Chapter 4

Computation in Local Rings

Many questions in algebraic geometry involve a study of *local properties* of varieties, that is, properties of a single point, or of a suitably small neighborhood of a point. For example, in analyzing $\mathbf{V}(I)$ for a zero-dimensional ideal $I \subset k[x_1, \ldots, x_n]$, even when k is algebraically closed, it sometimes happens that $\mathbf{V}(I)$ contains fewer distinct points than the dimension $d = \dim k[x_1, \ldots, x_n]/I$. In this situation, thinking back to the consequences of unique factorization for polynomials in one variable, it is natural to ask whether there is an algebraic *multiplicity* that can be computed locally at each point in $\mathbf{V}(I)$, with the property that the sum of the multiplicities is equal to d. Similarly in the study of *singularities* of varieties, one major object of study is local invariants of singular points. These are used to distinguish different types of singularities and study their local structure. In §1 of this chapter, we will introduce the algebra of *local rings* which is useful for both these types of questions. Multiplicities and some invariants of singularities will be introduced in §2. In §3 and §4, we will develop algorithmic techniques for computation in local rings parallel to the theory of Gröbner bases in polynomial rings. Applications of these techniques are given in §5.

In this chapter, we will often assume that k is an algebraically closed field containing $\mathbb{Q}$. The results of Chapters 2 and 3 are valid for such fields.

§1 Local Rings

One way to study properties of a variety V is to study functions on the variety. The elements of the ring $k[x_1, \ldots, x_n]/\mathbf{I}(V)$ can be thought of as the polynomial functions on V. Near a particular point $p \in V$ we can also consider rational functions defined at the point, power series convergent at the point, or even formal series centered at the point. Considering the collections of each of these types of functions in turn leads us to new rings that strictly contain the ring of polynomials. In a sense which we shall make precise as we go along, consideration of these larger rings corresponds to looking at smaller neighborhoods of points. We will begin with the following example. Let $V = k^n$, and let $p = (0, \ldots, 0)$ be the origin. The single point set $\{p\}$ is a variety, and $\mathbf{I}(\{p\}) = \langle x_1, \ldots, x_n \rangle \subset k[x_1, \ldots, x_n]$. Furthermore, a rational function f/g has a well-defined value at p provided $g(p) \neq 0$.

(1.1) Definition. We denote by $k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle}$ the collection of all rational functions f/g of $x_1, \ldots, x_n$ with $g(p) \neq 0$, where $p = (0, \ldots, 0)$.

The main properties of $k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle}$ are as follows.

(1.2) Proposition. *Let $R = k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle}$. Then*

a. *R is a subring of the field of rational functions $k(x_1, \ldots, x_n)$ containing $k[x_1, \ldots, x_n]$.*

b. *Let $M = \langle x_1, \ldots, x_n \rangle \subset R$ (the ideal generated by $x_1, \ldots, x_n$ in R). Then every element in $R \setminus M$ is a unit in R (i.e., has a multiplicative inverse in R).*

c. *M is a maximal ideal in R, and R has no other maximal ideals.*

Proof. As above, let $p = (0, \ldots, 0)$. Part a follows easily since R is closed under sums and products in $k(x_1, \ldots, x_n)$. For instance, if f_1/g_1 and f_2/g_2 are two rational functions with $g_1(p), g_2(p) \neq 0$, then

$$f_1/g_1 + f_2/g_2 = (f_1g_2 + f_2g_1)/(g_1g_2).$$

Since $g_1(p) \neq 0$ and $g_2(p) \neq 0$, $g_1(p) \cdot g_2(p) \neq 0$. Hence the sum is an element of R. A similar argument shows that the product $(f_1/g_1) \cdot (f_2/g_2)$ is in R. Finally, since $f = f/1$ is in R for all $f \in k[x_1, \ldots, x_n]$, the polynomial ring is contained in R.

For part b, we will use the fact that the elements in $M = \langle x_1, \ldots, x_n \rangle$ are exactly the rational functions $f/g \in R$ such that $f(p) = 0$. Hence if $f/g \notin M$, then $f(p) \neq 0$ and $g(p) \neq 0$, and g/f is a multiplicative inverse for f/g in R.

Finally, for part c, if $N \neq M$ is an ideal in R with $M \subset N \subset R$, then N must contain an element f/g in the complement of M. By part b, f/g is a unit in R, so $1 = (f/g)(g/f) \in N$, and hence $N = R$. Therefore M is maximal. M is the only maximal ideal in R, because it also follows from part b that every proper ideal $I \subset R$ is contained in M. □

Exercise 1. In this exercise you will show that if $p = (a_1, \ldots, a_n) \in k^n$ is any point and

$$R = \{f/g : f, g \in k[x_1, \ldots, x_n], g(p) \neq 0\},$$

then we have the following statements parallel to Proposition (1.2).

a. R is a subring of the field of rational functions $k(x_1, \ldots, x_n)$.

b. Let M be the ideal generated by $x_1 - a_1, \ldots, x_n - a_n$ in R. Then every element in $R \setminus M$ is a unit in R (i.e., has a multiplicative inverse in R).

c. M is a maximal ideal in R, and R has no other maximal ideals.

An alternative notation for the ring R in Exercise 1 is

$$R = k[x_1, \ldots, x_n]_{\langle x_1 - a_1, \ldots, x_n - a_n \rangle},$$

where $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is the ideal $\mathbf{I}(\{p\})$ in $k[x_1, \ldots, x_n]$, and in R we allow denominators that are *not* elements of this ideal.

In the following discussion, the term *ring* will always mean a commutative ring with identity. Every ring has maximal ideals. As we will see, the rings that give *local* information are the ones with the property given by part c of Proposition (1.2) above.

(1.3) Definition. A *local ring* is a ring that has exactly one maximal ideal.

The idea of the argument used in the proof of part c of the proposition also gives one general criterion for a ring to be a local ring.

(1.4) Proposition. *A ring R with a proper ideal $M \subset R$ is a local ring if every element of $R \setminus M$ is a unit in R.*

Proof. If every element of $R \setminus M$ is a unit in R, the unique maximal ideal is M. Exercise 5 below asks you to finish the proof. □

Definition (1.1) above is actually a special case of a general procedure called *localization* that can be used to construct many additional examples of local rings. See Exercise 8 below. An even more general construction of rings of fractions is given in Exercise 9. We will need to use that construction in §3 and §4.

We also obtain important examples of local rings by considering functions more general than rational functions. One way such functions arise is as follows. When studying a curve or, more generally, a variety near a point, one often tries to *parametrize* the variety near the point. For example, the curve

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

is a circle of radius 1 centered at the point $(-1, 0)$. To study this curve near the origin, we might use parametrizations of several different types.

Exercise 2. Show that one parametrization of the circle near the origin is given by

$$x = \frac{-2t^2}{1+t^2}, \qquad y = \frac{2t}{1+t^2}.$$

Note that both components are elements of the local ring $k[t]_{\langle t \rangle}$.

In this case, we might also use the parametrization in terms of trigonometric functions:

$$x = -1 + \cos t, \qquad y = \sin t.$$

The functions $\sin t$ and $\cos t$ are not polynomials or rational functions, but recall from elementary calculus that they can be expressed as convergent power series in t:

$$\begin{aligned}\sin t &= \sum_{k=0}^{\infty} (-1)^k t^{2k+1}/(2k+1)!\\ \cos t &= \sum_{k=0}^{\infty} (-1)^k t^{2k}/(2k)!\ .\end{aligned}$$

In this case parametrizing leads us to consider functions more general than polynomials or rational functions.

If $k = \mathbb{C}$ or $k = \mathbb{R}$, then we can consider the set of convergent power series in n variables (expanding about the origin)

$$\begin{aligned} k\{x_1, \ldots, x_n\} = \big\{\textstyle\sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} c_\alpha x^\alpha : c_\alpha \in k \text{ and the series}\\ \text{converges in some neighborhood of } 0 \in k^n\big\}.\end{aligned} \tag{1.5}$$

With the usual notion of addition and multiplication, this set is a ring (we leave the verification to the reader; see Exercise 3). In fact, it is not difficult to see that $k\{x_1, \ldots, x_n\}$ is also a local ring with maximal ideal generated by $x_1, \ldots, x_n$.

No matter what field k is, we can also consider the set $k[[x_1, \ldots, x_n]]$ of formal power series

$$k[[x_1, \ldots, x_n]] = \big\{\textstyle\sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} c_\alpha x^\alpha : c_\alpha \in k\big\}, \tag{1.6}$$

where, now, we waive the condition that the series need converge. Algebraically, a formal power series is a perfectly well defined object and can easily be manipulated—one must, however, give up the notion of evaluating it at any point of k^n other than the origin. As a result, a formal power series defines a *function* only in a rather limited sense. But in any case we can define addition and multiplication of formal series in the obvious way and this makes $k[[x_1, \ldots, x_n]]$ into a ring (see Exercise 3). Formal power series are also useful in constructing parametrizations of varieties over arbitrary fields (see Exercise 7 below).

At the beginning of the section, we commented that the three rings $k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n\rangle}$, $k\{x_1, \ldots, x_n\}$, and $k[[x_1, \ldots, x_n]]$ correspond to looking at smaller and smaller neighborhoods of the origin. Let us make this more precise. An element $f/g \in k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n\rangle}$ is defined not just at the origin but at every point in the complement of $\mathbf{V}(g)$. The domain of convergence of a power series can be a much smaller set than the complement of a variety. For instance, the geometric series $1 + x + x^2 + \cdots$

converges to the sum $1/(1-x) \in k[x]_{\langle x\rangle}$ only on the set of x with $|x| < 1$ in $k = \mathbb{R}$ or $\mathbb{C}$. A formal series in $k[[x_1, \ldots, x_n]]$ is only guaranteed to converge at the origin. Nevertheless, both $k\{x_1, \ldots, x_n\}$ and $k[[x_1, \ldots, x_n]]$ share the key algebraic property of $k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$.

(1.7) Proposition. *$k[[x_1, \ldots, x_n]]$ is a local ring. If $k = \mathbb{R}$ or $k = \mathbb{C}$ then $k\{x_1, \ldots, x_n\}$ is also a local ring.*

Proof. To show that $k[[x_1, \ldots, x_n]]$ is a local ring, consider the ideal $M = \langle x_1, \ldots, x_n\rangle \subset k[[x_1, \ldots, x_n]]$ generated by $x_1, \ldots, x_n$. If $f \notin M$, then $f = c_0 + g$ with $c_0 \neq 0$, and $g \in M$. Using the formal geometric series expansion

$$\frac{1}{1+t} = 1 - t + t^2 + \cdots + (-1)^n t^n + \cdots,$$

we see that

$$\begin{aligned}\frac{1}{c_0 + g} &= \frac{1}{c_0(1 + g/c_0)}\\ &= (1/c_0)\big(1 - g/c_0 + (g/c_0)^2 + \cdots\big).\end{aligned}$$

In Exercise 4 below, you will show that this expansion makes sense as an element of $k[[x_1, \ldots, x_n]]$. Hence f has a multiplicative inverse in $k[[x_1, \ldots, x_n]]$. Since this is true for every $f \notin M$, Proposition (1.4) implies that $k[[x_1, \ldots, x_n]]$ is a local ring.

To show that $k\{x_1, \ldots, x_n\}$ is also a local ring, we only need to show that the formal series expansion for $1/(c_0 + g)$ gives a convergent series. See Exercise 4. □

All three types of local rings share other key algebraic properties with rings of polynomials. See the exercises in §4. By considering the power series expansion of a rational function defined at the origin, as in the proof above, we have $k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle} \subset k[[x_1, \ldots, x_n]]$. In the case $k = \mathbb{R}$ or $\mathbb{C}$, we also have inclusions:

$$k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle} \subset k\{x_1, \ldots, x_n\} \subset k[[x_1, \ldots, x_n]].$$

In general, we would like to be able to do operations on ideals in these rings in much the same way that we can carry out operations on ideals in a polynomial ring. For instance, we would like to be able to settle the ideal membership question, to form intersections of ideals, compute quotients, compute syzygies on a collection of elements, and the like. We will return to these questions in §3 and §4.

Additional Exercises for §1

Exercise 3. The product operations in $k[[x_1, \ldots, x_n]]$ and $k\{x_1, \ldots, x_n\}$ can be described in the following fashion. Grouping terms by total degree, rewrite each power series

$$f(x) = \textstyle\sum_{\alpha\in\mathbb{Z}^n_{\geq 0}} c_\alpha x^\alpha$$

as $\sum_{n\geq 0} f_n(x)$, where

$$f_n(x) = \sum_{\substack{\alpha\in\mathbb{Z}^n_{\geq 0}\\ |\alpha|=n}} c_\alpha x^\alpha$$

is a homogeneous polynomial of degree n. The product of two series $f(x)$ and $g(x)$ is the series $h(x)$ for which

$$h_n = f_n g_0 + f_{n-1}g_1 + \cdots + f_0 g_n.$$

a. Show that with this product and the obvious sum, $k[[x_1,\ldots,x_n]]$ is a (commutative) ring (with identity).
b. Now assume $k=\mathbb{R}$ or $k=\mathbb{C}$, and suppose $f,g\in k\{x_1,\ldots,x_n\}$. From part a, we know that sums and products of power series give other formal series. Show that if f and g are both convergent on some neighborhood U of $(0,\ldots,0)$, then $f+g$ and $f\cdot g$ are also convergent on U.

Exercise 4. Let $h\in\langle x_1,\ldots,x_n\rangle\subset k[[x_1,\ldots,x_n]]$.
a. Show that the formal geometric series expansion

$$\frac{1}{1+h} = 1 - h + h^2 - h^3 + \cdots$$

gives a well-defined element of $k[[x_1,\ldots,x_n]]$. (What are the homogeneous components of the series on the right?)
b. Show that if h is convergent on some neighborhood of the origin, then the expansion in part a is also convergent on some (generally smaller) neighborhood of the origin. (Recall that

$$\frac{1}{1+t} = 1 - t + t^2 - t^3 + \cdots$$

is convergent only for t satisfying $|t|<1$.)

Exercise 5. Give a complete proof for Proposition (1.4).

Exercise 6. Let F be a field. A *discrete valuation* of F is an onto mapping $v : F\setminus\{0\}\to\mathbb{Z}$ with the properties that
1. $v(x+y)\geq\min\{v(x),v(y)\}$, and
2. $v(xy) = v(x)+v(y)$.

The subset of F consisting of all elements x satisfying $v(x)\geq 0$, together with 0, is called the *valuation ring* of v.

a. Show that the valuation ring of a discrete valuation is a local ring. Hint: Use Proposition (1.4).

b. For example, let $F = k(x)$ (the rational function field in one variable), and let f be an irreducible polynomial in $k[x] \subset F$. If $g \in k(x)$, then by unique factorization in $k[x]$, there is a unique expression for g of the form $g = f^a \cdot n/d$, where $a \in \mathbb{Z}$, and $n, d \in k[x]$ are not divisible by f. Let $v(g) = a \in \mathbb{Z}$. Show that v defines a discrete valuation on $k(x)$. Identify the maximal ideal of the valuation ring.

c. Let $F = \mathbb{Q}$, and let p be a prime integer. Show that if $g \in \mathbb{Q}$, then by unique factorization in $\mathbb{Z}$, there is a unique expression for g of the form $g = p^a \cdot n/d$, where $a \in \mathbb{Z}$, and $n, d \in \mathbb{Z}$ are not divisible by p. Let $v(g) = a \in \mathbb{Z}$. Show that v defines a discrete valuation on $\mathbb{Q}$. Identify the maximal ideal of this valuation ring.

Exercise 7. (A Formal Implicit Function Theorem) Let $f(x, y) \in k[x, y]$ be a polynomial of the form

$$f(x, y) = y^n + c_1(x)y^{n-1} + \cdots + c_{n-1}(x)y + c_n(x),$$

where $c_i(x) \in k[x]$. Assume that $f(0, y) = 0$ has n *distinct* roots $a_i \in k$.

a. Starting from $y_i^{(0)}(x) = a_i$, show that there is a unique $a_{i1} \in k$ such that $y_i^{(1)}(x) = a_i + a_{i1}x$ satisfies

$$f(x, y_i^{(1)}(x)) \equiv 0 \bmod \langle x^2 \rangle.$$

b. Show that if we have a polynomial $y_i^{(\ell)}(x) = a_i + a_{i1}x + \cdots + a_{i\ell}x^\ell$, that satisfies

$$f(x, y_i^{(\ell)}(x)) \equiv 0 \bmod \langle x^{\ell+1} \rangle,$$

then there exists a unique $a_{i,\ell+1} \in k$ such that

$$y_i^{(\ell+1)}(x) = y_i^{(\ell)}(x) + a_{i,\ell+1}x^{\ell+1}$$

satisfies

$$f(x, y_i^{(\ell+1)}(x)) \equiv 0 \bmod \langle x^{\ell+2} \rangle.$$

c. From parts a and b, deduce that there is a unique power series $y_i(x) \in k[[x]]$ that satisfies $f(x, y_i(x)) = 0$ and $y_i(0) = a_i$.

Geometrically, this gives a formal series parametrization of the branch of the curve $f(x, y)$ passing through $(0, a_i)$: $(x, y_i(x))$. It also follows that $f(x, y)$ *factors* in the ring $k[[x]][y]$:

$$f(x, y) = \prod_{i=1}^{n} (y - y_i(x)).$$

Exercise 8. Let R be an integral domain (that is, a ring with no zero-divisors), and let $P \subset R$ be a prime ideal (see Exercise 8 of Chapter 1, §1 for the definition, which is the same in any ring R). The *localization of R* *with respect to* P, denoted R_P, is a new ring containing R, in which every element in R not in the specified prime ideal P becomes a unit. We define

$$R_P = \{r/s : r, s \in R, s \notin P\},$$

so that R_P is a subset of the field of fractions of R.

a. Using Proposition (1.4), show that R_P is a local ring, with maximal ideal $M = \{p/s : p \in P, s \notin P\}$.
b. Show that every ideal in R_P has the form $I_P = \{a/s : a \in I, s \notin P\}$, where I is an ideal of R contained in P.

Exercise 9. The construction of R_P in Exercise 8 can be generalized in the following way. If R is any ring, and $S \subset R$ is a set which is closed under multiplication (that is, $s_1, s_2 \in S$ implies $s_1 \cdot s_2 \in S$), then we can form "fractions" a/s, with $a \in R, s \in S$. We will say two fractions a/s and b/t are *equivalent* if there is some $u \in S$ such that $u(at - bs) = 0$ in R. We call the collection of equivalence classes for this relation $S^{-1}R$.

a. Show that forming sums and products as with ordinary fractions gives *well-defined* operations on $S^{-1}R$.
b. Show that $S^{-1}R$ is a ring under these sum and product operations.
c. If R is any ring (not necessarily an integral domain) and $P \subset R$ is a prime ideal, show that $S = R \setminus P$ is closed under multiplication. The resulting ring of fractions $S^{-1}R$ is also denoted R_P (as in Exercise 8).

Exercise 10. Let $R = k[x_1, \ldots, x_n]$ and $I = \langle f_1, \ldots, f_m \rangle$ be an ideal in R. Let $M = \langle x_1, \ldots, x_n \rangle$ be the maximal ideal of polynomials vanishing at the origin and suppose that $I \subset M$.

a. Show that the ideal M/I generated by the cosets of $x_1, \ldots, x_n$ in R/I is a prime ideal.
b. Let IR_M denote the ideal generated by the f_i in the ring R_M, and let $(R/I)_{M/I}$ be constructed as in Exercise 8. Let $r/s \in R_M$, let $[r], [s]$ denote the cosets of the numerator and denominator in R/I, and let $[r/s]$ denote the coset of the fraction in R_M/IR_M. Show that the mapping

$$\begin{aligned} \varphi : R_M/IR_M &\to (R/I)_{M/I} \\ [r/s] &\mapsto [r]/[s] \end{aligned}$$

is well defined and gives an isomorphism of rings.

Exercise 11. Let $R = k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle}$. Show that every ideal $I \subset R$ has a generating set consisting of polynomials $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$.

Exercise 12. (Another interpretation of $k\{x_1, \ldots, x_n\}$) Let $k = \mathbb{R}$ or $\mathbb{C}$ and let $U \subset k^n$ be open. A function $f : U \to k$ is *analytic* if it can be represented by a power series with coefficients in k at each point of U. One can prove that every element of $k\{x_1, \ldots, x_n\}$ defines an analytic function on some neighborhood of the origin. We can describe $k\{x_1, \ldots, x_n\}$ in terms of analytic functions as follows. Two analytic functions, each defined on some neighborhood of the origin, are *equivalent* if there is some (smaller) neighborhood of the origin on which they are equal. An equivalence class of analytic functions with respect to this relation is called a *germ* of an analytic function (at the origin).

a. Show that the set of germs of analytic functions at the origin is a ring under the usual sum and product of functions.
b. Show that this ring can be identified with $k\{x_1, \ldots, x_n\}$ and that the maximal ideal is precisely the set of germs of analytic functions which vanish at the origin.
c. Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = \begin{cases} e^{-1/x^2} & \text{if } x > 0 \\ 0 & \text{if } x \le 0. \end{cases}$$

Show that f is C^∞ on $\mathbb{R}$, and construct its Taylor series, expanding at $a = 0$. Does the Taylor series converge to $f(x)$ for all x in some neighborhood of $0 \in \mathbb{R}$?

If $k = \mathbb{R}$, the example given in part c shows that the ring of germs of infinitely differentiable real functions is not equal to $k\{x_1, \ldots, x_n\}$. On the other hand, it is a basic theorem of complex analysis that a complex differentiable function is analytic.

§2 Multiplicities and Milnor Numbers

In this section we will see how local rings can be used to assign local multiplicities at the points in $\mathbf{V}(I)$ for a zero-dimensional ideal I. We will also use local rings to define the Milnor and Tjurina numbers of an isolated singular point of a hypersurface.

To see what the issues are, let us turn to one of the most frequent computations that one is called to do in a local ring, that of computing the dimension of the quotient ring by a zero-dimensional ideal. In Chapter 2, we learned how to compute the dimension of $k[x_1, \ldots, x_n]/I$ when I is a zero-dimensional polynomial ideal. Recall how this works. For any monomial order, we have

$$\dim k[x_1, \ldots, x_n]/I = \dim k[x_1, \ldots, x_n]/\langle \text{LT}(I) \rangle,$$

and the latter is just the number of monomials x^α such that $x^\alpha \notin \langle \text{LT}(I) \rangle$. For example, if

$$I = \langle x^2 + x^3, y^2 \rangle \subset k[x, y],$$

then using the *lex* order with $y > x$ for instance, the given generators form a Gröbner basis for I. So

$$\dim k[x, y]/I = \dim k[x, y]/\langle \text{LT}(I) \rangle = \dim k[x, y]/\langle x^3, y^2 \rangle = 6.$$

The rightmost equality follows because the cosets of $1, x, x^2, y, xy, x^2y$ form a vector space basis of $k[x,y]/\langle x^3, y^2\rangle$. The results of Chapter 2 show that there are at most six common zeros of $x^2 + x^3$ and y^2 in k^2. In fact, from the simple form of the generators of I we see there are precisely *two* distinct points in $\mathbf{V}(I)$: $(-1,0)$ and $(0,0)$.

To define the local multiplicity of a solution of a system of equations, we use a local ring instead of the polynomial ring, but the idea is much the same as above. We will need the following notation. If I is an ideal in $k[x_1,\ldots,x_n]$, then we sometimes denote by $Ik[x_1,\ldots,x_n]_{\langle x_1,\ldots,x_n\rangle}$ the ideal generated by I in the larger ring $k[x_1,\ldots,x_n]_{\langle x_1,\ldots,x_n\rangle}$.

(2.1) Definition. Let I be a zero-dimensional ideal in $k[x_1,\ldots,x_n]$, so that $\mathbf{V}(I)$ consists of finitely many points in k^n, and assume that $(0,0,\ldots,0)$ is one of them. Then the *multiplicity* of $(0,0,\ldots,0)$ as a point in $\mathbf{V}(I)$ is

$$\dim_k k[x_1,\ldots,x_n]_{\langle x_1,\ldots,x_n\rangle}/Ik[x_1,\ldots,x_n]_{\langle x_1,\ldots,x_n\rangle}.$$

More generally, if $p = (a_1,\ldots,a_n) \in \mathbf{V}(I)$, then the *multiplicity* of p, denoted $m(p)$, is the dimension of the ring obtained by localizing $k[x_1,\ldots,x_n]$ at the maximal ideal $M = \mathbf{I}(\{p\}) = \langle x_1 - a_1,\ldots,x_n - a_n\rangle$ corresponding to p, and taking the quotient:

$$\dim k[x_1,\ldots,x_n]_M/Ik[x_1,\ldots,x_n]_M.$$

Since $k[x_1,\ldots,x_n]_M$ is a local ring, it is easy to show that the quotient $k[x_1,\ldots,x_n]_M/Ik[x_1,\ldots,x_n]_M$ is also local (see Exercise 6 below). The intuition is that since M is the maximal ideal of $p \in \mathbf{V}(I)$, the ring $k[x_1,\ldots,x_n]_M/Ik[x_1,\ldots,x_n]_M$ should reflect the local behavior of I at p. Hence the multiplicity $m(p)$, which is the dimension of this ring, is a measure of how complicated I is at p. Theorem (2.2) below will guarantee that $m(p)$ is finite.

We can also define the multiplicity of a solution p of a specific system $f_1 = \cdots = f_s = 0$, provided that p is an *isolated solution* (that is, there exists a neighborhood of p in which the system has no other solutions). From a more sophisticated point of view, this multiplicity is sometimes called the *local intersection multiplicity* of the variety $\mathbf{V}(f_1,\ldots,f_s)$ at p. However, we caution the reader that there is a more sophisticated notion of multiplicity called the *Hilbert-Samuel multiplicity* of I at p. This is denoted $e(p)$ and is discussed in [BH], Section 4.6.

Let us check Definition (2.1) in our example. Let $R = k[x,y]_{\langle x,y\rangle}$ be the local ring of k^2 at $(0,0)$ and consider the ideal J generated by the polynomials $x^2 + x^3$ and y^2 in R. The multiplicity of their common zero $(0,0)$ is $\dim R/J$.

Exercise 1. Notice that $x^2 + x^3 = x^2(1 + x)$.

a. Show that $1 + x$ is a unit in R, so $1/(1 + x) \in R$.

b. Show that x^2 and y^2 generate the same ideal in R as x^2+x^3 and y^2.
c. Show that every element $f \in R$ can be written uniquely as $f = g/(1+h)$, where $g \in k[x,y]$ and $h \in \langle x,y\rangle \subset k[x,y]$.
d. Show that for each $f \in R$, the coset $[f] \in R/\langle x^2,y^2\rangle R$ is equal to the coset $[g(1-h+h^2)]$, where g, h are as in part c.
e. Deduce that every coset in $R/\langle x^2,y^2\rangle R$ can be written as $[a+bx+cy+dxy]$ for some unique $a,b,c,d \in k$.

By the result of Exercise 1,

$$\dim R/J = \dim R/\langle x^2,y^2\rangle R = 4.$$

Thus the multiplicity of $(0,0)$ as a solution of $x^2+x^3 = y^2 = 0$ is 4.

Similarly, let us compute the multiplicity of $(-1,0)$ as a solution of this system. Rather than localizing at the prime ideal $\langle x+1,y\rangle$, we change coordinates to translate the point $(-1,0)$ to the origin and compute the multiplicity there. (This often simplifies the calculations; we leave the fact that these two procedures give the same results to the exercises.) So, set $X = x+1, Y = y$ (we want X and Y to be 0 when $x=-1$ and $y=0$) and let $S = k[X,Y]_{\langle X,Y\rangle}$. Then $x^2+x^3 = (X-1)^2+(X-1)^3 = X^3-2X^2+X$ and $y^2 = Y^2$ and we want to compute the multiplicity of $(0,0)$ as a solution of $X^3-2X^2+X = Y^2 = 0$. Now we note that $X^3-2X^2+X = X(1-2X+X^2)$ and $1/(1-2X+X^2) \in S$. Thus, the ideal generated by X and Y^2 in S is the same as that generated by X^3-2X+X and Y^2 and, therefore,

$$\dim S/\langle X^3-2X^2+X, Y^2\rangle S = \dim S/\langle X,Y^2\rangle S = 2.$$

Again, the equality on the right follows because the cosets of $1, Y$ are a basis of $S/\langle X,Y^2\rangle$. We conclude that the multiplicity of $(-1,0)$ as a solution of $x^3+x^2 = y^2 = 0$ is 2.

Thus, we have shown that the polynomials x^3+x^2 and y^2 have two common zeros, one of multiplicity 4 and the other of multiplicity 2. When the total number of zeros is counted with multiplicity, we obtain 6, in agreement with the fact that the dimension of the quotient ring of $k[x,y]$ by the ideal generated by these polynomials is 6.

Exercise 2.
a. Find all points in $\mathbf{V}(x^2-2x+y^2, x^2-4x+4y^4) \subset \mathbb{C}^2$ and compute the multiplicity of each as above.
b. Verify that the sum of the multiplicities is equal to

$$\dim \mathbb{C}[x,y]/\langle x^2-2x+y^2, x^2-4x+4y^4\rangle.$$

c. What is the geometric explanation for the solution of multiplicity > 1 in this example?

Before turning to the question of computing the dimension of a quotient of a local ring in more complicated examples, we will verify that the total number of solutions of a system $f_1 = \cdots = f_s = 0$, counted with multiplicity, is the dimension of $k[x_1, \ldots, x_n]/I$ when k is algebraically closed and $I = \langle f_1, \ldots, f_s \rangle$ is zero-dimensional. In a sense, this is confirmation that our definition of multiplicity behaves as we would wish. In the following discussion, if $\{p_1, \ldots, p_m\}$ is a finite subset of k^n, and $M_i = \mathbf{I}(\{p_i\})$ is the maximal ideal of $k[x_1, \ldots, x_n]$ corresponding to p_i, we will write

$$k[x_1, \ldots, x_n]_{M_i} = \{f/g : g(p_i) \neq 0\} = \mathcal{O}_i$$

for simplicity of notation.

(2.2) Theorem. *Let I be a zero-dimensional ideal in $k[x_1, \ldots, x_n]$ (k algebraically closed) and let $\mathbf{V}(I) = \{p_1, \ldots, p_m\}$. Then, there is an isomorphism between $k[x_1, \ldots, x_n]/I$ and the direct product of the rings $A_i = \mathcal{O}_i/I\mathcal{O}_i$, for $i = 1, \ldots, m$.*

Proof. For each i, $i = 1, \ldots, m$, there are ring homomorphisms

$$\begin{aligned} \varphi_i : k[x_1, \ldots, x_n] &\to A_i \\ f &\mapsto [f]_i, \end{aligned}$$

where $[f]_i$ is the coset of f in the quotient ring $\mathcal{O}_i/I\mathcal{O}_i$. Hence we get a ring homomorphism

$$\begin{aligned} \varphi : k[x_1, \ldots, x_n] &\to A_1 \times \cdots \times A_m \\ f &\mapsto ([f]_1, \ldots, [f]_m). \end{aligned}$$

Since $f \in I$ implies $[f]_i = 0 \in A_i$ for all i, we have $I \subset \ker(\varphi)$. So to prove the theorem, we need to show first that $I = \ker(\varphi)$ (by the fundamental theorem on ring homomorphisms, this will imply that $\mathrm{im}(\varphi) \cong k[x_1, \ldots, x_n]/I$), and second that φ is onto.

To prepare for this, we need to establish three basic facts. We use the notation $f \equiv g \bmod I$ to mean $f - g \in I$.

(2.3) Lemma. *Let $M_i = \mathbf{I}(\{p_i\})$ in $k[x_1, \ldots, x_n]$.*

a. *There exists an integer $d \geq 1$ such that $(\cap_{i=1}^m M_i)^d \subset I$.*

b. *There are polynomials $e_i \in k[x_1, \ldots, x_n]$, $i = 1, \ldots, m$, such that $\sum_{i=1}^m e_i \equiv 1 \bmod I$, $e_i e_j \equiv 0 \bmod I$ if $i \neq j$, and $e_i^2 \equiv e_i \bmod I$. Furthermore, $e_i \in I\mathcal{O}_j$ if $i \neq j$ and $e_i - 1 \in I\mathcal{O}_i$ for all i.*

c. *If $g \in k[x_1, \ldots, x_n] \setminus M_i$, then there exists $h \in k[x_1, \ldots, x_n]$ such that $hg \equiv e_i \bmod I$.*

Proof of the Lemma. Part a is an easy consequence of the Nullstellensatz. We leave the details to the reader as Exercise 7 below.

Turning to part b, Lemma (2.9) of Chapter 2 implies the existence of polynomials $g_i \in k[x_1, \ldots, x_n]$ such that $g_i(p_j) = 0$ if $i \neq j$, and $g_i(p_i) = 1$

for each i. Let

$$(2.4) \qquad e_i = 1 - (1 - g_i^d)^d,$$

where d is as in part a. Expanding the right-hand side of (2.4) with the binomial theorem and canceling the 1s, we see that $e_j \in M_i^d$ for $j \neq i$. On the other hand, (2.4) implies $e_i - 1 \in M_i^d$ for all i. Hence for each i,

$$\sum_j e_j - 1 = e_i - 1 + \sum_{j \neq i} e_j$$

is an element of M_i^d. Since this is true for all i, $\sum_j e_j - 1 \in \cap_{i=1}^m M_i^d$. Because the M_i are distinct maximal ideals, $M_i + M_j = k[x_1, \ldots, x_n]$ whenever $i \neq j$. It follows that $\cap_{i=1}^m M_i^d = (\cap_{i=1}^m M_i)^d$ (see Exercise 8 below). Hence $\sum_j e_j - 1 \in (\cap_{i=1}^m M_i)^d \subset I$. Similarly, $e_i e_j \in \cap_{i=1}^m M_i^d = (\cap_{i=1}^m M_i)^d \subset I$ whenever $i \neq j$, and the congruence $e_i^2 \equiv e_i \bmod I$ now follows easily (see Exercise 9 below). This implies $e_i(e_i - 1) \in I\mathcal{O}_j$ for all i, j. If $i \neq j$, then $e_i - 1$ is a unit in $\mathcal{O}_j$ since $e_i(p_j) = 0$. Thus $e_i \in I\mathcal{O}_j$. The proof that $e_i - 1 \in I\mathcal{O}_i$ follows similarly using $e_i(p_i) = 1$.

For part c, by multiplying by a constant, we may assume $g(p_i) = 1$. Then $1 - g \in M_i$, and hence taking $h = (1 + (1 - g) + \cdots + (1 - g)^{d-1})e_i$,

$$hg = h(1 - (1 - g)) = (1 - (1 - g)^d)e_i = e_i - (1 - g)^d e_i.$$

Since $(1 - g)^d \in M_i^d$ and $e_i \in M_j^d$ for all $j \neq i$, as shown above, we have $(1 - g)^d e_i \in I$ by part a, and the lemma is established. □

We can now complete the proof of Theorem (2.2). Let $f \in \ker(\varphi)$, and note that that kernel is characterized as follows:

$$\begin{aligned} \ker(\varphi) &= \{f \in k[x_1, \ldots, x_n] : [f]_i = 0 \text{ for all } i\} \\ &= \{f : f \in I\mathcal{O}_i \text{ for all } i\} \\ &= \{f : \text{ there exists } g_i \notin M_i \text{ with } g_i f \in I\}. \end{aligned}$$

For each of the g_i, by part c of the lemma, there exists some h_i such that $h_i g_i \equiv e_i \bmod I$. As a result, $f \cdot \sum_{i=1}^m h_i g_i = \sum_{i=1}^m h_i(g_i f)$ is an element of I, since each $g_i f \in I$. But on the other hand, $f \cdot \sum_{i=1}^m h_i g_i \equiv f \cdot \sum_i e_i \equiv f \bmod I$ by part b of the lemma. Combining these two observations, we see that $f \in I$. Hence $\ker(\varphi) \subset I$. Since we proved earlier that $I \subset \ker(\varphi)$, we have $I = \ker(\varphi)$.

To conclude the proof, we need to show that φ is onto. So let $([n_1/d_1], \ldots, [n_m/d_m])$ be an arbitrary element of $A_1 \times \cdots \times A_m$, where $n_i, d_i \in k[x_1, \ldots, x_n]$, $d_i \notin M_i$, and the brackets denote the coset in A_i. By part c of the lemma again, there are $h_i \in k[x_1, \ldots, x_n]$ such that $h_i d_i \equiv e_i \bmod I$. Now let $F = \sum_{i=1}^m h_i n_i e_i \in k[x_1, \ldots, x_n]$. It is easy to see that $\varphi_i(F) = [n_i/d_i]$ for each i since $e_i \in I\mathcal{O}_j$ for $i \neq j$ and $e_i - 1 \in I\mathcal{O}_i$ by part b of the lemma. Hence φ is onto. □

An immediate corollary of this theorem is the result we want.

(2.5) Corollary. *Let k be algebraically closed, and let I be a zero-dimensional ideal in $k[x_1, \ldots, x_n]$. Then $\dim k[x_1, \ldots, x_n]/I$ is the number of points of $\mathbf{V}(I)$ counted with multiplicity. Explicitly, if $p_1, \ldots, p_m$ are the distinct points of $\mathbf{V}(I)$ and $\mathcal{O}_i$ is the ring of rational functions defined at p_i, then*

$$\dim k[x_1, \ldots, x_n]/I = \textstyle\sum_{i=1}^m \dim \mathcal{O}_i/I\mathcal{O}_i = \textstyle\sum_{i=1}^m m(p_i).$$

Proof. The corollary follows immediately from the theorem by taking dimensions as vector spaces over k. □

A second corollary tells us when a zero-dimensional ideal is radical.

(2.6) Corollary. *Let k be algebraically closed, and let I be a zero-dimensional ideal in $k[x_1, \ldots, x_n]$. Then I is radical if and only if every $p \in \mathbf{V}(I)$ has multiplicity $m(p) = 1$.*

Proof. If $\mathbf{V}(I) = \{p_1, \ldots, p_m\}$, then Theorem (2.10) of Chapter 2 shows that $\dim k[x_1, \ldots, x_n]/I \geq m$, with equality if and only if I is radical. By Corollary (2.5), this inequality can be written $\sum_{i=1}^m m(p_i) \geq m$. Since $m(p_i)$ is always ≥ 1, it follows that $\sum_{i=1}^m m(p_i) \geq m$ is an equality if and only if all $m(p_i) = 1$. □

We next discuss how to compute multiplicities. Given a zero-dimensional ideal $I \subset k[x_1, \ldots, x_n]$ and a polynomial $f \in k[x_1, \ldots, x_n]$, let m_f be multiplication by f on $k[x_1, \ldots, x_n]/I$. Then the characteristic polynomial $\det(m_f - uI)$ is determined by the points in $\mathbf{V}(I)$ *and* their multiplicities. More precisely, we have the following result.

(2.7) Proposition. *Let k be an algebraically closed field and let I be a zero-dimensional ideal in $k[x_1, \ldots, x_n]$. If $f \in k[x_1, \ldots, x_n]$, then*

$$\det(m_f - uI) = (-1)^d \prod_{p \in \mathbf{V}(I)} (u - f(p))^{m(p)},$$

where $d = \dim k[x_1, \ldots, x_n]/I$ and m_f is the map given by multiplication by f on $k[x_1, \ldots, x_n]/I$.

Proof. Let $\mathbf{V}(I) = \{p_1, \ldots, p_m\}$. Using Theorem (2.2), we get a diagram:

$$\begin{tikzcd} k[x_1, \ldots, x_n]/I \arrow[r, phantom, "\cong"] \arrow[d, "m_f"'] & A_1 \times \cdots \times A_m \arrow[d, "m_f"] \\ k[x_1, \ldots, x_n]/I \arrow[r, phantom, "\cong"] & A_1 \times \cdots \times A_m \end{tikzcd}$$

where $m_f : A_1 \times \cdots \times A_m \to A_1 \times \cdots \times A_m$ is multiplication by f on each factor. This diagram commutes in the same sense as the diagram (5.19) of Chapter 3.

Hence we can work with $m_f : A_1 \times \cdots \times A_m \to A_1 \times \cdots \times A_m$. If we restrict to $m_f : A_i \to A_i$, it suffices to show that $\det(m_f - uI) = (-1)^{m(p_i)}(u - f(p_i))^{m(p_i)}$. Equivalently, we must show that $f(p_i)$ is the only eigenvalue of m_f on A_i.

To prove this, consider the map $\varphi_i : k[x_1, \ldots, x_n] \to A_i$ defined in the proof of Theorem (2.2), and let $Q_i = \ker(\varphi_i)$. In Exercise 11 below, you will study the ideal Q_i, which is part of the *primary decomposition* of I. In particular, you will show that $\mathbf{V}(Q_i) = \{p_i\}$ and that $k[x_1, \ldots, x_n]/Q_i \cong A_i$. Consequently, the eigenvalues of m_f on A_i equal the eigenvalues of m_f on $k[x_1, \ldots, x_n]/Q_i$, which by Theorem (4.5) of Chapter 2 are the values of f on $\mathbf{V}(Q_i) = \{p_i\}$. It follows that $f(p_i)$ is the only eigenvalue, as desired. □

The ideas used in the proof of Proposition (2.7) make it easy to determine the *generalized eigenvectors* of m_f. See Exercise 12 below for the details.

If we know the points $p_1, \ldots, p_m$ of $\mathbf{V}(I)$ (for example, we could find them using the methods of Chapters 2 or 3), then it is a simple matter to compute their multiplicities using Proposition (2.7). First pick f so that $f(p_1), \ldots, f(p_m)$ are distinct, and then compute the matrix of m_f relative to a monomial basis of $k[x_1, \ldots, x_n]/I$ as in Chapters 2 or 3. In typical cases, the polynomials generating I have coefficients in $\mathbb{Q}$, which means that the characteristic polynomial $\det(m_f - uI)$ is in $\mathbb{Q}[u]$. Then factor $\det(m_f - uI)$ over $\mathbb{Q}$, which can easily be done by computer (the Maple command is `factor`). This gives

$$\det(m_f - uI) = h_1^{m_1} \cdots h_r^{m_r},$$

where $h_1, \ldots, h_r$ are distinct irreducible polynomials over $\mathbb{Q}$. For each $p_i \in \mathbf{V}(I)$, $f(p_i)$ is a root of a unique h_j, and the corresponding exponent m_j is the multiplicity $m(p_i)$. This follows from Proposition (2.7) and the properties of irreducible polynomials (see Exercise 13). One consequence is that those points of $\mathbf{V}(I)$ corresponding to the same irreducible factor of $\det(m_f - uI)$ all have the same multiplicity.

We can also extend some of the results proved in Chapter 3 about resultants. For example, the techniques used to prove Theorem (2.2) give the following generalization of Proposition (5.8) of Chapter 3 (see Exercise 14 below for the details).

(2.8) Proposition. *Let $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$ (k algebraically closed) have total degrees at most $d_1, \ldots, d_n$ and no solutions at ∞. If $f_0 = u_0 + u_1 x_1 + \cdots + u_n x_n$, where $u_0, \ldots, u_n$ are independent variables, then there is a nonzero constant C such that*

$$\mathrm{Res}_{1,d_1,\ldots,d_n}(f_0, \ldots, f_n) = C \prod_{p \in \mathbf{V}(f_1,\ldots,f_n)} \big(u_0 + u_1 a_1 + \cdots + u_n a_n\big)^{m(p)},$$

where a point $p \in \mathbf{V}(f_1, \ldots, f_n)$ is written $p = (a_1, \ldots, a_n)$.

This tells us that the *u-resultant* of Chapter 3, §5, computes not only the points of $\mathbf{V}(f_1, \ldots, f_n)$ but also their multiplicities. In Chapter 3, we also studied the *hidden variable method*, where we set $x_n = u$ in the equations $f_1 = \cdots = f_n = 0$ and regard u as a constant. After homogenizing with respect to x_0, we get the resultant $\mathrm{Res}_{x_0,\ldots,x_{n-1}}(\widehat{F}_1, \ldots, \widehat{F}_n)$ from Proposition (5.9) in Chapter 3, which tells us about the x_n-coordinates of the solutions. In Chapter 3, we needed to assume that the x_n-coordinates were distinct. Now, using Proposition (2.8), it is easy to show that when $f_1, \ldots, f_n$ have no solutions at ∞,

$$\begin{aligned}\mathrm{Res}_{1,d_1,\ldots,d_n}(u - x_n, f_1, \ldots, f_n) &= \mathrm{Res}_{x_0,\ldots,x_{n-1}}(\widehat{F}_1, \ldots, \widehat{F}_n)\\ &= C \prod_{p \in \mathbf{V}(f_1,\ldots,f_n)} \bigl(u - a_n\bigr)^{m(p)}\end{aligned} \tag{2.9}$$

where $p \in \mathbf{V}(f_1, \ldots, f_n)$ is written $p = (a_1, \ldots, a_n)$. See Exercise 14 for the proof.

The formulas given in (2.9) and Proposition (2.8) indicate a deep relation between multiplicities using resultants. In fact, in the case of two equations in two unknowns, one can use resultants to *define* multiplicities. This is done, for example, in Chapter 8 of [CLO] and Chapter 3 of [Kir].

Exercise 3. Consider the equations

$$\begin{aligned} f_1 &= y^2 - 3 = 0\\ f_2 &= 6y - x^3 + 9x, \end{aligned}$$

and let $I = \langle f_1, f_2 \rangle \subset k[x, y]$.

a. Show that these equations have four solutions with distinct x coordinates.
b. Draw the graphs of $f_1 = 0$ and $f_2 = 0$. Use your picture to explain geometrically why two of the points should have multiplicity > 1.
c. Show that the characteristic polynomial of m_x on $\mathbb{C}[x, y]/I$ is $u^6 - 18u^4 + 81u^2 - 108 = (u^2 - 3)^2(u^2 - 12)$.
d. Use part c and Proposition (2.7) to compute the multiplicities of the four solution points.
e. Explain how you would compute the multiplicities using $\mathrm{Res}(f_1, f_2, y)$ and Proposition (2.8). This is the hidden variable method for computing multiplicities. Also explain the meaning of the exponent 3 in $\mathrm{Res}(f_1, f_2, x) = (y^2 - 3)^3$.

Besides resultants and multiplicities, Theorem (2.2) has other interesting consequences. For instance, suppose that a collection of n polynomials $f_1, \ldots, f_n$ has a *single* zero in k^n, which we may take to be the origin. Let $I = \langle f_1, \ldots, f_n \rangle$. Then the theorem implies

$$k[x_1, \ldots, x_n]/I \cong k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n \rangle}/Ik[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n \rangle}. \tag{2.10}$$

This is very satisfying, but there is more to the story. With the above hypotheses on $f_1, \ldots, f_n$, one can show that most small perturbations of $f_1, \ldots, f_n$ result in a system of equations with distinct zeroes, each of which has multiplicity one, and that the number of such zeroes is precisely equal to the multiplicity of the origin as a solution of $f_1 = \cdots = f_n = 0$. Moreover, the ring $k[x_1, \ldots, x_n]/I$ turns out to be a limit, in a rather precise sense, of the set of functions on these distinct zeroes. Here is a simple example.

Exercise 4. Let $k = \mathbb{C}$ so that we can take limits in an elementary sense. Consider the ideals $I_t = \langle y - x^2, x^3 - t\rangle$ where $t \in \mathbb{C}$ is a parameter.

a. What are the points in $\mathbf{V}(I_t)$ for $t \neq 0$? Show that each point has multiplicity 1, so $A_i \cong k$ for each i.
b. Now let $t \to 0$. What is $\mathbf{V}(I_0)$ and its multiplicity?
c. Using the proof of Theorem (2.2), work out an explicit isomorphism between $\mathbb{C}[x, y]/I_t$, and the product of the A_i for $t \neq 0$.
d. What happens as $t \to 0$? Identify the image of a general f in $\mathbb{C}[x, y]/I_0$, and relate to the image of f in the product of A_i for $t \neq 0$.

Local rings give us the ability to discuss what's happening near a particular solution of a zero-dimensional ideal. This leads to some rich mathematics, including the following.

- As explained in Exercise 11, the isomorphism $A \cong A_1 \times \cdots \times A_m$ of Theorem (2.2) is related to primary decomposition. A method for computing this decomposition using the characteristic polynomial of a multiplication map is discussed in [Mon] and [YNT].
- The local ring A_i can be described in terms of the vanishing of certain linear combinations of partial derivatives. This is explained in [MMM1], [MMM2], [Möl], and [MöS], among others.
- When the number of equations equals the number of unknowns as in Chapter 3, the ring A is a *complete intersection*. Some of the very deep algebra related to this situation, including *Gorenstein duality*, is discussed in [ElM2].

The book [Stu5] gives a nice introduction to the first two bullets. The reader should also consult [YNT] for many other aspects of the ring A and [Rou] for an interesting method of representing the solutions and their multiplicities.

We also remark that we can compute multiplicities by passing to the formal power series ring or, in the cases $k = \mathbb{R}$ or $\mathbb{C}$, to the ring of convergent power series. More precisely, the following holds.

(2.11) Proposition. *Let $I \subset k[x_1,\ldots,x_n]$ be a zero-dimensional ideal such that the origin is a point of $\mathbf{V}(I)$ of multiplicity m. Then*

$$\begin{aligned} m &= \dim k[x_1,\ldots,x_n]_{\langle x_1,\ldots,x_n\rangle}/Ik[x_1,\ldots,x_n]_{\langle x_1,\ldots,x_n\rangle} \\ &= \dim k[[x_1,\ldots,x_n]]/Ik[[x_1,\ldots,x_n]]. \end{aligned}$$

If, moreover, $k = \mathbb{R}$ or $\mathbb{C}$, so that we can talk about whether a power series converges, then

$$m = \dim k\{x_1,\ldots,x_n\}/Ik\{x_1,\ldots,x_n\}$$

as well.

To see the idea behind why this is so, consider the example we looked at in Exercise 1 above. We showed that $\dim k[x,y]_{\langle x,y\rangle}/\langle x^2+x^3,y^2\rangle = 4$ by noting that in $k[x,y]_{\langle x,y\rangle}$, we have

$$\langle x^2+x^3,y^2\rangle = \langle x^2,y^2\rangle$$

because $1/(1+x) \in k[x,y]_{\langle x,y\rangle}$. As in §1, we can represent $1/(1+x)$ as the formal power series $1 - x + x^2 - x^3 + x^4 - \cdots \in k[[x,y]]$ and then

$$(x^2+x^3)(1 - x + x^2 - x^3 + x^4 - \cdots) = x^2$$

in $k[[x,y]]$. This shows that, in $k[[x,y]]$, $\langle x^2+x^3,y^2\rangle = \langle x^2,y^2\rangle$. It follows that

$$\dim k[[x,y]]/\langle x^2,y^2\rangle = 4$$

(as before, the four monomials $1, x, y, xy$ form a vector space basis of $k[[x,y]]/\langle x^2,y^2\rangle$). If $k = \mathbb{C}$, the power series $1 - x + x^2 - x^3 + x^4 - \cdots$ is convergent for x with $|x| < 1$, and precisely the same reasoning shows that $\langle x^2+x^3,y^2\rangle = \langle x^2,y^2\rangle$ in $k\{x,y\}$ as well. Therefore,

$$\dim k\{x,y\}/\langle x^2,y^2\rangle k\{x,y\} = 4.$$

It is possible to prove the proposition by generalizing these observations, but it will be more convenient to defer it to §5, so that we can make use of some additional computational tools for local rings.

We will conclude this section by introducing an important invariant in singularity theory—the *Milnor number* of a singularity. See [Mil] for the topological meaning of this integer. One says that an analytic function $f(x_1,\ldots,x_n)$ on an open set $U \subset \mathbb{C}^n$ has a *singularity* at a point $p \in U$ if the n first-order partial derivatives of f have a common zero at p. We say that the singular point p is *isolated* if there is some neighborhood of p containing no other singular points of f. As usual, when considering a given singular point p, one translates p to the origin. If we do this, then the assertion that the origin is isolated is enough to guarantee that

$$\dim \mathbb{C}\{x_1,\ldots,x_n\}/\langle \partial f/\partial x_1,\ldots,\partial f/\partial x_n\rangle < \infty.$$

Here, we are using the fact that in a neighborhood of the origin, any analytic function can be represented by a convergent power series. Thus f and its partial derivatives can be regarded as elements of $\mathbb{C}\{x_1, \ldots, x_n\}$.

(2.12) Definition. Let $f \in \mathbb{C}\{x_1, \ldots, x_n\}$ have an isolated singularity at the origin. The *Milnor number* of the singular point, denoted μ, is given by

$$\mu = \dim \mathbb{C}\{x_1, \ldots, x_n\}/\langle \partial f/\partial x_1, \ldots, \partial f/\partial x_n \rangle.$$

In view of Proposition (2.11), if the function f is a polynomial, the Milnor number of a singular point p of f is just the multiplicity of the common zero p of the partials of f.

Exercise 5. Each of the following $f(x, y) \in \mathbb{C}[x, y]$ has an isolated singular point at $(0, 0)$. For each, determine the Milnor number by computing

$$\mu = \dim \mathbb{C}[[x, y]]/\langle \partial f/\partial x, \partial f/\partial y \rangle.$$

a. $f(x, y) = y^2 - x^2 - x^3$.
b. $f(x, y) = y^2 - x^3$.
c. $f(x, y) = y^2 - x^5$.

In intuitive terms, the larger the Milnor number is, the more complicated the structure of the singular point is. To conclude this section, we mention that there is a closely related invariant of singularities called the Tjurina number, which is defined by

$$\tau = \dim k[[x_1, \ldots, x_n]]/\langle f, \partial f/\partial x_1, \ldots, \partial f/\partial x_n \rangle.$$

Over any field k, the Tjurina number is finite precisely when f has an isolated singular point.

Additional Exercises for §2

Exercise 6. If $p \in \mathbf{V}(I)$ and $M = \mathbf{I}(\{p\})$ is the maximal ideal of p, then prove that $k[x_1, \ldots, x_n]_M/Ik[x_1, \ldots, x_n]_M$ is a local ring. Also show that the dimension of this ring, which is the multiplicity $m(p)$, is ≥ 1. Hint: Show that the map $k[x_1, \ldots, x_n]_M/Ik[x_1, \ldots, x_n]_M \to k$ given by evaluating a coset at p is a well-defined linear map which is onto.

Exercise 7. Using the Nullstellensatz, prove part a of Lemma (2.3).

Exercise 8. Let I and J be any two ideals in a ring R such that $I + J = R$ (we sometimes say I and J are *comaximal*).
a. Show that $IJ = I \cap J$.

b. From part a, deduce that if $d \geq 1$, then $I^d \cap J^d = (I \cap J)^d$.
c. Generalize part b to any number of ideals $I_1, \ldots, I_r$ if $I_i + I_j = R$ whenever $i \neq j$.

Exercise 9. Show that if e_i are the polynomials constructed in (2.4) for part b of Lemma (2.3), then $e_i^2 \equiv e_i \bmod I$. Hint: Use the other two statements in part b.

Exercise 10. In this exercise, we will use Theorem (2.2) to give a new proof of Theorem (4.5) of Chapter 2. Let A_i be the local ring $\mathcal{O}_i/I\mathcal{O}_i$ as in the proof of Theorem (2.2). For $f \in k[x_1, \ldots, x_n]$, let $m_f : A_i \to A_i$ be multiplication by f. Also, the coset of f in A_i will be denoted $[f]_i$.
a. Prove that m_f is a vector space isomorphism if and only if $[f]_i \in A_i$ is invertible; i.e., there is $[g]_i \in A_i$ such that $[f]_i[g]_i = [1]_i$.
b. Explain why $[f]_i$ is in the maximal ideal of A_i if and only if $f(p_i) = 0$.
c. Explain why each of the following equivalences is true for a polynomial $f \in k[x_1, \ldots, x_n]$ and $\lambda \in \mathbb{C}$: λ is an eigenvalue of $m_f \Leftrightarrow m_{f-\lambda}$ is not invertible $\Leftrightarrow [f - \lambda]_i \in A_i$ is not invertible $\Leftrightarrow [f - \lambda]_i$ is in the maximal ideal of $A_i \Leftrightarrow f(p) = \lambda$. Hint: Use parts a and b of this exercise and part b of Exercise 1 from §1.
d. Combine part c with the isomorphism $k[x_1, \ldots, x_n]/I \cong A_1 \times \cdots \times A_m$ and the commutative diagram from Proposition (2.7) to give a new proof of Theorem (4.5) of Chapter 2.

Exercise 11. (Primary Decomposition) Let I be a zero-dimensional ideal with $\mathbf{V}(I) = \{p_1, \ldots, p_m\}$. This exercise will explore the relation between the isomorphism $A = k[x_1, \ldots, x_n]/I \cong A_1 \times \cdots \times A_m$ and the *primary decomposition* of I. More details on primary decomposition can be found in [CLO], Chapter 4, §7. We begin with the homomorphism $\varphi_i : k[x_1, \ldots, x_n] \to A_i$ defined by $\varphi(f) = [f]_i \in A_i$ (this is the notation used in the proof of Theorem (2.2)). Consider the ideal Q_i defined by

$$Q_i = \ker(\varphi_i) = \{f \in k[x_1, \ldots, x_n] : [f]_i = [0]_i \text{ in } A_i\}.$$

We will show that the ideals $Q_1, \ldots, Q_m$ give the primary decomposition of I. Let $M_i = \mathbf{I}(\{p_i\})$.
a. Show that $I \subset Q_i$ and that $Q_i = \{f \in k[x_1, \ldots, x_n] :$ there exists u in $k[x_1, \ldots, x_n] \setminus M_i$ such that $u \cdot f \in I\}$.
b. If $g_1, \ldots, g_m$ are as in the proof of Theorem (2.2), show that for $j \neq i$, some power of g_j lies in Q_i. Hint: Use part a and the Nullstellensatz.
c. Show that $\mathbf{V}(Q_i) = \{p_i\}$ and conclude that $\sqrt{Q_i} = M_i$. Hint: Use part b and the Nullstellensatz.
d. Show that Q_i is a *primary ideal*, which means that if $fg \in Q_i$, then either $f \in Q_i$ or some power of g is in Q_i. Hint: Use part c. Also, A_i is a local ring.

e. Prove that $I = Q_1 \cap \cdots \cap Q_m$. This is the primary decomposition of I (see Theorem 7 of [CLO], Chapter 4, §7).
f. Show that $k[x_1, \ldots, x_n]/Q_i \cong A_i$. Hint: Show that φ_i is onto using the proof of Theorem (2.2).

Exercise 12. (Generalized Eigenspaces) Given a linear map $T : V \to V$, where V is a finite-dimensional vector space, a *generalized eigenvector of* $\lambda \in k$ is a nonzero vector $v \in V$ such that $(T - \lambda I)^m(v) = 0$ for some $m \geq 1$. The *generalized eigenspace of* λ is the space of the generalized eigenvectors for λ. When k is algebraically closed, V is the direct sum of its generalized eigenspaces (see Section 7.1 of [FIS]). We will apply this theory to the linear map $m_f : A \to A$ to see how the generalized eigenspaces of m_f relate to the isomorphism $A \cong A_1 \times \cdots \times A_m$ of Theorem (2.2).
a. In the proof of Proposition (2.7), we proved that $f(p_i)$ is the only eigenvalue of $m_f : A_i \to A_i$. Use this to show that the generalized eigenspace of m_f is all of A_i.
b. If $f(p_1), \ldots, f(p_m)$ are distinct, prove that the decomposition of $A = k[x_1, \ldots, x_n]/I$ into a direct sum of generalized eigenspaces for m_f is *precisely* the isomorphism $A \cong A_1 \times \cdots \times A_m$ of Theorem (2.2).

Exercise 13.
a. If $h \in \mathbb{Q}[u]$ is irreducible, prove that all roots of h have multiplicity one. Hint: Compute h_{red}.
b. Let $h \in \mathbb{Q}[u]$ be irreducible and let $\lambda \in \mathbb{C}$ be a root of h. If $g \in \mathbb{Q}[u]$ and $g(\lambda) = 0$, prove that h divides g. Hint: If $\mathrm{GCD}(h, g) = 1$, there are polynomials $A, B \in \mathbb{Q}[u]$ such that $Ah + Bg = 1$.
c. If h_1 and h_2 are distinct irreducible polynomials in $\mathbb{Q}[u]$, prove that h_1 and h_2 have no common roots.
d. Use parts a and c to justify the method for computing multiplicities given in the discussion following Proposition (2.7).

Exercise 14. Prove Proposition (2.8) and the formulas given in (2.9). Hint: Use Exercise 12 and Proposition (5.8) of Chapter 3.

Exercise 15.
a. Let $\ell_1, \ldots, \ell_n$ be homogeneous linear polynomials in $k[x_1, \ldots, x_n]$ with $\mathbf{V}(\ell_1, \ldots, \ell_n) = \{(0, \ldots, 0)\}$. Compute the multiplicity of the origin as a solution of $\ell_1 = \cdots = \ell_n = 0$.
b. Now let $f_1, \ldots, f_n$ generate a zero-dimensional ideal in $k[x_1, \ldots, x_n]$, and suppose that the origin is in $\mathbf{V}(f_1, \ldots, f_n)$ and the Jacobian matrix

$$J = \big(\partial f_i/\partial x_j\big)$$

has nonzero determinant at the origin. Compute the multiplicity of the origin as a solution of $f_1 = \cdots = f_n = 0$. Hint: Use part a.

Exercise 16. We say $f \in \mathbb{C}[x_1, \ldots, x_n]$ has an *ordinary double point* at the origin 0 in $\mathbb{C}^n$ if $f(0) = \partial f/\partial x_i(0) = 0$ for all i, but the matrix of second-order partial derivatives is invertible at 0:

$$\det(\partial^2 f/\partial x_i \partial x_j)\big|_{(x_1,\ldots,x_n)=(0,\ldots,0)} \neq 0.$$

Find the Milnor number of an ordinary double point. Hint: Use Exercise 15.

Exercise 17. Let I be a zero-dimensional ideal in $k[x_1, \ldots, x_n]$ and let $p = (a_1, \ldots, a_n) \in \mathbf{V}(I)$. Let $X_1, \ldots, X_n$ be a new set of variables, and consider the set $\overline{I} \subset k[X_1, \ldots, X_n]$ consisting of all $f(X_1 + a_1, \ldots, X_n + a_n)$ where $f \in I$.

a. Show that $\overline{I}$ is an ideal in $k[X_1, \ldots, X_n]$, and that the origin is a point in $\mathbf{V}(\overline{I})$.

b. Show that the multiplicity of p as a point in $\mathbf{V}(I)$ is the same as the multiplicity of the origin as a point in $\mathbf{V}(\overline{I})$. Hint: One approach is to show that

$$\begin{aligned} \varphi : k[x_1, \ldots, x_n] &\to k[X_1, \ldots, X_n] \\ f(x_1, \ldots, x_n) &\mapsto f(X_1 + a_1, \ldots, X_n + a_n) \end{aligned}$$

defines an isomorphism of rings.

§3 Term Orders and Division in Local Rings

When working with an ideal $I \subset k[x_1, \ldots, x_n]$, for some purposes we can replace I with its ideal of leading terms $\langle \textsc{lt}(I) \rangle$. For example, if I is zero-dimensional, we can compute the dimension of the quotient ring $k[x_1, \ldots, x_n]/I$ by using the fact that $\dim k[x_1, \ldots, x_n]/I = \dim k[x_1, \ldots, x_n]/\langle \textsc{lt}(I) \rangle$. The latter dimension is easy to compute since $\langle \textsc{lt}(I) \rangle$ is a *monomial* ideal—the dimension is just the number of monomials not in the ideal). The heart of the matter is to compute $\langle \textsc{lt}(I) \rangle$, which is done by computing a Gröbner basis of I.

A natural question to ask is whether something similar might work in a local ring. An instructive example occurred in the last section, where we considered the ideal $I = \langle x^2 + x^3, y^2 \rangle$. For $R = k[x, y]_{\langle x,y \rangle}$ or $k[[x, y]]$ or $k\{x, y\}$, we computed $\dim R/IR$ by replacing I by the monomial ideal

$$\tilde{I} = \langle x^2, y^2 \rangle.$$

Note that $\tilde{I}$ is generated by the *lowest degree terms* in the generators of I. This is in contrast to the situation in the polynomial ring, where $\dim k[x, y]/I$ was computed from $\langle \textsc{lt}(I) \rangle = \langle x^3, y^2 \rangle$ using the *lex leading terms*.

To be able to pick out terms of lowest degree in polynomials as leading terms, it will be necessary to extend the class of orders on monomials we can use. For instance, to make the leading term of a polynomial or a power series be one of the terms of minimal total degree, we could consider what are known as *degree-anticompatible* (or anti-graded) orders. By definition these are orders that satisfy

$$(3.1) \qquad |\alpha| < |\beta| \Longrightarrow x^\alpha > x^\beta.$$

We still insist that our orders be total orderings and be compatible with multiplication. As in Definition (2.1) of Chapter 1, being a total ordering means that for any $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, exactly one of the following is true:

$$x^\alpha > x^\beta, \quad x^\alpha = x^\beta, \text{ or } x^\alpha < x^\beta.$$

Compatibility with multiplication means that for any $\gamma \in \mathbb{Z}^n_{\geq 0}$, if $x^\alpha > x^\beta$, then $x^{\alpha+\gamma} > x^{\beta+\gamma}$. Notice that property (3.1) implies that $1 > x_i$ for all i, $1 \leq i \leq n$. Here is a first example.

Exercise 1. Consider terms in $k[x]$.
a. Show that the only degree-anticompatible order is the antidegree order:

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

b. Explain why the antidegree order is not a well-ordering.

Any total ordering that is compatible with multiplication and that satisfies $1 > x_i$ for all i, $1 \leq i \leq n$ is called a *local order*. A degree-anticompatible order is a local order (but not conversely—see Exercise 2 below).

Perhaps the simplest example of a local order in n variables is degree-anticompatible lexicographic order, abbreviated *alex*, which first sorts by total degree, lower degree terms preceding higher degree terms, and which sorts monomials of the same total degree lexicographically.

(3.2) Definition (Antigraded Lex Order). Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $x^\alpha >_{alex} x^\beta$ if

$$|\alpha| = \sum_{i=1}^n \alpha_i < |\beta| = \sum_{i=1}^n \beta_i,$$

or if

$$|\alpha| = |\beta| \text{ and } x^\alpha >_{lex} x^\beta.$$

Thus, for example, in $k[x, y]$, with $x > y$, we have

$$1 >_{alex} x >_{alex} y >_{alex} x^2 >_{alex} xy >_{alex} y^2 >_{alex} x^3 >_{alex} \cdots.$$

Similarly one defines degree-anticompatible reverse lexicographic, or *arevlex*, order as follows.

(3.3) Definition (Antigraded Revlex Order). Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $x^\alpha >_{arevlex} x^\beta$ if

$$|\alpha| < |\beta|, \text{ or } |\alpha| = |\beta| \text{ and } x^\alpha >_{revlex} x^\beta.$$

So, for example, we have

$$\begin{aligned} &1 >_{arevlex} x >_{arevlex} y >_{arevlex} z >_{arevlex} x^2 >_{arevlex} \\ &xy >_{arevlex} y^2 >_{arevlex} xz >_{arevlex} yz >_{arevlex} z^2 >_{arevlex} \cdots . \end{aligned}$$

Degree-anticompatible and local orders lack one of the key properties of the monomial orders that we have used up to this point. Namely, the third property in Definition (2.1) from Chapter 1, which requires that a monomial order be a *well-ordering* relation, does not hold. Local orders are not well-orderings. This can be seen even in the one-variable case in Exercise 1 above.

In §4 of this chapter, we will need to make use of even more general orders than degree-anticompatible or local orders. Moreover, and somewhat surprisingly, the whole theory can be simplified somewhat by generalizing at once to consider the whole class of *semigroup orders* as in the following definition.

(3.4) Definition. An order $>$ on $\mathbb{Z}^n_{\geq 0}$ or, equivalently, on the set of monomials $x^\alpha, \alpha \in \mathbb{Z}^n_{\geq 0}$ in $k[x_1, \ldots, x_n]$ or any of the local rings $k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle}$, $k\{x_1, \ldots, x_n\}$, or $k[[x_1, \ldots, x_n]]$, is said to be a *semigroup order* if it satisfies:
a. $>$ is a total ordering on $\mathbb{Z}^n_{\geq 0}$;
b. $>$ is compatible with multiplication of monomials.

Semigroup orders include the monomial orders, which have the additional well-ordering property, as well as local orders and other orders which do not. Since the property of being a well-ordering is often used to assert that algorithms terminate, we will need to be especially careful in checking that procedures using semigroup orders terminate.

Recall that in §2 of Chapter 1 we discussed how monomial orders can be specified by matrices. If M is an $m \times n$ real matrix with rows $\mathbf{w}_1, \ldots, \mathbf{w}_m$, then we define $x^\alpha >_M x^\beta$ if there is an $\ell \leq m$ such that $\alpha \cdot \mathbf{w}_i = \beta \cdot \mathbf{w}_i$ for $i = 1, \ldots, \ell - 1$, but $\alpha \cdot \mathbf{w}_\ell > \beta \cdot \mathbf{w}_\ell$. Every semigroup order can be described by giving a suitable matrix M. The following exercise describes the necessary properties of M and gives some examples.

Exercise 2.
a. Show that $>_M$ is compatible with multiplication for every matrix M as above.
b. Show that $>_M$ is a total ordering if and only if $\ker(M) \cap \mathbb{Z}^n_{\geq 0} = \{(0, \ldots, 0)\}$.

c. Show that the *lex* monomial order with $x_1 > x_2 > \cdots > x_n$ is the order $>_I$, where I is the $n \times n$ identity matrix.

d. Show that the *alex* order is the order $>_M$ defined by the matrix

$$M = \begin{pmatrix} -1 & -1 & \cdots & -1 \\ 0 & -1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 \end{pmatrix}.$$

e. Show that the *arevlex* order is the order $>_M$ for

$$M = \begin{pmatrix} -1 & -1 & \cdots & -1 & -1 \\ 0 & 0 & \cdots & 0 & -1 \\ 0 & 0 & \cdots & -1 & 0 \\ \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & -1 & \cdots & 0 & 0 \end{pmatrix}.$$

f. Find a local order that is not degree-anticompatible. Hint: What is it about the corresponding matrices that makes *alex* and *arevlex* degree-anticompatible, resp. local?

If $f = \sum_\alpha c_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ is a polynomial and $>$ is a semigroup order, we define the multidegree, the leading coefficient, the leading monomial, and the leading term of f exactly as we did for a monomial order:

$$\begin{aligned} \text{multideg}(f) &= \max\{\alpha \in \mathbb{Z}^n_{\geq 0} : c_\alpha \neq 0\} \\ \text{LC}(f) &= c_{\text{multideg}(f)} \\ \text{LM}(f) &= x^{\text{multideg}(f)} \\ \text{LT}(f) &= \text{LC}(f) \cdot \text{LM}(f). \end{aligned}$$

In addition, each semigroup order $>$ defines a particular ring of fractions in $k(x_1, \ldots, x_n)$ as in Exercise 9 of §1 of this chapter. Namely, given $>$, we consider the set

$$S = \{1 + g \in k[x_1, \ldots, x_n] : g = 0, \text{ or } \text{LT}_>(g) < 1\}.$$

S is closed under multiplication since if $\text{LT}_>(g) < 1$ and $\text{LT}_>(g') < 1$, then $(1+g)(1+g') = 1 + g + g' + gg'$, and $\text{LT}(g + g' + gg') < 1$ as well by the definition of a semigroup order.

(3.5) Definition. Let $>$ be a semigroup order on monomials in the ring $k[x_1, \ldots, x_n]$ and let $S = \{1 + g : \text{LT}(g) < 1\}$. The *localization* of $k[x_1, \ldots, x_n]$ with respect to $>$ is the ring

$$\text{Loc}_>(k[x_1, \ldots, x_n]) = S^{-1}k[x_1, \ldots, x_n] = \{f/(1+g) : 1 + g \in S\}.$$

For example, if $>$ is a monomial order, then there are no nonzero monomials smaller than 1 so $S = \{1\}$ and $\mathrm{Loc}_>(k[x_1,\ldots,x_n]) = k[x_1,\ldots,x_n]$. On the other hand, if $>$ is a local order, then since $1 > x_i$ for all i,

$$\{g : g = 0, \text{ or } \mathrm{LT}_>(g) < 1\} = \langle x_1,\ldots,x_n\rangle.$$

Hence, for a local order, we have that S is contained in the set of units in $k[x_1,\ldots,x_n]_{\langle x_1,\ldots,x_n\rangle}$ so $\mathrm{Loc}_>(k[x_1,\ldots,x_n]) \subset k[x_1,\ldots,x_n]_{\langle x_1,\ldots,x_n\rangle}$. But in fact, by adjusting constants between the numerator and the denominator in a general $f/h \in k[x_1,\ldots,x_n]_{\langle x_1,\ldots,x_n\rangle}$, it is easy to see that $f/h = f'/(1+g)$ for some $1+g \in S$. Hence if $>$ is a local order, then

$$\mathrm{Loc}_>(k[x_1,\ldots,x_n]) = k[x_1,\ldots,x_n]_{\langle x_1,\ldots,x_n\rangle}.$$

The next two exercises give some additional, more general, and also quite suggestive examples of semigroup orders and their associated rings of fractions.

Exercise 3. Using $>_{alex}$ on the x-terms, and $>_{lex}$ on the y-terms, define a *mixed order* $>_{mixed}$ by $x^\alpha y^\beta >_{mixed} x^{\alpha'} y^{\beta'}$ if either $y^\beta >_{lex} y^{\beta'}$, or $y^\beta = y^{\beta'}$ and $x^\alpha >_{alex} x^{\alpha'}$.

a. Show that $>_{mixed}$ is a semigroup order and find a matrix M such that $>_{mixed} = >_M$.

b. Show that $>_{mixed}$ is *neither* a well-ordering, *nor* degree-anticompatible.

c. Let $g \in k[x_1,\ldots,x_n,y_1,\ldots,y_m]$. Show that $1 >_{mixed} \mathrm{LT}_{>_{mixed}}(g)$ if and only if g depends only on $x_1,\ldots,x_n$, and is in $\langle x_1,\ldots,x_n\rangle \subset k[x_1,\ldots,x_n]$.

d. Let $R = k[x_1,\ldots,x_n,y_1,\ldots,y_m]$. Deduce that $\mathrm{Loc}_{>_{mixed}}(R)$ is the ring $k[x_1,\ldots,x_n]_{\langle x_1,\ldots,x_n\rangle}[y_1,\ldots,y_m]$, whose elements can be written as polynomials in the y_j, with coefficients that are rational functions of the x_i in $k[x_1,\ldots,x_n]_{\langle x_1,\ldots,x_n\rangle}$.

Exercise 4. If we proceed as in Exercise 3 but compare the x-terms first, we get a new order defined by $>_{mixed'}$ by $x^\alpha y^\beta >_{mixed'} x^{\alpha'} y^{\beta'}$ if either $x^\alpha >_{alex} x^{\alpha'}$, or $x^\alpha = x^{\alpha'}$ and $y^\beta >_{lex} y^{\beta'}$.

a. Show that $>_{mixed'}$ is a semigroup order and find a matrix U such that $>_{mixed'} = >_U$.

b. Show that $>_{mixed'}$ is *neither* a well-ordering, *nor* degree-anticompatible.

c. Which elements $f \in k[x_1,\ldots,x_n,y_1,\ldots,y_n]$ satisfy $1 >_{mixed'} \mathrm{LT}_{>_{mixed'}}(f)$?

d. What is $\mathrm{Loc}_{>_{mixed'}}(k[x_1,\ldots,x_n,y_1,\ldots,y_m])$?

Note that the order $>_{mixed}$ from Exercise 3 has the following *elimination property*: if $x^\alpha >_{mixed} x^{\alpha'} y^{\beta'}$, then $\beta' = 0$. Equivalently, any monomial containing one of the y_j is greater than all monomials containing only the x_i. It follows that if the $>_{mixed}$ leading term of a polynomial depends only on the x_i, then the polynomial does not depend on any of the y_j.

We will return to this comment in §4 after developing analogs of the division algorithm and Gröbner bases for general term orders, because this is precisely the property we need for elimination theory.

Given any semigroup order $>$ on monomials in $k[x_1, \ldots, x_n]$, there is a natural extension of $>$ to $\mathrm{Loc}_>(k[x_1, \ldots, x_n])$, which we will also denote by $>$. Namely, if $1 + g \in S$ as in Definition (3.5), the rational function $1/(1+g)$ is a unit in $\mathrm{Loc}_>(k[x_1, \ldots, x_n])$, so it shouldn't matter in defining the leading term of $f/(1+g)$. For any $h \in \mathrm{Loc}_>(k[x_1, \ldots, x_n])$, we write $h = f/(1+g)$ and define

$$\begin{aligned} \mathrm{multideg}(h) &= \mathrm{multideg}(f) \\ \textsc{lc}(h) &= \textsc{lc}(f) \\ \textsc{lm}(h) &= \textsc{lm}(f) \\ \textsc{lt}(h) &= \textsc{lt}(f). \end{aligned}$$

Exercise 5. Write $A = k[x_1, \ldots, x_n]$ and let $h \in A$.

a. Show that $\mathrm{multideg}(h)$, $\textsc{lc}(h)$, $\textsc{lm}(h)$, $\textsc{lt}(h)$ are well-defined in $\mathrm{Loc}_>(A)$ in the sense that if $h = f/(1+g) = f'/(1+g')$, then $\mathrm{multideg}(h)$, $\textsc{lc}(h)$, $\textsc{lm}(h)$, $\textsc{lt}(h)$ will be the same whether f or f' is used to compute them.
b. Let $r \in R$ be defined by the equation

$$h = \textsc{lt}(h) + r.$$

Show that either $r = 0$ or $\textsc{lt}(r) < \textsc{lt}(h)$.

In Exercise 8, you will show that if $>$ is a local order, then every nonempty subset has a maximal element. This allows us to define $\mathrm{multideg}(h)$, $\textsc{lc}(h)$, $\textsc{lm}(h)$, $\textsc{lt}(h)$ when $h \in k[[x_1, \ldots, x_n]]$ (or $h \in k\{x_1, \ldots, x_n\}$ if $k = \mathbb{R}$ or $\mathbb{C}$). Moreover, in this case, the multidegree and leading term of $h = f/(1+g) \in k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n\rangle}$ agree with what one obtains upon viewing h as a power series (via the series expansion of $1/(1+g)$).

The goal of this section is to use general semigroup orders to develop an extension of the division algorithm in $k[x_1, \ldots, x_n]$ which will yield information about ideals in $R = \mathrm{Loc}_>(k[x_1, \ldots, x_n])$. The key step in the division algorithm for polynomials is the reduction of a polynomial f by a polynomial g. If $\textsc{lt}(f) = m \cdot \textsc{lt}(g)$, for some term $m = cx^\alpha$, we define

$$\mathrm{Red}\,(f, g) = f - m\,g,$$

and say that we have *reduced* f *by* g. The polynomial $\mathrm{Red}\,(f, g)$ is just what is left after the first step in dividing f by g—it is the first partial dividend. In general, the division algorithm divides a polynomial by a set of other polynomials by repeatedly reducing the polynomial by members of the set and adding leading terms to the remainder when no reductions are possible. This terminates in the case of polynomials because successive leading terms form a strictly decreasing sequence, and such sequences always terminate because a monomial order is always a well-ordering.

In the case of a local order on a power series ring, one can define $\mathrm{Red}\,(f, g)$ exactly as above. However, a sequence of successive reductions need no longer terminate. For example, suppose $f = x$ and we decide to divide f by $g = x - x^2$, so that we successively reduce by $x - x^2$. This gives the reductions:

$$\begin{aligned} f_1 &= \mathrm{Red}\,(f, g) = x^2 \\ f_2 &= \mathrm{Red}\,(f_1, g) = x^3 \\ &\vdots \\ f_n &= \mathrm{Red}\,(f_{n-1}, g) = x^{n+1}, \end{aligned}$$

and so on, which clearly does not terminate. The difficulty, of course, is that under the antidegree order in $k[x]_{\langle x\rangle}$ or $k[[x]]$, we have the infinite strictly decreasing sequence of terms $x > x^2 > x^3 > \cdots$.

We can evade this difficulty with a splendid idea of Mora's. When dividing f_i by g, for instance, we allow ourselves to reduce not just by g, but also *by the result of any previous reduction.* That is, we allow reductions by f itself (which we can regard as the "zeroth" reduction), or by any of $f_1, \ldots, f_{i-1}$. More generally, when dividing a set of polynomials or power series, we allow ourselves to reduce by the original set together with the results of any previous reduction. So, in our example, where we are dividing $f = x$ by $g = x - x^2$, the first reduction is $f_1 = \mathrm{Red}\,(f, g) = x^2$. For the next reduction, we allow ourselves to reduce f_1 by f as well as g. One checks that

$$\mathrm{Red}\,(f_1, f) = \mathrm{Red}\,(x^2, x) = 0,$$

so that we halt. Moreover, this reduction being zero implies $x^2 = xf$. If we combine this with the equation $f = 1 \cdot g + x^2$ which gives $f_1 = \mathrm{Red}\,(f, g) = x^2$, we obtain the relation $f = g + xf$, or $(1 - x)f = g$. This last equation tells us that in $k[x]_{\langle x\rangle}$, we have

$$f = \frac{1}{1 - x}\, g.$$

In other words, the remainder on division of f by g is zero since x and $x - x^2 = x(1 - x)$ generate the same ideal in $k[x]_{\langle x\rangle}$ or $k[[x]]$.

Looking at the above example, one might ask whether it would always suffice to first reduce by g, then subsequently reduce by f. Sadly, this is not the case: it is easy to construct examples where the sequence of reductions does not terminate. Suppose, for example, that we wish to divide $f = x + x^2$ by $g = x + x^3 + x^5$.

Exercise 6. Show that in this case too, f and g generate the same ideal in $k[[x]]$ or $k[x]_{\langle x\rangle}$.

Reducing f by g and then subsequently reducing the results by $f_0 = f$ gives the sequence

$$\begin{aligned} f_1 &= \operatorname{Red}(f, g) = x^2 - x^3 - x^5 \\ f_2 &= \operatorname{Red}(f_1, f) = -2x^3 - x^5 \end{aligned}$$

$$\begin{aligned} f_3 &= \operatorname{Red}(f_2, f) = 2x^4 - x^5 \\ f_4 &= \operatorname{Red}(f_3, f) = -3x^5 \\ f_5 &= \operatorname{Red}(f_4, f) = 3x^6 \\ f_6 &= \operatorname{Red}(f_5, f) = -3x^7, \end{aligned}$$

and so on, which again clearly does not terminate. However, we get something which does terminate by reducing f_5 by f_4:

$$\begin{aligned} f_5 &= \operatorname{Red}(f_4, f) = 3x^6 \\ \tilde{f}_6 &= \operatorname{Red}(f_5, f_4) = 0. \end{aligned}$$

From this, we can easily give an expression for f:

$$f = 1 \cdot g + (x - 2x^2 + 2x^3 - 3x^4) \cdot f + f_5.$$

However, we also have

$$f_5 = 3x^6 = 3x^5 \cdot x = 3x^5 \cdot \frac{x + x^2}{1 + x} = \frac{3x^5}{1 + x} f.$$

Backsubstituting this into the previous equation for f and multiplying by $1 + x$, we obtain

$$(1 + x)f = (1 + x)g + (1 + x)(x - 2x^2 + 2x^3 - 3x^4)f + 3x^5 f.$$

Then moving xf to the right-hand side gives an equation of the form

$$f = (\text{unit}) \cdot g + (\text{polynomial vanishing at } 0) \cdot f.$$

This, of course, is what we want according to Exercise 6; upon transposing and solving for f, we have $f = (\text{unit}) \cdot g$.

Our presentation will now follow the recent book [GrP], which describes the algorithms underlying the latest version of the computer algebra system `Singular`. We will introduce this system in the next section. Since we deal with orders that are not well-orderings, the difficult part is to give a division process that is guaranteed to terminate. The algorithm and termination proof from [GrP] use a clever synthesis of ideas due to Lazard and Mora, but the proof is (rather amazingly) both simpler and more general than Mora's original one. Using reductions by results of previous reductions as above, Mora developed a division process for polynomials based on a *local* order. His proof used a notion called the *écart* of a polynomial, a measurement of the failure of the polynomial to be homogeneous, and the strategy in the division process was to perform reductions that decrease the écart. This is described, for instance, in [MPT]. Also see Exercise 11 below for the basics of this approach. Lazard had shown how to do the same sort of division by homogenizing the polynomials and using an appropriate monomial order defined using the local order. In implementing `Singular`, the authors of [GrP] found that Mora's algorithm could be made to work for any semigroup order. The same result was found independently by Gräbe (see [Grä]). Theorem (3.10) below gives the precise statement.

To prepare, we need to describe Lazard's idea mentioned above. We will specify the algorithm by using the homogenizations of f and the f_i with respect to a new variable t. If $g \in k[x_1, \ldots, x_n]$ is any polynomial, we will write g^h for the homogenization of g with respect to t. That is, if $g = \sum_\alpha c_\alpha x^\alpha$ and d is the total degree of g, then

$$g^h = \sum_\alpha c_\alpha t^{d-|\alpha|} x^\alpha.$$

(3.6) Definition. Each semigroup order $>$ on monomials in the x_i extends to a semigroup order $>'$ on monomials in $t, x_1, \ldots, x_n$ in the following way. We define $t^a x^\alpha >' t^b x^\beta$ if either $a + |\alpha| > b + |\beta|$, or $a + |\alpha| = b + |\beta|$ and $x^\alpha > x^\beta$.

In Exercise 12 below, you will show that $>'$ is actually a *monomial order* on $k[t, x_1, \ldots, x_n]$.

By the definition of $>'$, it follows that if $t^a > t^{a'} x^\beta$ for some a, a', β with $a = a' + |\beta|$, then $1 > x^\beta$. Hence, writing $R = \mathrm{Loc}_>(k[x_1, \ldots, x_n])$,

$$(3.7) \qquad t^a > t^{a'} x^\beta \text{ and } a = a' + |\beta| \Rightarrow 1 + x^\beta \text{ is a unit in } R.$$

It is also easy to see from the definition that if $g \in k[x_1, \ldots, x_n]$, then homogenization takes the $>$-leading term of g to the $>'$-leading term of g^h—that is, $\mathrm{LT}_{>'}(g^h) = t^a \mathrm{LT}_>(g)$, where $a = d - |\mathrm{multideg}_>(g)|$. Conversely, if G is homogeneous in $k[t, x_1, \ldots, x_n]$, then dehomogenizing (setting $t = 1$) takes the leading term $\mathrm{LT}_{>'}(G)$ to $\mathrm{LT}_>(g)$, where $g = G|_{t=1}$.

Given polynomials $f, f_1, \ldots, f_s$ and a semigroup order $>$, we want to show that there is an algorithm (called Mora's normal form algorithm) for producing polynomials $h, u, a_1, \ldots, a_s \in k[x_1, \ldots, x_n]$, where $u = 1 + g$ and $\mathrm{LT}(g) < 1$ (so u is a unit in $\mathrm{Loc}_>(k[x_1, \ldots, x_n])$), such that

$$(3.8) \qquad u \cdot f = a_1 f_1 + \cdots + a_s f_s + h,$$

where $\mathrm{LT}(a_i)\mathrm{LT}(f_i) \leq \mathrm{LT}(f)$ for all i, and either $h = 0$, or $\mathrm{LT}(h) \leq \mathrm{LT}(f)$ and $\mathrm{LT}(h)$ is not divisible by any of $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$.

Several comments are in order here. First, note that the inputs $f, f_1, \ldots, f_s$, the remainder h, the unit u, and the quotients $a_1, \ldots, a_s$ in (3.8) are all *polynomials*. The equation (3.8) holds in $k[x_1, \ldots, x_n]$, and as we will see, all the computations necessary to produce it also take place in a polynomial ring. We get a corresponding statement in $\mathrm{Loc}_>(k[x_1, \ldots, x_n])$

by multiplying both sides by $1/u$:

$$f = (a_1/u)f_1 + \cdots + (a_s/u)f_s + (h/u).$$

By Exercise 11 of §1, restricting to ideals generated by polynomials entails no loss of generality when we are studying ideals in $k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle} = \mathrm{Loc}_>(k[x_1, \ldots, x_n])$ for a local order $>$. But the major reason for restricting the inputs to be polynomials is that that allows us to specify a completely *algorithmic* (i.e., finite) division process. In $k[[x_1, \ldots, x_n]]$ or $k\{x_1, \ldots, x_n\}$, even a single reduction—computing $\mathrm{Red}\,(f, g)$—would take infinitely many computational steps if f or g were power series with infinitely many non-zero terms.

Second, when dividing f by $f_1, \ldots, f_s$ as in (3.8), we get a "remainder" h whose *leading term* is not divisible by any of the $\mathrm{LT}(f_i)$. In contrast, if we divide using the division algorithm of Chapter 1, §2, we get a remainder containing *no terms* divisible by any of the $\mathrm{LT}(f_i)$. Conceptually, there would be no problem with removing a term not divisible by any of the $\mathrm{LT}(f_i)$ and continuing to divide. But as in the first comment, this process may not be finite.

On the surface, these differences make the results of the Mora normal form algorithm seem weaker than those of the division algorithm. Even so, we will see in the next section that the Mora algorithm is strong enough for many purposes, including local versions of Buchberger's criterion and Buchberger's algorithm.

Instead of working with the f, f_i, h, a_i, and u directly, our statement of the algorithm will work with their homogenizations, and with the order $>'$ from Definition (3.6). Let $F = f^h$ and $F_i = f_i^h$ for $i = 1, \ldots, s$. We first show that there are homogeneous polynomials $U, A_1, \ldots, A_n$ such that

$$U \cdot F = A_1F_1 + \cdots + A_sF_s + H, \tag{3.9}$$

where $\mathrm{LT}(U) = t^a$ for some a,

$$a + \deg(F) = \deg(A_i) + \deg(F_i) = \deg(H)$$

whenever $A_i, H \neq 0$. Note that since U is homogeneous, if $\mathrm{LT}(U) = t^a$, then by (3.7) when we set $t = 1$, the dehomogenization u is a unit in $\mathrm{Loc}_>(k[x_1, \ldots, x_n])$. The other conditions satisfied by $U, A_1, \ldots, A_s, H$ are described in the following theorem.

(3.10) Theorem (Homogeneous Mora Normal Form Algorithm). *Given nonzero homogeneous polynomials $F, F_1, \ldots, F_s$ in $k[t, x_1, \ldots, x_n]$ and the monomial order $>'$ extending the semigroup order $>$ on monomials in the x_i, there is an algorithm for producing homogeneous polynomials $U, A_1, \ldots, A_s, H \in k[t, x_1, \ldots, x_n]$ satisfying*

$$U \cdot F = A_1F_1 + \cdots + A_sF_s + H,$$

where $\text{LT}(U) = t^a$ *for some* a,

$$a + \deg(F) = \deg(A_i) + \deg(F_i) = \deg(H)$$

whenever $A_i, H \neq 0$, $t^a\text{LT}(F) \geq' \text{LT}(A_i)\text{LT}(F_i)$, *and no* $\text{LT}(F_i)$ *divides* $t^b\text{LT}(H)$ *for any* $b \geq 0$.

PROOF. We give below the algorithm for computing the remainder H. (The computation of the A_i and U is described in the correctness argument below.) An important component of the algorithm is a set L consisting of possible divisors for reduction steps. As the algorithm proceeds, this set records the results of previous reductions for later use, according to Mora's idea.

```
Input: $F, F_1, \ldots, F_s \in k[t, x_1, \ldots, x_n]$ homogeneous and nonzero
Output: $H$ as in the statement of Theorem (3.10)

$H := F; L := \{F_1, \ldots, F_s\}; M := \{G \in L : \text{LT}(G)|\text{LT}(t^aH)$ for some $a\}$
WHILE ($H \neq 0$ AND $M \neq \emptyset$) DO
    SELECT $G \in M$ with $a$ minimal
    IF $a > 0$ THEN
        $L := L \cup \{H\}$
    $H := \text{Red}(t^aH, G)$
    IF $H \neq 0$ THEN
        $M := \{G \in L : \text{LT}(G)|\text{LT}(t^aH)$ for some $a\}$
```

We claim that the algorithm terminates on all inputs and correctly computes H as described in the statement of the theorem.

To prove termination, let $\mathcal{M}_j$ denote the monomial ideal

$$\langle \text{LT}(L)\rangle = \langle \text{LT}(G) : G \in L\rangle \subset k[t, x_1, \ldots, x_n]$$

after the jth pass through the WHILE loop ($j \geq 0$). The loop either leaves L unchanged or adds the polynomial H. Thus

$$\mathcal{M}_j \subset \mathcal{M}_{j+1}.$$

Notice that when H is added to L, $\text{LT}(H)$ does not lie in $\mathcal{M}_j$, for if it did, then we would have

$$\text{LT}(G)|\text{LT}(H)$$

for some $G \in L$. Thus $\text{LT}(G)|\text{LT}(t^0H)$, which would contradict our choice of H since a was chosen to be minimal, yet adding H to L requires $a > 0$. It follows that $\mathcal{M}_j \subset \mathcal{M}_{j+1}$ is a strict inclusion when a new element is added to L during the jth pass.

Since the polynomial ring $k[t, x_1, \ldots, x_n]$ satisfies the ascending chain condition on ideals, there is some N such that $\mathcal{M}_N = \mathcal{M}_{N+1} = \cdots$. By what we just proved, it follows that no new elements are added to L after the Nth pass through the WHILE loop. Thus, from this point on, the algorithm continues with a fixed set of divisors L, and at each step a reduction takes place decreasing the $>'$-leading term of H. Since $>'$ is a monomial order on $k[t, x_1, \ldots, x_n]$, the process must terminate as in the proof of the usual division algorithm.

To prove correctness, observe that the algorithm terminates when $H = 0$ or $M = \emptyset$. In the latter case, $\{F_1, \ldots, F_s\} \subset L$ tells us that $\text{LT}(F_i)$ doesn't divide $\text{LT}(t^b H) = t^b \text{LT}(H)$ for any $1 \leq i \leq s$ and $b \geq 0$. Thus H has the correct divisibility properties when it is nonzero.

It remains to show that H satisfies an identity of the form (3.9) with $\text{LT}(U) = t^a$. We will count passes through the WHILE loop starting at $j = 0$ and let H_j be the value of H at the beginning of the jth pass through the loop (so $H_0 = F$ at the start of the 0th pass). We will prove by induction on $j \geq 0$ that we have identities of the form

$$(3.11) \qquad U_k F = A_{1,k} F_1 + \cdots + A_{s,k} F_s + H_k, \quad 0 \leq k \leq j,$$

where U_k and $A_{i,k}$ are homogeneous with

$$\text{LT}(U_k) = t^{a_k}$$

such that $a_k + \deg(F) = \deg(A_{i,k}) + \deg(F_i) = \deg(H_k)$ and, for $0 < k \leq j$,

$$(3.12) \qquad a_{k-1} \leq a_k \quad \text{and} \quad t^{a_k} \text{LT}(H_{k-1}) >' t^{a_{k-1}} \text{LT}(H_k).$$

Since $H_0 = F$, setting $U_0 = 1$ and $A_{l,0} = 0$ for all l shows that everything works for $j = 0$. Now assume $j > 0$. We need to prove that the polynomial H_{j+1} produced by the jth pass through the loop satisfies the above conditions.

If no $\text{LT}(G)$ divides $t^b \text{LT}(H_j)$ for any $b \geq 0$ and $G \in L$, then the algorithm terminates with H_j and we are done. Otherwise some $G \in L$ satisfies $\text{LT}(G) | \text{LT}(t^a H_j)$ with a minimal. Hence there is a term M such that

$$\text{LT}(t^a H_j) = \text{M}\, \text{LT}(G).$$

There are two possibilities to consider: either $G = F_i$ for some i, or $G = H_\ell$ for some $\ell < j$.

If $G = F_i$ for some i, and a is chosen as above, then $H_{j+1} = \text{Red}(t^a H_j, F_i)$ means that

$$t^a H_j = \text{M}\, F_i + H_{j+1}.$$

If we multiply the equation (3.11) with $k = j$ by t^a and substitute, then we obtain

$$\begin{aligned} t^a U_j F &= t^a A_{1,j} F_1 + \cdots + t^a A_{s,j} F_s + t^a H_j \\ &= t^a A_{1,j} F_1 + \cdots + t^a A_{s,j} F_s + \text{M}\, F_i + H_{j+1}. \end{aligned}$$

Taking $U_{j+1} = t^a U_j$ and

$$A_{l,j+1} = \begin{cases} t^a A_{l,j} & \text{if } l \neq i \\ t^a A_{l,j} + \text{M} & \text{if } l = i, \end{cases}$$

we get an expression of the form (3.11) with $k = j + 1$. Also note that $\text{LT}(U_{j+1}) = t^{a+a_j}$.

On the other hand, if G is a result H_ℓ of a previous reduction, then $H_{j+1} = \text{Red}(t^a H_j, H_\ell)$ means that

$$t^a H_j = \mathrm{M}\, H_\ell + H_{j+1}.$$

Now take (3.11) with $k = j$ (resp. $k = \ell$) and multiply by t^a (resp. M). Subtracting gives the equation

$$(t^a U_j - \mathrm{M}\, U_\ell)F = (t^a A_{1,j} - \mathrm{M}\, A_{1,\ell})F_1 + \cdots + (t^a A_{s,j} - \mathrm{M}\, A_{s,\ell})F_s + H_{j+1}.$$

Setting $U_{j+1} = t^a U_j - \mathrm{M}\, U_\ell$ and $A_{l,j+1} = t^a A_{l,j} - \mathrm{M}\, A_{l,\ell}$, we see that (3.11) holds for $k = j + 1$. As for $\text{LT}(U_{j+1})$, note that (3.12) implies $t^{a_j}\text{LT}(H_\ell) >' t^{a_\ell}\text{LT}(H_j)$ since $\ell < j$. Thus

$$t^{a+a_j}\text{LT}(H_\ell) = t^a t^{a_j}\text{LT}(H_\ell) >' t^a t^{a_\ell}\text{LT}(H_j) = t^{a_\ell}\text{LT}(t^a H_j) = t^{a_\ell}\mathrm{M}\,\text{LT}(H_\ell),$$

which gives $t^{a+a_j} >' t^{a_\ell}\mathrm{M}$. Using $\text{LT}(U_j) = t^{a_j}$ and $\text{LT}(U_\ell) = t^{a_\ell}$, we obtain

$$\text{LT}(U_{j+1}) = \text{LT}(t^a U_j - \mathrm{M}\, U_\ell) = t^{a+a_j}.$$

Finally, note that $\text{LT}(U_{j+1}) = t^{a+a_j}$ in both cases, so that $a_{j+1} = a + a_j \geq a_j$. Also

$$\text{LT}(t^a H_j) >' \text{LT}(H_{j+1})$$

since H_{j+1} is a reduction of $t^a H_j$. From here, it is straightforward to show that (3.12) holds for $k = j + 1$. This completes the induction and shows that H has the required properties.

To finish the proof, we need to show that

$$a + \deg(F) = \deg(A_i) + \deg(F_i) \quad \text{and} \quad t^a\text{LT}(F) \geq' \text{LT}(A_i)\text{LT}(F_i)$$

when $A_i \neq 0$. You will do this in Exercise 13. □

Next, we claim that after homogenizing, applying the homogeneous Mora normal form algorithm, and dehomogenizing, we obtain an expression (3.8) satisfying the required conditions. Here is the precise result.

(3.13) Corollary (Mora Normal Form Algorithm). *Suppose that $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ are nonzero and $>$ is a semigroup order on monomials in the x_i. Then there is an algorithm for producing polynomials $u, a_1, \ldots, a_s, h \in k[x_1, \ldots, x_n]$ such that*

$$uf = a_1 f_1 + \cdots + a_s f_s + h,$$

where $\text{LT}(u) = 1$ (so u is a unit in $\text{Loc}_>(k[x_1, \ldots, x_n])$), $\text{LT}(a_i)\text{LT}(f_i) \leq \text{LT}(f)$ for all i with $a_i \neq 0$, and either $h = 0$, or $\text{LT}(h)$ is not divisible by any $\text{LT}(f_i)$.

Proof. See Exercise 14. □

Exercise 7. Carry out the Mora normal form algorithm dividing $f = x^2 + y^2$ by $f_1 = x - xy$, $f_2 = y^2 + x^3$ using the *alex* order in $k[x, y]$.

In $\mathrm{Loc}_>(k[x_1, \ldots, x_n])$, we get a version of the Mora algorithm that doesn't require f to be a polynomial. Recall from Exercise 5 that $\mathrm{LT}(f)$ makes sense for any nonzero $f \in \mathrm{Loc}_>(k[x_1, \ldots, x_n])$.

(3.14) Corollary. *Let $>$ be a semigroup order on monomials in the ring $k[x_1, \ldots, x_n]$ and let $R = \mathrm{Loc}_>(k[x_1, \ldots, x_n])$. Let $f \in R$ and $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ be nonzero. Then there is an algorithm for computing $h, a_1, \ldots, a_s \in R$ such that*

$$f = a_1 f_1 + \cdots + a_s f_s + h,$$

where $\mathrm{LT}(a_i)\mathrm{LT}(f_i) \leq \mathrm{LT}(f)$ for all i with $a_i \neq 0$, and either $h = 0$, or $\mathrm{LT}(h) \leq \mathrm{LT}(f)$ and $\mathrm{LT}(h)$ is not divisible by any of $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$.

Proof. If we write f in the form f'/u' where $f', u' \in k[x_1, \ldots, x_n]$ and u' is a unit in R, then dividing f' by $f_1, \ldots, f_s$ via Corollary (3.13) gives

$$u \cdot f' = a_1' f_1 + \cdots + a_s' f_s + h',$$

where $u, h', a_1', \ldots, a_s'$ are as in the corollary. Also observe that $\mathrm{LT}(h') \leq \mathrm{LT}(h)$ follows from $\mathrm{LT}(a_i')\mathrm{LT}(f_i) \leq \mathrm{LT}(f')$. Since the leading term of a unit is a nonzero constant (see Exercise 2), dividing a polynomial by a unit doesn't affect the leading term (up to multiplication by a nonzero constant). Thus, dividing the above equation by the unit $u\,u'$ gives

$$f = a_1 f_1 + \cdots + a_s f_s + h,$$

where $a_i = a_i'/(uu')$, $h = h'/(uu')$ clearly have the required properties. □

In the next section, we will use the Mora normal form algorithm to extend Buchberger's algorithm for Gröbner bases to ideals in local rings.

Additional Exercises for §3

Exercise 8. Let $>$ be a local order on monomials in $k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n\rangle}$ and $k[[x_1, \ldots, x_n]]$.

a. Show that every nonempty set of monomials has a maximal element under $>$. Hint: Define $>_r$ by $x^\alpha >_r x^\beta$ if and only if $x^\alpha < x^\beta$. Use Corollary 6 of Chapter 2, §4 of [CLO] to prove that $>_r$ is a well-ordering.
b. Use part a to define $\mathrm{multideg}(h)$ and $\mathrm{LT}(h)$ for $h \in k[[x_1, \ldots, x_n]]$.
c. Let $i : k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n\rangle} \hookrightarrow k[[x_1, \ldots, x_n]]$ denote the inclusion obtained by writing each $h \in k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n\rangle}$ in the form $f/(1+g)$ and then expanding $1/(1 + h)$ in a formal geometric series. Show that $\mathrm{multideg}(h) = \mathrm{multideg}(i(h))$.

d. Deduce that

$$\text{LM}_>(h) = \text{LM}_>(i(h)),\ \text{LC}_>(h) = \text{LC}_>(i(h)),\ \text{and } \text{LT}_>(h) = \text{LT}_>(i(h)).$$

Exercise 9. In the homogeneous Mora normal form algorithm (3.10), suppose that $h = 0$ after dehomogenizing. Show that f belongs to the ideal generated by $f_1, \ldots, f_s$ in the ring $R = \text{Loc}_>(k[x_1, \ldots, x_n])$. Is the converse always true?

Exercise 10. How should the homogeneous Mora normal form algorithm (3.10) be extended to return the quotients A_i and the unit U as well as the polynomial H? Hint: Use the proof of correctness.

Exercise 11. This exercise describes the way Mora based the original version of the normal form algorithm (for local orders) on the écart of a polynomial. Let $g \neq 0 \in k[x_1, \ldots, x_n]$, and write g as a finite sum of homogeneous nonzero polynomials of distinct total degrees:

$$g = \sum_{i=1}^{k} g_i, \quad g_i \text{ homogeneous},$$

with $\deg(g_1) < \cdots < \deg(g_k)$. The *order* of g, denoted $\text{ord}(g)$, is the total degree of g_1. The *total degree* of g, denoted $\deg(g)$ is the total degree of g_k. The *écart* of g, denoted $E(g)$, is the difference of the degree of g and the order of g:

$$E(g) = \deg(g) - \text{ord}(g).$$

By convention, we set $E(0) = -1$. Thus $E(g) \geq -1$ for all g. (The word *écart* is French for “difference” or “separation”—clearly a good description of the meaning of $E(g)$!)

a. Let $>$ be a local order and let f and g be two nonzero polynomials such that $\text{LT}(g)$ divides $\text{LT}(f)$. Then show that

$$E(\text{Red}\,(f, g)) \leq \max(E(f), E(g)).$$

b. In the one-variable case, part a gives a strategy that guarantees termination of division. Namely, at each stage, among all the polynomials by which we can reduce, we reduce by the polynomial whose écart is least. Show that this will ensure that the écarts of the sequence of partial dividends decreases to zero, at which point we have a monomial which can be used to reduce any subsequent partial dividend to 0.

c. Apply this strategy, reducing by the polynomial with the smallest possible écart at each step, to show that g divides f in $k[x]_{\langle x \rangle}$ in each of the following cases.

   1. $g = x + x^2 + x^3$, $f = x^2 + 2x^7$. Note that there is no way to produce a sequence of partial dividends with *strictly* decreasing écarts in this case.

2. $g = x + x^2 + x^3$, $f = x + x^2 + x^3 + x^4$. Note that after producing a monomial with the first reduction, the écart must increase.

Exercise 12. Let $>$ be a semigroup order on monomials in $k[x_1, \ldots, x_n]$ and extend to $>'$ on monomials in $t, x_1, \ldots, x_n$ as in the text: define $t^a x^\alpha >' t^b x^\beta$ if either $a + |\alpha| > b + |\beta|$ or $a + |\alpha| = b + |\beta|$, but $x^\alpha > x^\beta$.

a. Show that $>'$ is actually a *monomial order* on $k[t, x_1, \ldots, x_n]$.

b. Show that if $> \, = \, >_M$ for an $m \times n$ matrix M, then $>'$ is the order $>_{M'}$ where M' is the $(m + 1) \times (n + 1)$ matrix

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & & & \\ \vdots & & M & \\ 0 & & & \end{pmatrix}.$$

Exercise 13. Prove that at every stage of the homogeneous Mora normal form algorithm from Theorem (3.10), the polynomials $U, A_1, \ldots, A_s, H$ are homogeneous and satisfy the conditions

$$\begin{aligned} a + \deg(F) &= \deg(A_i) + \deg(F_i) = \deg(H) \\ t^a \mathrm{LT}(F) &\geq' \mathrm{LT}(A_i)\mathrm{LT}(F_i) \end{aligned}$$

whenever $A_i, H \neq 0$.

Exercise 14. Prove Corollary (3.13) using the homogeneous polynomials produced by the homogeneous Mora normal form algorithm described in the proof of Theorem (3.10). Hint: See the paragraph following (3.7).

Exercise 15. In [GrP], Mora's original notion of écart (described in Exercise 11) is modified to create a version of the Mora normal form algorithm which works directly with the polynomial ring $k[x_1, \ldots, x_n]$ and the semigroup order $>$. Define the écart of $f \in k[x_1, \ldots, x_n]$ to be

$$\mathrm{ecart}(f) = \deg(f) - \deg(\mathrm{LT}(f)).$$

Given nonzero polynomials $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, prove that the remainder h from Corollary (3.13) is produced by the following algorithm.

```
$h := f; L := \{f_1, \ldots, f_s\}; M := \{g \in L : \mathrm{LT}(g) | \mathrm{LT}(h)\}$
WHILE ($h \neq 0$ AND $M \neq \emptyset$) DO
    SELECT $g \in M$ with ecart($g$) minimal
    IF ecart($g$) > ecart($h$) THEN
        $L := L \cup \{h\}$
    $h :=$ Red($h, g$)
    IF $h \neq 0$ THEN
        $M := \{g \in L : \mathrm{LT}(g) | \mathrm{LT}(h)\}$
```

§4 Standard Bases in Local Rings

In this section, we want to develop analogs of Gröbner bases for ideals in any one of our local rings $R = k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$, $R = k\{x_1, \ldots, x_n\}$, or $R = k[[x_1, \ldots, x_n]]$. Just as for well-orderings, given an ideal I in R, we define the *set of leading terms of* I, denoted $\mathrm{LT}(I)$, to be the set of all leading terms of elements of I with respect to $>$. Also, we define the ideal of leading terms of I, denoted $\langle \mathrm{LT}(I)\rangle$, to be the ideal generated by the set $\mathrm{LT}(I)$ in R. Also just as for ideals in polynomial rings, it can happen that $I = \langle f_1, \ldots, f_s\rangle$ but $\langle \mathrm{LT}(I)\rangle \neq \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)\rangle$ for an ideal $I \subset R$. By analogy with the notion of a Gröbner basis, we make the following definition.

(4.1) Definition. Let $>$ be a semigroup order and let R be the ring of fractions $\mathrm{Loc}_>(k[x_1, \ldots, x_n])$ as in Definition (3.5), or let $>$ be a local order and let $R = k[[x_1, \ldots, x_n]]$ or $k\{x_1, \ldots, x_n\}$. Let $I \subset R$ be an ideal. A *standard basis* of I is a set $\{g_1, \ldots, g_t\} \subset I$ such that $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle$.

In the literature, the term "standard basis" is more common than "Gröbner basis" when working with local orders and the local rings $R = k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$, $k[[x_1, \ldots, x_n]]$, or $k\{x_1, \ldots, x_n\}$ so we use that terminology here.

Every nonzero ideal in these local rings has standard bases. As a result, there is an analog of the Hilbert Basis Theorem for these rings: every ideal has a finite generating set. The proof is the same as for polynomials (see Exercise 2 of Chapter 1, §3 and Exercise 2 below). Moreover, the Mora normal form algorithm—Corollary (3.13)—is well behaved when dividing by a standard basis. In particular, we obtain a zero remainder if and only if f is in the ideal generated by the standard basis (see Exercise 2).

However, in order to construct algorithms for *computing* standard bases, we will restrict our attention once more to ideals that are generated in these rings by collections of *polynomials*. Most of the ideals of interest in questions from algebraic geometry have this form. This will give us algorithmic control over such ideals. For example, we obtain a solution of the *ideal membership problem* for ideals generated by polynomials in the local rings under consideration.

Given polynomial generators for an ideal, how can we compute a standard basis for the ideal? For the polynomial ring $k[x_1, \ldots, x_n]$ and Gröbner bases, the key elements were the division algorithm and Buchberger's algorithm. Since we have the Mora algorithm, we now need to see if we can carry Buchberger's algorithm over to the case of local or other semigroup orders. That is, given a collection $f_1, \ldots, f_s$ of polynomials, we would like to find a standard basis with respect to some local order of the ideal $\langle f_1, \ldots, f_s\rangle$ they generate in a local ring R. More generally, one could also look for algorithms for computing standard bases of ideals in $\mathrm{Loc}_>(k[x_1,\dots,x_n])$ for any semigroup order.

It is a pleasant surprise that the ingredients fall into place with no difficulty. First, the definition of S-polynomials in this new setting is exactly the same as in $k[x_1,\dots,x_n]$ (see Definition (3.2) of Chapter 1), but here we use the leading terms with respect to our chosen semigroup order.

Next, recall that Buchberger's algorithm consists essentially of forming S-polynomials of all elements in the input set $F = \{f_1,\dots,f_s\}$ of polynomials, finding remainders upon division by F, adding to F any nonzero remainders, and iterating this process (see §3 of Chapter 1). Since we have the Mora normal form algorithm, whose output is a sort of remainder on division, we can certainly carry out the same steps as in Buchberger's algorithm. As with any algorithm, though, we have to establish its correctness (that is, that it gives us what we want) and that it terminates.

In the case of well-orders, correctness of Buchberger's algorithm is guaranteed by Buchberger's criterion, which states that a finite set G is a Gröbner basis if and only if the remainder upon division by G of every S-polynomial formed from pairs of elements of G is 0 (see Chapter 1, §3).

The following theorem gives analogs of Buchberger's criterion and Buchberger's algorithm for the ring of a semigroup order.

(4.2) Theorem. *Let $S \subset k[x_1,\dots,x_n]$ be finite, let $>$ be any semigroup order, and let I be the ideal in $R = \mathrm{Loc}_>(k[x_1,\dots,x_n])$ generated by S.*

a. *(Analog of Buchberger's Criterion) $S = \{g_1,\dots,g_t\}$ is a standard basis for I if and only if applying the Mora normal form algorithm given in Corollary (3.13) to every S-polynomial formed from elements of the set S yields a zero remainder.*
b. *(Analog of Buchberger's Algorithm) Buchberger's algorithm, using the Mora normal form algorithm in place of the usual polynomial division algorithm, computes a polynomial standard basis for the ideal generated by S, and terminates after finitely many steps.*

Proof. Let $\overline{f}^{S,\mathrm{Mora}}$ be the remainder h computed by Corollary (3.13) on division of f by S. If S is a standard basis of I, then since $S(g_i,g_j) \in I$ for all i,j, Exercise 2 implies that $\overline{S(g_i,g_j)}^{S,\mathrm{Mora}} = 0$ for all i,j.

Conversely, we need to show that $\overline{S(g_i,g_j)}^{S,\mathrm{Mora}} = 0$ for all i,j implies that S is a standard basis, or equivalently that $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1),\dots,\mathrm{LT}(g_t)\rangle$, using the order $>$. We will give the proof in the special case when $>$ is degree-anticompatible, meaning that $|\alpha| > |\beta| \Rightarrow x^\alpha < x^\beta$. Examples are the orders $>_{alex}$ or $>_{arevlex}$ from Definitions (3.2) and (3.3). Given $f \in I = \langle g_1,\dots,g_t\rangle$, we prove that $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1),\dots,\mathrm{LT}(g_t)\rangle$ as follows. Consider the nonempty set

$$\mathcal{S}_f = \{\max\{\mathrm{LT}(a_ig_i)\} : a_1,\dots,a_s \in R \text{ satisfy } f = \textstyle\sum_{i=1}^t a_ig_i\}.$$

For a general semigroup order, we can't claim that $\mathcal{S}_f$ has a minimal element, even though $\mathcal{S}_f$ is bounded below by $\textsc{lt}(f)$. However, in Exercise 3, you will show that this is true for degree-anticompatible orders. Hence we can let $\delta = \min \mathcal{S}_f$. From here, the rest of the argument that $\textsc{lt}(f) \in \langle \textsc{lt}(g_1), \ldots, \textsc{lt}(g_t) \rangle$ is a straightforward adaptation of the proof of Theorem 6 of Chapter 2, §6 of [CLO] (you will verify this in Exercise 4). This proves Buchberger's criterion for degree-anticompatible orders. The general case requires an analysis of the syzygy module of $g_1, \ldots, g_s$ (see Theorem 2.5.9 of [GrP] for the details).

For part b, observe that the usual proof that Buchberger's algorithm terminates and yields a Gröbner basis depends only on the ascending chain condition for polynomial ideals (applied to the chain of monomial ideals generated by the leading terms of the "partial bases" constructed as the algorithm proceeds—see the proof of Theorem 2 of [CLO], Chapter 2, §2). It does not require that the order used for the division process be a well-order. It follows that, replacing each ordinary remainder computation by a computation of the remainder from Mora's algorithm, we get an algorithm that terminates after a finite number of steps. Moreover, on termination, the result gives a standard basis for I by part a. □

The Mora normal form algorithm and standard basis algorithms using local orders or more general semigroup orders $>$ are not implemented directly in the Gröbner basis packages in Maple or *Mathematica*. They could be programmed directly in those systems, however, using the homogenization process and the order $>'$ from Definition (3.6). Alternatively, according to Lazard's original idea, the standard Buchberger algorithm could be applied to the homogenizations of a generating set for I. This approach is sketched in Exercise 5 below and can be carried out in any Gröbner basis implementation. Experience seems to indicate that standard basis computation with Mora's normal form algorithm is more efficient than computation using Lazard's approach, however. The CALI package for REDUCE does contain an implementation of Buchberger's algorithm using semigroup orders including local orders.

There is also a powerful package called `Singular` described in [GrP] and available via the World Wide Web from the University of Kaiserslautern (see the `Singular` homepage at `http://www.singular.uni-kl.de/`) that carries out these and many other calculations. In particular, `Singular` is set up so that local orders, monomial orders (well-orderings), and mixed orders can be specified in a unified way as $>_M$ orders for integer matrices M. This means that it can be used for both Gröbner and standard basis computations. Here is a very simple `Singular` session computing a standard basis of the ideal generated by

$$x^5 - xy^6 + z^7,\ xy + y^3 + z^3,\ x^2 + y^2 - z^2$$

in $R = k[x, y, z]_{\langle x,y,z\rangle}$ using the *alex* order, and computing the multiplicity of the origin as a solution of the corresponding system of equations.

```
> ring r = 32003, (x,y,z), Ds;
> ideal i = x5-xy6+z7, xy+y3+z3, x2+y2-z2;
> ideal j=std(i);
4(2)s5.8-s(2)s9..s(3).10.---sH(11)
product criterion:8 chain criterion:7
> j;
j[1]=x2+y2-1z2
j[2]=xy+y3+z3
j[3]=y3-1yz2-1xy3-1xz3
j[4]=xz4-1y6+2y4z2-1y3z3+2yz5-1xy6+z7
j[5]=y2z4-1z6+xy6-2xy4z2+xy3z3-2xyz5+x2y6-1xz7
j[6]=yz7
j[7]=z9
> vdim(j);
24
```

`Singular` can work either with a finite field of coefficients or with $k = \mathbb{Q}$ or a finite extension of $\mathbb{Q}$. The first line here defines the characteristic of the field, the ring variables, and the monomial order. The `Ds` is an abbreviation for the *alex* order, which could also be specified by a matrix as follows

```
> ring r = 32003, (x,y,z), ((-1,-1,-1),(0,-1,-1),(0,0,-1));
```

as in Exercise 2 of §3. The ideal I is defined by the three polynomials above, J contains the standard basis (seven polynomials in all), and the `vdim` command computes the dimension of $\dim R/\langle \mathrm{LT}(J)\rangle$. For more information about this very flexible package, we refer the interested reader to [GrP].

We've already commented on how standard bases enable one to solve the ideal membership problem in local rings, just as Gröbner bases solve the corresponding problem in polynomial rings. Another important use of Gröbner bases is the computation of $\dim k[x_1, \ldots, x_n]/I$ when this dimension is finite. For the local version of this result, we will use the following terminology: given a local order $>$ and an ideal I in one of the local rings $k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$, $k[[x_1, \ldots, x_n]]$ or $k\{x_1, \ldots, x_n\}$, we say that a monomial x^α is *standard* if

$$x^\alpha \notin \langle \mathrm{LT}(I)\rangle.$$

Then we have the following result about standard monomials.

(4.3) Theorem. *Let R be one of the local rings $k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$, $k[[x_1, \ldots, x_n]]$ or $k\{x_1, \ldots, x_n\}$. If $I \subset R$ is an ideal and $>$ is a local order, then the following are equivalent.*
a. $\dim R/I$ *is finite.*

b. $\dim R/\langle \text{LT}(I)\rangle$ *is finite.*
c. *There are only finitely many standard monomials.*

Furthermore, when any of these conditions is satisfied, we have

$$\dim R/I = \dim R/\langle \text{LT}(I)\rangle = \textit{number of standard monomials}$$

and every $f \in R$ can be written uniquely as a sum

$$f = g + r,$$

where $g \in I$ and r is a linear combination of standard monomials. In addition, this decomposition can be computed algorithmically when $R = k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$.

Proof. We first prove a ⇒ c. Suppose that $x^{\alpha(1)}, \ldots, x^{\alpha(m)}$ are standard monomials with $m > \dim R/I$. It follows easily that there is a nontrivial linear combination

$$f = \sum_{i=1}^{\ell} c_i x^{\alpha(i)} \in I, \quad c_i \in k.$$

Then $\text{LT}(f) \in \langle \text{LT}(I)\rangle$ implies that some $x^{\alpha(i)} \in \langle \text{LT}(I)\rangle$, which is impossible since $x^{\alpha(i)}$ is standard. This shows that the number of standard monomials is bounded above by $\dim R/I$.

For c ⇒ a, suppose that $R = k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$. Then Exercise 11 of §1 implies that I is generated by polynomials, which means that we can compute a polynomial standard basis G of I. Now take $f \in R$ and divide f by G using Corollary (3.14) to obtain

$$f = g_1 + h_1,$$

where $g_1 \in I$ and either $h_1 = 0$ or $\text{LT}(h_1) \notin \langle \text{LT}(G)\rangle = \langle \text{LT}(I)\rangle$ (since G is a standard basis) and $\text{LT}(f) \geq \text{LT}(h_1)$. Note that we are using the extension of LT to R studied in Exercise 5 of §3.

If $h_1 \neq 0$, let $\text{LT}(h_1) = c_1 x^{\alpha(1)}$, $c_1 \in k$, $c_1 \neq 0$. Thus $x^{\alpha(1)}$ is standard and, by Exercise 5 of §3, $h_1 = c_1 x^{\alpha(1)} + r_1$, where $r_1 = 0$ or $x^{\alpha(1)} > \text{LT}(r_1)$. If $r_1 \neq 0$, then applying the above process gives

$$r_1 = g_2 + h_2 = g_2 + c_2 x^{\alpha(2)} + r_2$$

with $g_2 \in I$, $x^{\alpha(2)}$ standard, and $r_2 = 0$ or $x^{\alpha(2)} > \text{LT}(r_2)$. If we combine this with the formula for f, we obtain

$$f = g_1 + h_1 = g_1 + c_1 x^{\alpha(1)} + r_1 = (g_1 + g_2) + c_1 x^{\alpha(1)} + c_2 x^{\alpha(2)} + r_2,$$

where $g_1 + g_2 \in I$, $x^{\alpha(1)}, x^{\alpha(2)}$ standard, and $x^{\alpha(1)} > x^{\alpha(2)} > \text{LT}(r_2)$ if $r_2 \neq 0$. We can continue this process as long as we have nonzero terms to work with. However, since there are only finitely many standard monomials, this process must eventually terminate, which shows that f has the form $g + r$ described in the statement of the theorem. We will leave it for the reader to prove uniqueness and describe an algorithm that carries out this process (see Exercise 6 below). It follows that the cosets of the standard monomials give a basis of R/I, proving

$$\dim R/I = \text{number of standard monomials}$$

when $R = k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$.

When $R = k\{x_1, \ldots, x_n\}$ or $R = k[[x_1, \ldots, x_n]]$, if we assume that we can perform the Mora Normal Form Algorithm on inputs from R, then the above argument applies for any $f \in R$. The details of how this works will be discussed in Exercise 2 below. This completes the proof of c ⇒ a and the final assertions of the theorem.

It remains to prove b ⇔ c. This follows immediately from what we have already proved since I and $\langle \text{LT}(I)\rangle$ have the same standard monomials. □

When $R = k[[x_1, \ldots, x_n]]$ or $R = k\{x_1, \ldots, x_n\}$, there are more powerful versions of Theorem (4.3) that don't assume that $\dim R/\langle \text{LT}(I)\rangle$ is finite. In these situations, the remainder r is an infinite series, none of whose terms are in $\langle \text{LT}(I)\rangle$. See, for example, [Hir] or [MPT]. However, for $R = k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$, it is possible to find ideals $I \subset R$ where nice remainders don't exist (see [AMR], Example 2).

Additional Exercises for §4

Exercise 1. In this exercise and the next, we will show that every ideal I in one of our local rings R has standard bases, and derive consequences about the structure of R. Let $>$ be any local order on R.

a. Explain why $\langle \text{LT}(I)\rangle$ has a finite set of generators.
b. For each $x^{\alpha(i)}$, $i = 1, \ldots, t$, in a finite set of generators of $\langle \text{LT}(I)\rangle$, let $g_i \in I$ be an element with $\text{LT}(g_i) = x^{\alpha(i)}$. Deduce that $G = \{g_1, \ldots, g_t\}$ is a standard basis for I.

Exercise 2. If we ignore the fact that infinitely many computational steps are needed to perform reductions on power series in $k[[x_1, \ldots, x_n]]$ or $k\{x_1, \ldots, x_n\}$, then the Mora Normal Form Algorithm can be performed with inputs that are not polynomials. Hence we can assume that the Mora algorithm works for R, where R is either $k[[x_1, \ldots, x_n]]$ or $k\{x_1, \ldots, x_n\}$.

a. Let G be a standard basis for an ideal $I \subset R$. Show that we obtain a zero remainder on division of f by G if and only if $f \in I$.
b. Using part a, deduce that every ideal $I \subset R$ has a finite basis. (This is the analog of the Hilbert Basis Theorem for $k[x_1, \ldots, x_n]$.)
c. Deduce that the ascending chain condition holds for ideals in R. Hint: See Exercise 13 of §2 of Chapter 5.

Exercise 3. Let $>$ be a degree-anticompatible order on one of our local rings R. Show that any nonempty set of monomials $\mathcal{S}$ that is bounded below (meaning that there exists a monomial x^α such that $x^\beta \geq x^\alpha$ for all $x^\beta \in \mathcal{S}$) has a smallest element.

Exercise 4. Carry out the proof of the analog of Buchberger's Criterion for degree-anticompatible orders, using Exercise 3 and the discussion before the statement of Theorem (4.2).

Exercise 5. This exercise discusses an alternative method due to Lazard for computing in local rings. Let $>'$ be the order in $k[t, x_1, \ldots, x_n]$ from Definition (3.6). Given polynomials $f_1, \ldots, f_s$, let $f_1^h, \ldots, f_s^h$ be their homogenizations in $k[t, x_1, \ldots, x_n]$, and let G be a Gröbner basis for $\langle f_1^h, \ldots, f_s^h \rangle$ with respect to the $>'$ consisting of *homogeneous* polynomials (such Gröbner bases always exist—see Theorem 2 in Chapter 8, §3 of [CLO], for instance). Show that the *dehomogenizations* of the elements of G (that is, the polynomials in $k[x_1, \ldots, x_n]$ obtained from the elements of G by setting $t = 1$) are a standard basis for the ideal generated by F in the local ring R with respect to the semigroup order $>$.

Exercise 6. Let $I \subset R = k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle}$ be an ideal such that $\dim R/\langle \mathrm{LT}(I) \rangle$ is finite for some local order on R. Describe an algorithm which for the input $f \in R$ computes the remainder r from Theorem (4.3).

§5 Applications of Standard Bases

We will consider some applications of standard bases in this section. The multiplicity, and Milnor and Tjurina number computations we introduced in §2 can be carried out in an algorithmic fashion using standard bases. We begin by using Theorem (4.3) to prove Proposition (2.11), which asserts that if I is a zero-dimensional ideal of $k[x_1, \ldots, x_n]$ such that $0 \in \mathbf{V}(I)$, then the multiplicity of 0 is

$$\begin{aligned} &\dim k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle}/Ik[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle} \\ (5.1) \qquad &= \dim k[[x_1, \ldots, x_n]]/Ik[[x_1, \ldots, x_n]] \\ &= \dim k\{x_1, \ldots, x_n\}/Ik\{x_1, \ldots, x_n\}, \end{aligned}$$

where the last equality assumes $k = \mathbb{R}$ or $\mathbb{C}$. The proof begins with the observation that by Theorem (2.2), we know that

$$\dim k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle}/Ik[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle} < \infty.$$

By Theorem (4.3), it follows that this dimension is the number of standard monomials for a standard basis S for $I \subset k[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle}$. However, S is also a standard basis for $Ik[[x_1, \ldots, x_n]]$ and $Ik\{x_1, \ldots, x_n\}$ by Buchberger's criterion. Thus, for a fixed local order, the standard monomials are *the same* no matter which of the local rings R we are considering. Then (5.1) follows immediately from Theorem (4.3).

This gives an algorithm for computing multiplicities. Exercises 2 and 3 below give some nice examples. In the same way, we can compute the Milnor and Tjurina numbers defined in §2 (see Exercise 4).

Standard bases in local rings have other geometric applications as well. For instance, suppose that $V \subset k^n$ is a variety and that $p = (a_1, \ldots, a_n)$ is a point of V. Then the *tangent cone* to V at p, denoted $C_p(V)$, is defined to be the variety

$$C_p(V) = \mathbf{V}(f_{p,min} : f \in \mathbf{I}(V)),$$

where $f_{p,min}$ is the homogeneous component of lowest degree in the polynomial $f(x_1 + a_1, \ldots, x_n + a_n)$ obtained by translating p to the origin (see part b of Exercise 17 of §2). A careful discussion of tangent cones, including a Gröbner basis method for computing them, can be found in Chapter 9, §7 of [CLO]. However, standard bases give a more direct way to compute tangent cones than the Gröbner basis method. See Exercise 5 below for an outline of the main ideas.

Here is another sort of application, where localization is used to concentrate attention on one irreducible component of a reducible variety. To illustrate the idea, we will use an example from Chapter 6, §4 of [CLO]. In that section, we showed that the hypotheses and the conclusions of a large class of theorems in Euclidean plane geometry can be expressed as polynomial equations on the coordinates of points specified in the construction of the geometric figures involved in their statements. For instance, consider the theorem which states that the diagonals of a parallelogram $ABCD$ in the plane intersect at a point that bisects both diagonals (Example 1 of [CLO], Chapter 6, §4). We place the vertices A, B, C, D of the parallelogram as follows:

$$A = (0,0),\ B = (u,0),\ C = (v,w),\ D = (a,b),$$

and write the intersection point of the diagonals $\overline{AD}$ and $\overline{BC}$ as $N = (c,d)$. We think of the coordinates u, v, w as arbitrary; their values determine the values of a, b, c, d. The conditions that $ABCD$ is a parallelogram and N is the intersection of the diagonals can be written as the following polynomial equations:

$$\begin{aligned}
h_1 &= b - w = 0\\
h_2 &= (a-u)w - bv = 0\\
h_3 &= ad - cw = 0\\
h_4 &= d(v-u) - (c-u)w = 0,
\end{aligned}$$

as can the conclusions of the theorem (the equalities between the lengths $AN = DN$ and $BN = CN$)

$$\begin{aligned} g_1 &= a^2 - 2ac - 2bd + b^2 = 0 \\ g_2 &= 2cu - 2cv - 2dw - u^2 + v^2 + w^2 = 0. \end{aligned}$$

Since the geometric theorem is true, we might naively expect that the conclusions $g_1 = g_2 = 0$ are satisfied whenever the hypothesis equations $h_1 = h_2 = h_3 = h_4 = 0$ are satisfied. If we work over the algebraically closed field $\mathbb{C}$, then the Strong Nullstellensatz shows that our naive hope is equivalent to

$$g_i \in \mathbf{I}(\mathbf{V}(h_1, h_2, h_3, h_4)) = \sqrt{\langle h_1, h_2, h_3, h_4 \rangle}.$$

However, as the following exercise illustrates, this is unfortunately not true.

Exercise 1. Use the radical membership test from [CLO], Chapter 4, §2 to show that

$$g_1, g_2 \notin \sqrt{\langle h_1, h_2, h_3, h_4 \rangle} \subset \mathbb{C}[u, v, w, a, b, c, d].$$

Thus neither conclusion g_1, g_2 follows directly from the hypothesis equations.

In fact, in [CLO], Chapter 6, §4 we saw that the reason for this was that the variety $\mathbf{V}(h_1, h_2, h_3, h_4) \subset \mathbb{C}^7$ defined by the hypotheses is actually *reducible*, and the conclusion equations $g_i = 0$ are not identically satisfied on several of the irreducible components of H. The points on the "bad" components correspond to *degenerate special cases* of the configuration A, B, C, D, N such as "parallelograms" in which two of the vertices A, B, C, D coincide. In [CLO], Chapter 6, §4 we analyzed this situation very carefully and found the "good" component of H, on which the conclusions $g_1 = g_2 = 0$ do hold. Our purpose here is to point out that what we did in [CLO] can also be accomplished more easily by *localizing* appropriately.

Note that taking $(u, v, w) = (1, 1, 1)$ gives an "honest" parallelogram. If we now translate $(1, 1, 1)$ to the origin as in Exercise 17 of §2, and write the translated coordinates as (U, V, W, a, b, c, d), the hypotheses and conclusions become

$$\begin{aligned} h_1 &= b - W - 1 = 0 \\ h_2 &= (a - U - 1)(W + 1) - b(V + 1) = 0 \\ h_3 &= ad - c(W + 1) = 0 \\ h_4 &= d(V - U) - (c - U - 1)(W + 1) \\ g_1 &= a^2 - 2ac - 2cd + b^2 = 0 \\ g_2 &= 2c(U + 1) - 2c(V + 1) - 2d(W + 1) - (U + 1)^2 \\ &\quad + (V + 1)^2 + (W + 1)^2 = 0. \end{aligned}$$

Using `Singular`, we can compute a standard basis for the ideal generated by the h_i in the localization $R = \mathbb{Q}[U, V, W]_{\langle U,V,W \rangle}[a, b, c, d]$ as follows.

```
> ring r = 0, (a,b,c,d,U,V,W), (Dp(4),Ds(3));
> ideal i = b-W-1, (a-U-1)*(W+1)-b*(V+1), ad-c*(W+1), d*(V-U)-
(c-U-1)*(W+1);
> ideal j = std(i);
> j;
j[1]=a+aW-1b-1bV-1-1U-1W-1UW
j[2]=b-1-1W
j[3]=c+cW+dU-1dV-1-1U-1W-1UW
j[4]=2d+2dU+2dW+2dUW-1-1U-2W-2UW-1W2-1UW2
```

The first line sets up the ring R by specifying the coefficient field $k = \mathbb{Q}$ and a mixed order on the variables as in Exercise 3 of §3 of this chapter, with *alex* on the variables U, V, W, ordinary *lex* on a, b, c, d, and all monomials containing a, b, c, d greater than any monomial in U, V, W alone. If we now apply the Mora algorithm from Corollary (3.13), which is provided in the `Singular` command `reduce`, we find that both conclusions are actually in the ideal generated by h_1, h_2, h_3, h_4 in R.

```
> poly g=a2-2ac-2bd+b2;
> poly h=reduce(g,j);
> h;
0
> poly m = 2c*(U+1)-2c*(V+1)-2d*(W+1)-(U+1)^2+(V+1)^2+(W+1)^2;
> poly n = reduce(m,j);
> n;
0
```

This shows that *locally* near the point with $(u, v, w) = (1, 1, 1)$ on the variety $\mathbf{V}(h_1, h_2, h_3, h_4)$, the conclusions do follow from the hypotheses. Using the mixed order in the Mora algorithm, we have an equation

$$u \cdot g_1 = a_1 h_1 + \cdots + a_4 h_4,$$

where $u \in \mathbb{Q}[U, V, W]$ is a unit in $\mathbb{Q}[U, V, W]_{\langle U,V,W \rangle}$, and a similar equation for g_2. In particular, this shows that Proposition 8 of Chapter 6, §4 of [CLO] applies and the conclusions g_1, g_2 *follow generically* from the hypotheses h_i, as defined there.

Along the same lines we have the following general statement, showing that localizing at a point p in a variety V implies that we ignore components of V that do not contain p.

(5.2) Proposition. *Let $I \subset k[x_1, \ldots, x_n]$ and suppose that the origin in k^n is contained in an irreducible component W of $\mathbf{V}(I)$. Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ be a standard basis for I with respect to a local order, and let $g \in k[x_1, \ldots, x_n]$. If the remainder of g on division by $F = (f_1, \ldots, f_s)$ using the Mora algorithm from Corollary (3.13) is zero, then $g \in \mathbf{I}(W)$ (but not necessarily in I).*

PROOF. If the remainder is zero, the Mora algorithm yields an equation

$$u \cdot g = a_1 f_1 + \cdots + a_s f_s,$$

where $u \in k[x_1, \ldots, x_n]$ is a unit in $k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$. Since $W \subset \mathbf{V}(I)$, $u \cdot g$ is an element of $\mathbf{I}(W)$. But W is irreducible, so $\mathbf{I}(W)$ is a prime ideal, and hence $u \in \mathbf{I}(W)$ or $g \in \mathbf{I}(W)$. The first alternative is not possible since $u(0) \neq 0$. Hence $g \in \mathbf{I}(W)$. □

It is natural to ask if we can carry out operations on ideals in local rings algorithmically in ways similar to the Gröbner basis methods reviewed in Chapter 1 for ideals in polynomial rings. In the final part of this section, we will show that the answer is yes when $R = k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$. Since many of the proofs in the polynomial case use elimination, we first need to study elimination in the local context. The essential point will be to work the new ring $k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}[t]$, whose elements can be thought of first as polynomials in t whose coefficients are elements of $k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$.

In this situation, if we have an ideal $I \subset k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}[t]$, the basic problem is to find the intersection

$$I_0 = I \cap k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}.$$

Note that I_0 is analogous to an *elimination ideal* of a polynomial ideal. This elimination problem can be solved using a local order $>$ on the local ring to construct a suitable semigroup order on $S = k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}[t]$ as follows (see [AMR] and [Grä] for the details).

(5.3) Definition. An *elimination order* on S is any semigroup order $>_{elim}$ on the monomials on S defined in the following way. Let $>$ be a local order in $k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$. Then define

$$t^k x^\alpha >_{elim} t^l x^\beta$$

for $k, l \in \mathbb{Z}_{\geq 0}$, and $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ if and only if $k > l$, or $k = l$ and $\alpha > \beta$. In other words, an elimination order is a product order combining the degree order on powers of t and the given local order $>$ on x^α in $k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$.

Elimination orders on S are *neither* local nor well-orders. Hence, the full strength of the Mora algorithm for general semigroup orders is needed here. We have the following analog of the Elimination Theorem stated in Chapter 2, §1.

(5.4) Theorem (Local Elimination). *Fix an elimination order $>_{elim}$ on $S = k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}[t]$. Let $I \subset S$ be an ideal, and let G be a* *polynomial standard basis for I with respect to $>_{elim}$. Then*

$$G \cap k[x_1, \ldots, x_n] = \{g \in G : \textsc{lt}(g) \text{ does not contain } t\}$$

and this is a standard basis of $I_0 = I \cap k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$.

Proof. Let $G = \{g_1, \ldots, g_t\}$ be a standard basis of I and $G_0 = \{g \in G : \textsc{lt}(g)$ does not contain $t\}$. By the definition of $>_{elim}$, the condition that $\textsc{lt}(g)$ does not contain t implies that g does not contain t. Since $G_0 \subset I_0$, we need only show that if $f \in I_0 \cap k[x_1, \ldots, x_n]$, then f can be written as a combination of elements in G_0 with coefficients in $k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$. Since $f \in I$ and $\{g_1, \ldots, g_t\}$ is a standard basis of I, the Mora algorithm gives an expression

$$f = a_1 g_1 + \cdots + a_t g_t$$

(see Exercise 2 of §4), where $\textsc{lt}(f) \geq \textsc{lt}(a_i g_i)$ for all $a_i \neq 0$. By our choice of order, we have $a_i = 0$ for $g_i \notin G_0$ and $g_i \in k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$ otherwise, since t does not appear in $\textsc{lt}(f)$. □

With this out of the way, we can immediately prove the following.

(5.5) Theorem. *Let $I, J \subset k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$ and $f \in k[x_1, \ldots, x_n]$.*

a. $I \cap J = (t \cdot I + (1-t) \cdot J) \cap k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$.

b. $I : \langle f\rangle = \frac{1}{f} \cdot (I \cap \langle f\rangle)$.

c. $I : f^\infty = (I + \langle 1 - f \cdot t\rangle) \cap k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$.

d. $f \in \sqrt{I}$ *if and only if* $1 \in I + \langle 1 - f \cdot t\rangle$ *in* $k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}[t]$.

Proof. The proofs are the same as for polynomial ideals. (See Chapter 1 of this book, §2 and §3 of Chapter 4 of [CLO], and [AL] or [BW].)

We remind the reader that the *stable quotient* of I with respect to f, denoted $I : f^\infty$, is defined to be the ideal

$$I : f^\infty = \{g \in R : \text{ there exists } n \geq 1 \text{ for which } f^n g \in I\}.$$

The stable quotient is frequently useful in applications of local algebra. We also remark that the division in part b, where one divides the common factor f out from all generators of $I \cap \langle f\rangle$ in $k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$, uses the Mora algorithm. □

Just as the ability to do computations in polynomial rings extends to allow one to do computations in quotients (i.e., homomorphic images of polynomial rings), so, too, the ability to do computations in local rings extends to allow one to do computations in quotients of local rings. Suppose that $J \subset k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$ and let $\overline{R} = k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}/J$. Then one can do computations algorithmically in $\overline{R}$ due to the following elementary proposition.

(5.6) Proposition. *Let $\overline{I_1}, \overline{I_2} \subset \overline{R}$ be ideals, and let I_1, I_2 denote their preimages in $k[x_1,\dots,x_n]_{\langle x_1,\dots,x_n\rangle}$. Let $f \in k[x_1,\dots,x_n]_{\langle x_1,\dots,x_n\rangle}$ and $[f] \in \overline{R}$ be its coset. Then:*
a. $\overline{I_1} \cap \overline{I_2} = (I_1 \cap I_2)/J$;
b. $\overline{I_1} : [f] = (I_1 : f)/J$;
c. $\overline{I_1} : [f]^\infty = (I_1 : f^\infty)/J$.

Using a standard basis of J allows one to determine whether $f, g \in R$ represent the same element in $\overline{R}$ (that is, whether $[f] = [g]$.) One can also compute Hilbert functions and syzygies over $\overline{R}$.

The techniques we have outlined above also extend to rings that are finite algebraic extensions of $k[x_1,\dots,x_n]_{\langle x_1,\dots,x_n\rangle}$ in $k[[x_1,\dots,x_n]]$. This allows us to handle computations involving algebraic power series in $k[[x_1,\dots,x_n]]$ algorithmically. See [AMR] for details. There are still many open questions in this area, however. Basically, one would hope to handle any operations on ideals whose generators are defined in some suitably algebraic fashion (not just ideals generated by polynomials), but there are many instances where no algorithms are known.

Additional Exercises for §5

Exercise 2.
a. Let $f_1,\dots,f_n \in k[x_1,\dots,x_n]$ be homogeneous polynomials of degrees $d_1,\dots,d_n$, respectively. Assume that $I = \langle f_1,\dots,f_n\rangle$ is zero-dimensional, and that the origin is the only point in $\mathbf{V}(I)$. Show that the multiplicity is also the dimension of

$$k[x_1,\dots,x_n]/\langle f_1,\dots,f_n\rangle,$$

and then prove that the multiplicity of 0 as a solution of $f_1 = \cdots = f_n = 0$ is $d_1 \cdots d_n$. Hint: Regard $f_1,\dots,f_n$ as homogeneous polynomials in $x_0, x_1,\dots,x_n$, where x_0 is a new variable. Using $x_0, x_1,\dots,x_n$ as homogeneous coordinates for $\mathbb{P}^n$, show that $f_1 = \cdots = f_n = 0$ have no nontrivial solutions when $x_0 = 0$, so that there are no solutions at ∞ in the sense of Chapter 3. Then use Bézout's Theorem as stated in Chapter 3.
b. Let $f(x_1,\dots,x_n)$ be a homogeneous polynomial of degree d with an isolated singularity at the origin. Show that the Milnor number of f at the origin is $(d-1)^n$.

Exercise 3. Determine the multiplicity of the solution at the origin for each of the following systems of polynomial equations.
a. $x^2 + 2xy^4 - y^2 = xy - y^3 = 0$.
b. $x^2 + 2y^2 - y - 2z = x^2 - 8y^2 + 10z = x^2 - 7yz = 0$.
c. $x^2 + y^2 + z^2 - 2x^4 = x^3 - yz - x = x - y + 2z = 0$.

Exercise 4. Compute the Milnor and Tjurina numbers at the origin of the following polynomials (all of which have an isolated singularity at 0).

a. $f(x, y) = (x^2 + y^2)^3 - 4x^2y^2$. The curve $\mathbf{V}(f) \subset \mathbb{R}^2$ is the four-leaved rose—see Exercise 11 of [CLO], Chapter 3, §5.

b. $f(x, y) = y^2 - x^n$, $n \geq 2$. Express the Milnor number as a function of the integer n.

c. $f(x, y, z) = xyz + x^4 + y^4 + z^4$.

Exercise 5. (Tangent Cones) For each $f \in \langle x_1, \ldots, x_n\rangle$, let f_{min} be the homogeneous component of lowest degree in f. Let $V = \mathbf{V}(f_1, \ldots, f_s) \subset k^n$ be a variety containing the origin.

a. Let $G = \{g_1, \ldots, g_t\}$ be a standard basis for

$$I = \langle f_1, \ldots, f_s\rangle k[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$$

with respect to a degree-anticompatible order $>$. Explain why $\textsc{lt}_>(g_i)$ is one of the terms in $g_{i,min}$ for each i.

b. Show that $\mathbf{V}(g_{1,min}, \ldots, g_{t,min})$ is the tangent cone of V at the origin.

c. Consider the variety $V = \mathbf{V}(x^3 - yz - x, y^2 + 2z^3)$ in k^3. Using the $>_{alex}$ order on $k[x, y, z]_{\langle x,y,z\rangle}$, with $x > y > z$, show that the two given polynomials in the definition of V are a standard basis for the ideal they generate, and compute the tangent cone of V at the origin using part b.

Exercise 6. For an r-dimensional linear subspace $L \subset \mathbb{C}^n$, a polynomial $f \in \mathbb{C}[x_1, \ldots, x_n]$ restricts to a polynomial function f_L on L.

a. Show that if f has an isolated singularity at the origin in $\mathbb{C}^n$, then for almost all r-dimensional subspaces $L \subset \mathbb{C}^n$, f_L has an isolated singularity at the origin in L.

b. One can show, in fact, that there is an open dense set $\mathcal{N}$ of all r-dimensional subspaces of $\mathbb{C}^n$ such that the Milnor number $\mu(f_L)$ of f_L at the origin does not depend on the choice of L in $\mathcal{N}$. This number is denoted $\mu^r(f)$. Show that $\mu^1(f) = \mathrm{mult}(f) - 1$ where $\mathrm{mult}(f)$ (the multiplicity of f) is the degree of the lowest degree term of f that occurs with nonzero coefficient.

c. Compute $\mu^2(f)$ and $\mu^3(f)$ if
   1. $f = x^5 + y^4 + z^7$;
   2. $f = x^4 + y^5 + z^6 + xyz$;
   3. $f = x^5 + xy^6 + y^7z + z^{15}$;
   4. $f = x^5 + y^7z + z^{15}$.

   Note that if n is the number of variables, then $\mu^n(f) = \mu(f)$, so that $\mu^3(f)$ is just the usual Milnor number for these examples. To compute these numbers, use the `milnor` package in `Singular` and note that planes of the form $z = ax + by$ are an open set in the set of all planes in $\mathbb{C}^3$. One could also compute these Milnor numbers by hand. Note that examples 1, 3, and 4 are weighted homogeneous polynomials. For further background, the reader may wish to consult [Dim] or [AGV].

d. A family $\{f_t \in \mathbb{C}[x_1,\ldots,x_n]\}$ of polynomials with an isolated singularity at the origin for t near 0 is *μ-constant* if $\mu(f_0) = \mu(f_t)$ for t near 0. Show that $f_t = x^5 + y^4 + z^7 + tx^8y^2$ and $f_t = x^5 + txy^6 + y^7z + z^{15}$ are μ-constant families but $f_t = x^4 + y^5 + z^6 + txyz$ is not.

e. If $f \in \mathbb{C}[x_1,\ldots,x_n]$ has an isolated singularity at the origin, the n-tuple of integers $(\mu^1(f),\ldots,\mu^n(f))$ is called the *Teissier μ^*-invariant* of f. One says that a family $\{f_t\}$ is *μ^*-constant* if $\mu^*(f_0) = \mu^*(f_t)$. Show that $f_t = x^5 + txy^6 + y^7z + z^{15}$ is μ-constant, but not μ^* constant. This is a famous example due to Briançon and Speder—there are very few known examples of μ-constant families that are not μ^*-constant. At the time of writing, it is not known whether there exist μ-constant families in which μ^1 is not constant. The attempt to find such examples was one of the issues that motivated the development of early versions of `Singular`.