Math 615: Lecture of March 21, 2007

We shall no longer be assuming that all rings have prime characteristic $p > 0$. Our objective is to prove some basic results about the structure of complete local rings. We shall begin by studying complete local rings that contain a field. Here are three major results that we are aiming to prove:

Theorem. *Let $(R,\, m,\, K)$ be a complete local ring that contains a field.*

(a) *If R is regular, then $R \cong K[[x_1,\, \ldots\, , x_d]]$, a formal power series ring in n variables over K, where $d = \dim(R)$.*

(b) *R is a homomorphic image of a formal power series ring $K[[x_1,\, \ldots\, , x_n]]$ over a field K.*

(c) *R is a module-finite extension ring of a formal power series ring $K[[x_1,\, \ldots\, , x_d]]$, where $d = \dim(R)$.*

Note that part (c) is an analogue, for complete local rings, of the Noether normalization theorem.

We shall later analyze the situation where R does not contain a field in detail. But this is more difficult, and we begin with the field case.

By a *coefficient field* for a local ring $(R,\, m)$ we mean a subring $K \subseteq R$ such that the composite map

$$K \hookrightarrow R \twoheadrightarrow R/m$$

is an isomorphism. This implies that K is a field, since it is isomorphic with R/m. One may think of K as an isomorphic "copy" of the residue class field that is contained in R. The most difficult part in proving the structure theorems stated above is establishing:

Theorem. *A complete local ring that contains a field contains a coefficient field.*

Proving the preceding two Theorems will take a while. Note that if a local ring R has characteristic 0, which means that it contains $\mathbb{Z}$, the hypothesis that it contains a field is equvalent to the statement that it contains $\mathbb{Q}$. But $\mathbb{Q}$ will typically be much smaller than the residue field of R. The hypothesis that R has prime characteristic $p > 0$ already implies that R contains a field: R will contain the field $\mathbb{Z}/p\mathbb{Z}$.

Example. Let $p > 0$ be a prime integer, let P denote the prime ideal $p\mathbb{Z}$ in $\mathbb{Z}$, and let $\mathcal{Z}_p$ denote the completion of the Noetherian discrete valuation ring $\mathbb{Z}_P$ at its maximal ideal. The ring $\mathcal{Z}_p$ is called the *ring of p-adic integers.* Both Z_P and the $\mathcal{Z}_p$ are examples of local rings that do not contain a field. The ring $\mathcal{Z}_p$ may also be obtained by completing $\mathbb{Z}$ with respect to $p\mathbb{Z}$ without localizing first. The maximal ideal of $\mathcal{Z}_p$ is generated by p:

every nonzero element is a power of p times a unit. Every elenent of $\mathcal{Z}_p$ can be represented uniquely as a formal series

$$a_0 + a_1p + a_2p^2 + a_3p^3 + \cdots + a_np^n + \cdots$$

such that every a_i is an integer between 0 and $p - 1$ inclusive. If the coefficients are eventually all zero, we have the base p representation of an element of $\mathbb{N}$. Note, for example, that in $\mathcal{Z}_2$, we have

$$-1 = 1 + 2 + 4 + 8 + \cdots + 2^n + \cdots$$

Example. Local rings that contain a field but do not have a coefficient field are abundant. Here is a simple example of a local ring that contains a field but does not have a coefficient field. Let V be the localization of the polynomial ring $\mathbb{R}[t]$ in one variable over the real numbers $\mathbb{R}$ at the prime ideal $P = (t^2 + 1)$, and let $m = PV$. Note that V is a Noetherian discrete valuation ring. Then V/PV is the field of $\mathbb{R}[t]/(t^2 + 1) \cong \mathbb{C}$, which is $\mathbb{C}$. But $S \subseteq \mathbb{R}(t)$ does not contain any element whose square is -1: the square of a non-constant rational function is non-constant, and the square of a real scalar cannot be -1.

The completion of $\widehat{V}$ of V is also a DVR with residue class field $\mathbb{C}$, and so it must contain a square root of -1. The reader may want to attempt to find an explicit power series in $t^2 + 1$ that represents a square root of -1. Note that the structure theorems imply that there is an isomorphism $\mathbb{C}[[z]] \cong \widehat{V}$, and one can show that there is such an isomorphism sending $z \mapsto t^2 + 1$.

In characteristic 0 we shall show that any subring of the complete local ring R that is maximal with respect to the property of being a field is a coefficient field. The proof will depend on Hensel's Lemma. In characteristic $p > 0$, there may be maximal fields within the complete local ring R that are not coefficient fields. The proof we give will be quite different, and will not make any use of Hensel's Lemma at all.

We begin our analysis of the structure of complete local rings by proving Hensel's lemma.

Theorem (Hensel's Lemma). *Let $(R,\, m,\, K)$ be a complete local ring (or a completed and m-adically separated quasilocal ring) and let f be a monic polynomial of degree d in $R[x]$. Suppose that $^-$ indicates images in $K[x]$ under the the ring homomorphism $R[x] \twoheadrightarrow K[x]$ induced by $R \twoheadrightarrow K$. If $\overline{f} = GH$ where $G,\, H \in K[x]$ are monic of degrees s and t, respectively, and $G,\, H$* are relatively prime *in $K[x]$, then there are unique monic polynomials $g,\, h \in R[x]$ such that $f = gh$ and $\overline{g} = g$ while $\overline{h} = h$.*

Before giving the proof, we want to provide some examples that illustrate how powerful Hensel's Lemma is, as well as an instance where it cannot be applied.

Example 1. Let $R = \mathbb{Q}[[z_1,\, z_2,\, z_3]]$. Suppose that we want find a power series which is a square root of $1 + z_1z_2^{11}z_3 + z_1^7 + z_2^5z_3^3$. That is, we want to solve the equation

$$(*) \quad x^2 - (1 + z_1z_2^{11}z_3 + z_1^7 + z_2^5z_3^3) = 0$$

in the formal power series ring $\mathbb{Q}[[z_1, z_2, z_3]]$. This is equivalent to factoring the left hand side of $(*)$ in the form $(x-g)(x-h)$ for elements $g, h \in \mathbb{Q}[[z_1, z_2, z_3]]$. Hensel's Lemma enables us to solve this problem by solving it modulo (z_1, z_2, z_3). Modulo the maximal ideal, the equation becomes $x^2 - 1 = 0$, and the left hand side factors $(x-1)(x+1)$. Moreover, $x - 1$ and $x + 1$ are relatively prime over $\mathbb{Q}[x]$. We can therefore lift this factorization. This provides two square roots of $1 + z_1 z_2^{11} z_3 + z_1^7 + z_2^5 z_3^3$. These can also be found using Newton's binomial theorem: let $u = z_1 z_2^{11} z_3 + z_1^7 + z_2^5 z_3^3$. Then

$$(1+u)^{1/2} = 1 + \frac{1}{2}u + \frac{\frac{1}{2}(\frac{1}{2}-1)}{2!}u^2 + \frac{\frac{1}{2}(\frac{1}{2}-1)(\frac{1}{2}-2)}{3!}u^3 + \cdots$$

and one may substitute the expression $z_1 z_2^{11} z_3 + z_1^7 + z_2^5 z_3^3$ for u. Both methods may be used to show that if n is invertible in $K = R/m$ and $u \in m$, then $1 + u$ has an nth root in the complete local ring R. But Hensel's Lemma is much more general, as the next example shows.

Example 2. Let $R = K[[z_1, z_2, z_3]]$. We shall consider the cases where $K = \mathbb{Q}$ and $K = \mathbb{C}$. Suppose that we want to solve the eqation

$$(\#) \quad x^3 + (z_1^{17} - z_2 z_3^5)x^2 + (z_1 z_2 z_3^8)x - 1 + z_2^7 + z_3^9 = 0$$

over R. When the equation is considered modulo the maximal ideal of R, it becomes $x^3 - 1 = 0$ and has the three roots 1, ω, $\overline{\omega}$ where $\omega = \dfrac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity, and $\overline{\omega}$ is the conjugate root $\dfrac{-1+\sqrt{-3}}{2}$ (we also have $\overline{\omega} = 1/\omega = \omega^2$). Hensel's Lemma applied over $\mathbb{C}$ yields unique roots of the equation $(\#)$ with constant terms 1, ω, and $\overline{\omega}$, respectively. If we apply Hensel's Lemma over $\mathbb{Q}$, we still have the factorization

$$x^3 - 1 = (x-1)(x^2 + x + 1)$$

and the factors are relatively prime over $\mathbb{Q}[x]$. This factorization can therefore be lifted, and this shows that there is a unique root of the equation with constant term 1. This is, of course, the same root with constant term 1 that we found over $\mathbb{C}[[z_1, z_2, z_3]]$, but we have gained the information that the coefficients are rational numbers.

Example 3. Consider the equation $x^2 + 1 = 0$ in $\mathcal{Z}_{13}$. Modulo the maximal ideal, we find that there are two roots in $\mathbb{Z}/13\mathbb{Z}$, represented by 5 and $-5 = 8$. It follows that -1 has two square roots in $\mathcal{Z}_{13}$. Similarly, the reader may verify that 3 has a cube root in $\mathcal{Z}_{61}$ that is congruent to 5 modulo the maximal ideal of $\mathcal{Z}_{61}$.

Example 4. Let $R = \mathbb{C}[[z_1, z_2]]$ and consider the equation $x^2 - z_1^2 - z_2^3 = 0$. Modulo the maximal ideal, this becomes $x^2 = 0$. Of course, x^2 factors as $x \cdot x$, but *the factors are not relatively prime.* Therefore, Hensel's Lemma does not apply. In fact, $z_1^2 + z_2^3$ has no square root in the formal power series ring. Similarly, Hensel's Lemma does not give information about solving $x^2 - z_1 = 0$, which also has no solution.

Proof of Hensel's Lemma. Let F_n denote the image of f in $(R/m^n)[x]$. We recursively construct monic polynomials $G_n \in (R/m^n)[x]$, $H_n \in (R/m^n)[x]$ such that $F_n = G_n H_n$ for all $n \geq 1$, where G_n and H_n reduce to G and H, respectively, mod m, and show that F_n and G_n are unique. Note that it will follow that for all n, G_n has the same degree as G, namely s, and H_n has the same degree as H, namely t, where $s + t = d$. The uniqueness implies that mod m^{n-1}, G_n, H_n become G_{n-1}, H_{n-1}, respectively. This yields that the sequence of coefficients of x^i in the G_n is an element of $\varprojlim_n (R/m^n) = R$, since R is complete. Using the coefficients determined in this way, we get a polynomial g in $R[x]$, monic of degree s. Similarly, we get a polynomial $h \in R[x]$, monic of degree t. It is clear that $\overline{g} = G$ and $\overline{h} = H$, and that $f = gh$, since this holds mod m^n for all n: thus, every coefficient of $f - gh$ is in $\bigcap_n m^n = (0)$.

It remains to carry through the recursion, and we have $G_1 = G$ and $H_1 = H$ from the hypothesis of the theorem. Now assume that G_n and H_n have been constructed and shown unique for a certain $n \geq 1$. We must construct G_{n+1} and H_{n+1} and show that they are unique as well. It will be convenient to work mod m^{n+1} in the rest of the argument: replace R by R/m^{n+1}. Construct G^*, H^* in $R[x]$ by lifting each coefficient of G_n and H_n respectively, but such that the two leading coefficients occur in degrees s and t respectively and are both 1. Then, mod m^n, $F \equiv G^*H^*$, i.e., $\Delta = F - G^*H^* \in m^nR[x]$. We want to show that there are unique choices of $\delta \in m^nR[x]$ of degree at most $s-1$ and $\epsilon \in m^nR[x]$ of degree at most $t-1$ such that $F - (G^* + \delta)(H^* + \epsilon) = 0$, i.e., such that $\Delta = \epsilon G^* + \delta H^* + \delta\epsilon$. Since $\delta, \epsilon \in m^nR[x]$ and $n \geq 1$, their product is in $m^{2n}R[x] = 0$, because $2n \geq n+1$. Thus, our problem is to find such ϵ and δ with $\Delta = \epsilon G^* + \delta H^*$. Now, G and H generate the unit ideal in $K[x]$, and $R[x]_{\text{red}} = K[x]$. It follows that G^* and H^* generate the unit ideal in $R[x]$, and so we can write $1 = \alpha G^* + \beta H^*$. Multiplying by Δ, we get $\Delta = \Delta\alpha G^* + \Delta\beta H^*$. Then $\Delta\alpha$ and $\Delta\beta$ are in $m^nR[x]$, since Δ is, but do not yet satisfy our degree requirements. Since H^* is monic, we can divide $\Delta\alpha$ by H^* to get a quotient γ and remainder ϵ, i.e., $\Delta\alpha = \gamma H^* + \epsilon$, where the degree of ϵ is $\leq t-1$. If we consider this mod m^n, we have $0 \equiv \gamma H_n + \epsilon$, from which it follows that γ, $\epsilon \in m^nR[x]$. Then $\Delta = \epsilon G^* + \delta H^*$ where $\delta = \gamma G^* + \Delta\beta$. Since Δ and ϵG^* both have degree $< n$, so does δH^*, which implies that the degree of δ is $\leq s-1$.

Finally, suppose that we also have $\Delta = \epsilon' G^* + \delta' H^*$ where ϵ' has degree $\leq t-1$ and δ' has degree $\leq s-1$. Subtracting, we get an equation $0 = \mu G^* + \nu H^*$ where the degree of $\mu = \epsilon - \epsilon'$ is $\leq t-1$ and the degree of $\nu = \delta - \delta'$ is $\leq s-1$. Since G^* is a unit considered mod H^*, it follows that $\mu \in (H^*)$, i.e., that H^* divides μ. But H^* is monic, and so this cannot happen unless $\mu = 0$: the degree of μ is too small. Similarly, $\nu = 0$. □

We can now deduce:

Theorem. *Let (R, m, K) be a complete local ring that contains a field of characteristic 0. Then R has a coefficient field. In fact, R will contain a maximal subfield, and any such subfield is a coefficient field.*

Proof. Let $\mathcal{S}$ be the set of all subrings of R that happen to be fields. By hypothesis, this set is nonempty. Given a chain of elements of $\mathcal{S}$, the union is again a subring of R that is a field. By Zorn's lemma, $\mathcal{S}$ will have a maximal element K_0. To complete the proof of the theorem, we shall show that K_0 maps isomorphically onto K. Obviously, we have a map $K_0 \subseteq R \twoheadrightarrow R/m = K$, and so we have a map $K_0 \to K$. This map is automatically injective: call the image K_0'. To complete the proof, it suffices to show that it is surjective.

If not, let θ be an element of K not in the image of K_0. We consider two cases: the first is that θ is transcendental over K_0'. Let t denote an element of R that maps to θ. Then $K_0[t]$ is a polynomial subring of R, and every nonzero element is a unit: if some element were in m, then working mod m we would get an equation of algebraic dependence for θ over K_0' in K. By the universal mapping property of localization, the inclusion $K_0[t] \subseteq R$ extends to a map $K_0(t) \subseteq R$, which is necessarily an inclusion. This yields a subfield of R larger than K_0, a contradiction.

We now consider the case where θ is algebraic over the image of K_0. Consider the minimal polynomial of θ over K_0', and let f be the corresponding polynomial with coefficients in $K_0[x] \subseteq R[x]$. Modulo m, this polynomial factors as $(x-\theta)H(x)$, where these are relatively prime because θ is separable over K_0': this is the only place in the argument where we use that the field has characteristic 0. The factorization lifts uniquely: we have $f = (x-t)h(x)$ where $t \in R$ is such that $t \equiv \theta \bmod m$. That is, $f(t) = 0$. We claim that the map $K_0[t] \subseteq R \twoheadrightarrow R/m$, whose image is $K_0'[\theta]$, gives an isomorphism of $K_0[t]$ with $K_0'[\theta]$: we only need to show injectivity. But if $P(x) \in K_0[x]$ is a polynomial such that $P(t)$ maps to 0, then f divides $P(x)$, which implies that $P(t) = 0$. Since $K_0[t] \cong K_0'[\theta]$ (both are $\cong K_0[t]/\big(f(t)\big)$), $K_0[t]$ is a field contained in R that is strictly larger than K_0, a contradiction. $\square$

Remark. If R is a complete local domain of positive prime characteristic $p > 0$, the same argument shows that R contains a maximal subfield K_0, and that K is algebraic and purely inseparable over the image of K_0.