ALGEBRA III
SEPTEMBER 30, 2004

GABRIEL C. DRUMMOND-COLE

Lemma 1. *Look at $I \cap J$, for I, J ideals in $S = k[x_1, \dots, x_n]$. Let $T = S[t]$. Then $(tI + (1 - t)J) \cap S = I \cap J$.*

Exercise 1. *Prove it.*

How do you compute $(I : J)$? The easiest way is to use syzygies. We can also use revlex. Let I, J be as above. Take nongraded revlex. If $g_1, \dots, g_i$ are a Gr obner basis for I, then taking initials commutes with addition of the last variable $+(x_n)$. So $g_1, \dots, g_i, x_n$ is a Gr obner basis. This also commutes with the colon of the last variable, so that $(in(I) : x_n) = in(I : x_n)$. So if $\tilde{g}_i = g_i/gcd(g_i, x_n)$, then $\tilde{g}_1, \dots, \tilde{g}_n$ form a Gr obner basis for $(I : x_n)$. Here I must be homogeneous.

So for a proof of the first, we have obviously an inclusion $in(I) + (x_n) \subset in(I + x_n)$. Now let $f = g + x_n h$. Either $in(f)$ is divisible by x_n, in which case $in(f) \in (x_n)$, or the initial does not involve x_n. But in that case, $in(f) = in(g)$ because the initial of $x_n h$ has an x_n in it and is thus smaller than the initial of g. So $in(f)$ lies in the ideal generated by $in(I)$ and x_n.

Exercise 2. *Prove the second one.*

This is important because of the lemma, and also because it helps us with this question:

Is x_n a zero divisor for S/I?

Corollary 1. *It is if and only if it is for $S/in_{revlex}(I)$*

Exercise 3. *How do you check that a polynomial is a zero divisor in S/I?*

Corollary 2. *We know how to compute $(I : x_n)$*

Corollary 3. *To find $(I : (f))$, define $T = S[y]$, and look to $I' = I \cdot T + (y - f)T$. Then $(I' : y) \cap S = (I : (f))$.*

The proof is similar to the earlier one of the intersection.

So now how do I compute $I : J$? Let $J = (f_1, \dots, f_l)$. Then let $T = S[y]$ and let $f = f_1 + yf_2 + \dots + y^{l-1} f_l$. Then $(I' : (f)) \cap S = (I : J)$. There is another way to do this, with more variables, but with lower degree.

This is an unpleasant thing with software, that sometimes your computation takes too long and you have to reprogram it.

Everybody here knows what a module is, right? How does software look at a module? It writes a presentation. The easiest modules for Macaulay are M over S where $M \subset F$, a free S-module.

These modules are graded, so that $M = \oplus_i M_i$, so that $S_i \otimes M_j \to M_{i+j}$. Then we can put a monomial order on F. So we only compare monomials in F if they are in the same degree. I look first by degree (not of the polynomial but of the grading). The whole theory that we've been doing goes through. There is an initial module, and so on. When we need detail, I'll go into it. You need it because when you have a sheaf on an algebraic variety you want modules, not ideals. Questions about this? There are analogs to Dixon's lemma, Macaulay's lemma, elimination, and so on. If you add a new variable, you can tensor your module to extend it to new variables. I'm going to do localization pretty soon.

You've seen the quotient field of a domain, right? Well, we'll deal with this today.

There is a similar theory over local rings (we've been doing it over graded rings). The prototype is the ring of germs, of functions at a point if you know what germs are. We'll get to that.

I have to apologize for what I'm doing today. The real proof you have to know a lot of stuff, but here I'm going to prove it in two lines over $\mathbb{C}$.

Let $I \subset k[x_1, \ldots, x_n]$. Take this to $V(I) \subset k^n$, the set of common zeros of $f \in I$.

On the other hand, given a set $X \subset k^n$, you can look at the set $\{f \in k[x_1, \ldots, x_n] | f(x_1, \ldots, x_n) = 0\}$, which is an ideal. So this is an ill-formed correspondence.

So what are some fields? There are $\mathbb{Z}_p, \bar{\mathbb{Z}}_p = \mathbb{F}_p, \mathbb{Q}, \bar{\mathbb{Q}}, \mathbb{R}, \mathbb{C}$, and others. You can get ugly messy versions over R, but nothing nice. It has to do with sums of squares. $\mathbb{R}$ is not well-behaved.

Lemma 2.

- *Say $I_1 \subset I_2$. Then $V(I_1) \supset V(I_2)$.*
- $V(I_1) \cup V(I_2) = V(I_1 \cap I_2) = V(I_1 I_2)$
- $V(\sum_{i \in I} I_i) = \cap_{i \in I} V(I_i)$.
- *Then $V(I)$ form the closed sets of a topology on k^n, called the Zariski topology.*

If my field is $\mathbb{F}_p$, then I don't have any other topology. So over $\mathbb{R}$ or $\mathbb{C}$ I already have one, so how does this one compare? It's very bad. So things which are Zariski closed are the zero loci of finite sets of polynomials, so they are closed in the normal topology. But the converse is not true, and in fact the Zariski topology is not Hausdorff.

You can do similar things with smooth functions instead of polynomials, but it's harder. You end up in C^* algebras.
For every compact space you can find a perfect algebraic invariant which determines it, namely the ring of continuous functions on it.

Now two others:

- $V((x_1 - a_1, \ldots, x_n - a_n)) = \{(a_1, \ldots a_n)\} \subset k^n$. This was a maximal ideal
- $V(\sqrt{I}) = V(I)$.

Assume $I = \sqrt{I}$. Now I is the intersection of all prime ideals containing it. So assume the intersection $\cap^r p_i$ is finite and irredundant. Then these are uniquely determined by I. So what does this imply about $V(I)$? We get $V(I) = \cup^r V(p_i)$.

Definition 1. *If I is prime, then $V(I)$ is called an affine algebraic variety.*

. So if $I = (f)$, what does it mean that I is radical? It means that f is squarefree.

So $V(f) = \cup V(p_i)$ where $f = p_1 \dots p_e$, the distinct prime/irreducible factors of f.

Questions about this? I'm trying to motivate what will come.

When can you write an ideal like this? What if it's not radical? What is possible instead?

Lemma 3. *Let p be a prime ideal in R, with $x \in R$, then what is $(p : x)$? If $x \in p$ then you get 1, otherwise you get p.*

This is just the definition of a prime ideal!

Lemma 4. *Let $I = \cap^r p_i$, an irredundant intersection of prime ideals. Then $(I : x) = (\cap^r p_i : x) = \cap^r (p_i : x) = \cap_{x \notin p_i} p_i$.*

If $I : x$ is prime, one of the lemmas we proved at the beginning of the class tells us that $I : x = p_j$ for some j such that $x \notin p_j$.

Let's show the converse. For each i there exists an x_i which is in $\cap_{j \neq i} p_j \backslash p_i$. Then $I : x_i = (\cap p_e : x_i) = \cap (p_e : x_i) = p_i$. So the moral is all the p_i are of this type.

A prime ideal of form $I : x$ is called associated to I, or to R/I. So one looks to the associator of R/I, denoted $Ass(R/I)$ or $Ass(I)$. This is the collection of prime ideals of type $(I : x)$ for some x.

- $Ass(R/I) \neq \emptyset$
- $Ass(R/I)$ is finite (dropping nonminimal elements) if R is Noetherian.

Why is this nonempty?

Lemma 5. *The maximal elements with respect to inclusion in the collection of all proper ideals of this type are prime.*

This collection is nonempty so $Ass(R/I)$ is nonempty. This is really the lowest level primary decomposition you can learn about. Think about it as primary decomposition at the level of sets.

Example 1. $(x, yz) = (x, z) \cap (x, y)$. *Then look at this in terms of subsets of k^3. This is the locus $x = 0, yz = 0$, which is the union of the two lines $x = z = 0$ and $x = y = 0$.*

I'll prove the lemma. If I choose a, b in R so that $abx \in I$ but $ax \notin I$, then I want to show that $bx \notin I$, assuming that $I : x$ is a maximal element. Look at $(I : x) \subseteq (I : (ax)) \subsetneq (1)$. But this contradicts maximality. So $I : x = I : ax$, so that $b \in (I : ax)$ so that $b \in I : x$, i.e., $bx \in I$.

Theorem 1. *Hilbert Nullstellensatz*
Assume $k = \bar{k}$

- $I(V(I)) = \sqrt{I}$
- $V(I(V)) = V$. *This is always true.*

Corollary 4. *There is a one to one inclusion reversing correspondence between algebraic sets in k^n and radical ideals in $k[x_1, \dots, x_n]$.*

A point is the minimal algebraic set, which corresponds to a maximal ideal. Another consequence is then

Corollary 5. $I((a_1, \ldots, a_n)) = (x_1 - a_1, \ldots, x_n - a_n)$.

There is a four line proof if you assume that $k = \mathbb{C}$.

Definition 2. *Say $k \subset \mathbb{C}$. A k-generic point $x \in V(I)$ is a point such that for every polynomial f with coefficients in k, $f(x) = 0$ implies $f \in I$. So it vanishes on all of $V(I)$.*

Example 2. *Look at $t \to^{\varphi} (t, f_2(t), \ldots, f_r(t))$.*
Assume for now that $f_i \in \mathbb{Q}[t]$. Look now to $\varphi(\pi)$. Then this is a $\mathbb{Q}$-generic point, since π is transcendental.

I'll do this next time but it's rather short.

Oh, and by the way, to show the Nullstellensatz, it is enough by the decomposition to do it for prime ideals.

You have in Atiyah and MacDonald four or five proofs of the Nullstellensatz.