THE ALGEBRAIC GEOMETRY DICTIONARY FOR BEGINNERS

ALICE MARK

Abstract. This paper is a simple summary of the first most basic definitions in Algebraic Geometry as they are presented in Dummit and Foote ([1]), with a focus on establishing a dictionary between algebra and geometry. In particular this dictionary helps in visualizing certain computations that take place in polynomial rings. Among these are decomposing ideals in a manner analogous to prime factorization, and determining when coordinate rings are integrally closed.

Contents

1. Defining the dictionary

This section very closely follows the first two sections of Chapter 15 of Dummit & Foote [1] with some omission and reordering. Some of the ideas also come from [2]. Everything is presented at the level of a student who has had a first course in Abstract Algebra.

The first place in which most people encounter a geometric interpretation of an algebraic object is in the Fundamental Theorem of Algebra:

Theorem 1.1 (Fundamental Theorem of Algebra)**.** *Let k be a field with algebraic closure $\bar{k}$. Then if $f(x) \in k[x]$ is a polynomial, f has exactly n roots in $\bar{k}$.*

This theorem establishes a correspondence between algebra (the polynomial ring $k[x]$), and geometry (the set of roots in one dimensional affine space over k). The polynomial ring in n variables over a field k is closely associated with n-dimensional affine space $A^n(k)$, since a polynomial in the ring can be evaluated at a point in the space. A solution to a polynomial is a point at which it evaluates to zero.

Definition 1.2. Let $S \subseteq k[x_1, \ldots, x_n]$. Then

$$\mathcal{Z}(S) = \{(a_1, \ldots, a_n) \in A^n(k) | f(a_1, \ldots, a_n) = 0 \text{ for all } f \in S\}$$

A set of the form $\mathcal{Z}(S)$ for some S is called an *algebraic set*.

Date: August 2008.

The set of roots of a polynomial in one variable is an algebraic set.

$\mathcal{Z}$ is a surjective map from the power set of $k[x_1, \ldots, x_n]$ to the set of algebraic subsets of $A^n(k)$. This map reverses inclusions, since if more polynomials are added to a set of polynomials there can be no new points at which they are all zero, and there could be fewer. Using this fact, we can show the following:

Lemma 1.3. *Let $S \subseteq k[x_1 \ldots, x_n]$. If I is the ideal generated by S, then $\mathcal{Z}(S) = \mathcal{Z}(I)$.*

Proof. We already have $\mathcal{Z}(I) \subseteq \mathcal{Z}(S)$, since $S \subseteq I$. Now suppose $(a_1, \ldots, a_n) \in \mathcal{Z}(S)$. Every element f of I is a finite linear combination of elements of S, so $f(a_1, \ldots, a_n) = 0$, so $\mathcal{Z}(S) \subseteq \mathcal{Z}(I)$. Therefore $\mathcal{Z}(S) = \mathcal{Z}(I)$. □

This shows that when $\mathcal{Z}$ is restricted to the set of ideals of $k[x_1, \ldots, x_n]$, it remains surjective. It is not injective: $\mathcal{Z}(x) = \mathcal{Z}(x^2) = \{0\}$ in $\mathbb{R}$, but x and x^2 generate different ideals in $\mathbb{R}[x]$.

Example 1.4. Not every subset of n-dimensional affine space is an algebraic set. In 1-dimension, the algebraic sets are the finite sets, the empty set, and the whole space. This is because k is a field, so $k[x]$ is a PID, so every ideal is generated by only one polynomial. Therefore every algebraic set $\mathcal{Z}(S)$ is equal to $\mathcal{Z}(f)$ for some polynomial $f \in k[x]$. f can only have finitely many roots. In the special cases where f is a constant polynomial, $\mathcal{Z}(f)$ is either k or $\emptyset$, depending on whether f is zero or not.

$\mathcal{Z}$ gives us a way to interpret algebra geometrically. We still need a way to interpret geometry algebraically.

Definition 1.5. Let $A \subseteq A^n(k)$. Then

$$\mathcal{I}(A) = \{f \in k[x_1, \ldots, x_n] | f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in A\}$$

Proposition 1.6. *$\mathcal{I}(A)$ is an ideal for all $A \subseteq A^n(k)$*

Proof. The zero polynomial is in $\mathcal{I}(A)$ for any A, so $\mathcal{I}(A) \neq \emptyset$. Suppose $f, g \in \mathcal{I}(A)$, $h \in k[x_1 \ldots, x_n]$. Then for any $(a_1 \ldots, a_n) \in A$, we have $(f - hg)(a_1 \ldots, a_n) = f(a_1 \ldots, a_n) - h(a_1, \ldots, a_n)g(a_1, \ldots, a_n) = 0$, so $f - hg \in \mathcal{I}(A)$. Therefore $\mathcal{I}(A)$ is an ideal. □

$\mathcal{I}$ is not surjective from the power set of $A^n(k)$ to the set of ideals of $k[x_1, \ldots, x_n]$: In $\mathbb{R}[x]$, the ideal $(x^2 + 1)$ is not in the image of $\mathcal{I}$. This is because $x^2 + 1$ has no roots in $\mathbb{R}$.

Here are some basic, easily verified, and useful facts, each with a one sentence explanation by way of proof:

Proposition 1.7. *For all of the following, I and J are ideals with $I \subseteq J \subseteq k[x_1, \ldots, x_n]$, (we only need to consider ideals, because of Lemma 1.3) and $A \subseteq B \subseteq A^n(k)$.*

(1) $\mathcal{Z}(J) \subseteq \mathcal{Z}(I)$ and $\mathcal{I}(B) \subseteq \mathcal{I}(A)$.
(2) $\mathcal{Z}(I \cup J) = \mathcal{Z}(I) \cap \mathcal{Z}(J)$, and $\mathcal{I}(A \cup B) = \mathcal{I}(A) \cap \mathcal{I}(B)$.
(3) $\mathcal{Z}(0) = A^n(k)$ and $\mathcal{Z}(k[x_1, \ldots, x_n]) = \emptyset$. Also $\mathcal{I}(\emptyset) = k[x_1, \ldots, x_n]$.
(4) $\mathcal{Z}(I) \cup \mathcal{Z}(J) = \mathcal{Z}(IJ) = \mathcal{Z}(I \cap J)$.

Proof. (1) We have already used the first fact, but here is a more precise proof of it: Let $(a_1, \ldots, a_n) \in \mathcal{Z}(J)$, and let $f \in I$. Then $f \in J$, so $f(a_1, \ldots, a_n) = 0$, so $(a_1, \ldots, a_n) \in \mathcal{Z}(I)$.

For the second, if $f \in \mathcal{I}(B)$, $f(a_1, \ldots, a_n) = 0$ for $(a_1, \ldots, a_n) \in B \subseteq A$, so $f \in \mathcal{I}(A)$.

(2) $\mathcal{Z}(I \cup J) \subseteq \mathcal{Z}(I) \cap \mathcal{Z}(J)$ and $\mathcal{I}(A \cup B) \subseteq \mathcal{I}(A) \cap \mathcal{I}(B)$ because of (1).

If $(a_1, \ldots, a_n) \in \mathcal{Z}(I) \cap \mathcal{Z}(J)$, then for all $f \in I$ and all $g \in J$, $f(a_1, \ldots, a_n) = 0$ and $g(a_1, \ldots, a_n) = 0$, so $(a_1, \ldots, a_n) \in \mathcal{Z}(I \cup J)$.

If $f \in \mathcal{I}(A) \cap \mathcal{I}(B)$, then for all $(a_1, \ldots, a_n) \in A$, and all $(b_1, \ldots, b_n) \in B$, $f(a_1, \ldots, a_n) = 0$ and $f(b_1, \ldots, b_n) = 0$, so $f \in \mathcal{I}(A \cup B)$.

(3) The zero polynomial is zero on all of $A^n(k)$.

$1 \in k[x_1, \ldots, x_n]$, and the constant polynomial 1 never evaluates to zero.

$1 \in \mathcal{I}(\emptyset)$, and 1 is a unit so it generates the whole ring $k[x_1, \ldots, x_n]$.

(4) $IJ \subseteq I$ and J so by (1), $\mathcal{Z}(I) \cup \mathcal{Z}(J) \subseteq \mathcal{Z}(IJ)$. The same argument works with $I \cap J$ substituted for IJ.

If $(a_1, \ldots, a_n) \in \mathcal{Z}(IJ)$, then $(fg)(a_1, \ldots, a_n) = 0$ whenever $f \in I$, $g \in J$ which means $(a_1, \ldots, a_n) \in \mathcal{Z}(I)$ or $\mathcal{Z}(J)$.

$IJ \subseteq I \cap J$ so by (1), $\mathcal{Z}(I \cap J) \subseteq \mathcal{Z}(IJ) - \mathcal{Z}(I) \cup \mathcal{Z}(J)$.

□

Now it makes sense to return to the question of when $\mathcal{Z}$ and $\mathcal{I}$ are surjective and injective.

Theorem 1.8. *$\mathcal{I}$ restricted to the set of algebraic sets and $\mathcal{Z}$ restricted to the image of $\mathcal{I}$ are both bijections, and they are inverses of each other.*

Proof. To see that $\mathcal{I}$ restricted to the image of $\mathcal{Z}$ is surjective, pick $\mathcal{I}(A)$ in the image of $\mathcal{I}$. Let $V = \mathcal{Z}(\mathcal{I}(A))$. If $f \in \mathcal{I}(A)$ then $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in V$, so $f \in \mathcal{I}(V)$, so $\mathcal{I}(A) \subseteq \mathcal{I}(V)$. $A \subseteq V$, so $\mathcal{I}(V) \subseteq \mathcal{I}(A)$. Therefore $\mathcal{I}(A) = \mathcal{I}(V)$. V is an algebraic set, so $\mathcal{I}$ restricted to the set of algebraic sets is surjective onto the image of $\mathcal{I}$ without the restriction.

We already have that $\mathcal{I}$ is injective, so $\mathcal{I}$ is a bijection between the set of algebraic sets and ideals of the form $\mathcal{I}(A)$.

Now, let $V = \mathcal{Z}(I)$ be an algebraic set, where $I \subseteq k[x_1, \ldots, x_n]$ is an ideal. If $f \in I$, $f(a_1, \ldots, a_n) = 0$ for $(a_1, \ldots, a_n) \in V$, so $f \in \mathcal{I}(V)$. Then $I \subseteq \mathcal{I}(V)$, so $\mathcal{Z}(\mathcal{I}(V)) \subseteq \mathcal{Z}(I)$. If $(a_1, \ldots, a_n) \in V$, then $f(a_1, \ldots, a_n) = 0$ for $f \in \mathcal{I}(V)$, so $(a_1, \ldots, a_n) \in \mathcal{Z}(\mathcal{I}(V))$. Therefore $\mathcal{Z}$ restricted to the image of $\mathcal{I}$ is surjective. Furthermore, since $\mathcal{Z}(\mathcal{I}(V)) = V$ if V is an algebraic set, $\mathcal{Z}$ is the inverse of $\mathcal{I}$. □

Definition 1.9. An algebraic set is called *reducible* if it can be written as the union of proper algebraic subsets. An algebraic set that is not reducible is called a *variety*.

There is an associated algebraic idea of an irreducible ideal, which is kind of like a prime ideal.

Definition 1.10. An ideal I is called *irreducible* if it cannot be written as the intersection of two ideals in which it is properly contained.

All prime ideals are irreducible, since if $P \subset R$ is a prime ideal with $P = Q_1 \cap Q_2$, then $Q_1 Q_2 \subseteq P$. If P is properly contained in Q_1, pick $q_1 \in Q_1 - P$. Then $q_1 q_2 \in Q_1 Q_2 \subseteq P$ for all $q_2 \in Q_2$, but since P is prime this implies $q_2 \in P$, so $Q_2 = P$.

It would be nice to know how the dictionary works when it comes to irreducible varieties. To explore this further, we need a few more tools.

Definition 1.11. An ideal I is in a commutative ring with 1 is called *primary* if whenever $ab \in I$ either $a \in I$ or $b^n \in I$ for some n.

Lemma 1.12. *In a Noetherian ring, irreducible ideals are primary.*

Proof. Take an irreducible ideal I and an element $ab \in I$. If $b \notin I$, construct an ascending chain of ideals $A_i = \{x \in R | a^i x \in I\} \subseteq A_{i+1}$. By the ACC, this stabilizes at some n. If $a^n x + y \in ((a^n) + I) \cap ((b) + I)$ for some $x \in R$, $y \in I$, then $a^{n+1}x + ay \in I$, since $(ab) + I = I$. But $y \in I$, so $a^{n+1}x \in I$, so $x \in A^{n+1} = A_n$, so $a^n x \in I$, so $a^n x + y \in I$. Therefore $I = ((a^n) + I) \cap ((b) + I)$.

$I \subset (b) + I$ properly since $b \notin I$, so since I is irreducible and $I = (a^n) + I$, $a^n \in I$. □

Definition 1.13. An ideal I has a *primary decomposition* if it can be written as the intersection of finitely many primary ideals. The primary decomposition is called *minimal* if none of the primary ideals is contained in any other.

Proposition 1.14. *Every proper ideal in a Noetherian ring R is a finite intersection of irreducible ideals.*

Proof. This is sort of like an inductive proof. Let $\mathcal{A}$ be the set of ideals in R that don't have a primary decomposition. If $\mathcal{A}$ is nonempty, it has a maximal element I by the ACC, which cannot itself be irreducible. Then I is a proper intersection of two ideals $I = J \cap K$. But $J, K \notin \mathcal{A}$, so J and K both have primary decompositions. The intersection of these primary decompositions is itself a primary decomposition for I, so $\mathcal{A}$ is empty. □

Definition 1.15. Let I be an ideal in the commutative ring with 1, R. Then the *radical* of I, $radI$ is the set of all elements $r \in R$ such that $r^n \in I$ for some n. $rad(0)$ is the set of all nilpotent elements of R and is called the *nilradical* of R. I is called a *radical ideal* if $I = radI$.

The following three facts follow immediately from the definition, but are very important:

(1) $radI$ is an ideal for any I.
    This is because $0 \in radI$, so $radI \neq \emptyset$. If $r, s \in radI$, $t \in R$ then $r^n \in I$, and $s^m \in I$ for some $m, n \in \mathbb{N}$, then $(r - st)^{m+n} \in I$, since every term in the binomial expansion is either a multiple of r^n or s^m.
(2) $I \subseteq radI$.
(3) $(radI)/I$ is the nilradical of R/I.
    This is because if $r + I \in (radI)/I$, then $r \in radI$, sor$^n \in I$ for some n. $(r + I)^n = r^n + I = I$.

Definition 1.16. The polynomial ring $k[x_1, \ldots, x_n]$ is the coordinate ring of the space[1] $A^n(k)$. For a variety V, the coordinate ring of V is $k[V] = k[x_1, \ldots, x_n]/\mathcal{I}(V)$. $k[V]$ is a ring of k valued functions on V, since for f and $g \in k[x_1, \ldots, x_n]$, $\bar{f} \sim \bar{g} \in k[V]$ if $f|_V = g|_V$.

Proposition 1.17. *If V is an algebraic set, $\mathcal{I}(V)$ is always a radical ideal.*

[1]The topology on $A^n(k)$ is the one where the closed sets are the algebraic sets.

Proof. If $f^n \in \mathcal{I}(V)$ for some $f \in k[x_1, \ldots, x_n]$ then $f^n(a_1, \ldots, a_n) = 0$ for $(a_1, \ldots, a_n \in V$. But then $f(a_1, \ldots, a_n) = 0$ since f is $k-$valued. Therefore $f \in \mathcal{I}(V)$, so $\mathcal{I}(V)$ is a radical ideal. □

Now we have what we need to prove the following:

Proposition 1.18 (This is exercise 15 on page 689 of [1])**.** *Suppose $V \subseteq A^n(k)$ is an algebraic set with $\mathcal{I}(V) = (f)$ (note that this means $V = \mathcal{Z}(f)$) for some nonconstant polynomial f. Then V is an irreducible variety if and only if f is irreducible.*

Proof. First suppose f is irreducible but $V = U \cup W$, where U and W are algebraic sets, and both are properly contained in V (so neither one is empty). Then neither U nor W is contained in the other. Since $\mathcal{I}$ reverses inclusions and is injective on the set of algebraic sets, $\mathcal{I}(U)$ and $\mathcal{I}(W)$ are not equal, both properly contain $(f) = \mathcal{I}(V)$, and neither is contained in the other. $\mathcal{I}(U)$ and $\mathcal{I}(W)$ have minimal primary decompositions $\bigcap Q'_i$ and $\bigcap Q''_j$ respectively. Since neither ideal is contained in the other and both properly contain (f), their intersection $\bigcap Q'_i \cap \bigcap Q''_j$, when reduced (by removing any ideal in the decomposition that is contained in any other) has at least two ideals. But this is a contradiction since (f) is irreducible. Therefore if f is irreducible, so is V.

Now suppose V is irreducible and $(f) = I \cap J$. Then $V = \mathcal{Z}(f) = \mathcal{Z}(I \cap J) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$. Since V is irreducible, $\mathcal{Z}(I) = V$ or $\mathcal{Z}(J) = V$. WLOG $\mathcal{Z}(I) = V$, so $I \subseteq \mathcal{I}(\mathcal{Z}(I)) = \mathcal{I}(V) = (f)$, so (f) is irreducible. Therefore if V is irreducible, so is f. □

In the second half of the proof, it would be nice to be able to argue that $\mathcal{I}(\mathcal{Z}(I)) = I$ because I is a radical ideal. It is not true in general, however, that $\mathcal{I}$ surjects onto the set of radical ideals. For example, take $g = x^2 + 1 \in \mathbb{R}[x]$, $\mathcal{Z}(g) = \emptyset \subset \mathbb{R}$, so $\mathcal{I}(\mathcal{Z}(g)) = \mathbb{R}[x]$. Indeed, the radical ideal (g) does not arise as the ideal of any subset of $\mathbb{R}$. Any such set would be a subset of $\mathcal{Z}(g) = \emptyset$.

Now suppose that $g \in k[x]$ is some separable polynomial that splits over k. Then $\mathcal{Z}(g)$ is the set of roots of g, and $\mathcal{I}(\mathcal{Z}(g))$ is the ideal generated by $(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_m)$ where $\alpha_i \in Z(g)$, which is exactly (g), so the radical ideals $I \subseteq k[x]$ for which $\mathcal{I}(\mathcal{Z}(I)) = I$ are exactly those that are separable and split over k.

Note that polynomials in $k[x]$ that split over k but are not separable do not generate radical ideals. If $f = (x-\alpha_1)^{e_1} \ldots (x-\alpha_m)^{e_m}$, then $((x - \alpha_1) \ldots (x - \alpha_m))^{max_i e_i} \in (f)$.

Proposition 1.19. *If $radI$ is in the image of $\mathcal{I}$, then $\mathcal{I}(\mathcal{Z}(I)) = radI$.*

Proof. Since $radI$ is in the image of $\mathcal{I}$, we have $radI = \mathcal{I}(\mathcal{Z}(radI))$. Since $I \subseteq radI$, $\mathcal{Z}(radI) \subseteq \mathcal{Z}(I)$. Let $(a_1, \ldots, a_n) \in \mathcal{Z}(I)$, and let $f \in radI$. Then $f^m \in I$ for some m, so $f^m(a_1, \ldots, a_n)$, so $f(a_1, \ldots, a_n) \in \mathcal{Z}(radI)$, so $\mathcal{Z}(I) \subseteq \mathcal{Z}(radI)$. so

$$\begin{aligned} \mathcal{Z}(I) &= \mathcal{Z}(radI) \\ \mathcal{I}(\mathcal{Z}(I)) &= \mathcal{I}(\mathcal{Z}(radI)) \\ &= radI \end{aligned}$$

□

2. Computing Intersections of Ideals

In this section, I'll describe how to take the intersection of two ideals in a polynomial ring in a few different situations. Intersections come up in computing things to do with algebraic sets because of primary decomposition of ideals in a polynomial ring. In the world of PIDs, the difference between the product of ideals and the intersection of ideals is the same as the difference between the product of two numbers and their least common multiples. A polynomial ring in two or more variables over a field is not a PID, but intuitively what is going on is much the same.

Example 2.1. Compute $(x, y) \cap (x, z)$ in the ring $\mathbb{R}[x, y, z]$:

The ideal generated by the least-common-multiple of the pairs of generators is (x, xz, xy, yz). Since $xy, xz \in (x, yz)$ we don't need all the generators: $(x, xz, xy, yz) = (x, yz)$. (x, yz) looks like it should be the intersection, but so far all we know is that $(x, yz) \subseteq (x, y) \cap (x, z)$.

To get the reverse inclusion, we can use a few things from the previous section as well as Gröbner bases. Here I have included the relevant definitions and statements of the relevant theorems. The proofs are long and can be found in section 9.6 of [1]. The numbers from that text are included for easy reference.

For the rest of this section, we are working in the ring $R[x_1, \ldots, x_n]$, a polynomial ring in n variables where R is a commutative ring with 1 (usually, R will be a field, k). For all proofs, assume R is Noetherian, so that we have $R[x_1, \ldots, x_n]$ is also Noetherian by the Hilbert Basis Theorem.

Definition 2.2. For a monomial $M = rx_1^{e_1}x_2^{e_2}\ldots x_n^{e_n}$, the multidegree of M is $\sum_{i=1}^{n} e_i$.

To order the the monomials in $R[x_1, \ldots, x_n]$, fix an order $x_1 > \ldots > x_n$ (renumber for convenience). For monomials M and M', $M > M'$ if $deg(M) > deg(M')$. If $deg(M) = deg(M')$, then $M = x_1^{\alpha_1}\ldots x_n^{\alpha_n} > x_1^{\beta_1}\ldots x_n^{\beta_n} = M'$ when $\alpha_i = \beta_i$ for $1 \leq i \leq j$ and $\alpha_j > \beta_j$, $1 \leq j \leq n$. For a polynomial $f \in R[x_1, \ldots, x_n]$, the leading term $LT(f)$ is the largest term with respect to this ordering. For any ideal $I \in R[x_1 \ldots x_n]$ we can form $LT(I)$, the ideal generated by $\{LT(f) | f \in I\}$.

Assume we have fixed a monomial ordering with $x_1 > \ldots > x_n$ for the rest of this section.

Definition 2.3 (Gröbner basis)**.** Let I be an ideal in $R[x_1, \ldots, x_n]$. A Gröbner Basis for I is a finite generating set $\{g_1, \ldots, g_m\}$ for I such that $\{LT(g_1), \ldots, LT(g_m)\}$ generates $LT(I)$.

Theorem 2.4 (9.6.24 in [1])**.** *Every ideal in $k[x_1, \ldots, x_n]$ has a Gröbner basis.*

There is an algorithm for computing Gröbner bases given a generating set for an ideal. It requires the use of the general polynomial division algorithm. I haven't included it here, and the calculations involving it are omitted. The algorithm can be found on pages 320 and 324 of [1]. Part of the algorithm involves knowing when to stop, that is, knowing when the generating set you have is a Gröbner basis. A simple case is that when every generator is a monomial, the set is a Gröbner basis. (In this case, the ideal of leading terms is the ideal itself.)

Lemma 2.5 (9.6.29 in [1])**.** *If $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis for I in $k[x_1, \ldots, x_n]$, then $G \cap k[x_1, \ldots, x_i]$ is a Gröbner basis for $I \cap k[x_1, \ldots, x_i]$ in $k[x_1, \ldots, x_i]$.*

Gröbner bases behave nicely under sums and products:

Lemma 2.6 (page 330 in [1]). *For ideals I and J with Gröbner bases $\{f_1, \ldots, f_p\}$ and $\{g_1, \ldots, g_q\}$ respectively, $\{f_1, \ldots, f_p, g_1, \ldots, g_q\}$ is a Gröbner basis for $I + J$, and $\{f_1 g_1, f_1, g_2, \ldots, f_1 g_n, f_2, g_1, \ldots, f_n g_n\}$ is a Gröbner basis for IJ.*

Now we have what we need to finish example 2.1. Recall from the previous section that for ideals I and $J \subseteq k[x_1, \ldots, x_n]$, we have $\mathcal{Z}(I \cap J) = \mathcal{Z}(IJ) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$, and that $\mathcal{I}(A \cup B) = \mathcal{I}(A) \cap \mathcal{I}(B)$. Suppose I and J are both in the image of $\mathcal{I}$. Then since $\mathcal{I}$ and $\mathcal{Z}$ are inverses in this situation,

$$\begin{aligned} I \cap J =& \mathcal{I}(\mathcal{Z}(I)) \cap \mathcal{I}(\mathcal{Z}(J)) \\ =& \mathcal{I}(\mathcal{Z}(I) \cup \mathcal{Z}(J)) \\ =& \mathcal{I}(\mathcal{Z}(IJ)) \end{aligned}$$

The two ideals from Example 2.1 are $(x, y) = \mathcal{I}(\{(a, b, c) \in \mathbb{R}^3 | a = b = 0\})$ and $(x, z) = \mathcal{I}(\{(a, b, c) \in \mathbb{R}^3 | a = c = 0\})$, so the above applies. Both are written in terms of Gröbner bases, since all the generators are monomials. By Lemma 2.6, $(x, y)(x, z) = (x^2, xy, xz, yz)$ is a Gröbner basis for the product, so

$$\begin{aligned} (x, y) \cap (x, z) &= \mathcal{I}(\mathcal{Z}(x^2, xy, xz, yz)) \\ &= \mathcal{I}(\mathcal{Z}(x^2) \cap \mathcal{Z}(xy) \cap \mathcal{Z}(xz) \cap \mathcal{Z}(yz)) \\ &= \mathcal{I}(yz - plane \\ &\quad \cap (yz - plane \cup xz - plane) \\ &\quad \cap (yz - plane \cup xy - plane) \\ &\quad \cap (xz - plane \cup xy - plane)) \\ &= \mathcal{I}(yz - plane \cap (xz - plane \cup xy - plane)) \\ &= (x, yz) \end{aligned}$$

In this calculation, what we're really using is that $(x, yz) = rad(x^2, xy, xz, yz)$ which is true because if x^2 is a generator of an ideal, x is in the radical of that ideal.

This is a good method, but it only works for ideals in the image of $\mathcal{I}$. We'd like to be able to calculate intersections for more than just this special group of ideals.

Theorem 2.7 (9.6.30 in [1]). *Let $I, J \subseteq R[x_1, \ldots, x_n]$. We can form the ideal $tI + (1-t)J$ in the ring $R[t, x_1, \ldots, x_n]$. The intersection $I \cap J = (tI + (1-t)J) \cap R[x_1, \ldots, x_n]$.*

Proof. Without really showing what is going on, we can show both inclusions. First pick $f \in I \cap J$. Let $D = tI + (1-t)J \cap k[x_1, \ldots, x_n]$. Then $f = tf + (1-t)f \in D$. For the other direction, consider an element $g = tf_1 + (1-t)f_2 \in D$ ($D \neq \emptyset$ since $0 \in D$), where $f_1 \in I$, $f_2 \in J$. Then (tricky!) $t(f_1 - f_2) = g - f_2 \in k[x_1, \ldots, x_n]$ so $f_1 = f_2 = g$, so all are in $I \cap J$. □

Theorem 2.7 is technical and unsatisfactory. The rough geometric picture of what it describes is that there is a copy of $\mathcal{Z}(I)$ at $t = 1$ and copy of $\mathcal{Z}(J)$ at $t = 0$. Taking the intersection $tI + (1-t)J \cap k[x_1, \ldots, x_n]$ sort of super-imposes the two, resulting in the union $\mathcal{Z}(I) \cup \mathcal{Z}(J)$, which is predicted by $\mathcal{Z}(I \cap J) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$.

The proof itself does not use any of the Gröbner basis tools, but we will need them in order to carry out any calculations:

Example 2.8. It is easy to see that $(x^2) \cap (x^3) = (x^3)$ in the ring $\mathbb{R}[x]$, but this can't be computed using first method, since $rad(x^2) = rad(x^3) = (x)$. Using the second method, $t(x^2) + (1-t)(x^3) = (tx^2, tx^3 - x^3)$. A Gröbner basis for this ideal is $(tx^2, tx^3 - x^3, x^3)$. By 2.5, $(tx^2, tx^3 - x^3, x^3) \cap \mathbb{R}[x] = (x^3)$.

3. Integrally Closed and not Integrally closed things

This last section follows two examples of how the algebraic geometry dictionary can work for us.

Definition 3.1. Let R be an integral domain, and let F be its field of fractions with algebraic closure $\overline{F}$. $s \in \overline{F}$ is *integral over* R if it is the root of a monic polynomial with coefficients in R. R is called *integrally closed* if whenever $s \in F$ is integral over R, $s \in R$. In an extension E of F, the integral closure of R is $\{s \in E |\ s \text{ is integral over } R\}$.

Example 3.2. By the rational root theorem, $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.

Example 3.3. Consider $R = \mathbb{C}[x,y]/(x^2 - y^3)$. Let F be the field of fractions of R. The polynomial $t^3 - x \in R[t]$ is monic, and has $\sqrt[3]{x}$ as a root, so $\sqrt[3]{x}$ is integral over R.

$$\sqrt[3]{x} = \frac{\sqrt[3]{x}^4}{x} = \frac{\sqrt[3]{x^2}^2}{x} = \frac{\sqrt[3]{y^3}^2}{x} = \frac{y^2}{x} = \frac{y^3}{xy} = \frac{x^2}{xy} = \frac{x}{y} \in F$$

$t^3 - x$ is irreducible over R, so $\sqrt[3]{x} \notin R$, so R is not integrally closed.

Example 3.4. In his (unpublished) paper, Wadsworth [3] gives many proofs that the coordinate ring $\mathbb{R}[x,y]/(x^2 + y^2 - 1)$ is integrally closed. Here is one of them:

Lemma 3.5. *Let R be a UFD in which 2 is a unit, and let $a \in R$ be a squarefree nonzero nonunit. Then $R[\sqrt{a}]$ is the integral closure of R in the fraction field of $R[\sqrt{a}]$, so $R[\sqrt{a}]$ is integrally closed.*

Proof. Let F be the fraction field of R. Since a is squarefree, the minimal polynomial for a over F is $t^2 - a$. The fraction field of $R[\sqrt{a}]$ is a proper extension of F, and is contained in $F(\sqrt{a})$, so it is equal to $F(\sqrt{a})$ since $[F(\sqrt{a}) : F] = 2$. Let S be the integral closure of R in $F(\sqrt{a})$. Then $\sqrt{a} \in S$ since $t^2 - a \in R[t]$, so $R[\sqrt{a}] \subseteq S$.

To get the other inclusion, let $\alpha = c + d\sqrt{a} \in S \subseteq F(\sqrt{a})$, and let σ be the nonidentity element of $Gal(F(\sqrt{a})/F)$. Then $\sigma : \alpha \mapsto c - d\sqrt{a}$. If $f(t) \in F[t]$ has α as a root, it also has $\sigma(\alpha)$ as a root. In particular, since α is integral over R, so is $\sigma(\alpha)$. Therefore $Tr(\alpha)$ and $Norm(\alpha)$ are both in S, so both are is $S \cap F = R$. We can compute them both:

$$Tr(\alpha) = \alpha + \sigma(\alpha) = 2c$$

and

$$Norm(\alpha) = \alpha\sigma(\alpha) = c^2 - d^2 a$$

Since 2 is a unit in R, $c \in R$. From this we get $d^2 a \in R$. By unique factorization, $d \in R$. Therefore $\alpha \in R[\sqrt{a}]$, so $S = R[\sqrt{a}]$. □

Lemma 3.5 can be applied to the ring $\mathbb{C}[x,y]/(x^2 + y^2 - 1)$ as follows. Let $R = \mathbb{C}[x]$. Then $y^2 + (x^2 - 1)$ is an irreducible polynomial in $R[y]$, and

$$\mathbb{C}[x,y]/(x^2 + y^2 - 1) = R[y]/(y^2 + (x^2 - 1)) \simeq R[\sqrt{x^2 - 1}] = \mathbb{C}[x, \sqrt{x^2 - 1}]$$

Since $\mathbb{C}[x]$ is a UFD, $x^2 - 1 = (x-1)(x+1)$ is a unique factorization. Therefore $x^2 - 1 \in \mathbb{C}[x]$ is a nonzero squarefree nonunit, and 2 is a unit, so by the lemma, $\mathbb{C}[x, \sqrt{x^2-1}]$ is integrally closed.

The fact that one of these rings is integrally closed and the other is not is reflected in the geometry. $\mathcal{Z}(x^2+y^2-1)$ is smooth, and $\mathcal{Z}(x^2-y^3)$ has a cusp at $(0,0)$. In order to establish this connection, we need a bit more machinery.

Definition 3.6. Let V be a variety, $v \in V$. Then if $\mathcal{I}(V) = (f_1, \ldots, f_m)$, the *tangent space* of V at v is

$$\mathcal{Z}\left(\bigcap_{i=1}^{m} \sum_{j=1}^{n} \frac{df_i}{dx_j}(v) x_j\right)$$

V is said to be smooth if for all $v \in V$, the dimension of the tangent space at V is equal to the dimension of V.

Example 3.7. Continuing with example 3.3 from before, the tangent space to $\mathcal{Z}(x^2-y^3)$ at a point $(a,b) \in \mathcal{Z}(x^2-y^3)$ is $\mathcal{Z}(2bx - 3b^2y)$. At the point $(0,0)$, this becomes $\mathcal{Z}(0) = A^2(\mathbb{C})$ which has dimension 2. $\mathcal{Z}(x^2-y^3)$ has dimension 1, so $\mathcal{Z}(x^2-y^3)$ is not smooth at $(0,0)$.

Furthermore, if $(a,b) \in \mathcal{Z}(x^2-3)$ then $a = 0$ if and only if $b = 0$, so at any nonzero point in $\mathcal{Z}(x^2-y^3)$, the coeffecients of x and y in $2ax - 3b^2y$ are both nonzero, so $\mathcal{Z}(2ax - 3b^2y)$ is a curve, which has dimension 1. Therefore $\mathcal{Z}(x^2-y^3)$ is smooth at all other points.

Example 3.8. The same computation shows that the variety in example 3.4 is smooth. The tangent space to $\mathcal{Z}(x^2+y^2-1)$ at $(a,b) \in \mathcal{Z}(x^2+y^2-1)$ is $\mathcal{Z}(2ax+2by)$. For any $(a,b) \in \mathcal{Z}(x^2+y^2-1)$ this will be a curve in $A^2(\mathbb{C})$. The real part will just be the line $y = \frac{-a}{b}x$ when $b \neq 0$, and the y-axis when $b = 0$.

It is not generally true that all integrally closed coordinate rings correspond to smooth varieties, but it is true for one dimensional varieties.

References

[1] Dummit, David S., and Foote, Richard M. *Abstract Algebra* 3rd ed. USA: John Wiley & Sons Inc., 2004.

[2] Eisenbud, David. *Commutative Algebra With a View Toward Algebraic Geometry*. New York: Springer-Verlag, 1994.

[3] Wadsworth, A. *A Geometric Dedekind Domain* (as yet unpublished), 2005.