ALGEBRA III
DECEMBER 7, 2004

GABRIEL C. DRUMMOND-COLE

So, uh, let me review a couple of things. The plan for this week is to talk about Dedekind rings, rings of Krull dimension one. The standard example is

$$\begin{tikzcd} \mathbb{Z} \arrow[r] \arrow[d, "\subset"] & O_K \arrow[d, "\subset"'] \\ \mathbb{Q} \arrow[r] & K \subset \mathbb{C} \end{tikzcd}$$

Among other things O_K is an integral extension. People have been concerned with these because they are natural. One example is $\mathbb{Z}[i]$. You could have $\mathbb{Z}[\frac{1+\sqrt{-5}}{2}]$. So this is $O_{\mathbb{Q}(\sqrt{-5})}$.

What happens in a ring like this? The Gaussian integers are a UFD, but the second ring is not because $3 \cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5})$.

You have $z^n = x^n + y^n$, so the hope is to factor these in a UFD somewhere. So you go to an algebraic extension. But unique factorization doesn't hold. So how far is this from a UFD? What are its properties? This gets more complicated with nth roots. But what can we say about this ring?

One consequence of going up and incomparability is that O_K has the same Krull dimension as $\mathbb{Z}$, that is, one.

I had a homework for you, I should have said that. I'll start talking about such rings in a moment, I'd like to give this:

Exercise 1. *We talked about what it means for $R \hookrightarrow S$ to be an integral extension, an element satisfies a monic polynomial. But instead start with $I \subset R$ and look to $\bar{I} = \{x \in R : x$ satisfies a monic polynomial $x^n + a_1x^{n-1} + \cdots + a_n - 0$ with $a_j \in I^j$ for all j.*

1. *We had the lemma with four points, equivalent conditions for integrality. Use the same methods to show that $\bar{I}$ is an ideal.*
2. *If I is radical then I is integrally closed in R.*
3. *This has to do with convex geometry. This is due to Caratheodory. If $I \subset k[x_1, \cdots, x_n]$ is generated by a set of monomials Γ, then $\tilde{\Gamma}$, the collection of exponents of the monomials in Γ. This is in $\mathbb{N}^n \subset \mathbb{R}^n_+$. Take the cone Λ these generate (their convex hull), defined as $\tilde{\Gamma} + \mathbb{R}^n_+$. Then the monomials with generators in Λ are the generators of $\bar{I}$.*

Try to solve this: it is easy and instructive.

Okay, so how do we characterize O_K? What is special about these? The Krull dimension is one, and these are domains, which is equivalent to the statment that every nonzero prime ideal is maximal. I will show that every ring with this property has unique factorization of ideals.

Proposition 1. *Let R be a Noetherian domain such that every nonzero prime ideal is maximal. Then every nonzero ideal can be uniquely expressed as a product of primary ideals whose radicals are all distinct.*

I don't have unique factorization into primes of various powers; instead I get primary ideals for each prime.

Let's prove this. It's some unique factorization statement. This is better than nothing. This is specific to this situation; it wouldn't hold in general. For almost two centuries people believed that this would prove Fermat. Kummer got a little progress, but it didn't pan out.

This is the subject of basic algebraic number theory, but also basic arithmetic algebraic geometry.

How do we prove this? Take $I \subset R, I \neq 0$. How do I get this decomposition? What decompositions did we learn, in general for any Noetherian ring? Primary decomposition, so $I = \cap_{i=1}^n q_i$, where q_i are primary. I don't know if it's unique or not. I would know that $\cap q_i = \prod q_i$ (from the Chinese remainder lemma) if I knew that $q_i + q_j = (1)$ for all $i \neq j$. So $p_i = \sqrt{q_i}$. So the radical is bigger than the ideal $p_i \supset q_i \supset I \neq 0$ so p_i is maximal. So if I take a minimal decomposition, I can assume these are distinct maximal p_i. If you have two maximal ideals then $p_i + p_j = 1$. This is not quite what I want, I want this for q_i, q_j. It is enough to show that $\sqrt{q_i + q_j} = 1$; this is $\sqrt{\sqrt{q_i} + \sqrt{q_j}} = \sqrt{p_i + p_j} = \sqrt{1} = 1$.

Now why is this unique? Is primary decomposition unique? What was unique in a primary decomposition? This is not so long ago? The unique ones were the isolated, minimal ones. But here all the p_i are minimal associated primes, so all the q_i are unique.

Now let's make a change. I don't want to assume only this, I want to assume a little more. Let's make a little, let's start with R a Noetherian domain with Krull dimension one. What's missing is that every primary ideal is a power of a prime.

Assume that as well. Then every nonzero ideal is uniquely a product of prime ideals. This sounds like unique factorization, but it is in ideals. Maybe I can do algebra with these, form fractions or whatever. This is called the class group or for geometers the Picard group.

What can you say about such a ring? How special is it? I want to localize at a nonzero prime? If I localize at a maximal ideal the chains are the same; it's not very easy but you can show that if you localize at a maximal ideal you get the same. Here, though, that's easy. You get a local ring with a unique nonzero maximal ideal. If something was a power of a prime to start out with, it's also a power of a prime after localization. Then every nonzero ideal is a power of the single maximal ideal. This is quite special. It's a local ring with every nonzero ideal equal to $(pR_p)^n$ for some n. This is called a discrete valuation ring.

This number n has nice properties; it will behave like a logarithm.

Definition 1. *A discrete valuation on a field (here the field of fractions) is a function $v : K^* \to \mathbb{Z}$ which is onto with the following property:*
$v(xy) = v(x) + v(y)$
$v(x + y) \geq \min\{v(x), v(y))$ *with convention* $v(0) = \infty$.

So for each prime you get a different valuation defined by the n. You will sometimes see nondiscrete valuation with values in a group $\mathbb{R}$ or something.

So $R_v = \{x \in K : v(x) \geq 0\}$. I claim that this is a subring of K. It should contain 0 and 1. I have to show that it's closed under sums, differences, and products, which follow from these properties.

So let me give some examples.

The one we started with we have $\mathbb{Z} \subset \mathbb{Q}$ and I put a valuation which is the unique power of p which can be factored out of a rational.

The big question is, what is R_{v_p}? It is $\mathbb{Z}_p$. in this case.

How about another one. Let $K = k(x)$ and f an irreducible element. Then evaluation is the power of f in your fraction. Then $R_{v_p} = k[x]_{(f)}$. If you look to rings of power series $k[[x]]$ in one variable, you can look to the smallest coefficient which is nonzero in the expansion $v(f) = \min\{i : a_i \neq 0\}$.

Definition 2. *An integral domain is called a discrete valuation ring (DVR) if there exists a valuation v on K (the field of fractions) such that the original domain is the evaluation ring of v.*

For instance, $\mathbb{Z}_p$ and $k[x]_{(f)}$ are DVRs.

Did I prove that integral closure and localization commute? Assume I'm in this situation so that $R \subset K = Q(R)$ with $v : K^* \to \mathbb{Z}$. Let $x \neq 0$ be in K. If $v(x)$ is positive then $x \in R$. Say $v(x)$ is negative; then $v(x^{-1})$ is $-v(x)$ so $x^{-1} \in R$.

So now we will show that a discrete valuation ring is a local ring. The maximal ideal will be $\{x \in K : v(x) > 0\}$. The sum of elements is there because of the one property; the product can only increase the valuation. So what do I have to show? It contains the noninvertibles, which is obvious.

It has even more interesting properties. Now let's prove something about the Krull dimension.

Lemma 1. *Let $x, y \in R$ with $v(x) = v(y)$. Then $(x) = (y)$. This is equivalent to x and y differing by a unit. So $v(xy^{-1}) = 0$ and is thus a unit in R.*

Once you get rid of discrete valuation you are really in general rings. You have heard of the Hironaka theorem about desingularization. That's very hard. I didn't tell you what improved? The object that keeps track of the improvement is a valuation, but not a discrete one. This is a baby example because it is discrete.

Let's state what are the ideals of a DVR?

Lemma 2. *$m_n = \{x : v(x) \geq n\}$ is an ideal for all n.*

There is a descending sequence $m_1 \supset m_2 \supset \cdots$

Every ideal of I is one of these m_n and $m_k = (m_1)^k$.

From this lemma, the only chain is this one, so the ring is Noetherian.

If $I \neq 0$ then take n which is minimal for $v(x)$ for $x \in I$. This should remind you of proving $k[x]$ is a PID. Then $m_n = \{y \in R : v(y) \geq n\} \subset I$. If $y \in R$ then $yx^{-1} \in R$ so $y \in (x) \subset I$. Equality is easy too. Then $m_n = (x^n)$ for some $x \in m$.

Next time I'll prove some identities and then we'll go back to the nonlocal version.

Thursday we finish with Dedekind rings.