ALGEBRA III
OCTOBER 5, 2004

GABRIEL C. DRUMMOND-COLE

So, I would like to finish what I started last time, the quick proof of the Nullstellensatz and some consequences. So let's put some of the things we did last time.

Theorem 1. *Say k is algebraically closed, but today k is $\mathbb{C}$. Suppose $I \subset k[x_1, \ldots, x_n]$. Then $I(V(I)) = \sqrt{I}$*

We showed that if I is radical then I can be written as a finite intersection of prime ideals, depending only on I. These are elements in what we called the associator of I, $Ass(I)$. These were things that could be written $(I : J)$. So you can then choose this to be not redundant. You look in the finite set $Ass(I)$, and then pick the primes and discard redundants.

In general, if I is not radical, then you get something more sophisticated, namely the primary decomposition. If $I = (f)$ then $\sqrt{I} = I$ means I is square-free, and this is a decomposition into irreducible factors.

This can be done algorithmically, if you want, in Macaulay. But it only works under the assumption of radicality. There's an algorithm for primary decomposition, but it is not implemented in Macaulay. Taking radicals is quite involved. Most calculations to find it will never finish. Partly it's homological algebra, partly dimension theory, to find this.

The other thing I said was that if $l \subset \mathbb{C}$ was a subfield and p a prime ideal of S, then an l-generic point $x \in V(p)$ is a point such that if $f(x_1, \ldots, x_n) \in S$ with coefficients in l vanishes at x, then f is in p.

My example last time was that if you look to $g \to (t, g_2, \ldots, g_n)$, where these are polynomials in one variable. So $V(p)$ is the kernel of the map from $\mathbb{C}^n$ to $\mathbb{C}[t]$ which takes x_i to g_i. Here you note that $\mathbb{C}[x_1, \ldots, x_n]/p \hookrightarrow \mathbb{C}[t]$, since p is prime so the quotient has no zero divisors.

So what is a $\mathbb{Q}$-generic point? Assume that the g_i coefficients are rational. Then $\pi, g_1(\pi), \ldots$ is a $\mathbb{Q}$-generic point because otherwise you get an algebraic relation on π.

Proposition 1. *If $\mathbb{C}/L$ ha infinite transcendence degree then $V(p)$ has an L-generic point.*

My claim is that this proves the Nullstellensatz, and then I'll prove this.

First assume that $I = p$ a prime. I want to show that $I(V(I)) = \sqrt{I}$, so that $I(V(p)) = p$. If I take something that is not in I I don't vanish on $V(I)$; that's all I have to show. If $f \notin p$ then $f|_{V(p)} \neq 0$.

So we choose our favorite $f \in \mathbb{C}[x_1, \ldots, x_n]$. Then I look to L, a subfield of $\mathbb{C}$ generated over the rationals by the coefficients of f. This has finite transcendence degree over $\mathbb{Q}$ and then I'm in the situation of the proposition. Then there is $x \in V(p)$ which is L-generic. If $f(x) = 0$ then f vanishes identically on p. I want to show that if something vanishes identically on p then $f \in p$.

Take $\sqrt{I}$, write it as $\cap p_i$, and then look at $V(\sqrt{I}) = \cup V(p_i) = V(I)$. So now I look to $I(V(I)) = I(\cup V(p_i) = \cap I(V(p_i)) = \cap p_i = \sqrt{I}$. But I need to know that radical ideals are the intersections of primes. This is a set theoretic decomposition.

Now, how do we prove the proposition? Of course, it's mysterious. People who know about schemes can produce generic points, but they're not actually points, they're prime ideals.

So if you have A an integral domain, so no zero divisors, then from it you can produce $Q(A)$, the field of fractions. This parallels the construction when you go from $\mathbb{Z} \to \mathbb{Q}$. The elements in Q are fractions. Do you know this?

[Everyone: yes]

Do I have to go over it?

[Everyone: no]

If A is not integral then Q is not a field. Think of this as formally fractions. So you write pairs modulo an equivalence relation, with denominator nonzero. So $(a, b) \sim (c, d)$ if $ad - bc = 0$. Addition is $(a, b) + (c, d) = (ad + bc, bd)$, multiplication is $(a, b)(c, d) = (ac, bd)$, and then this is a field since $(a, b)(b, a) = 1$. Then you have $A \hookrightarrow Q$ by $a \to a/1$.

I'm going to force the point. You'll tell me it's invisible but I'm going to force it.

Take the generators f_j for p. You can always add to L by finitely many elements and still satisfy the hypotheses. So I enlarge L by adjoining all coefficients of the f_i, without changing hypotheses or conclusions.

So now I look to $p_0 = L[x_1, \ldots, x_n] \cap p$. Now, p sits in $\mathbb{C}[x_1, \ldots, x_n]$, yes? So I enlarged L so that it contained f_i for all i. Hmm, well this is bad notation.

Call $A = L[x_1, \ldots, x_n]/p_0$. This is a prime ideal, even in intersection. So A is a domain. Then I can look to its field of fractions M.

So let's look. I started with L and enlarged it. If I write this domain and then expand it to its field of fractions, and this still has infinite transcendence degree. I'm claiming it's a number field, that $Q(A)/L$ has finite transcendence degree.

One thing that people learn is that the transcendence degree is how many independent variables you can fit. So usually by definition or proof, the transcendence degree of the fraction field is the number of transcendents in A.

There is an injection $L \hookrightarrow L[x_1, \ldots, x_n] \to A \to Q(A)$. This field morphism is then an injection. Any transcendence basis will still fit in A because A is a finite extension. It depends on how much algebra you got in algebra two, I'll do this more when we go over finite extensions. This is a simple example.

Another fact of life is that when you have $\mathbb{C}/L$, and an extension over L of finite degree, you can fit that into $\mathbb{C}$ because it has infinite transcendence degree.

So you can write such a map. For those of you not comfortable with this, there is a one page chapter in Lang that discusses all of this. We all know how clear and elementary Lang's treatment is, so you can read it there. But you are suspicious.

What is $\mathbb{Q}(\pi)$? Rational functions of π. You map this into $\mathbb{C}$ by taking π to some transcendent. If you have e as well, you have to map them to independent elements of $\mathbb{C}$.

$$\begin{tikzcd}
L \arrow[r] \arrow[drr] & A \arrow[r] & Q(A) \arrow[d, "\phi"] \\
 & & \mathbb{C}
\end{tikzcd}$$

The map ϕ is mysterious. I look x_i in $L[x_1, \ldots, x_n]$, and map it into $A, Q(A)$, and then $\mathbb{C}$ as a_i. I claim that the point $(a_1, \ldots, a_n)$ is L-generic.

It would have been better to write some yoga about fractions. Anyway, what do I have to check? I need that $(a_1, \ldots, a_n) \in V(p)$, and if a polynomial vanishes at the point, then it is in p. Now, $f_i \in p_0$. Then in the quotient A, we get 0, so that in A, $f_i(\bar{x}_1, \ldots, \bar{x}_n) = 0$. Then ϕ takes this to 0. This map is compatible with products and sums, so $\phi(f(x_1, \ldots, x_n)) = f(a_1, \ldots, a_n)$, which is then zero, as desired.

Say $f \in L[x_1, \ldots, x_n]$, with $f \notin p$. Then $f \notin p_0$. In $f(\bar{x}_1, \ldots, \bar{x}_n)$, this is not zero in A. It's not zero in $Q(A)$ because we have an injection, and then ϕ is a map of fields, so injective, so $f(a_1, \ldots, a_n)$ is nonzero.

So how do you find $a_1, \ldots, a_n$? You can't. It's nonconstructive.

So I don't know how simple you think this proof is, but it doesn't use any algebra except fractions and transcendence degree. Once you accept that points do not need to be geometric points, then schemes have generic points. If you're just over some field you can't do that. This doesn't work over $\mathbb{F}_p$. In characteristic 0 you can always reduce yourself over the rationals and $\mathbb{C}$.

So, consequences. This tells two things. Consequence number one says the following:

Corollary 1. *A $\mathbb{C}$-algebra A is $\mathbb{C}[x_1, \ldots, x_n]/I(X)$, i.e., an affine coordinate ring of an algebraic set if and only if A is reduced and finitely generated.*

What does it mean, finitely generated?

Definition 1. *If A is a $\mathbb{C}$-algebra, we call it finitely generated if there are $f_1, \ldots, f_n \in A$ such that any element of A is a polynomial in f_i with coefficients in $\mathbb{C}$. This is equivalent to the existence of a surjective map from a polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$.*

The kernel of this map is your ideal.

It's the ideal of an algebraic set if and only if it's a radical ideal, i.e., if it is reduced, that is, has no nilpotents. This is an equivalence of categories, actually, between reduced finitely generated $\mathbb{C}$-algebras and algebraic sets.

Corollary 2. *In $\mathbb{C}[x_1, \ldots, x_n]$, every maximal ideal is of the type $(x_1 - a_1, \ldots, x_n - a_n)$ for some $a_1, \ldots, a_n \in \mathbb{C}$.*

The next interesting thing is what happens when $V(I)$ has only finitely many solutions? That corresponds to a big class of rings, called Artinian rings. It's a theorem of six points. But maybe I'll do something about fractions before.

I have a ring A, observe it's not a domain. I have a collection $S \subset A$ with some properties. I want S to be the set of denominators. Normally I want $1 \in S, 0 \notin S$. I would like to write what it means to have fractions (a, s) with $a \in A$ and $s \in S$. I want to identify two fractions when I can bring them to the same denominator. We just did the special case where A was a domain and S was everything but 0.

Now $a/s = b/s'$ means $as' = bs$. But this has to be an equivalence relation. Transitivity is the problem. I want to write $b/s' = c/s''$, so that $s''b - s'c = 0$. Now I want to show that $a/s = c/s''$ so that $as'' - cs = 0$. So I get by multiplication and addition that $as's'' - s'sc = 0$. This gives me that $s'(as'' - sc) = 0$. The problem is that we want to be able to divide by s'. But s' could be a zero divisor. In the previous case I had a domain, so no problem. But here this is a problem. It's not an equivalence relation. Too bad. How do I adjust this?

The new convention says $(a/s) = (b/s')$ if there exists $\bar{s} \in S$ so that $\bar{s}(as' - bs) = 0$. So then that gives an equivalence relation, and forces S to be closed under multiplication, which was already necessary for multiplication of fractions. Such an S is called a multiplicative set. All these properties, of equivalence, are satisfied, so we can build a ring. So, examples.

- $A \backslash \{0\}$ if A is a domain.
- $A \backslash$ all zero divisors.
- $A \backslash p$ for p a prime.
- $S = \{f^i\}$, for f a non-zerodivisor

As a set, $S^{-1}A = \{a/s | a \in A, s \in S\}$. This is my notation for the pair (a, s), modulo the equivalence relation above. Addition and multiplication are as before. Then $S^{-1}A$ is a ring.

So what do you get?

- For $A \backslash \{0\}$ you get a field.
- For $A \backslash$ all zero divisors you get what's called the total ring of fractions. You've inverted everything you can invert.
- $A \backslash p$ or $\{f^i\}$ is called localization of A at p or f. These are interesting to an algebraic geometer.

Now, two things. Let's list the properties.

(1) There exists a canonical map $\phi_S : A \to S^{-1}A$ sending a to $a/1$. It's not injective in general; its kernel consists of $\{a \in A : \exists s \in S : sa = 0\}$

(2) $S^{-1}A$ has the following universality property.

$$\begin{tikzcd}
A \arrow[rr, "\phi_S"] \arrow[dr, "g"'] & & S^{-1}A \arrow[dl, dotted, "\bar{g}"] \\
& B &
\end{tikzcd}$$

This is an extension of a map g with $g(s)$ invertible for $s \in S$. I can write

$$\bar{g}(a/s) = \bar{g}(a/1)\bar{g}(1/s) = \bar{g}\phi(a)\bar{g}\phi(s)^{-1} = g(a)g(s)^{-1}.$$

Let me finish with a word about localization. This will be fractions of polynomials with the denominator nonvanishing on p. This is looking to rational polynomials that are defined near p in some topology. This is equivalent to taking germs. I'll talk more about this next time. If you take the ring of power series you get holomorphic functions.