COMPUTATIONAL ALGEBRAIC GEOMETRY

HAL SCHENCK
Texas A&M University

CAMBRIDGE
UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011-4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

http://www.cambridge.org

First published 2003

Printed in the United States of America

Typeface Times Roman 10.25/13 pt. *System* LaTeX 2_ε [TB]

A catalog record for this book is available from the British Library.

Library of Congress Cataloging in Publication Data
Schenck, Hal.
Computational algebraic geometry / Hal Schenck.
p. cm. – (London Mathematical Society student texts ; 58)
Includes bibliographical references and index.
ISBN 0-521-82964-X (hardback) – ISBN 0-521-53650-2 (pbk.)
1. Geometry, Algebraic – Data processing – Congresses. I. Title. II. Series.
QA564.S29 2003
516.3′5 – dc21 2003053074

ISBN 0 521 82964 X hardback
ISBN 0 521 53650 2 paperback

Contents

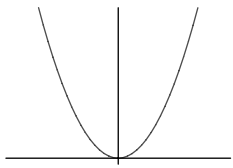
Chapter 1

Basics of Commutative Algebra

Somewhere early in our mathematical career we encountered the equation

$$f(x, y) = y - x^2 = 0,$$

and learned that the set of points in the plane satisfying this equation (the *zero locus* of f) is a parabola.



The natural generalization of this problem is to find the solutions to a system of polynomial equations, which is the realm of algebraic geometry. In this chapter we give a whirlwind tour of the basics of commutative algebra. We begin by studying the relationship between an ideal I in a polynomial ring R over a field k, and the set of common zeroes of the polynomials defining I. This object is called a *variety*, and denoted $V(I)$. We prove the Hilbert Basis Theorem, which shows that every ideal in R is finitely generated. Then we tackle the task of breaking a variety into simpler constituent pieces; this leads naturally to the concept of the primary decomposition of an ideal. You may want to warm up by browsing through the algebra appendix if you are hazy on the concepts of group, ring, ideal, and module.

Key concepts: Varieties and ideals, Hilbert Basis Theorem, associated primes and primary decomposition, Nullstellensatz, Zariski topology.

1.1 Ideals and Varieties

Let $R = k[x_1, \ldots, x_n]$ be a polynomial ring over a field k. *Affine n-space* k^n is the set of n-tuples of elements of k. An *affine variety* is the common zero locus of a collection of polynomials $f_i \in R$; the affine variety associated to the set $\{f_1, \ldots, f_m\}$ is written $V(f_1, \ldots, f_m)$. For example, $V(0) = k^n$ and $V(1)$ is the empty set. If you have not done this sort of thing before, try working Exercise A.2.5 in the appendix. Varieties arise quite naturally in many situations. Linear algebra is one special case (the polynomials are all of degree one); other examples of applied problems which involve solving polynomial systems range from computer vision and robot motion to understanding protein placement in cell walls. In fact, this sentence involves varieties: in PostScript, letters are drawn using Bezier cubics, which are parametric plane curves.

Exercise 1.1.1. [23] To define Bezier cubics, we need some terminology. A set $S \subseteq \mathbb{R}^n$ is called *convex* if the line segment between any two points $p, q \in S$ lies in S. Prove that if S is a convex subset of $\mathbb{R}^2$, and $\{p_0, \ldots, p_n\} \subset S$, then any *convex combination* $\sum_{i=0}^n t_i \cdot p_i$ with $t_i \geq 0$, $\sum_{i=0}^n t_i = 1$ is in S. For four points $p_i = (x_i, y_i)$ in $\mathbb{R}^2$ consider the parametric curve given by:

$$x = x_0(1-t)^3 + 3x_1t(1-t)^2 + 3x_2t^2(1-t) + x_3t^3$$
$$y = y_0(1-t)^3 + 3y_1t(1-t)^2 + 3y_2t^2(1-t) + y_3t^3$$

Prove that p_0 and p_3 lie on the parametric curve, and that the tangent line at p_0 goes through p_1 (chain rule flashback!). Given parametric equations, one might want to find the implicit equations defining an object. These equations can be found by computing a *Gröbner basis*, a technique we'll learn in Chapter 4. $\diamond$

One important observation is that the variety $V(f_1, \ldots, f_m)$ depends only on the ideal I *generated by* $\{f_1, \ldots, f_m\}$. This ideal consists of all linear combinations of $\{f_1, \ldots, f_m\}$ with polynomial coefficients; we write this as $I = \langle f_1, \ldots, f_m \rangle$. The variety $V(f_1, \ldots, f_m)$ depends only on I because if p is a common zero of $f_1, \ldots, f_m$, then p also zeroes out any polynomial combination

$$\sum_{i=1}^m g_i(x_1, \ldots, x_n) \cdot f_i(x_1, \ldots, x_n).$$

Thus, we can choose a different set of generators for I without altering $V(I)$. This is analogous to writing a linear transform with respect to different

choices of basis. Consider the ideal $I = \langle x^2 - y^2 - 3, 2x^2 + 3y^2 - 11\rangle$. Take a minute and find $V(I) \subseteq \mathbb{R}^2$. You can do this by just drawing a picture, but you can also do it by renaming x^2 and y^2 and using Gaussian elimination. Of course, this won't work in general. One of our goals will be to find a way to solve such problems systematically, for example, we might want to find a generating set for I where we can read off the solutions. For the ideal above, prove that $I = \langle x^2 - 4, y^2 - 1\rangle$. This is a set of generators from which it is certainly easy to read off $V(I)$!

Given an ideal J, we have the set of common zeroes $V(J)$, which is a geometric object. Conversely, given $S \subseteq k^n$, we can form the set $I(S)$ of all polynomials vanishing on S. It is easy to check (do so!) that this set is actually an ideal. If $S = V(J)$ for some ideal J, then it is natural to think that $J = I(V(J))$, but this is not the case. For example, if $J = \langle x^2\rangle \subseteq k[x]$, then $I(V(J)) = \langle x\rangle$. If $f \in J$ and $p \in V(J)$ then by definition $f(p) = 0$. Hence $f \in I(V(J))$, so there is a containment $J \subseteq I(V(J))$.

Exercise 1.1.2. Show that the process of passing between geometric and algebraic objects is inclusion reversing:

$$I_1 \subseteq I_2 \Rightarrow V(I_2) \subseteq V(I_1),$$

and

$$S_1 \subseteq S_2 \Rightarrow I(S_2) \subseteq I(S_1).$$

Use the set $S = \cup\{(0, i) | i \in \mathbb{Z}\} \subseteq \mathbb{R}^2$ to show that it can happen that $S_1 \subsetneq S_2$ but $I(S_1) = I(S_2)$. $\diamond$

For a ring element f and ideal I, a natural algebraic question is: "is $f \in I$?". If we can answer this question on *ideal membership*, then the exercise above shows that there is a geometric consequence: $V(I) \subseteq V(f)$, and we can restrict our search for points of $V(I)$ to points on $V(f)$. So one way to begin to get a handle on a variety is to understand the hypersurfaces on which it sits. Another natural thing to do is to try to break $V(I)$ up into a bunch of more manageable parts. What does "manageable" mean? Well, here is a first candidate:

Definition 1.1.3. *A nonempty variety V is irreducible if it is not the union of two proper subvarieties: $V \neq V_1 \cup V_2$ for any varieties V_i with $V_i \subsetneq V$.*

Theorem 1.1.4. *$I(V)$ is prime iff V is irreducible.*

Proof. First, we need to observe that if X is a *variety*, say $X = V(J)$, then $V(I(X)) = X$. As Exercise 1.1.2 shows, this need not be the case if we only assume X is some set. The inclusion $X \subseteq V(I(X))$ is obvious. By construction $J \subseteq I(X)$, so again by Exercise 1.1.2, $V(I(X)) \subseteq V(J) = X$. We're now ready to prove the theorem. Suppose $I(V)$ is prime but V is reducible with $V = V_1 \cup V_2$. Let $I_1 = I(V_1)$ and $I_2 = I(V_2)$. So there is a point $p \in V_2$ and $f \in I_1$ with $f(p) \neq 0$ (if every $f \in I_1$ vanishes on every $p \in V_2$, then $I_1 \subseteq I_2$, and we'd have a contradiction). By symmetry, there is a $g \in I_2$ and $q \in V_1$ with $g(q) \neq 0$. Clearly $fg \in I(V)$, with neither f nor g in $I(V)$, contradiction. We leave the other direction for the reader. □

As a last warm up before plunging into some proofs, we ask what happens geometrically when we perform standard operations on ideals.

Exercise 1.1.5. Recall that if I and J are ideals, then the sum $I + J = \{f + g | f \in I, g \in J\}$ is an ideal, as are $I \cdot J = \langle f \cdot g | f \in I, g \in J \rangle$ and $I \cap J$. Show that

$$V(I + J) = V(I) \cap V(J),$$

and that

$$V(I \cdot J) = V(I \cap J) = V(I) \cup V(J). \quad \diamond$$

1.2 Noetherian Rings and the Hilbert Basis Theorem

In the previous section we asked if it was possible to find a "nice" generating set for an ideal. For example, since $k[x]$ is a principal ideal domain, every ideal $I \subseteq k[x]$ has a single generator, which we can find by repeated use of the Euclidean algorithm. So the question of ideal membership is easily solved: once we have a generator for I, to see if $g \in I = \langle h \rangle$, we need only check that h divides g. If we work in rings where ideals can have minimal generating sets which are infinite, then finding a "nice" generating set or running a division algorithm is problematic, so we should begin by finding a sensible class of rings. In this book, *ring* always means *commutative ring with unit*.

Definition 1.2.1. *A ring is Noetherian if it contains no infinite ascending chains (infinite proper inclusions) of ideals, i.e. no sequences of the form*

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$$

A module is Noetherian if it contains no infinite ascending chains of submodules. Although this definition seems a bit abstract, it is in fact *exactly* the right thing to make all ideals finitely generated.

Lemma 1.2.2. *A ring is Noetherian iff every ideal is finitely generated.*

Proof. First, suppose every ideal is finitely generated, but that there exists an infinite ascending chain of ideals:

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$$

But (check!) $J = \bigcup_{i=1}^{\infty} I_i$ is an ideal. By assumption, J is finitely generated, say by $\{f_1, \ldots, f_k\}$, and each $f_i \in I_{l_i}$ for some l_i. So if $m = max\{l_i\}$ is the largest index, we have $I_{m-1} \subsetneq I_m = I_{m+1} = \cdots$, contradiction. Now suppose that I cannot be finitely generated. By taking a sequence of generators $\{f_1, f_2, \ldots\}$ for I with $f_i \notin \langle f_1, f_2, \ldots f_{i-1}\rangle$, we obtain

$$\langle f_1\rangle \subsetneq \langle f_1, f_2\rangle \subsetneq \langle f_1, f_2, f_3\rangle \subsetneq \cdots,$$

which is an infinite ascending chain of ideals. □

Exercise 1.2.3. Let M be a module. Prove the following are equivalent:

1. M contains no infinite ascending chains of submodules.
2. Every submodule of M is finitely generated.
3. Every nonempty subset Σ of submodules of M has a maximal element (Σ is a partially ordered set under inclusion).

This gives three equivalent conditions for a module to be Noetherian. ◇

Theorem 1.2.4 (Hilbert Basis Theorem). *If A is a Noetherian ring, then so is $A[x]$.*

Proof. Let I be an ideal in $A[x]$. By Lemma 1.2.2 we have to show that I is finitely generated. The set of lead coefficients of polynomials in I generates an ideal I' of A, which is finitely generated (A is Noetherian), say by $g_1, \ldots, g_k$. Now, for each g_i there is a polynomial

$$f_i \in I,\ f_i = g_i x^{m_i} + \text{ terms of lower degree in } x.$$

Let $m = max\{m_i\}$, and let I'' be the ideal generated by the f_i. Given any $f \in I$, we can chop it down by the elements of I'' until its lead term has degree less than m. Consider the *A-module M* generated by $\{1, x, \ldots, x^{m-1}\}$. It is finitely generated, hence Noetherian. So the submodule $M \cap I$ is also

Noetherian. Take generators $h_1, \ldots, h_j$, toss them in with the generators of I'', and we're done. □

Exercise 1.2.5. Prove that if A is Noetherian and M is a finitely generated A-module, then M is Noetherian. Hint: for some n, A^n surjects onto M. What would an infinite ascending chain of submodules of M imply? ◇

In a Noetherian ring, no matter how complicated an ideal I appears to be, there will always be a finite generating set for I. A field k is Noetherian, so the Hilbert Basis Theorem and induction tell us that the ring $k[x_1, \ldots, x_n]$ is Noetherian (of course, so is a polynomial ring over $\mathbb{Z}$ or any other principal ideal domain). Thus, our goal of finding a nice generating set for an ideal does make sense.

1.3 Associated Primes and Primary Decomposition

Throughout this book, we will dwell on the following theme: "To understand a complicated object, break it up into simpler objects". In this section we'll see how to write an ideal in a Noetherian ring in terms of "nice" ideals.

Exercise 1.3.1. (Decomposition I)

1. Prove that $\langle x^2 - 4, y^2 - 1\rangle$ can be written as the intersection of four *maximal* ideals in $\mathbb{R}[x, y]$. (Hint: what is the corresponding variety?)
2. Prove that $\langle x^2 - x, xy\rangle = \langle x\rangle \cap \langle x - 1, y\rangle$, hence is the intersection of a prime ideal and a maximal ideal in $\mathbb{R}[x, y]$. ◇

The two ideals in Exercise 1.3.1 are intersections of prime ideals (by Exercise A.2.6, maximal ideals are prime). By Theorem 1.1.4 we know that if X is an irreducible variety then $I(X)$ is prime. Since any variety can be written as a union of irreducible varieties, it seems natural to hope that any ideal is an intersection of prime ideals. As $\langle x^2\rangle \subseteq k[x]$ shows, this hope is vain. However, in a Noetherian ring, any ideal can be written as a finite intersection of irreducible ideals (an *irreducible decomposition*) or as a finite intersection of primary ideals (a *primary decomposition*). Warning: don't confuse an irreducible ideal with an irreducible variety. In fact, it might be good to review the definitions of irreducible and primary ideal at this point (Exercise A.2.5).

Lemma 1.3.2. *In a Noetherian ring R, any ideal is a finite intersection of irreducible ideals.*

Proof. Consider the set Σ consisting of ideals which may not be written as a finite intersection of irreducibles. Since R is Noetherian, Σ has a maximal element I'. But I' is reducible, so we can write $I' = I_1 \cap I_2$, and by assumption I_1 and I_2 are finite intersections (since they properly contain I', and I' is a maximal element of Σ), a contradiction. □

Lemma 1.3.3. *In a Noetherian ring R, irreducible ideals are primary.*

Proof. Let I be irreducible, and suppose $fg \in I$, with $f \notin I$. By passing to the quotient ring $A = R/I$, we only need to show that $g^m = 0$, for some m. There is a chain of ideals in A:

$$0 \subseteq ann(g) \subseteq ann(g^2) \subseteq \cdots,$$

where

$$ann(h) = \{e \in A | eh = 0\}.$$

Because A is Noetherian, there exists an n such that

$$ann(g^n) = ann(g^{n+1}).$$

Since the zero ideal is irreducible in A and $f \neq 0$, if we can show that $\langle g^n \rangle \cap \langle f \rangle = 0$, we'll be done. So suppose $a \in \langle f \rangle \cap \langle g^n \rangle$; $a \in \langle f \rangle$ implies $ag = 0$. But

$$a \in \langle g^n \rangle \Rightarrow a = bg^n \Rightarrow bg^{n+1} = 0 \Rightarrow bg^n = 0 \Rightarrow a = 0,$$

so indeed $\langle g^n \rangle \cap \langle f \rangle = 0$. □

Primary decompositions are generally used more often than irreducible decompositions, in fact, some books ignore irreducible decompositions completely. The treatment here follows that of [3]; it seems reasonable to include the irreducible decomposition since the proof is so easy! It turns out that primary ideals are very closely related to prime ideals. First, we need a definition:

Definition 1.3.4. *The radical of an ideal I (denoted $\sqrt{I}$) is the set of all f such that $f^n \in I$ for some $n \in \mathbb{N}$; I is radical if $I = \sqrt{I}$.*

Exercise 1.3.5. Prove that if Q is primary, then $\sqrt{Q} = P$ is a prime ideal, and P is the smallest prime ideal containing Q. We say that Q is *P-primary*. Show that if Q_1 and Q_2 are P-primary, so is $Q_1 \cap Q_2$. This is one reason for preferring primary decomposition to irreducible decomposition: the intersection of two irreducible ideals is obviously not irreducible. For the ideal $I = \langle x^2, xy \rangle$, show $\sqrt{I} = \langle x \rangle$ but I is not primary. ◇

A primary decomposition $I = \bigcap_{i=1}^{n} Q_i$ is *irredundant* if for each $j \in \{1, \ldots, n\}$

$$\bigcap_{i \neq j} Q_i \neq I$$

(there are no "extraneous" factors). By Exercise 1.3.5, we may assume that the radicals P_i of the Q_i are distinct; the P_i are called the *associated primes* of I. An associated prime P_i which does not properly contain any other associated prime P_j is called a *minimal* associated prime. The non-minimal associated primes are called *embedded* associated primes. The reason for this terminology is explained in the following example.

Example 1.3.6. Consider the two ideals

$$I_1 = \langle x^2, xy \rangle \text{ and } I_2 = \langle x^2 - x, xy \rangle.$$

Clearly $I_1 = \langle x^2, y \rangle \cap \langle x \rangle$, and $\langle x \rangle$, $\langle x^2, y \rangle$ are primary ideals. So I_1 has one minimal associated prime $\langle x \rangle$ and one embedded associated prime $\langle x, y \rangle$. By Exercise 1.1.5, $V(I \cap J) = V(I) \cup V(J)$. Thus,

$$V(I_1) = V(x) \cup V(x^2, y) = V(x) \cup V(x, y).$$

In the plane, $V(x, y)$ corresponds to the origin, which is "embedded in" the line $V(x)$. Notice that we can write

$$\langle x \rangle \cap \langle x^2, xy, y^2 \rangle = I_1 = \langle x^2, y \rangle \cap \langle x \rangle.$$

Verify that $\langle x^2, xy, y^2 \rangle$ is a primary ideal. This shows that the Q_i which appear in a primary decomposition are not unique. Let's ask the computer algebra package Macaulay 2 to check our work. Appendix A.3 describes how to get started with Macaulay 2; you should glance over the appendix (and, better still, try running the commands) before proceeding.

```
i1 : R=QQ[x,y]

o1 = R

o1 : PolynomialRing

i2 : intersect(ideal(x),ideal(x^2,x*y,y^2))
```

```
                    2
o2 = ideal (x*y, x )

o2 : Ideal of R

i3 : intersect(ideal(x),ideal(x^2,y))

                    2
o3 = ideal (x*y, x )

o3 : Ideal of R

i4 : o2==o3

o4 = true
```

In Macaulay 2, the command == tests for equality (of course, in this example we could see that the two ideals are equal, but sometimes it won't be so obvious). In Exercise 1.3.12 you'll prove that passing from I to $\sqrt{I}$ causes embedded components to disappear.

```
i5 : radical o2

o5 = ideal x
```

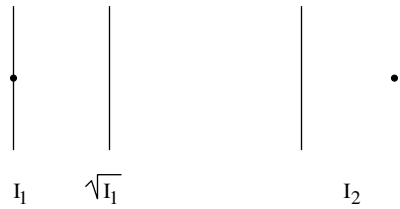
For the ideal I_2 we obtain a primary decomposition

$$I_2 = \langle x \rangle \cap \langle x - 1, y \rangle,$$

hence I_2 has two minimal associated prime ideals, and the primary components are actually prime already, so $\sqrt{I_2} = I_2$.

```
i6 : primaryDecomposition ideal(x^2-x,x*y)

o6 = {ideal (y, x - 1), ideal x}

o6 : List

i7 : (radical ideal(x^2-x,x*y))==ideal(x^2-x,x*y)

o7 = true
```

The zero loci of *all* the primary components of I_1 and I_2 are shown below; the pictures hint that while varieties capture all the geometry of the minimal primes, they forget about embedded primes. Understanding the entire set of primary components of an ideal is part of the motivation for studying *schemes* [34].



Why bother worrying about the embedded primes? Well, for one thing, they carry important information about I. In Chapter 4, we'll learn how to define an order on monomials in a polynomial ring, so that we can define the lead monomial of a polynomial. The set $in(I)$ of all lead monomials of elements of I generates an ideal, and will often have embedded primes *even if I does not*. So what? Well, the point is that many numerical invariants are the same for I and for $in(I)$, but $in(I)$ is often much easier to compute. Punchline: embedded primes matter.

Next we consider how to actually find associated primes and a primary decomposition. A key tool is the operation of *ideal quotient*:

Definition 1.3.7. *Let R be a ring and I, J ideals of R. Then the ideal quotient* $I : J = \{f \in R | f \cdot J \subseteq I\}$.

As usual, you should take a minute and scrawl down a proof that $I : J$ is an ideal (it really will fit in the margin!).

Lemma 1.3.8. *If Q is a P-primary ideal, and $f \in R$, then*

$$\begin{array}{ll} f \in Q \Rightarrow & Q : f = R \\ f \notin Q \Rightarrow & Q : f \text{ is } P\text{-primary} \\ f \notin P \Rightarrow & Q : f = Q \end{array}$$

Proof. The first statement is automatic, and for the second, if $fg \in Q$, then since $f \notin Q$ we must have $g^n \in Q$ so $g \in P$;

$$Q \subseteq (Q : f) \subseteq P, \text{ so } \sqrt{Q : f} = P,$$

and it is straightforward to show $Q : f$ is P-primary. For the last statement, if $fg \in Q$, then $f^n \notin Q$ (else $f \in P$) so $g \in Q$ and $Q : f \subseteq Q$. $\square$

Exercise 1.3.9. (Distributivity).

1. Show that if a prime ideal $P = P_1 \cap P_2$, then P is one of the P_i.
2. Show that $(I_1 \cap I_2) : f = (I_1 : f) \cap (I_2 : f)$.
3. Show that $\sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2}$. $\diamond$

Lemma 1.3.8 and Exercise 1.3.9 show that in a Noetherian ring, the associated primes of an ideal are independent of the decomposition – in other words, even though the Q_i are not unique, the P_i are! To see this, write

$$I = \bigcap_{i=1}^{n} Q_i,$$

which we can assume is irredundant by the remarks following Exercise 1.3.5. Now, since the decomposition is irredundant, for any j we can find $f_j \notin Q_j$ but which is in all the other Q_i, $i \neq j$. By Lemma 1.3.8 and Exercise 1.3.9, $I : f_j = Q_j : f_j$ is P_j-primary. In particular $\sqrt{Q_j : f_j} = P_j$, which proves:

Lemma 1.3.10. *The associated primes of I are contained in the set $\{\sqrt{I : f} \mid f \in R\}$.*

On the other hand, if P is a prime in the set $\{\sqrt{I : f} \mid f \in R\}$, then it must be associated to I (hint: Exercise 1.3.9).

We can also define the associated primes of a module M. In this case, the set of associated primes $Ass(M)$ consists of primes P such that P is the annihilator of some $m \in M$.

Exercise 1.3.11. ([28], Proposition 3.4) Let M be an R-module, and $S = \{I \subseteq R | I = ann(m), \text{ some } m \in M\}$. Prove that a maximal element of S is prime. $\diamond$

By the previous exercise, the union of the associated primes of M consists precisely of the set of all zero divisors on M. One caution – the associated primes of the module R/I are usually referred to as the associated primes of the ideal I. This seems confusing at first, but is reasonable in the following context: if R is a domain, then no nonzero element of R has nontrivial annihilator. In particular, if $I \subseteq R$ a domain, then *as a module* I has no

interesting associated primes. For example, let $R = k[x, y]$, and consider the R-module $M = R/I_1$ with I_1 as in Example 1.3.6. The annihilator of $x \in M$ is $\langle x, y\rangle$, and the annihilator of $y \in M$ is $\langle x\rangle$, so $\{\langle x\rangle, \langle x, y\rangle\} \subseteq Ass(M)$. Is this everything?

Exercise 1.3.12. (Decomposition II).

1. Prove that $\sqrt{I}$ is the intersection of the minimal primes of I.
2. Find (by hand) a primary decomposition for the radical of $\langle y^2 + yz, x^2 - xz, x^2 - z^2\rangle$
3. Find a primary decomposition for $\langle xz - y^2, xw - yz\rangle$ as follows: First, observe that when x and y both vanish then both generators of the ideal vanish, so $\langle xz - y^2, xw - yz\rangle \subseteq \langle x, y\rangle$. Use ideal quotient to strip off $\langle x, y\rangle$. You should find that $\langle xz - y^2, xw - yz\rangle : \langle x, y\rangle = \langle xz - y^2, xw - yz, z^2 - yw\rangle$. It turns out (Deus ex machina!) that $J = \langle xz - y^2, xw - yz, z^2 - yw\rangle$ is the kernel of the map

$$R = k[x, y, z, w] \longrightarrow k[s^3, s^2t, st^2, t^3]$$

given by

$$x \to s^3, y \to s^2t, z \to st^2, w \to t^3.$$

Since $R/J \simeq k[s^3, s^2t, st^2, t^3] \subseteq k[s, t]$ and a subring of a domain is a domain, we see that J is a prime ideal, and we have found a primary decomposition $\langle xz - y^2, xw - yz\rangle = J \cap \langle x, y\rangle$. $\diamond$

1.4 The Nullstellensatz and Zariski Topology

Varieties are geometric objects. Given two geometric objects X and Y, it is very natural to ask if there is a map $f : X \to Y$. In analysis we might stipulate that f be continuous or differentiable; the notion of continuity depends on having a *topology*. When X and Y are varieties, one reasonable class of maps to consider are maps which are polynomial (or at least "locally" polynomial). It turns out that there is a specific topology which gives us the right language to study these maps. First, some terminology:

Definition 1.4.1 (Topology). *A topology on a set X is a collection $\mathcal{U}$ of subsets of X which satisfy:*

1. *$\emptyset$ and X are in $\mathcal{U}$.*
2. *$\mathcal{U}$ is closed under finite intersection.*
3. *$\mathcal{U}$ is closed under arbitrary union.*

Members of $\mathcal{U}$ are called the *open sets* of the topology. There is an equivalent formulation using closed sets – a finite union of closed sets is closed, as is any intersection of closed sets. By Exercise 1.1.5, a finite union of affine varieties is itself an affine variety, as is any intersection of affine varieties. This shows that we can define a topology on k^n in which the closed sets are affine varieties. This topology is called the *Zariski topology*, and for this reason the terms affine variety and *Zariski closed* set are used interchangeably. If X is a variety in k^n, then X is endowed with the *subspace topology* – an open set in X is the intersection of X with an open set in k^n. Even though we may not always say it, we'll always have in mind the case where k is algebraically closed (despite the fact that the computations we make are over $\mathbb{Q}$ or a finite field). In this book, when you see $\mathbb{A}^n_k$ think "k^n with Zariski topology", and when you see the word "point", think of a point in the usual topology. If $U \subseteq k^n$ is the complement of the vanishing locus of a polynomial f, then U is called a *distinguished open set*, and written U_f.

Exercise 1.4.2. Show that the distinguished open sets U_f are a *basis* for the Zariski topology on $\mathbb{A}^n_k$: every Zariski open set can be written as a union of distinguished open sets. $\diamond$

The Zariski topology is *quasicompact*: any cover of $\mathbb{A}^n_k$ has a finite subcover. To see this, let $\{U_i\}_{i\in S}$ be a cover of $\mathbb{A}^n_k$ which does not admit a finite subcover. The previous exercise shows that we may suppose the U_i are of the form U_{f_i}. By assumption we can find an infinite sequence $U_{f_1} \subsetneq (U_{f_1} \cup U_{f_2}) \subsetneq \cdots$. Then taking complements of these sets yields an infinite descending chain of varieties $V(f_1) \supsetneq V(f_1, f_2) \supsetneq \cdots$, which is impossible since $k[x_1, \ldots, x_n]$ is Noetherian. A similar argument shows that any subvariety of $\mathbb{A}^n_k$ is quasicompact.

Polynomial functions on k^n obviously restrict to give polynomial functions on a variety $X \subseteq k^n$, and any two polynomials which differ by an element of $I(X)$ define the same function on X. So polynomial functions on an affine variety X correspond to elements of the *coordinate ring* $R/I(X)$. It will be useful to have a local description for this; the reason is that later in the book we shall be constructing objects by patching together *Zariski open* subsets of affine varieties.

Definition 1.4.3. *Let U be an open subset of an affine variety $X \subseteq \mathbb{A}^n_k$, k algebraically closed. A function f is* regular *at a point $p \in U$ if there is a Zariski open neighborhood V of p in X such that $f = \frac{g}{h}$ on V, with $g, h \in k[x_1, \ldots, x_n]/I(X)$, and $h(p) \neq 0$. A function is regular on an open set U if it is regular at every point of U.*

A *regular* map is a map defined by regular functions. Two affine varieties X and Y are isomorphic if there exist regular maps $i : X \longrightarrow Y$ and $j : Y \longrightarrow X$ which compose to give the identity.

Exercise 1.4.4. Prove that affine varieties X and Y are isomorphic iff their coordinate rings are isomorphic. (Hint: section 5.4 of [23]). $\diamond$

We'll see shortly that if k is algebraically closed, then the *ring* of regular functions on a distinguished open subset U_f of an affine variety X is isomorphic to $k[x_1, \ldots, x_n, y]/\langle I(X), yf - 1\rangle$. To prove this, we need to make a detour back to algebra and understand better the relation between J and $I(V(J))$. In §1, we found that $J \subseteq I(V(J))$, and saw that this containment could be proper. From the definition of the radical, $\sqrt{J} \subseteq I(V(J))$. The precise relation between J and $I(V(J))$ follows by first answering the following innocuous question:

When is the variety of an ideal empty?

It is clear that if $1 \in I$ then $V(I)$ is empty, but notice that over a field which is not algebraically closed, $V(I)$ can be empty even if I is a proper ideal (e.g. $\langle x^2 + 1\rangle \subseteq \mathbb{R}[x]$). However, there is a second beautiful theorem of Hilbert:

Theorem 1.4.5 (Weak Nullstellensatz). *If k is algebraically closed and $V(I)$ is empty, then $1 \in I$.*

To prove the Nullstellensatz properly requires a fair amount of work and is done in almost all books (save this one!) on algebraic geometry; there are nice readable treatments in Chapter 2 of [78] and Chapter 4 of [23], and [28] offers five (!) different proofs. Let's use the Nullstellensatz to answer an earlier question we had:

Theorem 1.4.6 (Strong Nullstellensatz). *If k is algebraically closed and $f \in I(V(I)) \subseteq k[x_1, \ldots, x_n] = R$, then $f^m \in I$, for some m. More tersely put, $\sqrt{I} = I(V(I))$.*

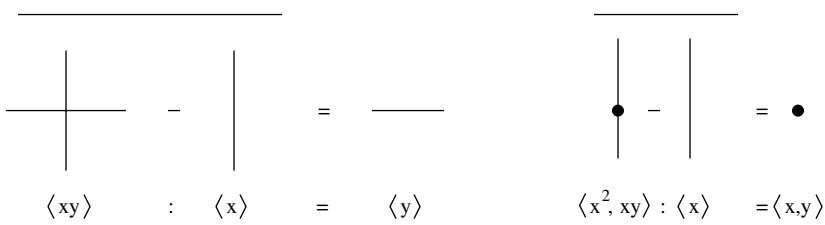
Proof. (The "trick of Rabinowitch"). Given $I = \langle f_1, \ldots, f_j\rangle \subseteq R$ and $f \in I(V(I))$, put $I' = \langle I, 1 - y \cdot f\rangle \subseteq R[y]$. Check that $V(I')$ is empty. So by the weak Nullstellensatz, we can write $1 = \sum a_i \cdot f_i + g(1 - y \cdot f)$. Now just plug in $y = 1/f$ to obtain $1 = \sum a_i(x_1, \ldots, x_n, 1/f) \cdot f_i$, and multiply by a high enough power of f to clean out the denominators. $\square$

With the Nullstellensatz in hand, we can show that if k is algebraically closed, then the ring of regular functions on a distinguished open subset $X_f = U_f \cap X$ of an *irreducible* affine variety $X \subseteq \mathbb{A}^n_k$ is isomorphic to $k[x_1, \ldots, x_n, y]/\langle I(X), yf - 1\rangle$. Let g be a regular function on X_f. By definition, for each point $p \in X_f$ there is a Zariski open neighborhood U_p of p with $g = \frac{h_p}{k_p}$ on U_p, with h_p and k_p in $R/I(X)$ and k_p nonzero at p. By Exercise 1.4.2 and quasicompactness, we can assume that the cover of X_f is actually finite and given by distinguished open sets $X_{f_i} = X \cap U_{f_i}$, $i = 1 \ldots j$ with $g = \frac{h_i}{k_i}$ on X_{f_i}. The k_i cannot simultaneously vanish at any point $p \in X_f$, since p lies in some X_{f_m}, and $k_m \neq 0$ on X_{f_m}. So $V(k_1, \ldots, k_j) \cap X_f$ is empty, hence $V(k_1, \ldots, k_j) \cap X \subseteq V(f)$. By the Nullstellensatz, there exist l_i with $f^m = \sum_{i=1}^{j} l_i k_i$ (the equations defining $I(X)$ are implicit in this expression, because the k_i are defined modulo $I(X)$). Since $\frac{h_i}{k_i} = \frac{h_j}{k_j}$ on $X_{f_i} \cap X_{f_j}$, on the common intersection of *all* the X_{f_i} we can write

$$f^m \cdot g = \sum_{i=1}^{j} l_i k_i \frac{h_i}{k_i}.$$

By Lemma 1.3.8 and Lemma 1.4.7 (below), the common intersection of the X_{f_i} is Zariski dense (we assumed X irreducible). Thus, the expression above is actually valid on all of X_f, so we can write g as an element of $R/I(X)$ over f^m, as claimed. Setting $f = 1$ shows that the ring of functions regular everywhere on a variety $X \subseteq \mathbb{A}^n_k$ is simply $R/I(X)$. The hypothesis that X is irreducible can be removed, but the proof is a bit more difficult: see [53], II.2.2.

For any set $S \subseteq \mathbb{A}^n_k$, Exercise 1.1.2 shows that $V(I(S))$ is the smallest variety containing S. So in the Zariski topology $V(I(S))$ is the *closure* of S; we write $\overline{S}$ for $V(I(S))$ and call $\overline{S}$ the *Zariski closure* of S. For $S \subseteq \mathbb{R}^2$ as in Exercise 1.1.2, $\overline{S} = V(x)$. A second nice application of the Nullstellensatz relates the Zariski closure of a set and the ideal quotient. Lemma 1.3.8 tells us that ideal quotient can be used to pull apart the irreducible pieces of an ideal. As an example, compute $\langle xy\rangle : \langle x\rangle$ and $\langle x^2, xy\rangle : \langle x\rangle$. What you should see is the following:



The picture on the left makes perfect sense, but the picture on the right is meant to make you think. How does it relate to primary decomposition?

Lemma 1.4.7.

$$\overline{V(I) - V(J)} \subseteq V(I : J),$$

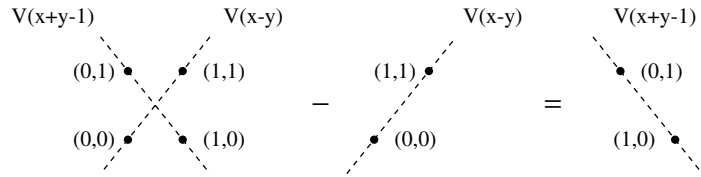
and if k is algebraically closed and I is radical, then this is an equality.

Proof. By Exercise 1.1.2, we need to show $I : J \subseteq I(V(I) - V(J))$. So let $f \in I : J$, and take $p \in V(I) - V(J)$. Since $p \notin V(J)$, there is a $g \in J$ with $g(p) \neq 0$. From the definition of ideal quotient, $f \cdot g$ is in I, and so $p \in V(I)$ means $f(p) \cdot g(p) = 0$, and we're over a field, so this shows that $\overline{V(I) - V(J)} \subseteq V(I : J)$. For the second part, since k must be algebraically closed, you can guess that the Nullstellensatz plays a role. Figure it out! □

Example 1.4.8. Let $S = \{p_1, \ldots, p_4\} = \{(0,0), (0,1), (1,0), (1,1)\} \subseteq \mathbb{A}_k^2$ be a set of four points in the affine plane. Then

$$I(S) = \bigcap_{i=1}^{4} I(p_i) = \langle x^2 - x, y^2 - y \rangle.$$

To remove the points lying on the line $V(x - y)$, we need to form $I(S) : \langle x - y \rangle$, the result should be the ideal of the two remaining points.




```
i8 : ideal(x^2-x,y^2-y):ideal(x-y)

                              2
o8 = ideal (x + y - 1, y  - y)

o8 : Ideal of R
```

We've been computing radicals, intersections, quotients, and primary decompositions using Macaulay 2, with no discussion of the underlying algorithms. Chapter 4 gives an overview of Gröbner basis techniques, which is the