \to \psi \circ \alpha,$$

and conversely every $\mathbb{k}$-algebra homomorphism $\Phi : \mathbb{k}[B] \to \mathbb{k}[A]$ is of the form $\Phi = \alpha^*$ for a unique morphism $\alpha : A \to B$. It follows that α is an isomorphism (of algebraic sets) iff α^* is an isomorphism (of $\mathbb{k}$-algebras). So $\mathbb{k}[A]$ is an invariant under isomorphisms; it is less dependent on the ambient space $\mathbb{k}^n$ than $\mathrm{I}(A)$.

When considering $\mathbb{k}^n$ with its ring of polynomial functions one usually writes $\mathbb{A}^n(\mathbb{k}) = \mathbb{k}^n$ and calls it the affine n-space over $\mathbb{k}$. Algebraic subsets of $\mathbb{A}^n(\mathbb{k})$ are sometimes called affine algebraic sets to distinguish them from the algebraic subsets of projective n-space which we consider later on in this book. Locally, every projective algebraic set is an affine algebraic set.

1.1 Zero Loci

Let $\mathbb{k}$ be a field. The **affine n-space** over $\mathbb{k}$ is the set

$$\mathbb{A}^n(\mathbb{k}) := \{(a_1, \dots, a_n) \mid a_1, \dots, a_n \in \mathbb{k}\}.$$

An element $p \in \mathbb{A}^n(\mathbb{k})$ is called a **point**, and if $p = (a_1, \dots, a_n)$, the a_i are called the **coordinates** of p. We call $\mathbb{A}^1(\mathbb{k})$ the **affine line**, and $\mathbb{A}^2(\mathbb{k})$ the **affine plane** over $\mathbb{k}$.

A polynomial $f \in \mathbb{k}[x_1, \dots, x_n]$ defines a function on $\mathbb{A}^n(\mathbb{k})$, called a **polynomial function**,

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

the value $f(a_1, \dots, a_n)$ is obtained by substituting the a_i for the x_i in f, and evaluating the corresponding expression in $\mathbb{k}$. In particular, the x_i give the **coordinate functions** $x_i : \mathbb{A}^n(\mathbb{k}) \to \mathbb{k}$. Viewing a polynomial f as a function on $\mathbb{A}^n(\mathbb{k})$ allows us to talk about the **locus of zeros** of f in $\mathbb{A}^n(\mathbb{k})$, namely

$$\mathrm{V}(f) := \{p \in \mathbb{A}^n(\mathbb{k}) \mid f(p) = 0\}.$$

Definition 1.1.1. A subset $A \subset \mathbb{A}^n(\mathbb{k})$ is a **hypersurface** if $A = \mathrm{V}(f)$ for a nonconstant polynomial $f \in \mathbb{k}[x_1, \ldots, x_n]$. In this case, we say that $f(x_1, \ldots, x_n) = 0$ is a **defining equation** for A.

Exercise 1.1.2. Let $\mathbb{k}$ be an infinite field, and let $f \in \mathbb{k}[x_1, \ldots, x_n]$ be a polynomial. If f is nonzero, show that the complement $\mathbb{A}^n(\mathbb{k}) \setminus \mathrm{V}(f)$ is an infinite set. In particular, the polynomial f is zero iff the polynomial function $f : \mathbb{A}^n(\mathbb{k}) \to \mathbb{k}$ is zero.
Hint. It follows from Euclidean division with remainder that every nonzero polynomial in one variable has at most finitely many roots (see Theorem 2.2.1 for Euclidean division with remainder).

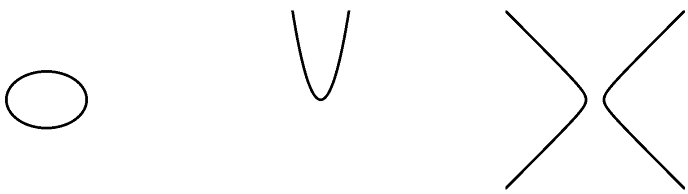
Exercise 1.1.3. Let $\mathbb{F}_2$ be the field with two elements. Find a nonzero polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]$ which involves all of $x_1, \ldots, x_n$, and which vanishes at every point of $\mathbb{A}^n(\mathbb{F}_2)$.

An **affine plane curve** is a hypersurface in $\mathbb{A}^2(\mathbb{k})$.

Example 1.1.4. Let $\mathbb{k} = \mathbb{R}$.

1. **Nondegenerate conics**.

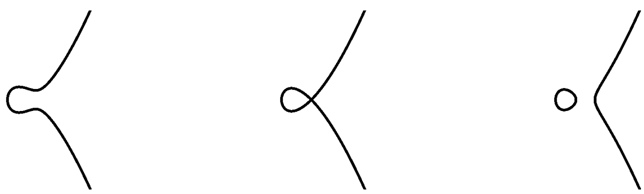
   (a) ellipse (b) parabola (c) hyperbola



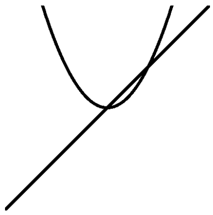
$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \qquad\qquad y = mx^2 \qquad\qquad \frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$$

2. A family of cubic curves C_λ, $\lambda \in \mathbb{R}$: $y^2 - x((x-1)^2 + \lambda) = 0$.

   (a) $\lambda = 1/2$ (b) $\lambda = 0$ (c) $\lambda = -1/2$



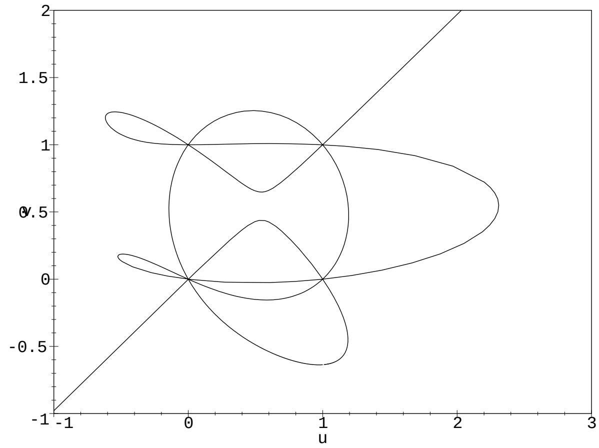
3. The union of a parabola with a line.



$$y^2 - xy - x^2y + x^3 = 0$$

4. A curve with 3 triple points and a quadruple point, defined by the equation

$$11\,y^7 + 7\,y^6x + 8\,y^5x^2 - 3\,y^4x^3 - 10\,y^3x^4 - 10\,y^2x^5 - x^7 - 33\,y^6 - 29\,y^5x$$
$$-13\,y^4x^2 + 26\,y^3x^3 + 30\,y^2x^4 + 10\,yx^5 + 3\,x^6 + 33\,y^5 + 37\,y^4x - 8\,y^3x^2$$
$$-33\,y^2x^3 - 20\,yx^4 - 3\,x^5 - 11\,y^4 - 15\,y^3x + 13\,y^2x^2 + 10\,yx^3 + x^4 = 0\,.$$



We will see in Exercise **??** that this curve admits a rational parametrization, namely

$$x\,(t) = \frac{121\,t^7 - 253\,t^6 - 133\,t^5 + 364\,t^4 + 39\,t^3 - 92\,t^2 + 10\,t}{121\,t^7 - 127\,t^6 - 114\,t^5 + 29\,t^4 + 54\,t^3 + 106\,t^2 - 20\,t + 1}\,,$$

$$y\,(t) = \frac{-77\,t^7 + 72\,t^6 + 246\,t^5 - 192\,t^4 - 138\,t^3 + 116\,t^2 - 20\,t + 1}{121\,t^7 - 127\,t^6 - 114\,t^5 + 29\,t^4 + 54\,t^3 + 106\,t^2 - 20\,t + 1}\,.$$

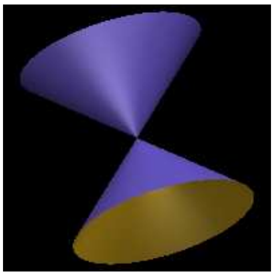
How to compute a parametrization from a given equation is one of the nontrivial problems which we will treat in this book.

Remark 1.1.5. A formal definition of what we mean by a rational parametrization is given in Section 2.7. Most curves do not admit such a parametrization. See Section **??** for a more precise statement.

Here are some hypersurfaces in affine 3-space.

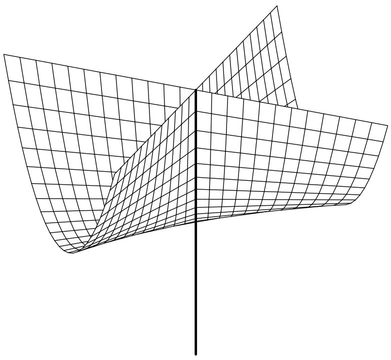
Example 1.1.6. Let $\Bbbk = \mathbb{R}$.

1. A **cone**.



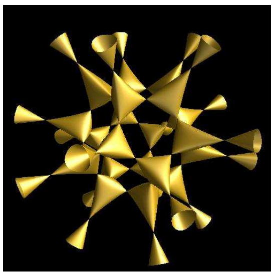
$$x^2 + y^2 - z^2 = 0$$

2. The **Whitney umbrella**.



$$x^2 - y^2 z = 0$$

3. The **Barth sextic**.



$$(8c+4)x^2y^2z^2 - c^4(x^4y^2 + y^4z^2 + x^2z^4) + c^2(x^2y^4 + y^2z^4 + x^4z^2) - \tfrac{2c+1}{4}(x^2+y^2+z^2-1)^2 = 0, \quad \text{with } c = \tfrac{1+\sqrt{5}}{2}$$

In general, we are concerned with more than one polynomial equation. If $I \subset \Bbbk[x_1, \dots, x_n]$ is any subset, its **locus of zeros** in $\mathbb{A}^n(\Bbbk)$ is the set of common zeros of all the elements of I, namely

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

If $I = \{f_1, \dots, f_r\}$ is finite, we write $\mathrm{V}(f_1, \dots, f_r) = \mathrm{V}(I)$.

Definition 1.1.7. A subset $A \subset \mathbb{A}^n(\Bbbk)$ is called **affine algebraic**, or simply **algebraic**, if $A = \mathrm{V}(f_1, \dots, f_r)$ for some polynomials $f_1, \dots, f_r \in \Bbbk[x_1, \dots, x_n]$. In this case, we say that

$$f_1(x_1, \dots, x_n) = 0, \dots, f_r(x_1, \dots, x_n) = 0$$

is a system of **defining equations** for A.

In other words, a subset of $\mathbb{A}^n(\Bbbk)$ is algebraic iff it is the intersection of finitely many hypersurfaces.

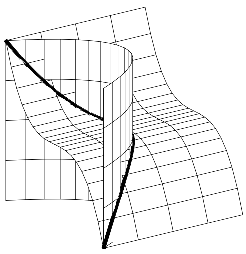
Example 1.1.8. A **hyperplane** in $\mathbb{A}^n(\Bbbk)$ is a hypersurface defined by a polynomial

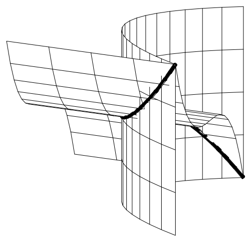
$$f = a_1x_1 + \dots + a_nx_n + b \in \Bbbk[x_1, \dots, x_n]$$

of degree one. Thus, a hyperplane is defined by a single linear equation, and the intersection of finitely many hyperplanes, called a **linear subvariety**, is the set of solutions of a system of linear equations. The study of linear subvarieties is a topic of linear algebra. See also Exercise 1.5.15.

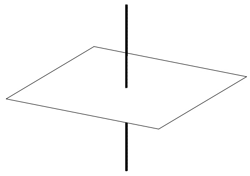
Example 1.1.9. Let $\Bbbk = \mathbb{R}$.

1. The intersection of the two hypersurfaces $\mathrm{V}(y - x^2)$ and $\mathrm{V}(z - x^3)$ in $\mathbb{A}^3(\mathbb{R})$ is called the **twisted cubic curve**:





2. Intersecting the hypersurfaces $\mathrm{V}(xz)$ and $\mathrm{V}(yz)$ in $\mathbb{A}^3(\mathbb{R})$ gives the union of the xy-plane and the z-axis:



Exercise 1.1.10. Realize all the explicit examples considered so far with the help of your favorite system(s) for visualization.

An algebraic set $A \subset \mathbb{A}^n(\Bbbk)$ can be described by many different systems of polynomial equations. Indeed, if A is defined by the vanishing of $f_1, \ldots, f_r \in \Bbbk[x_1, \ldots, x_n]$, then each $\Bbbk[x_1, \ldots, x_n]$-linear combination

$$g_1 f_1 + \cdots + g_r f_r$$

vanishes on A, too, and A is the locus of common zeros of all these linear combinations. That is, A is the locus of zeros of the ideal $(f_1, \ldots, f_r)$ generated by $f_1, \ldots, f_r$ in $\Bbbk[x_1, \ldots, x_n]$, and every finite set of generators for the ideal gives a system of defining equations for A. For instance, in the case of the twisted cubic curve,

$$(y - x^2, z - x^3) = (y - x^2, z - x^3, z - xy) = (y - x^2, z - xy).$$

The starting point of the geometry-algebra dictionary is the idea of representing algebraic sets by ideals rather than by specific systems of defining equations. Strong support for this idea comes from the fact that every ideal in $\Bbbk[x_1, \ldots, x_n]$ can be generated by finitely many elements. This is clear in the case of one variable, in which even more is true:

Remark 1.1.11. The polynomial ring $\Bbbk[x]$ in one variable x is a principal ideal domain. That is, every ideal $I \subset \Bbbk[x]$ is generated by a single polynomial. Indeed, if $f \in I$ is a nonzero polynomial of minimal degree, use Euclidean division with remainder to show that $I = (f)$.

Hilbert, in the first of his two famous papers on invariant theory [1890, 1893], settled the case of several variables by an induction argument.

Theorem 1.1.12 (Hilbert's basis theorem). *Every ideal in $\Bbbk[x_1, \ldots, x_n]$ has a finite set of generators.*

Note that Hilbert and his contemporaries used the word "basis" as another name for a "finite set of generators". In Chapter 2 we will consider special bases, nowadays called Gröbner bases, which are well-suited for computational purposes. Historically, Gröbner bases were introduced by Gordan to give a simplified proof of Hilbert's basis theorem. We will discuss Gordan's proof in Exercise 2.1.2 and Corollary 2.3.3.

Corollary 1.1.13. *If $I \subset \Bbbk[x_1, \ldots, x_n]$ is any subset, its locus of zeros in $\mathbb{A}^n(\Bbbk)$ is algebraic.*

Proof. Apply the basis theorem to the ideal generated by I in $\Bbbk[x_1, \ldots, x_n]$. □

Aside from the basis theorem, we will discuss in this book three other fundamental results of Hilbert proved in [1890, 1893]: the Nullstellensatz[1] 1.3.2, the syzygy theorem 2.5.24, and the theorem on the polynomial nature of what is called a Hilbert function **??**.

The theory of rings in which every ideal is finitely generated was developped in a systematic and abstract way by Emmy Noether [1921]. In particular, Noether realized the importance of the ascending chain condition below, from which she derived the existence of primary decompositions (see Remark 1.4.12).

Exercise 1.1.14. Prove that the following conditions on a ring R are equivalent.

1. **(Finiteness condition)**. Every ideal in R is finitely generated.
2. **(Ascending chain condition)**. Every chain
$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset R$$
of ideals of R is eventually stationary. That is,
$$I_m = I_{m+1} = I_{m+2} = \ldots \quad \text{for some} \quad m \geq 1.$$
3. **(Maximal condition)**. Every nonempty set of ideals of R has a maximal element with respect to inclusion.

Definition 1.1.15. A ring satisfying the equivalent conditions above is called a **Noetherian ring.**

[1] theorem of zeros

Exercise 1.1.16 (Hilbert's basis theorem, general version). If R is a Noetherian ring, show that $R[x]$ is Noetherian. Conclude that $\mathbb{Z}[x_1, \ldots, x_n]$ and $\Bbbk[x_1, \ldots, x_n]$ are Noetherian.
Hint. If $I \subset R[x]$ is an ideal which is not finitely generated, let $f_1 \in I$ be a polynomial of minimal degree, and let $a_1 \in R$ be the leading coefficient of f_1. Construct an ascending chain of ideals

$$(a_1) \subsetneq (a_1, a_2) \subsetneq \cdots \subsetneq R.$$

Coming back to geometry, we summarize some properties of V.

Proposition 1.1.17. *Let* $R = \Bbbk[x_1, \ldots, x_n]$.

1. $\mathrm{V}(0) = \mathbb{A}^n(\Bbbk)$. $\quad \mathrm{V}(1) = \emptyset$.
2. *If* $I \subset J \subset R$ *are subsets, then* $\mathrm{V}(I) \supset \mathrm{V}(J)$.
3. *If* $I, J \subset R$ *are ideals, then*
$$\mathrm{V}(I) \cup V(J) = \mathrm{V}(I \cdot J) = \mathrm{V}(I \cap J).$$
In particular, the union of finitely many algebraic sets is an algebraic set.
4. *If* (I_α) *is a family of ideals in* R*, then*
$$\bigcap_\alpha \mathrm{V}(I_\alpha) = \mathrm{V}\left(\sum_\alpha I_\alpha\right).$$
In particular, the intersection of any family of algebraic sets is an algebraic set.
5. *If* $a_1, \ldots, a_n \in \Bbbk$*, then*
$$\mathrm{V}(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\}.$$

Exercise 1.1.18. Prove Proposition 1.1.17.

Remark-Definition 1.1.19. By properties 1, 3 and 4 above, the algebraic subsets of $\mathbb{A}^n(\Bbbk)$ satisfy the axioms for the closed sets of a topology on $\mathbb{A}^n(\Bbbk)$, called the **Zariski topology** on $\mathbb{A}^n(\Bbbk)$. The open sets in this topology are then of type

$$\begin{aligned}\mathbb{A}^n(\Bbbk) \setminus \mathrm{V}(f_1, \ldots, f_r) &= \mathbb{A}^n(\Bbbk) \setminus (\mathrm{V}(f_1) \cap \cdots \cap \mathrm{V}(f_r)) \\ &= \bigcup_{i=1}^r (\mathbb{A}^n(\Bbbk) \setminus \mathrm{V}(f_i)),\end{aligned}$$

with $f_1, \dots, f_r \in \Bbbk[x_1, \dots, x_n]$. In particular, the **distinguished open sets**

$$\mathrm{D}(f) := \mathbb{A}^n(\Bbbk) \setminus \mathrm{V}(f),\ f \in \Bbbk[x_1, \dots, x_n],$$

form a basis for the Zariski topology on $\mathbb{A}^n(\Bbbk)$.

If not otherwise mentioned, the affine n-space $\mathbb{A}^n(\Bbbk)$ is endowed with the Zariski topology, and topological notions like open, closed, dense, or neighborhood refer to this topology. If $A \subset \mathbb{A}^n(\Bbbk)$ is a subset, then $\bar{A}$ denotes its closure in the Zariski topology.

Remark 1.1.20. If $\Bbbk = \mathbb{R}$ or $\Bbbk = \mathbb{C}$, every subset of $\mathbb{A}^n(\Bbbk)$ which is open in the Zariski topology is also open in the usual Euclidean topology. Indeed, polynomial functions on $\mathbb{A}^n(\Bbbk)$ are continous in the Euclidean topology.

Exercise 1.1.21. Let $A \subset \mathbb{A}^n(\Bbbk)$ be a finite set. Prove that A is an algebraic set which can be defined by n polynomial equations.
Hint. Use interpolation.

1.2 Vanishing ideals

The remarks of the preceeding section give us a surjective map

$$\{\text{algebraic subsets } A \subset \mathbb{A}^n(\Bbbk)\} \xleftarrow[\mathrm{V}]{} \{\text{ideals } I \subset \Bbbk[x_1, \dots, x_n]\}.$$

Now we define a map in the other direction by associating to each algebraic set A the ideal of all the polynomials vanishing on A.

Remark-Definition 1.2.1. If $A \subset \mathbb{A}^n(\Bbbk)$ is any subset, the set

$$\mathrm{I}(A) := \{f \in \Bbbk[x_1, \dots, x_n] \mid f(p) = 0 \text{ for every } p \in A\}$$

is an ideal, called the **vanishing ideal** of A.

Exercise 1.2.2. 1. Show that every polynomial $f \in \Bbbk[x, y, z]$ has a representation of type

$$f = g_1(y - x^2) + g_2(z - x^3) + h,$$

with $g_1, g_2 \in \Bbbk[x, y, z]$ and $h \in \Bbbk[x]$.

2. Let $\mathbb{k}$ be infinite, and let $C = \mathrm{V}(y - x^2, z - x^3) \subset \mathbb{A}^3(\mathbb{k})$ be the twisted cubic curve over $\mathbb{k}$. Show that

$$\mathrm{I}(C) = (y - x^2, z - x^3).$$

Hint. Use that C can be parametrized:

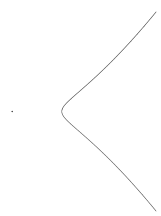
$$C = \{(t, t^2, t^3) \mid t \in \mathbb{k}\}.$$

The above expression for f in terms of $y - x^2$ and $z - x^3$ is reminiscent of Euclidean division with remainder, except that we are dividing by two polynomials instead of one. In Exercise 2.2.14 you will recompute the expression in a more systematic way, using a generalized division algorithm.

Exercise 1.2.3. Let $\mathbb{k}$ be infinite, and let

$$C = \{(t^2 + 1, t^3 + t) \mid t \in \mathbb{k}\} \subset \mathbb{A}^2(\mathbb{k}).$$

Determine $\mathrm{I}(C)$ and deduce that $\bar{C} = C \cup \{(0, 0)\}$.



Remark 1.2.4. Our computations in the examples above are based on a parametric representation of each given curve. In general, no such representation exists, and it can be a very difficult task to compute $\mathrm{I}(A)$. See also Theorem 1.3.2 and Remark 2.4.7.

Let us summarize some properties of I, and start examining, how V and I are related.

Proposition 1.2.5. *Let $R = \mathbb{k}[x_1, \dots, x_n]$.*

1. $\mathrm{I}(\emptyset) = R$. $\mathrm{I}(\mathbb{A}^n(\mathbb{k})) = (0)$ *if $\mathbb{k}$ is infinite.*
2. *If $A \subset B \subset \mathbb{A}^n(\mathbb{k})$ are subsets, then* $\mathrm{I}(A) \supset \mathrm{I}(B)$.
3. *If $A, B \subset \mathbb{A}^n(\mathbb{k})$ are subsets, then*

$$\mathrm{I}(A \cup B) = \mathrm{I}(A) \cap \mathrm{I}(B).$$

4. *If* $(a_1, \ldots, a_n) \in \mathbb{A}^n(\Bbbk)$ *is a point, then*

$$\mathrm{I}(\{(a_1, \ldots, a_n)\}) = (x_1 - a_1, \ldots, x_n - a_n).$$

5. *If* $A \subset \mathbb{A}^n(\Bbbk)$ *is a subset, then*

$$\mathrm{V}(\mathrm{I}(A)) \supset A,$$

with equality iff A *is algebraic. In fact,* $\mathrm{V}(\mathrm{I}(A)) = \bar{A}$.

6. *If* $I \subset R$ *is a set of polynomials, then*

$$\mathrm{I}(\mathrm{V}(I)) \supset I,$$

with equality iff I *is the vanishing ideal of a subset of* $\mathbb{A}^n(\Bbbk)$.

Exercise 1.2.6. Prove Proposition 1.2.5 .

Not every ideal $I \subset \Bbbk[x_1, \ldots, x_n]$ can occur as a vanishing ideal $\mathrm{I}(A)$. That is, the inclusion $\mathrm{I}(\mathrm{V}(I)) \supset I$ may well be strict. To put it yet in another way, the map V is not injective. In fact, there are two different ways in which distinct ideals can represent the same algebraic set. To understand what may happen, consider a first example:

$$\{0\} = \mathrm{V}(x) = \mathrm{V}(x^2) = \mathrm{V}(x^3) = \cdots \subset \mathbb{A}^1(\Bbbk).$$

In general, if a power f^m of a polynomial f vanishes on a subset $A \subset \mathbb{A}^n(\Bbbk)$, then f itself vanishes on A. Thus vanishing ideals have a property not shared by all ideals: they are radical ideals in the sense of the following definition.

Remark-Definition 1.2.7. Let R be a ring, and let $I \subset R$ be an ideal. The set

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

is an ideal, called the **radical** of I. Clearly, $\operatorname{rad} I$ contains I. If equality holds, I is called a **radical ideal**.

Example 1.2.8. If R is a unique factorization domain, the radical of every principal ideal is again a principal ideal. In fact, if $f \in R$ is a nonzero nonunit, decompose f into its distinct irreducible factors:

$$f = u \cdot f_1^{\mu_1} \cdot \ldots \cdot f_s^{\mu_s},$$

where u is a unit, the μ_i are integers ≥ 1, and the f_i are irreducible and pairwise coprime. Then

$$\operatorname{rad}(f) = (f_1 \cdot \ldots \cdot f_s).$$

The product $f_1 \cdot \ldots \cdot f_s$ is uniquely determined by f up to unit factors. It is called the **square-free part** of f.

1.3 Hilbert's Nullstellensatz

Even distinct radical ideals may represent the same algebraic set. For instance,

$$\mathrm{V}(1+x^2) = \mathrm{V}(\mathbb{R}[x]) = \emptyset \subset \mathbb{A}^1(\mathbb{R}).$$

Here, the problem is the existence of nonconstant polynomials in $\mathbb{R}[x]$ without real roots. If we allow complex roots as well, the situation is better due to Gauss' fundamental theorem of algebra. More generally, if $\mathbb{k}$ is any field, and if $\bar{\mathbb{k}}$ is its algebraic closure, then every nonconstant polynomial $f \in \mathbb{k}[x]$ has a root in $\bar{\mathbb{k}}$. Since every ideal in $\mathbb{k}[x]$ is principal, we conclude that a given ideal $I \subset \mathbb{k}[x]$ represents the empty subset of $\mathbb{A}^1(\bar{\mathbb{k}})$ iff $I = \mathbb{k}[x]$. This result can be extended to polynomials in more than one variable:

Theorem 1.3.1 (Hilbert's Nullstellensatz, weak version)**.** *Let $\bar{\mathbb{k}}$ be the algebraic closure of $\mathbb{k}$, and let $I \subset \mathbb{k}[x_1, \dots, x_n]$ be an ideal. Then the following are equivalent.*

1. $1 \in I$.
2. *The locus of zeros of I in $\mathbb{A}^n(\bar{\mathbb{k}})$ is empty.*

We will prove this theorem in Section 3.1. Now, we derive from it a strong version of the Nullstellensatz which shows that over an algebraically closed field $\mathbb{k} = \bar{\mathbb{k}}$ the correspondence between algebraic sets and radical ideals is well-behaved. Again, this is clear in the case of one variable. If every nonconstant polynomial in $\mathbb{k}[x]$ has a root in $\mathbb{k}$, then every such polynomial is a product of linear factors. Hence if $I = (f) \subsetneq \mathbb{k}[x]$ is an ideal, then $\mathrm{I}(\mathrm{V}(I))$ is generated by the square-free part of f. We conclude that $\mathrm{I}(\mathrm{V}(I)) = \operatorname{rad} I$.

Theorem 1.3.2 (Hilbert's Nullstellensatz, strong version)**.** *Let $\mathbb{k} = \bar{\mathbb{k}}$ be algebraically closed, and let*

$$I \subset \mathbb{k}[x_1, \dots, x_n]$$

be an ideal. Then

$$\mathrm{I}(\mathrm{V}(I)) = \operatorname{rad} I.$$

Proof. If $f \in \operatorname{rad} I$, that is, if $f^m \in I$ for some $m \geq 1$, then f^m and thus also f vanish on $\mathrm{V}(I)$. Hence

$$\operatorname{rad} I \subset \mathrm{I}(\mathrm{V}(I)).$$

For the opposite inclusion, let $f \in \mathrm{I}(\mathrm{V}(I))$, and let $f_1, \dots, f_r$ be generators of I. Then f vanishes on $\mathrm{V}(I)$, and we have to show that $f^m = g_1 f_1 + \ldots + g_r f_r$ for some $m \geq 1$ and for some $g_1, \dots, g_r \in \mathbb{k}[x_1, \dots, x_n]$.

The proof is based on the ingenious trick of Rabinowitch. Introduce a slack variable y and consider the ideal

$$\tilde{I} := (f_1, \dots, f_r, yf - 1) \subset \mathbb{k}[x_1, \dots, x_n, y].$$

We first show that the zero locus $\mathrm{V}(\tilde{I}) \subset \mathbb{A}^{n+1}(\mathbb{k})$ is empty. Then we apply the weak version of the Nullstellensatz to conclude that $1 \in \tilde{I}$. Representing 1 as a $\mathbb{k}[x_1, \dots, x_n]$-linear combination of the generators of $\tilde{I}$ gives the result.

1. Consider a point $(a_1, \dots, a_{n+1}) \in \mathbb{A}^{n+1}(\mathbb{k})$. We distinguish two cases. If $(a_1, \dots, a_n) \in \mathrm{V}(I)$, then $f(a_1, \dots, a_n) = 0$ since $f \in \mathrm{I}(\mathrm{V}(I))$. Substituting $(a_1, \dots, a_{n+1})$ into $yf - 1$ gives

$$1 - a_{n+1} f(a_1, \dots, a_n) = 1 \neq 0,$$

whence $(a_1, \dots, a_{n+1}) \notin \mathrm{V}(\tilde{I})$. If $(a_1, \dots, a_n) \notin \mathrm{V}(I)$, then $f_i(a_1, \dots, a_n) \neq 0$ for some i, $1 \leq i \leq r$. Since $f_i \in \tilde{I}$, we obtain that $(a_1, \dots, a_{n+1}) \notin \mathrm{V}(I)$. So $\mathrm{V}(\tilde{I}) = \emptyset$.

2. The weak version of the Nullstellensatz implies that $1 \in \tilde{I}$. Hence there are polynomials $p_i,\ q \in \mathbb{k}[x_1, \dots, x_n, y]$ such that

$$1 = \sum_{i=1}^{r} p_i(x_1, \dots, x_n, y) f_i + q(x_1, \dots, x_n, y)(yf - 1).$$

Substituting $1/f$ for y yields

$$1 = \sum_{i=1}^{r} p_i(x_1, \dots, x_n, 1/f) f_i.$$

To clear denominators we multiply both sides of this equation by a suitable power f^m of f and obtain

$$f^m = \sum_{i=1}^{r} g_i f_i$$

for some polynomials $g_i \in \mathbb{k}[x_1, \dots, x_n]$. □

Corollary 1.3.3. *If $\mathbb{k} = \bar{\mathbb{k}}$ is algebraically closed, then* I *and* V *define a one-to-one correspondence*

$$\{\textit{algebraic subsets } A \subset \mathbb{A}^n(\mathbb{k})\} \underset{\mathrm{V}}{\overset{\mathrm{I}}{\rightleftarrows}} \{\textit{radical ideals } I \subset \mathbb{k}[x_1, \dots, x_n]\}.$$

As a consequence of Hilbert's Nullstellensatz, we may express geometric properties of algebraic sets in terms of ideals $I \subset \Bbbk[x_1, \ldots, x_n]$, or, in turn, of quotient rings $\Bbbk[x_1, \ldots, x_n]/I$. The exercise below gives a first example. Note that if $I \subsetneq \Bbbk[x_1, \ldots, x_n]$ is a proper ideal, then the natural map $\Bbbk \to \Bbbk[x_1, \ldots, x_n] \to \Bbbk[x_1, \ldots, x_n]/I$ allows us to regard $\Bbbk$ as a subring of $\Bbbk[x_1, \ldots, x_n]/I$ and thus $\Bbbk[x_1, \ldots, x_n]/I$ as a $\Bbbk$-algebra.

Exercise 1.3.4. Let $\bar{\Bbbk}$ be the algebraic closure of $\Bbbk$, and let $I \subset \Bbbk[x_1, \ldots, x_n]$ be an ideal. Show that the following are equivalent.

1. The locus of zeros of I in $\mathbb{A}^n(\bar{\Bbbk})$ is finite.
2. For each i, $1 \leq i \leq n$, there is a nonzero polynomial in $I \cap \Bbbk[x_i]$.
3. The $\Bbbk$-vector space $\Bbbk[x_1, \ldots, x_n]/I$ has finite dimension.

How to decide whether conditions 2 and 3 are satisfied is a topic of Sections 2.3 and 2.4.

Exercise 1.3.5. Show that every algebraic subset of $\mathbb{A}^n(\mathbb{R})$ can be defined by a single polynomial equation. Give examples of ideals $I \subset \mathbb{R}[x_1, \ldots, x_n]$ whose locus of zeros in $\mathbb{A}^n(\mathbb{R})$ is finite though $\dim_{\mathbb{R}} \mathbb{R}[x_1, \ldots, x_n]/I = \infty$.

See Exercise 1.6.1 for a more general result.

1.4 Irreducible Components

The algebraic set $\mathrm{V}(xz, yz) \subset \mathbb{A}^3(\mathbb{R})$ in Example 1.1.9 decomposes as the union of the plane $\mathrm{V}(z)$ and the line $\mathrm{V}(x, y)$. In this section, we show that every algebraic set is the union of finitely many algebraic sets which "cannot be decomposed any further". Let us start with a formal definition:

Definition 1.4.1. An algebraic set $A \subset \mathbb{A}^n(\Bbbk)$ is **reducible** if it can be expressed as the union $A = A_1 \cup A_2$ of proper subsets $A_1, A_2 \subsetneq A$ which are both algebraic. Otherwise, A is called **irreducible**, or an **affine variety**, or simply a **variety**.

To decide whether a given algebraic set is a variety, it is usually most promising to check the corresponding condition on the algebraic side.

Theorem 1.4.2. *An algebraic set* $A \subset \mathbb{A}^n(\Bbbk)$ *is irreducible iff* $\mathrm{I}(A) \subset \Bbbk[x_1, \ldots, x_n]$ *is a prime ideal.*

Proof. If A is irreducible, and if $f, g \in \Bbbk[x_1, \ldots, x_n]$ with $f \cdot g \in \mathrm{I}(A)$, then

$$A = (A \cap \mathrm{V}(f)) \cup (A \cap \mathrm{V}(g)).$$

Whence $A = A \cap \mathrm{V}(f)$ or $A = A \cap \mathrm{V}(g)$, and we conclude that either $f \in \mathrm{I}(A)$ or $g \in \mathrm{I}(A)$. Conversely, if

$$A = A_1 \cup A_2 \text{ with algebraic sets } A_i \subsetneq A,$$

then $\mathrm{I}(A_i) \supsetneq \mathrm{I}(A)$; that is, there exist $f_i \in \mathrm{I}(A_i) \setminus \mathrm{I}(A)$, $i = 1, 2$. But then $f_1 \cdot f_2 \in \mathrm{I}(A_1) \cap \mathrm{I}(A_2) = \mathrm{I}(A)$, so $\mathrm{I}(A)$ is not prime. □

Clearly, every prime ideal is radical.

Corollary 1.4.3. *If $\Bbbk = \bar{\Bbbk}$ is algebraically closed, then* I *and* V *define a one-to-one correspondence*

$$\{\textit{varieties } V \subset \mathbb{A}^n(\Bbbk)\} \underset{\mathrm{V}}{\overset{\mathrm{I}}{\rightleftarrows}} \{\textit{prime ideals } \mathfrak{p} \subset \Bbbk[x_1, \ldots, x_n]\}.$$

Example 1.4.4. If $\Bbbk$ is infinite, then $\mathrm{I}(\mathbb{A}^n(\Bbbk)) = (0)$. In particular, $\mathrm{I}(\mathbb{A}^n(\Bbbk))$ is a prime ideal, so $\mathbb{A}^n(\Bbbk)$ is a variety. If $\Bbbk = \mathbb{F}_q$ is the finite field with q elements, however, then $\mathrm{I}(\mathbb{A}^n(\Bbbk))$ is not prime. Indeed, you will show in Exercise 2.8.1 that

$$\mathrm{I}(\mathbb{A}^n(\mathbb{F}_q)) = (x_1^q - x_1, \ldots, x_n^q - x_n).$$

Example 1.4.5. If $\Bbbk$ is infinite, every linear subvariety of $\mathbb{A}^n(\Bbbk)$ is indeed a variety (see Exercise 1.5.15). In particular, the plane and the line in Example 1.1.9 are varieties.

Example 1.4.6. Let $\Bbbk$ be infinite. We show that the vanishing ideal of the twisted cubic curve

$$C = \mathrm{V}(y - x^2, z - x^3) = \{(t, t^2, t^3) \mid t \in K\} \subset \mathbb{A}^3(\Bbbk)$$

is prime, so C is a variety. If $f, g \in \Bbbk[x, y, z]$ with $f \cdot g \in \mathrm{I}(C)$, set

$$F(t) = f(t, t^2, t^3) \text{ and } G(t) = g(t, t^2, t^3) \in \Bbbk[t].$$

Then $F \cdot G = 0$, so $F = 0$ or $G = 0$. Consequently, $f \in \mathrm{I}(C)$ or $g \in \mathrm{I}(C)$.

A set consisting of a single point is a variety, hence its vanishing ideal is a prime ideal. In fact, even more is true:

Remark 1.4.7. Let $p = (a_1, \ldots, a_n) \in \mathbb{A}^n(\Bbbk)$ be a point. Each polynomial $f \in \Bbbk[x_1, \ldots, x_n]$ can be written as a polynomial in the $x_i - a_i$:

$$f = f(p) + \text{terms of degree} \geq 1 \text{ in the } x_i - a_i.$$

Indeed, substitute the $(x_i - a_i) + a_i$ for x_i, and expand. This shows that the vanishing ideal

$$\mathrm{I}(p) := \mathrm{I}(\{p\}) = (x_1 - a_1, \ldots, x_n - a_n)$$

is the kernel of the evaluation map

$$\Bbbk[x_1, \ldots, x_n] \to \Bbbk,\ f \mapsto f(p).$$

Hence $\Bbbk[x_1, \ldots, x_n]/\mathrm{I}(p) \cong \Bbbk$ is a field, and thus $\mathrm{I}(p)$ a maximal ideal.

Conversely, the following holds:

Proposition 1.4.8. *If $\Bbbk = \bar{\Bbbk}$ is algebraically closed, every maximal ideal in $\Bbbk[x_1, \ldots, x_n]$ is of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for some $a_1, \ldots, a_n \in \Bbbk$.*

Proof. Let $\mathfrak{m} \subsetneq \Bbbk[x_1, \ldots, x_n]$ be a maximal ideal. Then $\mathrm{V}(\mathfrak{m}) \neq \emptyset$ by the weak version of the Nullstellensatz. That is, there exists a point $p = (a_1, \ldots, a_n) \in \mathrm{V}(\mathfrak{m})$. It follows that

$$\mathfrak{m} \subset \mathrm{I}(p) = (x_1 - a_1, \ldots, x_n - a_n),$$

and thus

$$\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$$

since $\mathfrak{m}$ is maximal. □

Corollary 1.4.9. *If $\Bbbk = \bar{\Bbbk}$ is algebraically closed, then* I *and* V *define a one-to-one correspondence*

$$\{\textit{points in } \mathbb{A}^n(\Bbbk)\} \underset{\mathrm{V}}{\overset{\mathrm{I}}{\rightleftarrows}} \{\textit{maximal ideals in } \Bbbk[x_1, \ldots, x_n]\}.$$

Exercise 1.4.10. If $\Bbbk$ is not necessarily algebraically closed, the maximal ideals in $\Bbbk[x_1, \ldots, x_n]$ can be described as follows. Let $\bar{\Bbbk}$ be the algebraic closure of $\Bbbk$, and let G be the Galois group of $\bar{\Bbbk}$ over $\Bbbk$. Prove that the following hold.

1. Let $p = (a_1, ..., a_n) \in \mathbb{A}^n(\bar{\Bbbk})$ be a point, and let $\mathfrak{m}_p$ be the kernel of the evaluation map
$$\Bbbk[x_1, \ldots, x_n] \to \bar{\Bbbk},\ f \mapsto f(p).$$
Then $\mathfrak{m}_p$ is a maximal ideal in $\Bbbk[x_1, \ldots, x_n]$. Moreover, the vanishing locus of $\mathfrak{m}_p$ in $\mathbb{A}^n(\bar{\Bbbk})$ is the orbit of p under the natural action of G on $\mathbb{A}^n(\bar{\Bbbk})$.

2. Every maximal ideal in $\Bbbk[x_1, \ldots, x_n]$ is of type $\mathfrak{m}_p$ for some point $p \in \mathbb{A}^n(\bar{\Bbbk})$.

We now establish the main result of this section:

Theorem-Definition 1.4.11. Let $A \subset \mathbb{A}^n(\Bbbk)$ be an algebraic set. There exists a decomposition
$$A = V_1 \cup \cdots \cup V_s$$
into varieties $V_i \subset \mathbb{A}^n(\Bbbk)$. The V_i are uniquely determined up to order if we require that the decomposition is **minimal**, that is, $V_i \not\subset V_j$ for $i \neq j$. In this case, the V_i are called the **irreducible components** of A.

Proof. The existence part of the proof is a typical example of Noetherian induction. First note that every nonempty collection $\{A_\lambda\}$ of algebraic subsets of $\mathbb{A}^n(\Bbbk)$ has a minimal element with respect to inclusion. Indeed, the corresponding collection $\{I(A_\lambda)\}$ of ideals in $\Bbbk[x_1, \ldots, x_n]$ has a maximal element with respect to inclusion since $\Bbbk[x_1, \ldots, x_n]$ is Noetherian.

We use this argument to show that the collection Γ of algebraic subsets of $\mathbb{A}^n(\Bbbk)$ which are not a finite union of varieties is empty.

Suppose that $\Gamma \neq \emptyset$. Then there exists an element $A \in \Gamma$ which is minimal with respect to inclusion. That A is an element of Γ implies that A is reducible, say $A = A_1 \cup A_2$, with algebraic sets $A_i \subsetneq A$. The A_i are not contained in Γ by the minimality of $A \in \Gamma$. Hence both A_i and thus also A are a finite union of varieties, a contradiction to $A \in \Gamma$.

We conclude that A can be written as a finite union of varieties. By throwing away superfluous varieties if necessary we obtain a minimal decomposition.

To show uniqueness, let
$$A = V_1 \cup \cdots \cup V_s = V_1' \cup \cdots \cup V_t'.$$
be two minimal decompositions. Then
$$V_i = V_i \cap A = V_i \cap (V_1' \cup \cdots \cup V_t') = (V_i \cap V_1') \cup \cdots \cup (V_i \cap V_t')$$

for each i. But V_i is irreducible, so $V_i = V_i \cap V'_j$ and thus $V_i \subset V'_j$ for some j. The same argument yields an inclusion $V'_j \subset V_k$ for some k. By minimality $i = k$ and $V_i = V'_j$. So each V_i occurs as one of the V'_j, in particular $s \leq t$. Similarly we obtain $t \leq s$ and thus uniqueness up to order. $\square$

Remark 1.4.12. The Nullstellensatz allows us to rephrase Theorem 1.4.11 in algebraic terms as follows: If $\mathbb{k} = \bar{\mathbb{k}}$ is algebraically closed, the radical of every ideal $I \subset \mathbb{k}[x_1, \dots, x_n]$ has a unique **minimal prime decomposition**. That is, rad I can be uniquely written as the intersection of finitely many prime ideals,

$$\operatorname{rad} I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s,$$

with $\mathfrak{p}_i \not\supset \mathfrak{p}_j$ for $i \neq j$.

In Exercise 3.2.15 you will use purely algebraic arguments to show that the radical of every ideal I in an arbitrary Noetherian ring R has a unique minimal prime decomposition. More generally, I itself has a so called **minimal primary decomposition**; some uniqueness results hold (see Eisenbud [1995, Chapter 3] for more details).

The ideal $I = (xz, yz) \subset \mathbb{R}[x, y, z]$ in Example 1.1.9 is the intersection of the prime ideals (z) and (x, y). In particular, I is a radical ideal. See Exercise 2.4.14 for a slightly more complicated example.

Now, we consider the case of a hypersurface.

Proposition 1.4.13. *Let $\mathbb{k} = \bar{\mathbb{k}}$ be algebraically closed. If $f \in \mathbb{k}[x_1, \dots, x_n]$ is a polynomial, and if*

$$f_1 \cdot \ldots \cdot f_s$$

is the decomposition of its square-free part into its irreducible factors, then

$$\mathrm{V}(f) = \mathrm{V}(f_1) \cup \cdots \cup \mathrm{V}(f_s)$$

is the decomposition of $\mathrm{V}(f)$ *into its irreducible components, and*

$$\mathrm{I}(\mathrm{V}(f)) = (f_1 \cdot \ldots \cdot f_s) = \bigcap_{i=1}^{s} (f_i)$$

is the minimal prime decomposition of $\mathrm{I}(\mathrm{V}(f))$.

Proof. Over any field,

$$\mathrm{V}(f) = \mathrm{V}(f_1 \cdot \ldots \cdot f_s) = \bigcup_{i=1}^{s} \mathrm{V}(f_i).$$

Since the f_i are irreducible and pairwise coprime, the result follows from the Nullstellensatz: If $\mathbb{k} = \bar{\mathbb{k}}$ is algebraically closed, then

$$\mathrm{I}(\mathrm{V}(f_i)) = \mathrm{rad}\,(f_i) = (f_i) \text{ for all } i.$$

□

Exercise 1.4.14. If $\mathbb{k}$ is any field, show that the following hold.

1. Every nonempty, proper algebraic subset of $\mathbb{A}^1(\mathbb{k})$ is a finite set of points.
2. If $f, g \in \mathbb{k}[x, y]$ are coprime polynomials, then
$$\mathrm{V}(f, g) = \mathrm{V}(f) \cap \mathrm{V}(g) \subset \mathbb{A}^2(\mathbb{k})$$
is a finite set of points.
Hint. Prove that f and g are coprime in the principal ideal domain $\mathbb{k}(x)[y]$ and deduce that there exist $a, b \in \mathbb{k}(x)[y]$ such that $af + bg = 1$.
3. Every nonempty, proper algebraic subset of $\mathbb{A}^2(\mathbb{k})$ is the finite union of points and irreducible affine plane curves.

1.5 Coordinate rings and morphisms

Viewing polynomials as functions on $\mathbb{A}^n(\mathbb{k})$ allowed us to talk about their loci of zeros in $\mathbb{A}^n(\mathbb{k})$. In the same spirit, we now consider polynomial functions on an arbitrary algebraic subset $A \subset \mathbb{A}^n(\mathbb{k})$. These functions form a ring which may be naturally identified with the quotient ring $\mathbb{k}[x_1, \ldots, x_n]/\mathrm{I}(A)$.

Remark-Definition 1.5.1. Let $A \subset \mathbb{A}^n(\mathbb{k})$ be a nonempty algebraic set. A **polynomial function** on A is the restriction of a polynomial function on $\mathbb{A}^n(\mathbb{k})$ to A. That is, a map $\varphi : A \to \mathbb{k}$ is a polynomial function on A if there exists a polynomial $f \in \mathbb{k}[x_1, \ldots, x_n]$ with $\varphi(p) = f(p)$ for all $p \in A$. We make the set of all polynomial functions on A into a ring which we denote by $\mathbb{k}[A]$. The ring structure is defined by adding and multiplying values in $\mathbb{k}$: if $\varphi, \psi \in \mathbb{k}[A]$, then

$$(\varphi + \psi)(p) = \varphi(p) + \psi(p) \text{ and } (\varphi \cdot \psi)(p) = \varphi(p) \cdot \psi(p) \text{ for all } p \in A.$$

We regard $\mathbb{k}$ as the subring of all constant functions and thus $\mathbb{k}[A]$ as a $\mathbb{k}$-algebra. In other words, $\mathbb{k}[A]$ is the $\mathbb{k}$-algebra of functions on A which is generated by the restrictions of the coordinate functions to A. It is therefore called the **coordinate ring** of A.

Since two polynomials $f, g \in \mathbb{k}[x_1, \ldots, x_n]$ define the same element of $\mathbb{k}[A]$ iff $f - g \in \mathrm{I}(A)$, we may and will identify

$$\mathbb{k}[A] = \{\text{polynomial functions on } A\} = \mathbb{k}[x_1, \ldots, x_n]/\mathrm{I}(A).$$

That $\mathrm{I}(A)$ is a radical ideal means that $\mathbb{k}[A]$ is reduced (a ring is **reduced**, if 0 is its only nilpotent element).

Exercise 1.5.2. Let $\mathbb{k}$ be a finite field, and let $A \subset \mathbb{A}^n(\mathbb{k})$ be an algebraic set. Show that $\mathbb{k}[A]$ is the ring of all $\mathbb{k}$-valued functions on A.

Since an ideal I of a ring R is prime iff the quotient ring R/I is a domain, we may restate Theorem 1.4.2 as follows:

Theorem 1.5.3. *For an algebraic set $A \subset \mathbb{A}^n(\mathbb{k})$, the following are equivalent.*

1. *A is a variety.*
2. *$\mathrm{I}(A)$ is a prime ideal.*
3. *$\mathbb{k}[A]$ is a domain.*

Let $A \subset \mathbb{A}^n(\mathbb{k})$ be an arbitrary algebraic set. An **algebraic subset** of A is an algebraic subset of $\mathbb{A}^n(\mathbb{k})$ which is contained in A. Similarly, a **subvariety** of A is a variety contained in A. In analogy to the correspondence between algebraic subsets of $\mathbb{A}^n(\mathbb{k})$ and ideals in $\mathbb{k}[x_1, \ldots, x_n]$ we now define a correspondence between algebraic subsets of A and ideals in $\mathbb{k}[A]$. Let us start with a few remarks on ideals in quotient rings.

Exercise 1.5.4. Let R be a ring, and let $I \subset R$ be an ideal.

1. Prove that there is a one-to-one correspondence between ideals in R/I and ideals in R containing I. Show that radical ideals correspond to radical ideals. Similarly for prime and maximal ideals.
2. Prove that R/I is Noetherian if R is Noetherian.
3. Describe all ideals in R/I for $R = \mathbb{R}[x]$ and $I = (x^2 - 4x + 3)$.

Definition 1.5.5. Let $A \subset \mathbb{A}^n(\mathbb{k})$ be an algebraic set.

1. If $J \subset \Bbbk[A]$ is a subset, its **locus of zeros** in A is
$$\mathrm{V}_A(J) := \{p \in A \mid \varphi(p) = 0 \text{ for any } \varphi \in J\}.$$
2. If $B \subset A$ is a subset, its **vanishing ideal** in $\Bbbk[A]$ is
$$\mathrm{I}_A(B) := \{\varphi \in \Bbbk[A] \mid \varphi(p) = 0 \text{ for any } p \in B\}.$$

zzzzzzzzzzz B subset A menas ideal (B) contains ideal (A)

Exercise 1.5.6. Let $A \subset \mathbb{A}^n(\Bbbk)$ be an algebraic set. Show that the following hold:

1. A subset $B \subset A$ is an algebraic subset iff $B = \mathrm{V}_A(J)$ for some ideal $J \subset \Bbbk[A]$.
2. If $B \subset A$ is a subset, then $\mathrm{I}_A(B)$ is indeed an ideal in $\Bbbk[A]$.
3. If $B \subset A$ is an algebraic subset, then
$$\mathrm{V}_A(\mathrm{I}_A(B)) = B.$$
4. The algebraic subsets of A form the closed sets of a topology on A, called the **Zariski topology** on A.
5. The **distinguished open sets**
$$\mathrm{D}_A(f) := A \setminus \mathrm{V}_A(f),\ f \in \Bbbk[A],$$
form a basis of the Zariski topology on A.
6. **(Nullstellensatz for A)** If $\Bbbk = \bar{\Bbbk}$ is algebraically closed, and if $J \subset \Bbbk[A]$ is an ideal, then
$$\mathrm{I}_A(\mathrm{V}_A(J)) = \operatorname{rad} J.$$
7. If $\Bbbk = \bar{\Bbbk}$ is algebraically closed, then I_A and V_A define a one-to-one correspondence
$$\{\text{algebraic subsets of } A\} \underset{\mathrm{V}_A}{\overset{\mathrm{I}_A}{\rightleftarrows}} \{\text{radical ideals } I \subset \Bbbk[A]\}.$$
Under this correspondence, subvarieties correspond to prime ideals, and points to maximal ideals.

To really understand a class of sets carrying a mathematical structure of a certain type, it is usually necessary to consider maps between these sets which respect that type of structure. For instance, $\mathbb{k}$-linear maps are compatible with the addition and scalar multiplication in $\mathbb{k}$-vector spaces. Or, continous maps are the natural maps between topological spaces. One usually says, that a $\mathbb{k}$-linear map is a morphism between $\mathbb{k}$-vector spaces, or, that a continous map is a morphism between topological spaces. To introduce morphisms between affine algebraic sets, let $x_1, \ldots, x_n$ be the coordinate functions on $\mathbb{A}^n(\mathbb{k})$, and let $y_1, \ldots, y_m$ be the coordinate functions on $\mathbb{A}^m(\mathbb{k})$.

Definition 1.5.7. Let $A \subset \mathbb{A}^n(\mathbb{k})$ and $B \subset \mathbb{A}^m(\mathbb{k})$ be algebraic sets. A map $\alpha : A \to B \subset \mathbb{A}^m(\mathbb{k})$ is a **morphism** or a **polynomial map** if its components $\alpha_j = y_j \circ \alpha : A \to \mathbb{k}$ are polynomial functions on A.

Theorem 1.5.8. *Let $A \subset \mathbb{A}^n(\mathbb{k})$ and $B \subset \mathbb{A}^m(\mathbb{k})$ be algebraic sets.*

1. *If $\alpha : A \to B$ is a morphism, then for any polynomial function ψ on B the composite $\psi \circ \alpha$ is a polynomial function on A. The induced map*

$$\alpha^* : \mathbb{k}[B] \to \mathbb{k}[A],\ \psi \mapsto \psi \circ \alpha,$$

is a $\mathbb{k}$-algebra homomorphism.

2. *Conversely, if $\phi : \mathbb{k}[B] \to \mathbb{k}[A]$ is a $\mathbb{k}$-algebra homomorphism, there exists a unique morphism $\alpha : A \to B$ with $\phi = \alpha^*$.*

3. *zzzzzzzzzzzzzzzz Funktoreigenschaften*

Proof. 1. If $\alpha : A \to B$ is a morphism, there exist polynomials $f_1, \ldots, f_m \in \mathbb{k}[x_1 \ldots, x_n]$ such that

$$\alpha(p) = (f_1(p), \ldots, f_m(p)) \in B \text{ for all } p \in A.$$

Whence if ψ is a polynomial function on B, defined by a polynomial $g(y_1 \ldots, y_m) \in \mathbb{k}[y_1 \ldots, y_m]$, then $\psi \circ \alpha$ is a polynomial function on A, defined by the polynomial $g(f_1, \ldots, f_m) \in \mathbb{k}[x_1 \ldots, x_n]$. We thus obtain a well-defined map

$$\alpha^* : \mathbb{k}[B] \to \mathbb{k}[A],\ \psi \mapsto \psi \circ \alpha,$$

which is in fact a $\mathbb{k}$-algebra homomorphism.

2. Let $\phi : \mathbb{k}[B] \to \mathbb{k}[A]$ be a $\mathbb{k}$-algebra homomorphism. For $j = 1, \ldots, m$ pick a polynomial $f_j \in \mathbb{k}[x_1, \ldots, x_n]$ which represents $\phi(y_j + \mathrm{I}(B))$. Then

$f_1, \ldots, f_m$ define a polynomial map $\alpha : A \to \mathbb{A}^m(\Bbbk)$. We leave it to the reader to show that α maps A to B, that $\phi = \alpha^*$, and that α is uniquely determined by ϕ. $\square$

Exercise 1.5.9. Complete the proof of Theorem 1.5.8.

Remark 1.5.10. Thus any morphism $\alpha : A \to B$ can be extended to a morphism of the ambient affine spaces so that the resulting commutative diagram

$$\begin{tikzcd} \mathbb{A}^n(\Bbbk) \arrow[r, "F=(f_1,\ldots,f_m)"] & \mathbb{A}^m(\Bbbk) \\ A \arrow[u] \arrow[r, "\alpha"] & B \arrow[u] \end{tikzcd}$$

corresponds on the ring level to the diagram of $\Bbbk$-algebra homomorphism

$$\begin{tikzcd} \Bbbk[x_1, \ldots, x_n] \arrow[d] & \Bbbk[y_1, \ldots, y_m] \arrow[l, "F^*"'] \arrow[d] \\ \Bbbk[A] & \Bbbk[B] \arrow[l, "\alpha^*"'] \end{tikzcd},$$

where F^* is obtained by substituting f_j for y_j, $j = 1, \ldots, m$. Note that any $\Bbbk$-algebra homomorphism $\Phi : \Bbbk[y_1, \ldots, y_m] \to \Bbbk[x_1, \ldots, x_n]$ is a substitution homomorphism. But Φ defines a morphism $A \to B$ only if $\Phi(\mathrm{I}(B)) \subset \mathrm{I}(A)$. Therefore, although there are always plenty of morphisms $A \to \mathbb{A}^m(\Bbbk)$, there are quite often only constant morphisms $A \to B$.

Observe that the composite of two morphisms $A \to B$ and $B \to C$ is a morphism $A \to C$.

Definition 1.5.11. Let $A \subset \mathbb{A}^n(\Bbbk)$ and $B \subset \mathbb{A}^m(\Bbbk)$ be algebraic sets. A morphism $\alpha : A \to B$ is an **isomorphism** if there exists a morphism $\beta : B \to A$ with $\beta \circ \alpha = \mathrm{id}_A$ and $\alpha \circ \beta = \mathrm{id}_B$. (For any set X we write id_X for the identity map from X to itself.) One says that A and B are **isomorphic**, written $A \cong B$, if there exists an isomorphism $A \to B$.

Corollary 1.5.12. *Let $A \subset \mathbb{A}^n(\Bbbk)$ and $B \subset \mathbb{A}^m(\Bbbk)$ be algebraic sets, and let $\alpha : A \to B$ be a morphism. Then α is an isomorphism (of affine algebraic sets) iff $\alpha^* : \Bbbk[B] \to \Bbbk[A]$ is an isomorphism (of $\Bbbk$-algebras). Two affine algebraic sets over $\Bbbk$ are isomorphic iff their coordinate rings are isomorphic.*

Exercise 1.5.13. 1. Show that the parametrization of the twisted cubic curve,

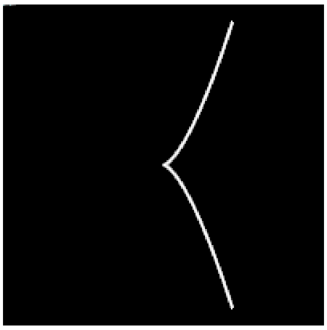
$$\mathbb{A}^1(\Bbbk) \to V(y - x^2, z - x^3) \subset \mathbb{A}^3(\Bbbk),\ t \mapsto (t, t^2, t^3),$$

is an isomorphism.

2. Show that the map

$$\mathbb{A}^1(\Bbbk) \to V(y^2 - x^3) \subset \mathbb{A}^2(\Bbbk),\ t \mapsto (t^2, t^3),$$

is a morphism but not an isomorphism.



Exercise 1.5.14. Let $\Bbbk$ be infinite. Consider the parabola $A = \mathrm{V}(y - x^2) \subset \mathbb{A}^2(\Bbbk)$ and the hyperbola $B = \mathrm{V}(xy-1) \subset \mathbb{A}^2(\Bbbk)$. Show that every morphism $A \to B$ is constant. In particular, the curves A and B are not isomorphic.

Exercise 1.5.15. 1. Let

$$f_i = a_{i1}x_1 + \cdots + a_{in}x_n + b_i \in \Bbbk[x_1, \ldots, x_n],\ i = 1, \ldots, n,$$

be polynomials of degree one, and let $\alpha : \mathbb{A}^n(\Bbbk) \to \mathbb{A}^n(\Bbbk)$ be the morphism given by $f_1, \ldots .f_n$. Show that α is an isomorphism iff the matrix (a_{ij}) is invertible. In this case, α is called an **affine change of coordinates on** $\mathbb{A}^n(\Bbbk)$.

2. If $A \subset \mathbb{A}^n(\Bbbk)$ is a nonempty linear subvariety, show that there is an affine change of coordinates α on $\mathbb{A}^n(\Bbbk)$ which takes A to $\mathrm{V}(x_1, \ldots, x_{n-d})$ for some number d. Show that this number is independent of the choice of α. It is called the **dimension** of A. Observe that if $\Bbbk$ is infinite, then $\mathrm{I}(\mathrm{V}(x_1, \ldots, x_{n-d})) = (x_1, \ldots, x_{n-d})$, hence A is a variety since $\Bbbk[x_1, \ldots, x_n]/(x_1, \ldots, x_{n-d}) \cong \Bbbk[x_{n-d+1}, \ldots, x_n]$ is a domain.

3. If $p = (a_1, \ldots, a_n), q = (b_1, \ldots, b_n)$ are distinct points in $\mathbb{A}^n(\Bbbk)$, the **line** through p and q is defined to be

$$\{(a_1 + t(b_1 - a_1), \ldots, a_n + t(b_n - a_n)) \mid t \in \Bbbk\} \subset \mathbb{A}^n(\Bbbk).$$

Show that a line is a linear subvariety of dimension 1, and that conversely every linear subvariety of dimension 1 is the line through any two of its points.

We refer to every isomorphism $\mathbb{A}^n(\Bbbk) \to \mathbb{A}^n(\Bbbk)$ as a **change of coordinates on** $\mathbb{A}^n(\Bbbk)$. The map $\mathbb{A}^2(\Bbbk) \to \mathbb{A}^2(\Bbbk)$ given by $f_1 = x$ and $f_2 = y + x^2$ is an example of a change of coordinates which is not affine.

We already know that the coordinate ring of an affine algebraic set A over $\Bbbk$ is reduced and finitely generated as a $\Bbbk$-algebra. Over algebraically closed fields, also the converse is true.

Proposition 1.5.16. *If $\Bbbk = \bar{\Bbbk}$ is algebraically closed, every reduced finitely generated commutative $\Bbbk$-algebra T is of the form $T = \Bbbk[A]$ for some affine algebraic set A over $\Bbbk$.*

Proof. Choose generators $t_1, \ldots, t_n$ of T, and let I be the kernel of the map

$$\Bbbk[x_1, \ldots, x_n] \to T = \Bbbk[t_1, \ldots, t_n],\ x_i \mapsto t_i.$$

Then

$$\Bbbk[x_1, \ldots, x_n]/I \cong T,$$

and I is a radical ideal since T is reduced. The Nullstellensatz yields $I = \mathrm{I}(\mathrm{V}(I))$, and we may take $A = \mathrm{V}(I)$. $\square$

The proof shows that if $\Bbbk$ is any field, then every finitely generated commutative $\Bbbk$-algebra is of type $\Bbbk[x_1, \ldots, x_n]/I$ for some ideal I in some polynomial ring $\Bbbk[x_1, \ldots, x_n]$. These algebras are often called **affine $\Bbbk$-algebras**, or simply **affine rings**.

Remark 1.5.17.
1. In the language of categories (see Mac Lane [1998]), Theorem 1.5.8 can be rephrased as follows. Over an algebraically closed field $\Bbbk = \bar{\Bbbk}$, the functor $A \mapsto \Bbbk[A]$ identifies the category of affine algebraic sets with the category of reduced affine rings. The category of affine varieties corresponds to that of **affine domains**, that is, of integral affine rings.

2. Grothendieck's concept of affine schemes gives a geometric interpretation of the full category of commutative rings with a multiplicative identity (see Hartshorne [1977], Eisenbud and Harris [2000]).

1.6 Additional exercises

Exercise 1.6.1. If $\Bbbk$ is a not algebraically closed, show that every algebraic subset of $\mathbb{A}^n(\Bbbk)$ can be defined by a single polynomial equation. See also Exercise 1.3.5.
Hint. Consider the case of the origin in $\mathbb{A}^2(\Bbbk)$ first.

Chapter 2

Gröbner Bases

The results of the first chapter allow us to attack geometric proSblems by means which require computations in polynomial rings and, more generally, arbitrary affine rings. Consider, for example, the basic problem of solvability: Given $f_1, \ldots, f_r \in \Bbbk[x_1, \ldots, x_n]$, decide whether the system

$$f_1(x_1, \ldots, x_n) = f_2(x_1, \ldots, x_n) = \ldots = f_r(x_1, \ldots, x_n) = 0$$

has no solution over the algebraic closure $\bar{\Bbbk}$ of $\Bbbk$. According to Hilbert's Nullstellensatz, this problem can be reformulated as follows: Given $f_1, \ldots, f_r \in \Bbbk[x_1, \ldots, x_n]$, decide whether

$$1 \in (f_1, \ldots, f_r).$$

A more general problem is the **ideal membership problem** in $\Bbbk[x_1, \ldots, x_n]$: Given $g, f_1, \ldots, f_r \in \Bbbk[x_1, \ldots, x_n]$, decide whether

$$g \in (f_1, \ldots, f_r).$$

That is, decide whether there exist polynomials $g_1, \ldots, g_r \in \Bbbk[x_1, \ldots, x_n]$ such that

$$g = \sum_{i=1}^{r} g_i f_i.$$

In principle, this asks for solving a linear system of equations in the unknown coefficients of the g_i. However, as long as we do not have a bound on the degrees of the g_i, we face a system in an unknown number of coefficients. There exist general bounds for the ideal membership problem, see Hermann

[1926], Mayr and Meyer [1982], Bayer and Stillman [1988], Kollár [1999], but we will not discuss these bounds here. Instead, we settle the problem via a different approach, without using any bounds.

To see what can be done, we first consider the case of one variable. In this case, ideal membership may be decided with the help of Euclidean division with remainder. To attack the general case, we extend the division algorithm to polynomials in more than one variable. Unfortunately, the extended algorithm shows some undesirable behavior. To remedy the situation (and thus to decide ideal membership), we consider special sets of generators of ideals, which are well behaved with respect to the extended division algorithm, and which can be computed from any given finite set of generators by a fundamental algorithm due to the thesis of Buchberger [1965, 1970] Following Buchberger, these special sets of generators are called Gröbner bases (Gröbner was Buchberger's thesis advisor).

The concept of Gröbner bases allows us to reduce many questions on arbitrary ideals in polynomial rings to questions on ideals generated by monomials, which are much easier. In this way, Buchberger's algorithm computes, for instance, a $\Bbbk$-vector space basis of any given affine ring (that is, every finite part of the basis). This gives an algorithmic way of computing in affine rings.

Buchberger's algorithm relies on Buchberger's criterion which allows us to test whether a given set of polynomials $f_1, \dots, f_r$ is in fact a Gröbner basis. If so, the test yields certain $\Bbbk[x_1, \dots, x_n]$-linear relations on $f_1, \dots, f_r$ which play a key role in the proof of Buchberger's criterion. We think of a $\Bbbk[x_1, \dots, x_n]$-linear relation

$$g_1 f_1 + \dots g_r f_r = 0$$

as a column vector

$${}^t(g_1, \dots, g_r) \in \Bbbk[x_1, \dots, x_n]^r,$$

and call it a syzygy on $f_1, \dots, f_r$. The concept of Gröbner bases extends from ideals to submodules of free modules $\Bbbk[x_1, \dots, x_n]^r$, and Buchberger's algorithm computes syzygies as well. In fact, if $f_1, \dots, f_r$ form a Gröbner basis, the special syzygies obtained by Buchberger's test form a Gröbner basis for the module of all the syzygies on $f_1, \dots, f_r$. Theoretically, this allows us to give a short proof of Hilbert's syzygy theorem which in turn will be used in Chapter **??** to verify the polynomial nature of Hilbert functions.

Practically, we use syzygy computations to manipulate ideals, for instance, to compute ideal intersections.

Another important application of Buchberger's algorithm is closely related to solving polynomial equations, namely the elimination of variables from a given system of polynomial equations.

2.1 Monomials and monomial ideals

We use multiindices to write monomials in several variables: A **monomial** in $\mathbb{k}[x_1, \ldots, x_n]$ is a product

$$x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n},$$

where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$.

A number of operations on polynomials are simpler for monomials than for arbitrary polynomials. For instance, if x^α and x^β are two monomials in $\mathbb{k}[x_1, \ldots, x_n]$, with $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}_0^n$, their **least common multiple** is

$$\mathrm{LCM}(x^\alpha, x^\beta) = x_1^{\max(\alpha_1, \beta_1)} \cdot \ldots \cdot x_n^{\max(\alpha_n, \beta_n)},$$

and their **greatest common divisor** is

$$\mathrm{GCD}(x^\alpha, x^\beta) = x_1^{\min(\alpha_1, \beta_1)} \cdot \ldots \cdot x_n^{\min(\alpha_n, \beta_n)}.$$

Similarly, many operations on ideals are easier for ideals generated by monomials than for arbitrary ideals.

Definition 2.1.1. An ideal $I \subset \mathbb{k}[x_1, \ldots, x_n]$ is a **monomial ideal** if it is generated by monomials.

The first step in Gordan's proof of Hilbert's basis theorem 1.1.12 is to show that monomial ideals are finitely generated (see Corollary 2.3.3 for the remaining part of the proof) .

Exercise 2.1.2 (Gordan's Lemma). Prove by induction on the number of variables that every nonempty set of monomials in $\mathbb{k}[x_1, \ldots, x_n]$ has only finitely many minimal elements in the partial order defined by divisibility (x^α is greater than or equal to x^β iff x^α is divisible by x^β iff $\alpha - \beta \in \mathbb{N}_0^n$). Deduce that every monomial ideal $I \subset \mathbb{k}[x_1, \ldots, x_n]$ can be generated by finitely many monomials.

If $I \subset \Bbbk[x_1, \ldots, x_n]$ is a monomial ideal, the minimal elements in the partial order defined by divisibility on the monomials of I are uniquely determined. They can be obtained from any set of monomial generators by removing those which are divisible by others. We refer to them as the **minimal generators of I**.

Exercise 2.1.3. Let $I = (m_1, \ldots, m_r)$ and $J = (n_1, \ldots, n_s)$ be monomial ideals of $\Bbbk[x_1, \ldots, x_n]$ given by monomial generators, and let m be a monomial in $\Bbbk[x_1, \ldots, x_n]$.

1. Show that

$$I \cap J = (\mathrm{LCM}(m_i, n_j) \mid 1 \leq i \leq r,\, 1 \leq j \leq s).$$

2. Show that

$$(I : m) := \{f \in \Bbbk[x_1, \ldots, x_n] \mid fm \in I\}$$

is an ideal which is generated by the monomials

$$\mathrm{LCM}(m_i, m)/m = m_i/\,\mathrm{GCD}(m_i, m),\ 1 \leq i \leq r.$$

In particular, $I \cap J$ and $(I : m)$ are again monomial ideals.

Recall that if R is a ring, a **free R-module** is an R-module F which has a basis (in this context, a basis is a set of generators whose elements are R-linearly independent). If F has a finite basis, the number of basis elements only depends on F. This number is the **rank** of F. That F is a free R-module of rank s means that $F \cong R^s$. Indeed, map the ith basis vector of F to the ith canonical basis vector $\epsilon_i = {}^t(0, \ldots, 1, \ldots, 0)$ of R^s.

Most of the terminology used when working with polynomials extends to elements of free modules over polynomial rings. In what follows, let $R = \Bbbk[x_1, \ldots, x_n]$, and let F be a free R-module with a fixed basis $e_1, \ldots, e_s$.

Definition 2.1.4. A **monomial** in F, **involving the basis element** $\mathbf{e}_i$, is a monomial in R multiplied by e_i. A **term** in F is a monomial in F multiplied by a **coefficient** $c \in \Bbbk$. Every nonzero element $f \in F$ can be uniquely expressed as the sum of finitely many nonzero terms involving distinct monomials. These terms are called the **terms of f**.

For terms in F, notions like multiple or divisible are defined in the obvious way. For instance, $ax^\alpha e_i$ is **divisible** by $bx^\beta e_j \neq 0$, with **quotient**

$a/b\ x^{\alpha-\beta} \in R$, if $i = j$ and x^α is divisible by x^β. Similarly, we define the **least common multiple**

$$\mathrm{LCM}(ax^\alpha e_i, bx^\beta e_i) = \mathrm{LCM}(x^\alpha, x^\beta) \in R$$

and the **greatest common divisor**

$$\mathrm{GCD}(ax^\alpha e_i, bx^\beta e_i) = \mathrm{GCD}(x^\alpha, x^\beta) \in R$$

of nonzero terms involving the same basis element. If $ax^\alpha e_i$ and $bx^\beta e_j$ involve distinct basis elements, we set $\mathrm{LCM}(ax^\alpha e_i, bx^\beta e_j) = 0$.

A submodule of F is a **monomial submodule** if it is generated by monomials. It easily follows from Gordan's lemma that every such submodule is generated by finitely many monomials. As in the ideal case, we have a uniquely determined set of **minimal generators**.

Exercise 2.1.5. If I, J are monomial submodules of F given by monomial generators, and if $m \in F$ is a term, show how to obtain monomial generators for the subbmodule $I \cap J \subset F$ and the ideal $(I : m) := \{f \in R \mid fm \in I\} \subset R$.

For monomial submodules of F (and thus in particular for monomial ideals of R), membership can be decided as follows. If $I \subset F$ is a submodule generated by monomials $m_1, \ldots, m_r$, then a term $m \in F$ is contained in I iff m is divisible by some m_i. An arbitrary element $g \in F$ is contained in I iff each of its terms is contained in I.

2.2 Division with remainder

We first consider the case of polynomials in one variable x. The monomials in $\mathbb{k}[x]$, and thus the terms of any nonzero polynomial $f \in \mathbb{k}[x]$, can be arranged unambiguously in decreasing order by degree. If we list the terms of f in this way, the term of highest degree, the leading term of f, comes first. We denote this term by $\mathbf{L}(f)$.

Theorem 2.2.1 (Euclidean division with remainder). *Let f be a nonzero polynomial in $\mathbb{k}[x]$. For every $g \in \mathbb{k}[x]$ there exist uniquely determined $g_1, h \in \mathbb{k}[x]$ such that*

$$g = g_1 f + h \quad \textit{and} \quad \deg h < \deg f.$$

We call h the **remainder** *of g on division by f.*

Indeed, Euclid's division algorithm finds the desired g_1 and h as follows. If $\deg g < \deg f$, pick $g_1 = 0$ and $h = g$. If $\deg g \geq \deg f$, then $\mathbf{L}(g)$ is a multiple of $\mathbf{L}(f)$, say $\mathbf{L}(g) = m\mathbf{L}(f)$, and we can remove $\mathbf{L}(g)$ by subtracting mf from g. In this way, we obtain a new dividend, namely $g - mf$, whose leading term has a smaller degree than that of g. Therefore, recursively, we can remove all multiples of $\mathbf{L}(f)$ from g in finitely many steps.

Remark 2.2.2. Observe that Euclidean division with remainder also works for univariate polynomials with coefficients in a ring, provided that the divisor f is monic.

Exercise 2.2.3. If an expression $g = g_1 f + h$ as in Theorem 2.2.1 is given, show that $\mathrm{GCD}(f, g) = \mathrm{GCD}(f, h)$ (here GCD refers to the monic greatest common divisor). Deduce Euclid's algorithm for computing GCD's in $\Bbbk[x]$.

Euclidean division with remainder allows us to decide ideal membership in $\Bbbk[x]$ as follows. If nonzero polynomials $g, f_1, \ldots, f_r \in \Bbbk[x]$ are given, use Euclid's algorithm to compute $f = \mathrm{GCD}(f_1, \ldots, f_r)$. Then $(f_1, \ldots, f_r) = (f)$, so $g \in (f_1, \ldots, f_r)$ iff the remainder of g on division by f is zero.

To solve the ideal membership problem for polynomials in more than one variable in a similar way, we have to extend the division algorithm. Since for $n \geq 2$ not every ideal in $\Bbbk[x_1, \ldots, x_n]$ is generated by just one element, we ask for an algorithm which divides by several polynomials in $\Bbbk[x_1, \ldots, x_n]$ instead of one. As in the case of one variable, we need a total order on the set of monomials in $\Bbbk[x_1, \ldots, x_n]$ which singles out leading terms of polynomials in a suitable way.

Example 2.2.4. If $f_1 = x^2 + xy \in \Bbbk[x, y]$, every polynomial $g \in \Bbbk[x, y]$ can be written in the form $g = g_1 f_1 + h$, where no term of h is a multiple of x^2. Similarly, we may use $f_2 = y^2 + xy \in \Bbbk[x, y]$ to remove multiples of y^2. We cannot use f_1 and f_2, however, to remove multiples of x^2 and multiples of y^2 at the same time. That is, not every polynomial $g \in \Bbbk[x, y]$ can be written in the form

$$g = g_1 f_1 + g_2 f_2 + h,$$

where no term of h is contained in the ideal (x^2, y^2). Otherwise, the quotient ring $\Bbbk[x, y]/(f_1, f_2)$ would have a $\Bbbk$-vector space basis represented by a subset of $1, x, y, xy$. Hence the locus of zeros $\mathrm{V}(f_1, f_2) \subset \mathbb{A}^2(\bar{\Bbbk})$ would be finite by Exercise 1.3.4, a contradiction to $\mathrm{V}(f_1, f_2) \supset \mathrm{V}(x + y)$.

Note that every total order on the monomials which singles out the leading terms x^2 of f_1 and y^2 of f_2 is not compatible with the multiplication in $\Bbbk[x, y]$ in the sense of the following definition.

Definition 2.2.5. A **monomial order** on $\mathbb{k}[x_1, \dots, x_n]$ is a total order $>$ on the set of monomials in $\mathbb{k}[x_1, \dots, x_n]$ such that if $\alpha, \beta, \gamma \in \mathbb{N}_0^n$, then

$$x^\alpha > x^\beta \implies x^\gamma x^\alpha > x^\gamma x^\beta.$$

By renaming the variables we can always achieve that $x_1 > \cdots > x_n$. We will only describe monomial orders with this property. Here are our first examples.

Example 2.2.6. 1. **(Lexicographic order)**. Set

$$x^\alpha >_{\text{lex}} x^\beta \iff \text{the first nonzero entry of } \alpha - \beta \text{ is positive.}$$

2. **(Weight orders)**. If $w\colon \mathbb{R}^n \to \mathbb{R}$ is a linear form with $\mathbb{Q}$-linearly independent coefficients, set

$$x^\alpha >_w x^\beta \iff w(\alpha) > w(\beta).$$

Exercise 2.2.7. Let $>$ be a monomial order on $\mathbb{k}[x_1, \dots, x_n]$, and let X be a finite set of monomials in $\mathbb{k}[x_1, \dots, x_n]$. Prove that there exists a weight order $>_w$ on $\mathbb{k}[x_1, \dots, x_n]$ which coincides on X with the given order $>$.
Hint. Consider the set of differences

$$\{\alpha - \beta \mid x^\alpha, x^\beta \in X, x^\alpha > x^\beta\}.$$

By abuse of notation, if a monomial order $>$ on $\mathbb{k}[x_1, \dots, x_n]$ is given, we may extend $>$ to terms. We write $cx^\alpha \geq dx^\beta$ (respectively, $cx^\alpha > dx^\beta$), if cx^α and dx^β are nonzero terms with $x^\alpha \geq x^\beta$ (respectively, $x^\alpha > x^\beta$), or if cx^α is any term and dx^β is zero. This allows us, for instance, to compare the terms of any given nonzero polynomial $f \in \mathbb{k}[x_1, \dots, x_n]$ with each other (although we do not obtain a partial order on the set of all terms in $\mathbb{k}[x_1, \dots, x_n]$). We usually list the terms of f in decreasing order under $>$.

Remark-Definition 2.2.8. Let $>$ be a monomial order on $\mathbb{k}[x_1, \dots, x_n]$.

1. Let $f \in \mathbb{k}[x_1, \dots, x_n]$ be a nonzero polynomial. The **leading term** (or, **initial term**) of f, written

$$\mathbf{L}_>(f) = \mathbf{L}(f),$$

is the greatest term of f with repect to $>$. We extend this notation to the zero polynomial by writing $\mathbf{L}(0) = 0$.

2. If $f, g \in \Bbbk[x_1, \dots, x_n]$, then

$$\mathbf{L}(fg) = \mathbf{L}(f)\mathbf{L}(g),$$

and

$$\mathbf{L}(f + g) \leq \max\{\mathbf{L}(f), \mathbf{L}(g)\},$$

with equality iff $\mathbf{L}(f)$ and $\mathbf{L}(g)$ do not cancel each other in $f + g$ (in this case, to really get equality, the constant on the right hand side has to be adjusted correctly if $\mathbf{L}(f)$ and $\mathbf{L}(g)$ involve the same monomial).

With respect to a monomial order as in Definition **??**, the leading term of the new dividend in any single step of the division process will be smaller than that of the preceding dividend. This does not imply, however, that the process terminates in finitely many steps.

Example 2.2.9. In the case of one variable x, single out the terms of lowest degree as leading terms. Then dividing $g = x$ by $f = x - x^2$, for instance, yields leading terms of the intermediate dividends which are higher and higher powers of x.

Proposition 2.2.10. *If $>$ is a monomial order on $\Bbbk[x_1, \dots, x_n]$, the following are equivalent:*

1. *$>$ is* **artinian***, that is, every nonempty set of monomials has a least element.*
2. *$>$ is* **global***, that is,*

$$x_i > 1 \quad \textit{for} \quad i = 1, \dots, n.$$

3. *$>$* **refines the partial order defined by divisibility***, that is,*

$$x^\alpha \ \textit{divisible by} \ x^\beta \implies x^\alpha > x^\beta.$$

Proof. The only nontrivial part of the proof is to show that 3 implies 1. If 3 holds, and if X is a nonempty set of monomials, the monomial ideal $I = (X) \subset \Bbbk[x_1, \dots, x_n]$ generated by X is in fact generated by a finite subset of monomials Y of X due to Gordan's lemma. Whence every monomial in X is divisible by a monomial in Y, and the least element of Y is the least element of X. $\square$

We use the word global to distinguish the monomial orders considered here from those used for computations in local rings later on (see Section **??**). The lexicographic order is global. A weight order $>_w$ is global iff the coefficients of w are strictly positive.

Theorem 2.2.11 (Division with remainder, determinate version). *Let $>$ be a global monomial order on $R = \mathbb{k}[x_1, \dots, x_n]$, and let $f_1, \dots, f_r \in R \setminus \{0\}$. For every $g \in R$ there exist uniquely determined $g_1, \dots, g_r, h \in R$ such that*

1. *$g = g_1 f_1 + \ldots + g_r f_r + h$,*
2. *for $i > j$ no term of $g_i \, \mathbf{L}(f_i)$ is divisible by $\mathbf{L}(f_j)$, and*
3. *for all i no term of h is divisible by $\mathbf{L}(f_i)$.*

We call h the **remainder** *of g on determinate division by $f_1, \dots, f_r$.*

Proof. Uniqueness. The nonzero leading terms $\mathbf{L}(g_i f_i) = \mathbf{L}(g_i)\mathbf{L}(f_i)$, $1 \le i \le r$, and $\mathbf{L}(h)$ on the right hand side of any presentation as in the assertion involve different monomials and hence do not cancel. If two such presentations for g are given, their difference is a presentation for the zero polynomial satisfying conditions 2 and 3. Since the leading terms do not cancel, the difference must be the trivial presentation.

Existence (**determinate division algorithm**). We proceed as in the case of one variable. If $f_1, \dots, f_r$ are monomials, we obtain the desired presentation by successively removing all multiples of f_1, f_2, $\dots$, and f_r from g (in that order). In the general case, we first divide g by $\mathbf{L}(f_1), \dots, \mathbf{L}(f_r)$, that is, we compute the unique presentation

$$g = \sum_{i=1}^{r} g_i \, \mathbf{L}(f_i) + h$$

satisfying 2 and 3. Then $\tilde{g} = g - \sum_{i=1}^{s} g_i f_i - h$ is either zero, and we are done, or $\mathbf{L}(\tilde{g}) < \mathbf{L}(g)$. By recursion, since $>$ is artinian, we can assume in the latter case that $\tilde{g}$ has a presentation $\tilde{g} = \sum_{i=1}^{r} \tilde{g}_i f_i + \tilde{h}$ which satisfies 2 and 3. Then $h + \tilde{h}$ and the $g_i + \tilde{g}_i$ give the desired presentation for g. $\square$

Due to condition 2 the order in which $f_1, \dots, f_r$ are listed plays a crucial role in the determinate division algorithm.

Example 2.2.12. Consider $f_1 = x^2y - y^3, f_2 = x^3 \in \Bbbk[x, y]$ with the lexicographic order (with x larger than y). Then $\mathbf{L}(f_1) = x^2y$. For $g = x^3y$ the determinate division algorithm proceeds as follows:

$$x^3y = x \cdot \mathbf{L}(f_1) + 0 \cdot \mathbf{L}(f_2) + 0,$$

$$\tilde{g} = g - x \cdot f_1 = xy^3 = 0 \cdot \mathbf{L}(f_1) + 0 \cdot \mathbf{L}(f_2) + xy^3,$$

and

$$\tilde{\tilde{g}} = \tilde{g} - xy^3 = g - x \cdot f_1 - xy^3 = 0.$$

Hence the desired representation is

$$g = x^3y = x \cdot (x^2y - y^3) + 0 \cdot (x^3) + xy^3.$$

If we interchange f_1 and f_2, determinate division yields the expression

$$x^3y = y\,(x^3) + 0\,(x^2y - y^3) + 0.$$

Remark 2.2.13 (Division with remainder, indeterminate versions). If $>$ is a global monomial order on $\Bbbk[x_1, \ldots, x_n]$, the division algorithm still terminates if on each stage we remove *some* term of the dividend with the help of *some* $\mathbf{L}(f_i)$ by which it is divisible. In this case the resulting representation 1, which is no longer uniquely determined, only satisfies the following condition:

2'. $\mathbf{L}(g) \geq \mathbf{L}(g_i f_i)$ whenever both sides are nonzero.

If we only remove the leading terms of the dividends in this way, we obtain a representation 1 which satisfies 2' and the following condition:

3'. If h is nonzero, then $\mathbf{L}(h)$ is not divisible by $\mathbf{L}(f_i)$ for all i.

Any such representation is called a **standard expression for g in terms of the f$_i$ with remainder h**.

Exercise 2.2.14. Define a global monomial order on $\Bbbk[x, y, z]$ which yields the leading terms y of $y - x^2$ and z of $z - x^3$, and reconsider the first part of Exercise 1.2.2.

To extend division with remainder to free modules over polynomial rings, we write $R = \Bbbk[x_1, \ldots, x_n]$ and consider a free R-module F with a fixed basis $e_1, \ldots, e_s$.

Definition 2.2.15. A **monomial order** on F is a total order $>$ on the set of monomials in F such that if $x^\alpha e_i$ and $x^\alpha e_j$ are monomials in F, and x^γ is a monomial in R, then

$$x^\alpha e_i > x^\beta e_j \implies x^\gamma x^\alpha e_i > x^\gamma x^\beta e_j.$$

Remark 2.2.16. In this book we require in addition that

$$x^\alpha e_i > x^\beta e_i \iff x^\alpha e_j > x^\beta e_j \quad \text{for all} \quad i, j.$$

Then $>$ induces a unique monomial order on R in the obvious way, and notions like **global** carry over to monomial orders on F.

Exercise 2.2.17 (Division with remainder in free modules). Establish determinate and indeterminate division algorithms with remainder for elements in F. Extend the relevant definitions and results from R to F.

Remark 2.2.18. One way of getting a monomial order on F is to pick a monomial order $>$ on R, and extend it to F. This can be done in at least two ways: giving priority to the monomials in R,

$$x^\alpha e_i > x^\beta e_j \iff x^\alpha > x^\beta \text{ or } x^\alpha = x^\beta \text{ and } i > j,$$

or to the components of F,

$$x^\alpha e_i > x^\beta e_j \iff i > j \text{ or } i = j \text{ and } x^\alpha > x^\beta.$$

Exercise 2.2.19. Consider the free module $F = \mathbb{k}[x, y]^3$ with its canonical basis vectors $e_1 = {}^t(1, 0, 0)$, $e_2 = {}^t(0, 1, 0)$, and $e_3 = {}^t(0, 0, 1)$, and the elements

$$g = \begin{pmatrix} x^2y + x^2 + xy^2 + xy \\ xy^2 - 1 \\ xy + y^2 \end{pmatrix}, \; f_1 = \begin{pmatrix} xy + x \\ 0 \\ y \end{pmatrix}, \; f_2 = \begin{pmatrix} 0 \\ y^2 \\ x + 1 \end{pmatrix} \in F.$$

Extend the lexicographic order on $\mathbb{k}[x, y]$ to F in the two ways described above, and divide g by f_1, f_2 with respect to both orders (use the determinate division algorithm).

2.3 Gröbner bases and Buchberger's algorithm

In Example 2.2.12, with $f_1 = x^2y - y^3$ and $f_2 = x^3$, we obtained the standard expressions

$$g = x^3y = x \cdot f_1 + 0 \cdot f_2 + xy^3$$

and

$$x^3y = y \cdot f_2 + 0 \cdot f_1 + 0,$$

which in particular have two different remainders. Even worse, the remainder in the first standard expression is nonzero though, as shown by the second standard expression, the dividend x^3y is in the ideal I generated by the divisors. The problem is that x^3y and thus also the remainder xy^3 are contained in the ideal $(x^2y - y^3, x^3)$, but xy^3 cannot be removed, since it is not divisible by the leading terms x^2y and x^3 of the divisors. To decide ideal membership, we need to be able to remove all leading terms of the elements of I using the leading terms of the divisors.

Definition 2.3.1. Let $>$ be a monomial order on $\Bbbk[x_1, \dots, x_n]$.

1. Let $I \subset \Bbbk[x_1, \dots, x_n]$ be an ideal. The **leading ideal** (or, **initial ideal**) of I with respect to $>$ is the monomial ideal

$$\mathbf{L}(I) := \mathbf{L}_>(I) := (\mathbf{L}_>(f) \mid f \in I).$$

   That is, $\mathbf{L}(I)$ is generated by the leading terms of the elements of I.

2. A finite set of polynomials $f_1, \dots, f_r \in \Bbbk[x_1, \dots, x_n]$ is a **Gröbner basis** with respect to $>$ if

$$\mathbf{L}_>(f_1, \dots, f_r) = (\mathbf{L}_>(f_1), \dots, \mathbf{L}_>(f_r)).$$

   That is, the leading terms $\mathbf{L}(f_1), \dots, \mathbf{L}(f_r)$ generate the leading ideal of the ideal $I := (f_1, \dots, f_r)$. We then say that $f_1, \dots, f_r$ form a **Gröbner basis for I** with respect to $>$.

Proposition 2.3.2. *Let $f_1, \dots, f_r \in \Bbbk[x_1, \dots, x_n] \setminus \{0\}$ form a Gröbner basis with respect to a global monomial order on $\Bbbk[x_1, \dots, x_n]$. If $g \in \Bbbk[x_1, \dots, x_n]$ is any polynomial, and if $g = \sum_{i=1}^r g_i f_i + h$ is any standard expression for g in terms of $f_1, \dots, f_r$, then $g \in (f_1, \dots, f_r)$ iff the remainder h is zero.*

Proof. If h is zero, then obviously $g \in (f_1, \dots, f_r)$. Conversely, if $g \in (f_1, \dots, f_r)$, then $h \in (f_1, \dots, f_r)$ and thus $\mathbf{L}(h) \in \mathbf{L}(f_1, \dots, f_r) = (\mathbf{L}(f_1), \dots, \mathbf{L}(f_r))$. Whence $h = \mathbf{L}(h) = 0$ by condition 3' on the remainder in a standard expression. $\square$

So Gröbner bases are well behaved with respect to division with remainder.

Corollary 2.3.3 (Gordan). *There is a Gröbner for any ideal $I \subset \Bbbk[x_1,\dots,x_n]$ with respect to any global monomial order on $\Bbbk[x_1,\dots,x_n]$. The elements of every such basis generate I. In particular, $\Bbbk[x_1,\dots,x_n]$ is Noetherian.*

Proof. Monomial ideals of $\Bbbk[x_1,\dots,x_n]$ are finitely generated by Gordan's Lemma 2.1.2. Hence there exist finitely many polynomials $f_1,\dots,f_r \in I$ with $\mathbf{L}(I) = (\mathbf{L}(f_1),\dots,\mathbf{L}(f_r))$. That is, $f_1,\dots,f_r$ form a Gröbner basis for I. If $f_1,\dots,f_r$ is any such basis, we deduce from the proposition that every element $g \in I$ has a standard expression in terms of the f_i with remainder zero. In particular, $f_1,\dots,f_r$ generate I. □

Remark 2.3.4. Gordan's proof has as every other proof of Hilbert's basis theorem two ingredients, namely induction on the number of variables (here used to verify Gordan's Lemma 2.1.2), and division with remainder. The advantage of Gordan's proof is that it separates these ingredients.

In what follows, let $>$ be a fixed global monomial order on $\Bbbk[x_1,\dots,x_n]$.

Macaulay [1927] used the idea of obtaining information on an ideal from information on its initial ideal to study Hilbert functions (see Section **??** for Hilbert functions). On his way, he proved the following important result.

Theorem 2.3.5 (Macaulay). *Let $I \subset \Bbbk[x_1,\dots,x_n]$ be an ideal. The monomials not in $\mathbf{L}(I)$ represent a $\Bbbk$-vector space basis for the quotient ring $\Bbbk[x_1,\dots,x_n]/I$.*

Proof. Write $R = \Bbbk[x_1,\dots,x_n]$, let

$$\mathcal{B} := \{m + I \mid m \in R \text{ a monomial}, m \notin \mathbf{L}(I)\} \subset R/I,$$

and pick polynomials $f_1,\dots,f_r \in R\setminus\{0\}$ which form a Gröbner basis for I.

Let $g \in R$, and let $g = \sum_{i=1}^r g_i f_i + h$ be a standard expression satisfying condition 3 of determinate division. Then no term of h is in $(\mathbf{L}(f_1),\dots,\mathbf{L}(f_r)) = \mathbf{L}(I)$, hence the class $g+I = h+I$ is a $\Bbbk$-linear combination of the elements in $\mathcal{B}$. That is, the elements of $\mathcal{B}$ generate $\Bbbk[x_1,\dots,x_n]/I$ as a $\Bbbk$-vector space.

If in addition $g \in I$, then $h = 0$ by Proposition 2.3.2, and $\mathbf{L}(g)$ is divisible by some $\mathbf{L}(f_i)$ since the largest of the leading terms $\mathbf{L}(g_i f_i) = \mathbf{L}(g_i)\mathbf{L}(f_i)$ on the right hand side of the standard expression do not cancel due to condition 2' of division with remainder. Thus $g = 0$ if no term of g is in $(\mathbf{L}(f_1),\dots,\mathbf{L}(f_r))$. In particular, the elements of $\mathcal{B}$ are $\Bbbk$-linearly independent. □

Remark-Definition 2.3.6. If $g \in R = \Bbbk[x_1, \dots, x_n]$, a remainder h as in the proof above is uniquely determined by g, I, and $>$. It represents the class $g + I$ in terms of monomials that are not in $\mathbf{L}(I)$. We call h the **canonical representative of $\mathbf{g + I \in R/I}$** (or, the **normal form of g mod I**) with respect to $>$, written $\mathrm{NF}(g, I)$.

If a Gröbner basis for I is given, we may use canonical representatives to perform the sum and product operations in the affine ring R/I:

Exercise 2.3.7. Let $I \subset \Bbbk[x_1, \dots, x_n]$ be an ideal. If $f, g \in \Bbbk[x_1, \dots, x_n]$, show that

$$\mathrm{NF}(f + g, I) = \mathrm{NF}(f, I) + \mathrm{NF}(g, I), \text{ and}$$
$$\mathrm{NF}(f \cdot g, I) = \mathrm{NF}(\mathrm{NF}(f, I) \cdot \mathrm{NF}(g, I), I).$$

We refer to Example 2.3.11 for an explicit computation.

So Proposition 2.3.2 and Macaulay's Theorem 2.3.5 allow us to decide ideal membership and to compute in affine rings, provided that we can compute Gröbner bases (Corollary 2.3.3 only guarantees their existence). At this point, however, we do not even know how to recognize whether a given set of polynomials $f_1, \dots, f_r \in \Bbbk[x_1, \dots, x_n] \setminus \{0\}$ forms a Gröbner basis. Indeed, to verify the defining condition of a Gröbner basis means to test for each of the infinitely many $g \in (f_1, \dots, f_r)$ whether $\mathbf{L}(g)$ is divisible by one of the $\mathbf{L}(f_i)$.

If $g \in (f_1, \dots, f_r)$, then $g = a_1 f_1 + \dots + a_r f_r$ for some $a_i \in \Bbbk[x_1, \dots, x_n]$, and

$$\mathbf{L}(g) = \max\{\mathbf{L}(a_1)\mathbf{L}(f_1), \dots, \mathbf{L}(a_r)\mathbf{L}(f_r)\} \in (\mathbf{L}(f_1), \dots, \mathbf{L}(f_r)),$$

provided that the largest of the leading terms $\mathbf{L}(a_i f_i) = \mathbf{L}(a_i)\mathbf{L}(f_i)$ on the right hand side of the representation of g do not cancel. As already remarked, such cancellations do not occur in standard expressions. Taking Proposition 2.3.2 into account, we see that $f_1, \dots, f_r$ form a Gröbner basis iff each $g \in (f_1, \dots, f_r)$ has a standard expression in terms of the f_i with remainder zero (in this case, the remainder in every such standard expression is zero). Again, this amounts to checking a condition for the infinitely many $g \in (f_1, \dots, f_r)$. But now, a wonderful thing happens: According to Buchberger's criterion below, it is enough to check the condition for finitely many well-determined test elements in $(f_1, \dots, f_r)$. In fact, the simplest possible cancellations of the leading terms, involving just two of the generators, account for all obstructions to $f_1, \dots, f_r$ being a Gröbner basis.

Remark 2.3.8. Relations such as $fg - gf = 0$ show that ideal bases in the sense of Hilbert and Noether are not bases in the sense of linear algebra: the generators of ideals of $R = \Bbbk[x_1, \dots, x_n]$ are not R-linearly independent. For instance, if $m_1, m_2 \in R$ are two nonzero terms, and if

$$m_{ij} = \mathrm{LCM}(m_i, m_j)/m_j,$$

then

$$m_{12}m_2 - m_{21}m_1 = 0.$$

In fact, if $fm_2 - gm_1 = 0$ is any R-linear combination which is zero, then there exists a polynomial $h \in R$ such that

$$\begin{pmatrix} f \\ g \end{pmatrix} = h \begin{pmatrix} m_{12} \\ m_{21} \end{pmatrix} \in R^2$$

(see Exercise 2.1.3, 2).

Theorem 2.3.9 (Buchberger's criterion, first version). *Let $f_1, \dots, f_r \in \Bbbk[x_1, \dots, x_n]$ be nonzero polynomials. For all i, j, set*

$$m_{ij} = \mathrm{LCM}(\mathbf{L}(f_i), \mathbf{L}(f_j))/\mathbf{L}(f_j),$$

define the **S-polynomial** *of f_i and f_j to be*

$$\mathrm{S}(f_i, f_j) = m_{ji}f_i - m_{ij}f_j,$$

and let h_{ij} be a remainder on division of $\mathrm{S}(f_i, f_j)$ by the f_k. Then $f_1, \dots, f_r$ form a Gröbner basis iff all the h_{ij} are zero.

Note that we only need to check the remainders h_{ij} with $i > j$ since $\mathrm{S}(f_i, f_j) = -\mathrm{S}(f_j, f_i)$. We occasionally refer to the computation of these remainders as **Buchberger's test**. Before proving the criterion, we show how to use it for computing Gröbner.

Corollary 2.3.10. *If nonzero polynomials $f_1, \dots, f_r \in \Bbbk[x_1, \dots, x_n]$ are given, a Gröbner basis for the ideal $(f_1, \dots, f_r) \subset \Bbbk[x_1, \dots, x_n]$ can be computed in finitely many steps.*

Proof **(Buchberger's algorithm)**. If $f_1, \dots, f_r$ satisfy Buchberger's criterion, we are done. Otherwise Buchberger's test yields a nonzero remainder $h \in (f_1, \dots, f_r)$ with $\mathbf{L}(h) \notin (\mathbf{L}(f_1), \dots, \mathbf{L}(f_r))$, that is, with $(\mathbf{L}(f_1), \dots, \mathbf{L}(f_r)) \subsetneq (\mathbf{L}(f_1), \dots, \mathbf{L}(f_r), \mathbf{L}(h))$. In this case we include

$f_{r+1} := h$ in the set of generators and start over again. The resulting process terminates after finitely many steps with a Gröbner basis $f_1, \ldots, f_r, f_{r+1}, \ldots, f_{r'}$ for $(f_1, \ldots, f_r)$ since every ascending chain of (monomial) ideals of $\mathbb{k}[x_1, \ldots, x_n]$ is eventually stationary. □

Example 2.3.11. Consider $f_1 = x^2, f_2 = xy - y^2 \in \mathbb{k}[x, y]$ with the lexicographic order. Then $\mathbf{L}(f_2) = xy$. We compute the standard expression

$$\mathrm{S}(f_2, f_1) = x \cdot f_2 - y \cdot f_1 = -xy^2 = 0 \cdot f_1 - y \cdot f_2 - y^3,$$

and include the nonzero remainder $f_3 = -y^3$ in the set of generators. Computing the standard expressions

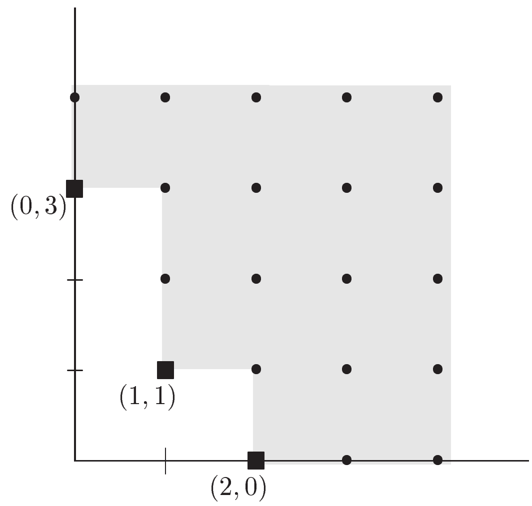
$$\mathrm{S}(f_3, f_1) = f_1 \cdot f_3 - f_3 \cdot f_1 = 0 = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3$$

and

$$\mathrm{S}(f_3, f_2) = x \cdot f_3 + y^2 \cdot f_2 = -y^4 = 0 \cdot f_1 + 0 \cdot f_2 + y \cdot f_3$$

with remainder zero, we find that f_1, f_2, f_3 form a Gröbner basis for the ideal $I = (f_1, f_2)$.

We visualize the monomials in $\mathbb{k}[x, y]$ by printing their exponent vectors:



The dots in the shaded region correspond to the monomials in $\mathbf{L}(I)$. The minimal generators of $\mathbf{L}(I)$ are y^3, xy, and x^2. By Macaulay's Theorem 2.3.5, the monomials $1, x, y, y^2$ not contained in the shaded region represent a $\mathbb{k}$-vector space basis for $\mathbb{k}[x, y]/I$. Hence every class in $\mathbb{k}[x, y]/I$ is canonically represented by a uniquely determined $\Bbbk$-linear combination $a + bx + cy + dy^2$ (see Remark 2.3.6). To add and multiply classes we add and multiply the canonical representatives according to the rules in Exercise 2.3.7. The multiplication in $\Bbbk[x, y]/I$ is thus determined by the following multiplication table:

$\cdot$	1	$\bar{x}$	$\bar{y}$	$\bar{y}^2$
1	1	$\bar{x}$	$\bar{y}$	$\bar{y}^2$
$\bar{x}$	$\bar{x}$	0	$\bar{y}^2$	0
$\bar{y}$	$\bar{y}$	$\bar{y}^2$	$\bar{y}^2$	0
$\bar{y}^2$	$\bar{y}^2$	0	0	0

In general it is not true that the multiplication table contains only monomials.

Exercise 2.3.12. Consider $f_1 = x^2y - y^3, f_2 = x^3 \in \Bbbk[x, y]$ with $>_{\text{lex}}$ as in Example 2.2.12. Compute a Gröbner basis for the ideal $I = (f_1, f_2)$. Visualize the monomials in $\mathbf{L}(I)$, and compute a multiplication table for $\Bbbk[x, y]/I$.

Once more, the S-polynomials in Buchberger's criterion are designed to cancel leading terms:

$$m_{ji}\mathbf{L}(f_i) - m_{ij}\mathbf{L}(f_j) = 0.$$

By rewriting the standard expressions with remainder zero in Buchberger's test,

$$\mathrm{S}(f_i, f_j) = g_1^{(ij)} f_1 + \ldots + g_r^{(ij)} f_r + 0,$$

we may rephrase Buchberger's criterion as follows: Nonzero polynomials $f_1, \ldots, f_r \in \Bbbk[x_1, \ldots, x_n]$ form a Gröbner basis iff each of the relations $m_{ji}\mathbf{L}(f_i) - m_{ij}\mathbf{L}(f_j) = 0$ "lifts" to a relation

$$-g_1^{(ij)} f_1 - \cdots + (-m_{ij} - g_j^{(ij)}) f_j + \cdots + (m_{ji} - g_i^{(ij)}) f_i - \cdots - g_r^{(ij)} f_r = 0$$

such that $\mathbf{L}(\mathrm{S}(f_i, f_j)) \geq \mathbf{L}(g_k^{(ij)} f_k)$ whenever both sides are nonzero. With respect to such relations, we use the following terminology.

Definition 2.3.13. Let R be a ring, let M be an R-module, and let $f_1, \ldots, f_r$ be elements of M. An **R-module relation** or a **syzygy** on $f_1, \ldots, f_r$ is an R-linear combination of the f_i which is zero:

$$g_1 f_1 + \ldots + g_r f_r = 0 \in M.$$

Formally, we think of such a syzygy as a column vector ${}^t(g_1, \dots, g_r)$ of the free R-module R^r: A syzygy on $f_1, \dots, f_r$ is an element of the kernel of the map

$$\pi : R^r \to M,\ \epsilon_i \mapsto f_i,$$

where $\epsilon_1, \dots, \epsilon_r$ form the canonical basis of R^r. We write

$$\mathrm{Syz}\,(f_1, \dots, f_r) = \ker \pi,$$

and call $\mathrm{Syz}\,(f_1, \dots, f_r)$ the (first) **syzygy module** of $f_1, \dots, f_r$. If R is Noetherian, this module is finitely generated (see Exercise 2.3.15 below). In this case we think of finitely many generators of $\mathrm{Syz}\,(f_1, \dots, f_r)$ as the columns of a matrix which we call a **syzygy matrix** of $f_1, \dots, f_r$.

Remark 2.3.14. The S in S-polynomial stands for syzygy. With the above notations, the matrix $\begin{pmatrix} m_{ji} \\ -m_{ij} \end{pmatrix}$ is a syzygy matrix of $\mathbf{L}(f_i)$, $\mathbf{L}(f_j)$.

Exercise 2.3.15. Let R be a ring. An R-module M is **Noetherian**, if every submodule of M is finitely generated. If R is a Noetherian ring, show that every finitely generated R-module is Noetherian.
Hint. Reduce the general case to the case of free R-modules. For free R-modules, use induction on the rank.

Remark-Definition 2.3.16. Let $R = \Bbbk[x_1, \dots, x_n]$, and let $F \cong R^s$ be a free R-module with a fixed basis. Given elements $f_1, \dots, f_r \in F$ and a monomial order $>_0$ on F, there is a natural **induced monomial order** $>_1$ on the free R-module R^r with its canonical basis $\epsilon_1, \dots, \epsilon_r$: set

$$x^\alpha \epsilon_i >_1 x^\beta \epsilon_j \iff \begin{array}{l} x^\alpha \mathbf{L}(f_i) >_0 x^\beta \mathbf{L}(f_j) \ \text{ or} \\ x^\alpha \mathbf{L}(f_i) = x^\beta \mathbf{L}(f_j) \ \text{ (up to scalar)} \quad \text{and} \quad i > j. \end{array}$$

If $>_0$ is global, then $>_1$ is global.

Proof of Buchberger's criterion. Since the S-polynomials are elements of $(f_1, \dots, f_r)$, all the remainders h_{ij} are zero if $f_1, \dots, f_r$ form a Gröbner basis.

Conversely, suppose that all the h_{ij} are zero. Then we have for each $i > j$ a standard expression of type

$$\mathrm{S}(f_i, f_j) = g_1^{(ij)} f_1 + \ldots + g_r^{(ij)} f_r + 0.$$

With the notations above, let

$$G^{(ij)} := {}^t(-g_1^{(ij)}, \dots, -m_{ij} - g_j^{(ij)}, \dots, m_{ji} - g_i^{(ij)}, \dots, -g_r^{(ij)}) \in R^r$$

be the corresponding syzygy on $f_1, \dots, f_r$. On R^r we consider the monomial order induced by $f_1, \dots, f_r$ and the given order on R. The leading term of $G^{(ij)}$ with respect to the induced order is

$$\mathbf{L}(G^{(ij)}) = m_{ji}\epsilon_i$$

since

$$m_{ji}\mathbf{L}(f_i) = m_{ij}\mathbf{L}(f_j) \ \text{ but } \ i > j,$$

and

$$m_{ji}\mathbf{L}(f_i) > \mathbf{L}(\mathrm{S}(f_i, f_j)) \geq \mathbf{L}(g_k^{(ij)})\mathbf{L}(f_k),$$

whenever these terms are nonzero.

Let $0 \neq g = a_1 f_1 + \ldots + a_r f_r$ be an arbitrary element of I. To show that $\mathbf{L}(g) \in (\mathbf{L}(f_1), \dots, \mathbf{L}(f_r))$, we replace the given representation of g by a standard expression with remainder zero. Consider $A = {}^t(a_1, \dots, a_r) \in R^r$, and let $G = {}^t(g_1, \dots, g_r) \in R^r$ be the remainder of A under determinate division by the $G^{(ij)}$ (listed in some order). Then

$$g = a_1 f_1 + \ldots + a_r f_r = g_1 f_1 + \ldots + g_r f_r$$

since the $G^{(ij)}$ are syzygies on $f_1, \dots, f_r$. By condition 3 for determinate division by the $G^{(ij)}$ in R^r no term of G is divisible by some $\mathbf{L}(G^{(ij)}) = m_{ji}\epsilon_i$. Hence for $i > j$ no term of $g_i\,\mathbf{L}(f_i)$ is divisible by $\mathbf{L}(f_j) = m_{ji}\,\mathrm{GCD}(\mathbf{L}(f_i), \mathbf{L}(f_j))$. In other words, the g_i satisfy condition 2 for determinate division by $f_1, \dots, f_r$ in R. Hence

$$\mathbf{L}(g) = \max\{\mathbf{L}(g_1)\mathbf{L}(f_1), \dots, \mathbf{L}(g_r)\mathbf{L}(f_r)\} \in (\mathbf{L}(f_1), \dots, \mathbf{L}(f_r)).$$

□

In what follows, let $R = \Bbbk[x_1, \dots, x_n]$, let F be a free R-module with a fixed basis $e_1, \dots, e_s$, and let $>$ be a fixed global monomial order on F.

Exercise 2.3.17. Show that the notion of Gröbner bases and the results on Gröbner bases proved so far carry over from ideals of R to submodules of F (in particular, if $I \subset F$ is a submodule, explain how to compute in F/I). Extend the relevant definitions from R to F. If $f_1, \dots, f_r \in F \setminus \{0\}$, the analogue $\mathrm{S}(f_i, f_j)$ to the S-polynomial in Theorem 2.3.9 is defined for all pairs f_i, f_j such that $\mathbf{L}(f_i)$ and $\mathbf{L}(f_j)$ involve the same basis element of F.

Corollary 2.3.18. *Let $f_1, \ldots, f_r \in F \setminus \{0\}$ form a Gröbner basis with respect to $>$. As in the proof of Buchberger's criterion for F, consider the syzygies $G^{(ij)} \in R^r$, $i > j$, arising from Buchberger's test. The $G^{(ij)}$ form a Gröbner basis for the syzygy module* $\operatorname{Syz}(f_1, \ldots, f_r)$ *with respect to the induced monomial order on R^r. In particular, the $G^{(ij)}$ generate all the syzygies on $f_1, \ldots, f_r$.*

Proof. Let $A \in R^r$ be an arbitrary syzygy on $f_1, \ldots, f_r$, and let $G = (g_1, \ldots, g_r) \in R^r$ be the remainder of A under determinate division by the $G^{(ij)}$ (listed in some order) as in the proof of Buchberger's criterion. Then

$$0 = g_1 f_1 + \ldots + g_r f_r$$

since A is a syzygy, and the g_i satisfy condition 2 of determinate division by $f_1, \ldots, f_r$. Since standard expressions under determinate division are uniquely determined, $G = 0$ and the result follows. □

Example 2.3.19. If $f_1, \ldots, f_r \in F \setminus \{0\}$, the relations of type

$$m_{ji}\mathbf{L}(f_i) - m_{ij}\mathbf{L}(f_j) = 0,$$

where $\mathbf{L}(f_i)$ and $\mathbf{L}(f_j)$ involve the same basis element of F, generate all the syzygies on the leading terms $\mathbf{L}(f_1), \ldots, \mathbf{L}(f_r)$.

Remark 2.3.20. Let $f_1, \ldots, f_r \in F \setminus \{0\}$, and let $I = (f_1, \ldots, f_r) \subset F$. If we compute a Gröbner basis $f_1, \ldots, f_r, f_{r+1}, \ldots, f_{r'}$ for I with Buchberger's algorithm, the syzygies $G^{(ij)}$ generating $\operatorname{Syz}(f_1, \ldots, f_r, f_{r+1}, \ldots, f_{r'})$ are obtained in two ways: Either, such a syzygy arises from a division with remainder zero,

$$\mathrm{S}(f_i, f_j) = g_1^{(ij)} f_1 + \ldots + g_r^{(ij)} f_l + 0,$$

or, it arises from a division which leads to a new generator f_k, $k \geq r + 1$:

$$\mathrm{S}(f_i, f_j) = g_1^{(ij)} f_1 + \ldots + g_r^{(ij)} f_{k-1} + f_k.$$

Example 2.3.21. In Example 2.3.11, the matrix

$$\begin{pmatrix} -y & 0 \\ x + y & y^2 \\ -1 & x - y \end{pmatrix}$$

is a syzygy matrix of $f_1 = x^2, f_2 = xy - y^2, f_3 = -y^3 \in \Bbbk[x, y]$ (the relation $f_1 f_3 - f_3 f_1$ in 2.3.11 can be omitted since it is an R-linear combination of the two relations above).

One way of improving Buchberger's algorithm is to show that fewer S-polynomials need to be considered in Buchberger's test. The first version of Buchberger's criterion asks for testing the S-polynomials $\mathrm{S}(f_i, f_j)$ for all i and j with $i > j$. The monomial ideals M_i in the following version of the criterion, however, have frequently less than the maximal possible number of $i-1$ minimal generators (see again Exercise 2.1.3, 2).

Theorem 2.3.22 (Buchberger's criterion, second version). *Let elements $f_1, \dots, f_r \in F \backslash \{0\}$ be given. For $i = 2, \dots, r$, let M_i be the monomial ideal*

$$M_i = ((\mathbf{L}(f_1), \dots, \mathbf{L}(f_{i-1})) : \mathbf{L}(f_i)) \subset R.$$

For each i and each minimal generator x^α of M_i we may and will choose an S-polynomial of type $\mathrm{S}(f_i, f_j) = m_{ji} f_i - m_{ij} f_j$ with $i > j$ and m_{ji} a term involving x^α. Let $h_{i,\alpha}$ be a remainder on division of $\mathrm{S}(f_i, f_j)$ by the f_k. Then $f_1, \dots, f_r$ form a Gröbner basis iff all the $h_{i,\alpha}$ are zero.

Exercise 2.3.23. Prove the second version of Buchberger's criterion and deduce an algorithm for computing Gröbner bases. Show that the syzygies $G^{(i,\alpha)}$ appearing in the proof generate all the syzygies on $f_1, \dots, f_r$ if $f_1, \dots, f_r$ form a Gröbner basis.

Example 2.3.24. Consider again $f_1 = x^2, f_2 = xy - y^2 \in \Bbbk[x, y]$ with the lexicographic order. Then $\mathbf{L}(f_2) = xy$, hence $M_2 = ((x^2) : (xy)) = (x)$. We compute the standard expression

$$\mathrm{S}(f_2, f_1) = x \cdot f_2 - y \cdot f_1 = -xy^2 = 0 \cdot f_1 - y \cdot f_2 - y^3,$$

include $f_3 = -y^3$ in the set of generators, and obtain

$$M_3 = ((x^2, xy) : (y^3)) = (x).$$

Since the remainder in the standard expression

$$\mathrm{S}(f_3, f_2) = x \cdot f_3 + y^2 \cdot f_2 = -y^4 = 0 \cdot f_1 + 0 \cdot f_2 + y \cdot f_3$$

is zero, we conclude that f_1, f_2, f_3 form a Gröbner basis for the ideal (f_1, f_2).

Example 2.3.25. Consider $f_1 = x^2 - y$, $f_2 = xy - z \in \Bbbk[x, y, z]$ with the lexicographic order. Then $M_2 = ((x^2) : (xy)) = (x)$. We compute the standard expression

$$\mathrm{S}(f_2, f_1) = x(xy - z) - y(x^2 - y) = -xz + y^2 =: f_3,$$

and include f_3 in the set of generators. Then $M_3 = ((x^2, xy) : (xz)) = (x, y)$, and we have the standard expressions

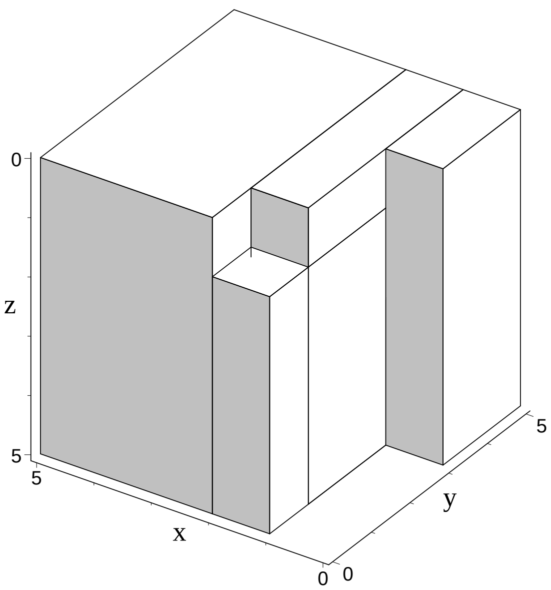
$$\mathrm{S}(f_3, f_1) = x(-xz + y^2) + z(x^2 - y) = xy^2 - yz = y(xy - z), \text{ and}$$
$$\mathrm{S}(f_3, f_2) = y(-xz + y^2) + z(xy - z) = y^3 - z^2 =: f_4.$$

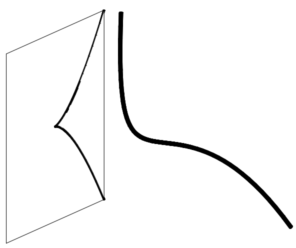
In the next step, $M_4 = ((x^2, xy, xz) : (y^3)) = (x)$, and

$$\mathrm{S}(f_4, f_2) = x(y^3 - z^2) - y^2(xy - z) = -xz^2 + y^2z = z(-xz + y^2)$$

is a standard expression with remainder zero. Hence f_1, f_2, f_3, f_4 form a Gröbner basis for (f_1, f_2).

We visualize the monomials in $\mathbf{L}(f_1, f_2)$ via their exponents as follows:





Observe that the polynomial $f_4 = y^3 - z^2$ involves only y and z, the variable x is eliminated. In the (y, z)-plane, the equation $f_4 = 0$ gives the image of the twisted cubic curve $\mathrm{V}(f_1, f_2)$ under the linear projection which sends (a, b, c) to (b, c). We will prove general results in this direction in the following sections.

Exercise 2.3.26. If

$$f_1 = xz - y^2,\ f_2 = wz - xy,\ f_3 = wy - x^2 \in \mathbb{k}[w, x, y, z],$$

show that

$$\begin{pmatrix} -w & x \\ x & -y \\ -y & z \end{pmatrix}$$

is a syzygy matrix of f_1, f_2, f_3. Notice that f_1, f_2, f_3 are the 2×2 minors of the syzygy matrix (with appropriate signs).

A Gröbner basis $\{f_1, \dots, f_r\} \subset F$ computed with Buchberger's algorithm quite often contains elements whose leading terms are unneeded generators of $\mathbf{L}(f_1, \dots, f_r)$. By eliminating superfluous generators and by adjusting constants so that the coefficient of each leading term is 1 we arrive at a **minimal Gröbner basis**, that is, a Gröbner basis whose leading terms are the minimal generators of $\mathbf{L}(f_1, \dots, f_r)$. In addition, we may "reduce the tail" of each element in the Gröbner basis.

Exercise 2.3.27. A minimal Gröbner basis $\{f_1, \dots, f_r\} \subset F$ is **reduced**, if for $i \neq j$ no term of f_i is divisible by $\mathbf{L}(f_j)$. Show that if $(0) \neq I \subset F$ is a submodule, there is a uniquely determined reduced Gröbner basis for I with respect to the given monomial order, namely $m_1 - \mathrm{NF}(m_1, I), \dots, m_r - \mathrm{NF}(m_r, I)$, where $m_1, \dots, m_r$ are the minimal generators of $\mathbf{L}(I)$. Explain how to compute the reduced Gröbner basis from any given Gröbner basis.

Remark 2.3.28.

1. Let

   $$f_i = a_{i1}x_1 + \cdots + a_{in}x_n \in \mathbb{k}[x_1, \dots, x_n],\ i = 1, \dots, r,$$

   be linear polynomials, and let $>$ be a fixed global monomial order on $\mathbb{k}[x_1, \dots, x_n]$ with $x_1 > \cdots > x_n$. Computing a minimal Gröbner basis for $(f_1, \dots, f_r)$ amounts to transforming the coefficient matrix $A = (a_{ij})$ into a matrix in row echelon form with pivots 1. The uniquely determined reduced Gröbner basis is independent of the choice of $>$ and corresponds to the uniquely determined reduced row echelon form of A (each pivot 1 is the only nonzero entry in its column). Hence Buchberger's algorithm generalizes Gaussian elimination.

2. In the case of one variable x, there is precisely one global monomial order:

   $$\cdots > x^3 > x^2 > x > 1.$$

If $f_1, \dots, f_r \in \mathbb{k}[x]$, the reduced Gröbner basis for $(f_1, \dots, f_r)$ with respect to this order consists of exactly one element, namely the greatest common divisor $\mathrm{GCD}(f_1, \dots, f_r)$. Thus Buchberger's algorithm also generalizes Euclid's algorithm for computing GCD's in $\mathbb{k}[x]$.

3. If $I \subset F$ is a monomial submodule, its reduced Gröbner basis consists of the minimal generators of I (with respect to any global monomial order on F).

Exercise 2.3.29. If $I \subset \mathbb{Q}[x, y, z]$ is the ideal generated by the polynomials

$$\begin{aligned} f_1 &= 3xz + 4x - 2y - z^2 - 4z, \\ f_2 &= -2x + 3yz - 2y + 2z^2 - z, \\ f_3 &= -3xy + 5x + 3y^2 - y - 2z^2 - 2z, \end{aligned}$$

show that the reduced Gröbner basis for I with respect to $>_{\mathrm{lex}}$ is given by the polynomials

$$\begin{aligned} g_1 &= x - 1/12z^4 + 1/3z^3 + 1/12z^2 - 4/3z, \\ g_2 &= y + 1/3z^4 + 1/6z^3 - 4/3z^2 - 1/6z, \\ g_3 &= z^5 - 5z^3 + 4z. \end{aligned}$$

So as in Example 2.3.25, the computation of a Gröbner basis with respect to $>_{\mathrm{lex}}$ amounts to eliminate variables from the given system of equations. Deduce from the new set of generators that the zero locus $\mathrm{V}(I) \subset \mathbb{A}^3(\mathbb{C})$ consists of precisely five points:

$$(0,0,0), (1,1,1), (-1,1,-1), (1,-1,2), (1,1,-2).$$

More systematic remarks on finding explicit solutions for polynomial systems of equations will be given in the following sections.

2.4 First applications

As already remarked, division with remainder, Proposition 2.3.2, and Buchberger's algorithm provide a solution to the ideal membership problem. More generally, they allow us to decide submodule membership.

Algorithm 2.4.1 (Submodule membership). Given nonzero elements $g, f_1, \dots, f_r$ of a free $R = \mathbb{k}[x_1, \dots, x_n]$-module F with a fixed finite basis, decide whether

$$g \in I := (f_1, \dots, f_r) \subset F.$$

[If so, express g as an R-linear combination

$$g = g_1 f_1 + \ldots + g_r f_r.]$$

1. Compute a Gröbner basis $f_1, \ldots, f_r, f_{r+1}, \ldots, f_{r'}$ for I with Buchberger's algorithm. [Store each syzygy in Buchberger's test arising from a division that leads to a new generator f_k.]

2. Compute a standard expression for g in terms of $f_1, \ldots, f_{r'}$ with remainder h (use the same global monomial order on F as in step 1).

3. If $h = 0$, then $g \in I$. [In this case, express each new generator f_j in terms of $f_1, \ldots, f_{k-1}$ by rewriting the syzygy which lead to f_k in step 1. For $r' \geq k \geq r+1$ substitute this expression for f_k into the standard expression

$$g = a_1 f_1 + \ldots + a_{r'} f_{r'}$$

obtained in step 2.]

Example 2.4.2. Consider the lexicographic Gröbner basis $f_1 = x^2, f_2 = xy - y^2, f_3 = -y^3$ for the ideal $I = (f_1, f_2) \subset \mathbb{k}[x, y]$ computed in Example 2.3.24. If $g = x^3 - x^2 + xy^2$, division with remainder yields the standard expression $g = (x-1)f_1 + y f_2 - f_3$, hence $g \in I$. Substituting the expression $(x+y)f_2 - y f_1$ obtained for f_3 in Example 2.3.24 gives

$$g = (x - 1 + y) f_1 - x f_2.$$

As pointed out in the introduction to this chapter, we can apply Algorithm 2.4.1 in particular to decide whether a given system of polynomial equations defined over $\mathbb{k}$ has a solution over the algebraic closure $\bar{\mathbb{k}}$ of $\mathbb{k}$. In this case, we can make use of the Gröbner basis computed in the first step of the algorithm to obtain further information on the set of solutions.

Remark 2.4.3. Let $f_1, \ldots, f_r \in \mathbb{k}[x_1, \ldots, x_n]$, let $I := (f_1, \ldots, f_r)$, and let $\bar{\mathbb{k}}$ be the algebraic closure of $\mathbb{k}$. According to Hilbert's Nullstellensatz, Exercise 1.3.4 and Macaulay's Theorem 2.3.5 we can distinguish, whether the system

$$f_1(x_1, \ldots, x_n) = f_2(x_1, \ldots, x_n) = \ldots = f_r(x_1, \ldots, x_n) = 0$$

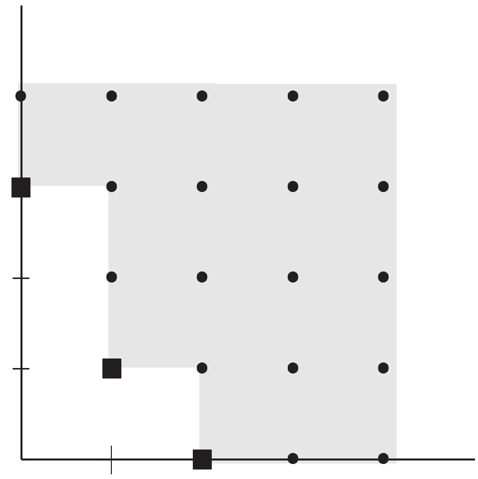
has

1. no solution in $\mathbb{A}^n(\bar{\Bbbk})$,
2. finitely many solutions in $\mathbb{A}^n(\bar{\Bbbk})$, or
3. infinitely many solutions in $\mathbb{A}^n(\bar{\Bbbk})$

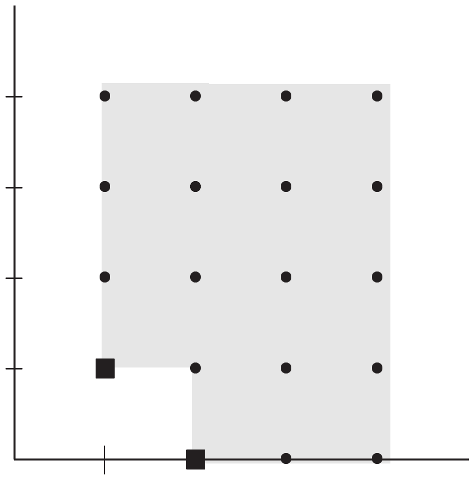
by distinguishing whether

1. every monomial of $\Bbbk[x_1, \ldots, x_n]$ is contained in $\mathbf{L}(I)$,
2. only finitely many monomials are not contained in $\mathbf{L}(I)$, or
3. infinitely many monomials are not contained in $\mathbf{L}(I)$.

To check which of the conditions holds, inspect the leading terms of a Gröbner basis for I. The first condition means that a nonzero constant is among the leading terms. The second condition holds iff for each i, $1 \leq i \leq n$, one of the leading terms is of type $cx_i^{\alpha_i}$, with c a nonzero constant, and $\alpha_i \geq 1$.



Finitely many solutions.



Infinitely many solutions.

Notice that though this check gives a result over $\bar{\Bbbk}$, the actual Gröbner basis computation is carried through over $\Bbbk$. There is no need to leave the ground field.

Exercise 2.4.4. If the system defined by $f_1, \ldots, f_r \in \Bbbk[x_1, \ldots, x_n]$ has only finitely many solutions in $\mathbb{A}^n(\bar{\Bbbk})$, prove that the number of these solutions is at most $\dim_{\Bbbk} \Bbbk[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$. That is, the number of monomials not in $\mathbf{L}(f_1, \ldots, f_r)$ is an upper bound for the number of solutions. Show that equality holds if $(f_1, \ldots, f_r)$ is a radical ideal.

Example 2.4.5. For the ideal $I \subset \mathbb{Q}[x, y, z]$ in Exercise 2.3.29, the five monomials z^i, $0 \leq i \leq 4$, represent a $\mathbb{Q}$-vector space basis of $\mathbb{Q}[x, y, z]/I$. Hence

$$\mathrm{V}(I) = \{(0,0,0), (1,1,1), (-1,1,-1), (1,-1,2), (1,1,-2)\} \subset \mathbb{A}^3(\mathbb{C})$$

contains the maximal possible number of points.

Exercise 2.4.6. If $I \subset \mathbb{Q}[x, y, z]$ is the ideal generated by the polynomials

$$\begin{aligned} f_1 &= x^3 + y^3 + z^3 - 1, \\ f_2 &= x^2 + y^2 + z^2 - 1, \\ f_3 &= x + y + z - 1, \end{aligned}$$

show that the reduced Gröbner basis for I with respect to $>_{\mathrm{lex}}$ is given by the polynomials

$$\begin{aligned} g_1 &= x + y + z - 1 \\ g_2 &= y^2 + yz - y + z^2 - z, \\ g_3 &= z^3 - z^2. \end{aligned}$$

Conclude that $\dim_{\mathbb{Q}} \mathbb{Q}[x, y, z]/(f_1, f_2, f_3) = 6$ though there are only three solutions:

$$\mathrm{V}(I) = \{(1,0,0), (0,1,0), (0,0,1)\} \subset \mathbb{A}^3(\mathbb{C}).$$

Remark 2.4.7.

1. Let $I \subset \mathbb{k}[x_1, \ldots, x_n]$ be an ideal such that $\mathrm{V}(I) \subset \mathbb{A}^n(\bar{\mathbb{k}})$ is finite. Since $\mathrm{V}(I) = \mathrm{V}(\operatorname{rad} I)$, Exercise 2.4.4 shows how to find the exact number of solutions over $\bar{\mathbb{k}}$ without actually computing the solutions, provided that we know $\operatorname{rad} I$. An algorithm for computing radicals in the zero-dimensional case will be described in Exercise **??**. Notice that this algorithm requires the computation of square-free parts of polynomials in one variable. Contrary to Buchberger's algorithm, the known algorithms for computing square-free parts (more generally, for factorizing polynomials) are sensitive to the ground field (see Exercise **??**).

2. One basic way of computing radicals for arbitrary ideals is to reduce the general case to the zero-dimensional case by means of Gröbner basis techniques. We will not discuss this challenging topic of computational algebraic geometry in this book (see Decker, Greuel and Pfister [1999] for a survey).

If one is just interested in radical membership, there is no need to compute the radical itself. Indeed, ideal membership and, once more, the trick of Rabinowitch solve the problem:

Exercise 2.4.8 (Radical membership). If $g, f_1, \dots, f_r \in \mathbb{k}[x_1, \dots, x_n]$ are polynomials, and if y is a slack variable, show that

$$g \in \text{rad}\,(f_1, \dots, f_r) \iff 1 \in (f_1, \dots, f_r, yg - 1) \subset \mathbb{k}[x_1, \dots, x_n, y].$$

Next, we come back to the computation of syzygies, which so far appeared in this book only as a byproduct of our proof of Buchberger's criterion. Let us point out, however, that computing syzygies is a fundamental tool for many operations which are central to computational algebraic geometry (see for instance Eisenbud[1995]).

We already know that Buchberger's algorithm computes the syzygies on the elements of a Gröbner basis (see Corollary 2.3.18 and Exercise 2.3.23). Based on this, one can compute the syzygies on any set of generators:

Algorithm 2.4.9 (Syzygy modules). Given a map between free $R = \mathbb{k}[x_1, \dots, x_n]$-modules, compute its kernel. That is, given nonzero elements $f_1, \dots, f_r$ of a free R-module F with a fixed basis, compute a syzygy matrix of $f_1, \dots, f_r$.

1. Use Buchberger's algorithm to compute a Gröbner basis $f_1, \dots, f_r, f_{r+1}, \dots, f_{r'}$ for the submodule $(f_1, \dots, f_r) \subset F$. Store all the syzygies on $f_1, \dots, f_{r'}$ obtained by Buchberger's test during the computation. Let t be the number of these syzygies.
2. Sort the syzygies so that those which are obtained from a division leading to a new generator f_k come first (and those arising from a division with remainder zero come second). Then the syzygies fit as columns into an $r' \times t$ matrix which has block form $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$, where C is an upper triangular square matrix of size $r' - r$ with diagonal entries 1 (where signs are adjusted appropriately).
3. The $r \times (t - r' + r)$ matrix $B - AC^{-1}D$ is a syzygy matrix of $f_1, \dots, f_r$.

Proof (of correctness). By Corollary 2.3.18 and Exercise 2.3.23 the columns of $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ generate all the syzygies on $f_1, \dots, f_r, f_{r+1}, \dots, f_{r'}$. We multiply $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ with the invertible $t \times t$ matrix $\begin{pmatrix} E_{r'-r} & -C^{-1}D \\ 0 & E_{t-r'+r} \end{pmatrix}$, where E_j

stands for the $j \times j$ identity matrix. As a result, we obtain new generators of the syzygies, namely the columns of the matrix $M = \begin{pmatrix} A & -AC^{-1}D + B \\ C & 0 \end{pmatrix}$. An R-linear combination of the columns of M which defines a syzygy on $f_1, \dots, f_r$ alone, that is, whose last $r' - r$ entries are zero, is in fact an R-linear combination of the last $t - r' + r$ columns of M since C has maximal rank. Hence $B - AC^{-1}D$ is a syzygy matrix of $f_1, \dots, f_r$. $\square$

Example 2.4.10. Consider again how we computed the lexicographic Gröbner basis $f_1 = x^2, f_2 = xy - y^2, f_3 = -y^3$ for the ideal $I = (f_1, f_2) \subset \Bbbk[x, y]$ in Exercise 2.3.24. The resulting syzygy matrix, with conventions as in step 2 above, is

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} y & 0 \\ -x - y & y^2 \\ 1 & x - y \end{pmatrix}.$$

The relations on the original generators f_1, f_2 are thus generated by the syzygy

$$\begin{pmatrix} 0 \\ y^2 \end{pmatrix} - \begin{pmatrix} y \\ -x - y \end{pmatrix} (x - y) = \begin{pmatrix} -f_2 \\ f_1 \end{pmatrix}.$$

We give two examples of how syzygy computations may be used to perform other operations. Our first application is an algorithm for computing ideal intersections and thus unions of algebraic sets (the correctness of the algorithm is obvious):

Algorithm 2.4.11 (Ideal intersection). Given ideals $I = (f_1, \dots, f_r)$ and $J = (g_1, \dots, g_s)$ in $R = \Bbbk[x_1, \dots, x_n]$, compute generators of the intersection

$$I \cap J.$$

1. Compute the kernel of the map $R^{r+s+1} \to R^2$ with matrix

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

2. The entries of the last row of the resulting syzygy matrix generate $I \cap J$.

Our second application of syzygy computations has a geometric interpretation as well.

Definition 2.4.12. If R is a ring, and if $I, J \subset R$ are ideals of R, the **ideal quotient of I by J** is the ideal

$$(I : J) = \{f \in R \mid fJ \subset I\}.$$

The **saturation of I with respect to J** is the ideal

$$(I : J^{\infty}) = \{f \in R \mid fJ^m \subset I \text{ for some } m \geq 1\} = \bigcup_{m=1}^{\infty} (I : J^m).$$

Notice that

$$(I : J) \subset (I : J^2) \subset \cdots \subset (I : J^{\infty}).$$

Exercise 2.4.13. Let I and J be ideals of $\mathbb{k}[x_1, \ldots, x_n]$.

1. Show that
$$\mathrm{V}(I) \setminus \mathrm{V}(J) \subset \mathrm{V}(I : J) \subset \mathrm{V}(I) \subset \mathbb{A}^n(\mathbb{k}).$$

2. If A and B are algebraic subsets of $\mathbb{A}^n(\mathbb{k})$, show that
$$\mathrm{I}(A \setminus B) = (\mathrm{I}(A) : \mathrm{I}(B)).$$

3. Now consider the loci of zeros over the algebraic closure $\bar{\mathbb{k}}$. Show that
$$\overline{\mathrm{V}(I) \setminus \mathrm{V}(J)} = \mathrm{V}(I : J^{\infty}) \subset \mathbb{A}^n(\bar{\mathbb{k}}).$$
If I is radical, show that
$$\overline{\mathrm{V}(I) \setminus \mathrm{V}(J)} = \mathrm{V}(I : J) \subset \mathbb{A}^n(\bar{\mathbb{k}}).$$

4. Show by an example that the conclusios of 2 may not hold if we consider the loci of zeros over $\mathbb{k}$ only.

5. Design algorithms for computing $(I : J)$ and $(I : J^{\infty})$.

The following exercise contains examples of how these algorithms work.

Exercise 2.4.14. Let $\mathbb{k}$ be infinite. Consider the ideal

$$I = (xz - y^2, x^2 - y) \subset \mathbb{k}[x, y, z].$$

1. Observe that the line $\mathrm{V}(x, y)$ is contained in $\mathrm{V}(I) \subset \mathbb{A}^3(\mathbb{k})$.

2. Compute that $(I : (x,y)) = (I : (x,y)^\infty)$ is the vanishing ideal $I(C) = (x^2 - y, xy - z)$ of the twisted cubic curve $C \subset \mathbb{A}^3(\Bbbk)$.

3. Compute that $I = (x,y) \cap I(C)$. Deduce that this intersection is a prime decomposition of I, that $\mathrm{V}(I) = \mathrm{V}(x,y) \cup C$ is the decomposition of $\mathrm{V}(I)$ into irreducible components, and that $I = \mathrm{I}(\mathrm{V}(I))$.

The example shows in particular that the intersection of two varieties need not be a variety.

Remark 2.4.15. The arguments used in the example are special to the case $I = (xz - y^2, x^2 - y)$. There are, however, general algorithms for computing prime decompositions (more generally, primary decompositions) over certain ground fields. The design of such algorithms is a difficult task and still one of the big challenges of computational algebraic geometry. Essentially, the known algorithms use Gröbner basic techniques (or, characteristic set methods), to reduce the general case to the hypersurface case, and algorithms for polynomial factorization to solve the hypersurface case. To discuss these algorithms is beyond the scope of this book. We refer to Decker, Greuel and Pfister [1999] and Kaltofen [1982,1990, 1992] for surveys.

2.5 The fundamental algorithms revised

To compute a Gröbner basis with Buchberger's algorithm, we have to pick a global monomial order. The computation and the resulting Gröbner basis depend in a crucial way on the choice of the order. For most applications, any Gröbner basis will do, and thus, in principle, any monomial order may be used. With respect to effiency, however, the following global monomial order appears to be the best choice (see ... [], Bayer and Stillman [1987a, 1987b] for some experimental and theoretical observations in this direction).

Definition 2.5.1. The **degree reverse lexicographic order** $>_{\mathrm{drlex}}$ on $R = \Bbbk[x_1, \dots, x_n]$ is defined by

$$x^\alpha >_{\mathrm{drlex}} x^\beta \iff \begin{array}{l}\deg x^\alpha > \deg x^\beta, \text{ or } \deg x^\alpha = \deg x^\beta \text{ and the} \\ \text{last nonzero entry of } \alpha - \beta \in \mathbb{Z}^n \text{ is negative.}\end{array}$$

It is extended to free R-modules as in Remark 2.2.18.

Thus, the degree reverse lexicographic order refines the partial order by total degree.

Example 2.5.2. With respect to $>_{\text{lex}}$ and $>_{\text{drlex}}$, the monomials of degree 2 in $\mathbb{k}[x_1, x_2, x_3]$ are ordered as follows:

$$x_1^2 >_{\text{lex}} x_1x_2 >_{\text{lex}} x_1x_3 >_{\text{lex}} x_2^2 >_{\text{lex}} x_2x_3 >_{\text{lex}} x_3^2$$

and

$$x_1^2 >_{\text{drlex}} x_1x_2 >_{\text{drlex}} x_2^2 >_{\text{drlex}} x_1x_3 >_{\text{drlex}} x_2x_3 >_{\text{drlex}} x_3^2.$$

Remark 2.5.3. For monomials of the same degree, the difference between $>_{\text{lex}}$ and $>_{\text{drlex}}$ is subtle but crucial. The use made of these orders depends on their key properties.

The lexicographic order has the key property that for all subrings $\mathbb{k}[x_k, \dots, x_n] \subset \mathbb{k}[x_1, \dots, x_n]$ the following holds:

$$f \in \mathbb{k}[x_1, \dots, x_n],\ \mathbf{L}(f) \in \mathbb{k}[x_k, \dots, x_n] \implies f \in \mathbb{k}[x_k, \dots, x_n].$$

This makes $>_{\text{lex}}$ useful for eliminating variables (see Algorithm 2.5.7 below).

The key property of $>_{\text{drlex}}$ is that it refines the partial order by total degree; and, it chooses the leading term of a homogeneous polynomial so that the leading term is in a subring $\mathbb{k}[x_1, \dots, x_k]$ with k as small as possible. This property has usually the effect that the monomial ideals M_i in Buchberger's test have fewer minimal generators than with any other monomial order. hence the resulting Gröbner basis has fewer elements (see ... [], Bayer and Stillman [1987a, 1987b] for further remarks in this direction). We therefore choose $>_{\text{drlex}}$ as our default monomial order in Buchberger's algorithm.

Remark 2.5.4. Also the order in which the Gröbner basis elements are listed at each stage of Buchberger's algorithm plays a crucial role. We prefer to list b before b' if $\deg \mathbf{L}(b) < \deg \mathbf{L}(b')$, or $\deg \mathbf{L}(b) = \deg \mathbf{L}(b')$ and $\mathbf{L}(b) >_{\text{drlex}} \mathbf{L}(b')$. In the same way, we list the minimal generators of the monomial ideals M_i in Buchberger's test.

Algorithm 2.5.5 (Buchberger's algorithm with details). Given nonzero elements $f_1, \dots, f_r$ in a free $R = \mathbb{k}[x_1, \dots, x_n]$-module F with a fixed finite basis, compute a Gröbner basis of the submodule $I = (f_1, \dots, f_r) \subset F$.

1. Choose a suitable global monomial order on F.
2. List $f_1, \dots, f_r$ in a suitable order as $b_1, \dots, b_r$.
3. Initialize $i = 2$, $r' = r$.

4. **Syzygy initializing step.** Let $\mathcal{M}$ be the list of the minimal generators of $M_i = ((\mathbf{L}(b_1), \dots, \mathbf{L}(b_{i-1})) : \mathbf{L}(b_i))$ suitably ordered.

5. **while** $\mathcal{M}$ is nonempty **do**

   5.1 **Division step.** Remove the first minimal generator x^α from $\mathcal{M}$, pick an S-polynomial of type $\mathrm{S}(f_i, f_j) = m_{ji}f_i - m_{ij}f_j$ with $j < i$ and m_{ji} a term involving x^α, and compute a standard expression for $\mathrm{S}(f_i, f_j)$ in terms of the b_k with remainder h.

   5.2 **if** $h \neq 0$ **then**
   list $b_i, \dots, b_{r'}, h$ in a suitable order as $b_i, \dots, b_{r'+1}$.
   $r' = r' + 1$; let j be defined by $h = b_j$.
   if $j = i$ **then break** the **while** loop and **goto** 4.

6. i =i+1; **if** $i > r'$ **return** $b_1, \dots, b_{r'}$ **else goto** 4.

The question of strategies for improving the efficiency of Buchberger's algorithm is still an active area of research (see [**?**], [**?**], [**?**]), and will not be discussed in this book.

Some applications of Buchberger's algorithm require Gröbner bases with special properties and thus the choice of special monomial orders. Eliminating variables from a given system of polynomial equations is a fundamental application of this type which we already encountered in Example 2.3.25 and in Exercises 2.3.29 and 2.4.6.

Remark-Definition 2.5.6. Let $I \subset \Bbbk[x_1, \dots, x_n]$ be an ideal. For any $k = 0, \dots n-1$, the set

$$I_k = I \cap \Bbbk[x_{k+1}, \dots, x_n]$$

is an ideal of $\Bbbk[x_{k+1}, \dots, x_n]$, called the **kth elimination ideal** of I. Observe that $I_0 = I$.

Algorithm 2.5.7 (Elimination using $>_{\mathrm{lex}}$). Given an ideal $I \subset \Bbbk[x_1, \dots, x_n]$, compute all the elimination ideals I_k.

1. Compute a Gröbner basis $\mathcal{G}$ for I with respect to the lexicographic order on $\Bbbk[x_1, \dots, x_n]$.

2. The elements $g \in \mathcal{G}$ with $\mathbf{L}(g) \in \Bbbk[x_{k+1}, \dots, x_n]$ form a Gröbner basis for I_l with respect to the lexicographic order on $\Bbbk[x_{k+1}, \dots, x_n]$.

Proof (of correctness). If $f \in I \cap \Bbbk[x_{k+1}, \ldots, x_n]$, then $\mathbf{L}(f)$ is divisible by $\mathbf{L}(g)$ for some $g \in \mathcal{G}$. Since f does not involve $x_1, \ldots, x_k$, the same holds for $\mathbf{L}(g)$ and thus also for g due to the key property of $>_{\text{lex}}$ (see Remark 2.5.3). □

Thus, one Gröbner basis computation with respect to $>_{\text{lex}}$ yields the whole flag of elimination ideals I_k, $k = 0, \ldots, n-1$. For instance, in Example 2.3.25, $I_0 = I = (x^2 - y, xy - z, -xz + y^2, y^3 - z^2 \subset \Bbbk[x, y, z]$, $I_1 = (y^3 - z^2)$, and $I_2 = (0)$. If only one of the elimination ideals is needed, other monomial orders are usually more effective.

Definition 2.5.8. A monomial order $>$ on the polynomial ring

$$\Bbbk[x, y] = \Bbbk[x_1, \ldots, x_n, y_1, \ldots y_m]$$

is an **elimination order** with respect to $x_1, \ldots, x_n$ if the following holds:

$$f \in \Bbbk[x, y],\ \mathbf{L}(f) \in \Bbbk[y] \implies f \in \Bbbk[y].$$

Example 2.5.9. Given monomial orders $>_1$ on $\Bbbk[x]$ and $>_2$ on $\Bbbk[y]$, the **product order** or **block order** $> = (>_1, >_2)$ on $\Bbbk[x, y]$, defined by

$$x^\alpha y^\gamma > x^\beta y^\delta \iff x^\alpha >_1 x^\beta, \textit{ or } x^\alpha = x^\beta \textit{ and } y^\gamma >_2 y^\delta,$$

is an elimination order with respect to $x_1, \ldots, x_n$. It is global if $>_1$ and $>_2$ are global.

It is often most efficient to pick $>_1$ and $>_2$ to be degree reverse lexicographic.

As above one shows:

Proposition 2.5.10 (Elimination). *Let $I \subset \Bbbk[x, y]$ be an ideal, let $>$ be a global elimination order on $\Bbbk[x, y]$ with respect to $x_1, \ldots, x_n$, and let $\mathcal{G}$ be a Gröbner basis for I with respect to $>$. Then $\mathcal{G} \cap \Bbbk[y]$ is a Gröbner basis for $I \cap \Bbbk[y]$ with respect to the restriction of $>$ to $\Bbbk[y]$.*

Remark 2.5.11. Computing a Gröbner basis for I with respect to an elimination order may be costly. In some cases, a better performance is achieved along the following lines. First compute a Gröbner basis $\mathcal{G}$ for I with respect to $>_{\text{drlex}}$. Then apply a **Gröbner walk algorithm** which computes the desired Gröbner basis with respect to an elimination order, starting from $\mathcal{G}$ (see for instance []). For an alternative approach using Hilbert functions see Remark **??**.

Geometrically, elimination means to compute the Zariski closure of the image of an affine algebraic set under a linear projection. We will explain this in Section 2.7. More generally, we will make use of the following application of elimination to compute the Zariski closure of the image of an affine algebraic set under an arbitrary morphism.

Rather than considering R-module relations as in Definition 2.3.13, we are now interested in $\mathbb{k}$-algebra relations.

Definition 2.5.12. Let S be a $\mathbb{k}$-algebra, and let $s_1, \dots, s_m$ be elements in S. A **$\mathbb{k}$-algebra relation** on $s_1, \dots, s_m$ is a polynomial expression of type

$$\sum c_\alpha s_1^{\alpha_1} \cdot \ldots \cdot s_m^{\alpha_m} = 0 \in S,$$

with coefficients $c_\alpha \in \mathbb{k}$. Formally, we consider a polynomial ring $\mathbb{k}[y_1, \dots, y_m]$, and think of a $\mathbb{k}$-algebra relation as an element of the kernel of the map

$$\phi : \mathbb{k}[y_1, \dots, y_m] \to S,\ y_i \mapsto s_i.$$

If only the trivial such relation exists, $s_1, \dots, s_m$ are **algebraically independent** over $\mathbb{k}$.

Proposition 2.5.13 (Algebra relations on elements in affine rings). *Let $R = \mathbb{k}[x_1, \dots, x_n]$, let $I \subset R$ be an ideal, and let $\bar{f}_1 = f_1 + I, \dots, \bar{f}_m = f_m + I \in \mathbb{k}[x_1, \dots, x_n]/I$. Consider the map*

$$\phi : \mathbb{k}[y_1, \dots, y_m] \to \mathbb{k}[x_1, \dots, x_n]/I,\ y_i \mapsto \bar{f}_i.$$

If J is the ideal

$$J = I\mathbb{k}[x, y] + (f_1 - y_1, \dots, f_m - y_m) \subset \mathbb{k}[x, y],$$

then

$$\ker \phi = J \cap \mathbb{k}[y].$$

Proof. Let $g \in \mathbb{k}[x, y]$. To prove the assertion, we have to show:

$$g(x_1, \dots, x_n, f_1, \dots, f_m) \in I \iff g \in J.$$

If $g = h + \sum g_j(f_j - y_j) \in J$ with $h \in I\mathbb{k}[x, y]$, then $g(x_1, \dots, x_n, f_1, \dots, f_m) = h(x_1, \dots, x_n, f_1, \dots, f_m) \in I$. For the converse, observe that substituting the $f_j - (f_j - y_j)$ for y_j in g and expanding gives an expression of type

$$g(x, y) = g(x_1, \dots, x_n, f_1, \dots, f_m) + \sum g_j(f_j - y_j).$$

$\square$

The proposition gives us a method of computing in the algebra $\mathbb{k}[\bar{f}_1, \ldots, \bar{f}_m] \cong \mathbb{k}[y_1, \ldots, y_m]/\ker \phi$ since we already know how to compute in affine rings. Once we have the required Gröbner basis for J, we know in particular, whether there is only the trivial polynomial relation on $\bar{f}_1, \ldots, \bar{f}_m$, that is, whether $\bar{f}_1, \ldots, \bar{f}_m$ are algebraically independent over $\mathbb{k}$. Besides the injectivity of ϕ we may also check its surjectivity by inspecting the Gröbner basis elements. More generally, we can decide subalgebra membership:

Exercise 2.5.14 (Subalgebra membership). With notations as above, let $\bar{g} = g + I \in \mathbb{k}[x_1, \ldots, x_n]/I$. Fix an elimination order $>$ on $\mathbb{k}[x, y]$ with respect to $x_1, \ldots, x_n$, and let $h = \mathrm{NF}(g, J) \in \mathbb{k}[x, y]$ be the corresponding normal form. Show that $\bar{g} \in \mathbb{k}[\bar{f}_1, \ldots, \bar{f}_m]$ iff $h \in \mathbb{k}[y]$. In this case, $\bar{g} = h(\bar{f}_1, \ldots, \bar{f}_m)$ is a polynomial expression for $\bar{g}$ in terms of the $\bar{f}_j$. If $\mathcal{G}$ is the reduced Gröbner basis for J with respect to $>$, show that ϕ is surjective iff $\mathcal{G}$ contains for each i an element of type $x_i - h_i(y)$.

Exercise 2.5.15.

1. Compute the algebra relations on the polynomials $f_1 = x^2 + y^2, f_2 = x^2y^2, f_3 = x^3y - xy^3 \in \mathbb{k}[x, y]$.
2. Consider $g = x^4 + y^4, f_1 = x + y, f_2 = xy \in \mathbb{k}[x, y]$. Show that g is contained in the subalgebra $\mathbb{k}[f_1, f_2] \subset \mathbb{k}[x, y]$, and express g as a polynomial in f_1, f_2.

Exercise 2.5.16. Consider the ideal $I = (x_1x_2x_3 - 1) \subset \mathbb{k}[x_1, x_2, x_3]$ and the homomorphism

$$\phi : \mathbb{k}[y_1, y_2, y_3] \to \mathbb{k}[x_1, x_2, x_3]/I, y_1 \mapsto x_2x_3, y_2 \mapsto x_1x_3, y_3 \mapsto x_1x_2.$$

Prove that ϕ induces an isomorphism $\mathbb{k}[y_1, y_2, y_3]/(y_1y_2y_3 - 1) \cong \mathbb{k}[x_1, x_2, x_3]/(x_1x_2x_3 - 1)$. Thus $A = \mathrm{V}(x_1x_2x_3 - 1) \subset \mathbb{A}^3(\mathbb{k})$ has a "nonlinear" automorphism. Determine the fixed points of this automorphism.

As a final application of Gröbner bases in this section, we give an elementary proof of Hilbert's syzygy theorem. Hilbert's own proof is based on elimination and, as Hilbert remarks, "nicht ganz ohne Mühe"[1] (see Hilbert [1890]). The syzygy theorem is the starting point of homological algebra, a mathematical discipline of its own, which is crosslinked to many other mathematical disciplines (see for instance Eisenbud [1995]).

We use the following terminology.

---

[1] not entirely without effort

Definition 2.5.17. Let R be a ring, and let

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\phi_{i+1}} M_i \xrightarrow{\phi_i} M_{i-1} \longrightarrow \dots$$

be a finite or infinite sequence of R-modules and homomorphisms. If $\operatorname{im}\phi_{i+1} = \ker\phi_i$ for a pair (ϕ_{i+1}, ϕ_i) of consecutive homomorphisms, the sequence is said to be **exact at $\mathbf{M_i}$**. If this condition holds for each pair of consecutive homomorphisms, the entire sequence is said to be **exact**.

For instance, a finite sequence

$$M_r \to M_{r-1} \to \cdots \to M_{s+1} \to M_s$$

is exact, if it is exact at each M_i, $r-1 \leq i \leq s+1$.

Example 2.5.18. Let R be a ring, and let $\phi : M \to N$ be a homomorphism of R-modules. Write 0 for the trivial R-module, and let $0 \to M$ and $N \to 0$ be the zero homomorphisms. Then:

1. ϕ is injective $\iff$ the sequence $0 \to M \to N$ is exact.
2. ϕ is surjective $\iff$ the sequence $M \to N \to 0$ is exact.
3. ϕ is bijective $\iff$ the sequence $0 \to M \to N \to 0$ is exact.

Example 2.5.19. Let R be a ring. A **short exact sequence** is an exact sequence of R-modules of type

$$0 \longrightarrow M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \longrightarrow 0.$$

That is, ϕ is injective, ψ is surjective, and $\operatorname{im}\phi = \ker\psi$. For instance, if M is an R-module, and if $N \subset M$ is a submodule, we have a canonical short exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0.$$

A sequence

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\phi_{i+1}} M_i \xrightarrow{\phi_i} M_{i-1} \longrightarrow \dots$$

as in Definition 2.5.17 is exact iff each induced short exact sequence

$$0 \longrightarrow M_{i+1}/\ker\phi_{i+1} \longrightarrow M_i \longrightarrow \operatorname{im}\phi_i \longrightarrow 0$$

is exact.

Following Hilbert, we now consider exact sequences of a special type. Sequences of this type will allow us to obtain information on an arbitrary module from information on free modules. Hilbert's original application, namely the theorem on the polynomial nature of Hilbert functions, will be presented in Chapter **??**.

As we already know, every finitely generated module M over a ring R is the epimorphic image of a free R-module. Indeed, choose generators $f_1, \dots, f_{s_0}$ of M, and consider the map

$$R^{s_0} \xrightarrow{\pi} M \ , \epsilon_i \mapsto f_i,$$

which sends the ith canonical basis vector of R^{s_0} to f_i. If R is Noetherian, the syzygy module $\ker \pi = \mathrm{Syz}\,(f_1, \dots, f_{s_0})$ is finitely generated, too, and the same argument as above yields an epimorphism $R^{s_1} \to \ker \pi$. If ϕ_1 is the composite map $R^{s_1} \to \ker \pi \to R^{s_0}$, then $M = \operatorname{coker} \phi_1$.

Definition 2.5.20. Let M be a module over a ring R. A **presentation** for M is a set of generators $f_1, \dots, f_{s_0}$ for M, together with a set of generators for the module of relations $\mathrm{Syz}\,(f_1, \dots, f_{s_0})$. If such a presentation is given, we say that M is **given by generators and relations**.

We may think of a presentation for M as an exact sequence

$$R^{s_1} \xrightarrow{\phi_1} R^{s_0} \longrightarrow M \longrightarrow 0,$$

representing M as the cokernel of a homomorphism between free R-modules. In computational algebraic geometry, a module is usually specified by an explicit presentation matrix ϕ_1.

Exercise 2.5.21. kernels

Exercise 2.5.22. hom

Further repetition in our construction above yields a sequence of free R-modules and R-module homomorphisms

$$\dots \xrightarrow{\phi_{k+2}} R^{s_{k+1}} \xrightarrow{\phi_{k+1}} R^{s_k} \longrightarrow \dots \longrightarrow R^{s_1} \xrightarrow{\phi_1} R^{s_0},$$

with $M \cong \operatorname{coker} \phi_1$, and with $\operatorname{im} \phi_{i+1} = \ker \phi_i$ for all $i \geq 1$.

Definition 2.5.23. Every exact sequence as above is called a **free resolution of M**. It is a **finite free resolution** of M if there exists an integer c with ϕ_c injective, that is, with $R^{s_k} = 0$ for $k \geq c + 1$. In this case, the least such c is the **length** of the resolution.

Theorem 2.5.24 (Hilbert's syzygy theorem). *Every finitely generated $R = \Bbbk[x_1, \dots, x_n]$-module M has a finite free resolution of length at most n.*

Proof. We give a constructive proof, supposing that M is given by generators and relations as the cokernel of a map $R^r \xrightarrow{\phi} R^{s_0}$ between free R-modules. The columns $f_1, \dots, f_r$ of ϕ generate $\operatorname{im} \phi$. Compute a Gröbner basis $f_1, \dots, f_r, f_{r+1}, \dots, f_{s_1}$ for $\operatorname{im} \phi$ with respect to any global monomial order on R^{s_0} (we may and will assume that the leading terms of $f_1, \dots, f_r$ involve different monomials). During this computation, keep track of the syzygies $G^{(i,\alpha)}$ obtained by Buchberger's test. With respect to the induced order, the $G^{(i,\alpha)}$ form a Gröbner basis for the kernel of the composite map $\phi_1 : R^{s_1} \to \operatorname{im} \phi \to R^{s_0}$ which sends the ith canonical basis vector ϵ_i of R^{s_1} to f_i. Suppose that for some $k \leq n$ none of the leading terms $\mathbf{L}(f_i)$ involves the variables $x_1, \dots, x_k$. We may and will assume that the f_i are sorted so that for $i > j$ the exponent of x_{k+1} in $\mathbf{L}(f_i)$ is greater than or equal to that in $\mathbf{L}(f_j)$, whenever these terms involve the same basis element. Then none of the leading terms $\mathbf{L}(G^{(i,\alpha)}) = c^{(i,\alpha)} x^\alpha \epsilon_i$ involves x_{k+1}. Continuing in this way, we obtain after $l \leq n$ steps an exact sequence of free R-modules

$$R^{s_l} \xrightarrow{\phi_l} R^{s_{l-1}} \longrightarrow \cdots \longrightarrow R^{s_1} \xrightarrow{\phi_1} R^{s_0},$$

with $M \cong \operatorname{coker} \phi_1$, and a Gröbner basis $\{g_1, \dots, g_t\}$ of $\ker \phi_l$ such that none the leading terms $\mathbf{L}(g_i)$ involves $x_1, \dots, x_n$. We then have an induced exact sequence

$$0 \longrightarrow R^{s_l}/\ker \phi_l \longrightarrow R^{s_{l-1}} \cdots \longrightarrow R^{s_1} \xrightarrow{\phi_1} R^{s_0},$$

and the result follows since $R^{s_l}/\ker \phi_l$ is a free R-module. Indeed, the initial terms $\mathbf{L}(g_i)$ are constants times basis vectors of R^{s_l}, hence $\ker \phi_l$ is the free submodule of R^{s_l} generated by the involved basis vectors. If F is the free submodule generated by the other basis vectors, the composite map

$$F \subset R^{s_0} \longrightarrow R^{s_l}/\ker \phi_l$$

is an isomorphism by Macaulay's theorem 2.3.5, hence $R^{s_l}/\ker \phi_l \cong F$ is free. □

Example 2.5.25. Consider the ideal

$$I = (f_1, \dots, f_5) \subset R = \Bbbk[w, x, y, z],$$

generated by the polynomials

$$f_1 = w^2 - xz, f_2 = wx - yz, f_3 = x^2 - wy, f_4 = xy - z^2, f_5 = y^2 - wz.$$

We compute a finite free resolution of $M = R/I$, starting with the degree reverse lexicographic order on $\mathbb{k}[w, x, y, z]$. We successively obtain three syzygy matrices ϕ_1, ϕ_2 and ϕ_3 which we present in a compact way as follows:

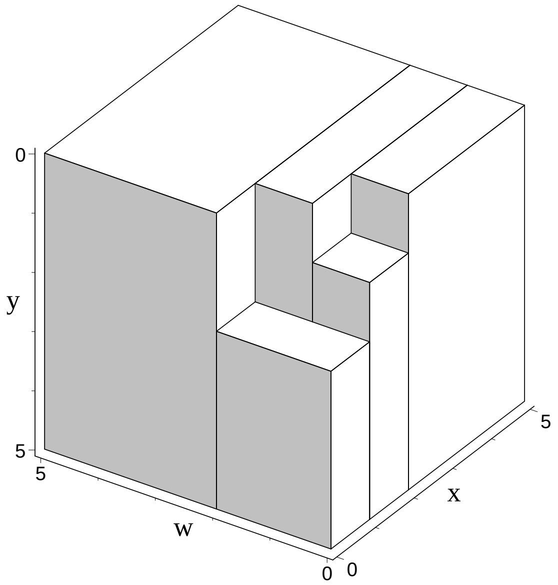
$$
\begin{array}{c|cccccc}
\mathbf{w^2} - xz & -x & y & 0 & -z & 0 & -y^2 + wz \\
\mathbf{wx} - yz & \mathbf{w} & -x & -y & 0 & z & z^2 \\
\mathbf{x^2} - wy & -z & \mathbf{w} & 0 & -y & 0 & 0 \\
\mathbf{xy} - z^2 & 0 & 0 & \mathbf{w} & \mathbf{x} & -y & yz \\
\mathbf{y^2} - wz & 0 & 0 & -z & -w & \mathbf{x} & \mathbf{w^2} \\
\hline
 & 0 & y & -x & \mathbf{w} & -z & 1 \\
 & -y^2 + wz & z^2 & -wy & yz & -w^2 & \mathbf{x}
\end{array}
$$

All the initial terms are printed in bold. The first column of our table is the transposed of ϕ_1. It contains the original generators of I which as Buchberger's test shows form already a Gröbner basis for I. The syzygy matrix ϕ_2 resulting from the test is the 5×6 matrix in the middle of our table. Notice that for instance $M_4 = (w, x)$ can be read off the 4th row of ϕ_2. At this point we already know that the columns of ϕ_2 form a Gröbner basis for Syz $(f_1, \ldots, f_r)$ with respect to the induced order on R^5. Buchberger's test applied to these Gröbner basis elements yields a 6×2 syzygy matrix ϕ_3 whose transposed is printed in the two bottom rows of our table. The map defined by ϕ_3 is injective since the initial terms involve different basis vectors. Thus we obtain a free resolution of type

$$0 \longrightarrow R^2 \xrightarrow{\phi_3} R^6 \xrightarrow{\phi_2} R^5 \xrightarrow{\phi_1} R.$$

Notice that once we have the initial terms of the Gröbner basis for I, we can easily compute the initial terms of the Gröbner bases for all the syzygy modules, that is, all the bold face entries of our table. This gives us an idea on the amount of the computations lying ahead.

Let us visualize the monomials in $\mathbf{L}(I)$:



Exercise 2.5.26. Compute a finite free resolution of the ideal generated by the 2×2 minors of the matrix

$$\begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}.$$

Remark 2.5.27. It took a long time to understand the syzygy theorem completely. For example, it is not true that every finitely generated module over a Noetherian ring has a finite free resolution. For instance, if $R = \mathbb{k}[x,y]/(xy)$, the ideal generated by the class $\bar{x} = x + (xy)$ in R has the infinite periodic resolution

$$0 \longleftarrow (\bar{x}) \longleftarrow R \xleftarrow{\bar{y}} R \xleftarrow{\bar{x}} R \xleftarrow{\bar{y}} R \longleftarrow \dots .$$

Some references for further reading on this topic are [**?**], [**?**], [**?**, **?**] and [**?**].

2.6 The geometry of elimination

To explore the geometric meaning of elimination over an arbitrary ground field, we will go back and forth between $\mathbb{k}$ and its algebraic closure $\bar{\mathbb{k}}$. We use the following notations. If $I \subset \mathbb{k}[x_1, \dots, x_n]$ is an ideal, then $A = \mathrm{V}(I)$ denotes its zero locus in $\mathbb{A}^n(\bar{\mathbb{k}})$, and $A(\mathbb{k}) = A \cap \mathbb{A}^n(\mathbb{k})$ its zero locus in $\mathbb{A}^n(\mathbb{k})$. We write $\mathbb{A}^n = \mathbb{A}^n(\bar{\mathbb{k}})$ for short.