Math 615: Lecture of March 23, 2007

Remark. It is worth noting that Cauchy sequences in an I-adic topology are much easier to study, in some ways, than Cauchy sequences of, say, real numbers. In an I-adic topology, for $\{r_n\}_n$ to be a Cauchy sequence it suffices that $r_n - r_{n+1} \to 0$ as $n \to \infty$, i.e., that for any specified $N \in \mathbb{N}$, the differences $r_n - r_{n+1}$ are eventually in I^N. The reason is that if this is true for all $n \geq n_0$, we also have that

$$r_{n'} - r_n = r_{n'} - r_{n'-1} + \cdots + r_{n+1} - r_n \in I^n$$

for all $n' \geq n \geq n_0$. In consequence, a necessary and *sufficient* condition for an infinite series $\sum_{n=0}^{\infty} r_n$ to converge in the I-adic topology is that $r_n \to 0$ as $n \to \infty$, which, of course, is false over $\mathbb{R}$: the series $\sum_{n=1}^{\infty} 1/n$ does not converge, and the corresponding sequence of partial sums $\{r_n\}_n$ does not converge, even though $r_{n+1} - r_n = 1/(n+1) \to 0$ as $n \to \infty$.

Our next result on coefficient fields uses a completely different argument:

Theorem. *Let (R, m, K) be a complete local ring of positive prime characteristic p. Suppose that K is perfect. Let $R^{p^n} = \{r^{p^n} : r \in R\}$ for every $n \in \mathbb{N}$. Then $K_0 = \bigcap_{n=0}^{\infty} R^{p^n}$ is a coefficient field for R, and it is the only coefficient field for R.*

Proof. Consider any coefficient field L for R, assuming for the moment that one exists. Then $L \cong K$, and so L is perfect. Then

$$L = L^p = \cdots = L^{p^n} = \cdots,$$

and so for all n,

$$L \subseteq L^{p^n} \subseteq R^{p^n}.$$

Therefore, $L \subseteq K_0$. If we know that K_0 is a field, it follows that $L = K_0$, proving uniqueness.

It therefore suffices to show that K_0 is a coefficient field for K. We first observe that K_0 meets m only in 0. For if $u \in K_0 \cap m$, then u is a p^n th power for all n. But if $u = v^{p^n}$ then $v \in m$, so $u \in \bigcap_n m^{p^n} = (0)$.

Thus, every element of $K_0 - \{0\}$ is a unit of R. Now if $u = v^{p^n}$ and u is a unit of R, then $1/u = (1/v)^{p^n}$. Therefore, the inverse of every nonzero element of K_0 is in K_0. Since K_0 is clearly a ring, it is a subfield of R.

Finally, we want to show that given $\theta \in K$ some element of K_0 maps to θ. Let r_n denote an element of R that maps to $\theta^{1/p^n} \in K$. Then $r_n^{p^n}$ maps to θ. We claim that $\{r_n^{p^n}\}_n$ is a

Cauchy sequence in R, and so has a limit r. To see this, note that r_n and r_{n+1}^p both map to θ^{1/p^n} in K, and so $r_n - r_{n+1}^p$ is in m. Taking p^n powers, we find that

$$r_n^{p^n} - r_{n+1}^{p^{n+1}} \in m^{p^n}.$$

Therefore, the sequence is Cauchy, and has a limit $r \in R$. It is clear that r maps to θ. Therefore, it suffices to show that $r \in R^{p^k}$ for every k. But

$$r_k, r_{k+1}^p, \ldots, r_{k+h}^{p^h} \cdots$$

is a sequence of the same sort for the element θ^{1/p^k}, and so is Cauchy and has a limit s_k in R. But $s_k^{p^k} = r$ and so $r \in R^{p^k}$ for all k. $\square$

Before pursuing the issue of the existence of coefficient fields further, we show that the existence of a coefficient field implies that the complete local ring is a homomorphic image of a power series ring in finitely many variables over a field, and is also a module-finite extension of such a ring.

We first prove the following result, which bears some resemblance to Nakayama's Lemma, but is rather different, since M is not assumed to be finitely generated.

Proposition. *Let R be separated and complete in the I-adic topology, where I is a finitely generated ideal of R, and let M be an I-adically separated R-module. Let $u_1, \ldots, u_h \in M$ have images that span M/IM over R/I. Then $u_1, \ldots, u_h$ span M over R.*

Proof. Since $M = Ru_1 + \cdots + Ru_h + IM$, we find that for all n,

$$(*) \qquad I^nM = I^nu_1 + \cdots + I^nu_h + I^{n+1}M.$$

Let $u \in M$ be given. Then u can be written in the form $r_{01}u_1 + \cdots + r_{0h}u_h + \Delta_1$ where $\Delta_1 \in IM$. Therefore $\Delta_1 = r_{11}u_1 + \cdots r_{1h}u_h + \Delta_2$ where the $r_{1j} \in IM$ and $\Delta_2 \in I^2M$. Then

$$u = (r_{01} + r_{11})u_1 + \cdots + (r_{0n} + r_{1h})u_h + \Delta_2,$$

where $\Delta_2 \in I^2M$. By a straightforward induction on n we obtain, for every n, that

$$u = (r_{01} + r_{11} + \cdots + r_{n1})u_1 + \cdots + (r_{0h} + r_{1h} + \cdots + r_{nh})u_n + \Delta_{n+1}$$

where every $r_{jk} \in I^j$ for $1 \le k \le h$ and all $j \ge 0$ and $\Delta_{n+1} \in I^{n+1}M$. In the recursive step, the formula $(*)$ is applied to the element $\Delta_{n+1} \in I^{n+1}M$.

For every k, $\sum_{j=0}^{\infty} r_{jk}$ represents an element s_k of the complete ring R. We claim that

$$u = s_1u_1 + \cdots + s_hu_h.$$

The point is that if we subtract

$$\sigma_n = (r_{01} + r_{11} + \cdots + r_{n1})u_1 + \cdots + (r_{0h} + r_{1h} + \cdots + r_{nh})u_h$$

from u we get $\Delta_{n+1} \in I^{n+1}M$, and if we subtract σ_n from

$$s_1u_1 + \cdots + s_hu_h$$

we also get an element of $I^{n+1}M$, which we shall justify in greater detail below. Therefore,

$$u - (s_1u_1 + \cdots + s_hu_h) \in \bigcap_n I^{n+1}M = 0,$$

since M is I-adically separated.

It remains to see why $s_1u_1 + \cdots + s_hu_h - \sigma_n$ is in $I^{n+1}M$. This difference can be rewritten as $s'_1u_1 + \cdots + s'_hu_h$ where $s'_k = r_{n+1,k} + r_{n+2,k} + \cdots$. Hence, we simply need to justify the assertion that assertion that if $r_{jk} \in I^j$ for $j \geq n+1$ then

$$r_{n+1,k} + r_{n+2,k} + \cdots + r_{n+t,k} + \cdots \in I^{n+1},$$

which needs a short argument. Since I is finitely generated, we know that I^{n+1} is finitely generated by the monomials of degree $n+1$ in the generators of I, say, $g_1, \ldots, g_d$. Then $r_{n+1+t,k} = \displaystyle\sum_{\nu=1}^{d} q_{t\nu}g_\nu$ with every $q_{t\nu} \in I^t$ and $\displaystyle\sum_{t=0}^{\infty} r_{n+1+t,k} = \sum_{\nu=1}^{d}(\sum_{t=0}^{\infty} q_{t\nu})g_\nu$. □

We also note:

Proposition. *Let $f : R \to S$ be a ring homomorphism. Suppose that S is J-adically complete and separated for an ideal $J \subseteq S$ and that $I \subseteq R$ maps into J. Then there is a unique induced homomorphism $\widehat{R}^I \to S$ that is continuous (i.e., preserves limits of Cauchy sequences in the appropriate ideal-adic topology).*

Proof. $\widehat{R}^I$ is the ring of I-adic Cauchy sequences mod the ideal of sequences that converge to 0. The continuity condition forces the element represented by $\{r_n\}_n$ to map to

$$\lim_{n\to\infty} f(r_n)$$

(Cauchy sequences map to Cauchy sequences: if $r_m - r_n \in I^N$, then $f(r_m) - f(r_n) \in J^N$, since $f(I) \subseteq J$.) It is trivial to check that this is a ring homomorphism that kills the ideal of Cauchy sequences that converge to 0, which gives the required map $\widehat{R}^I \to S$. □

A homomorphism of quasilocal rings $h : (A, \mu, \kappa) \to (R, m, K)$ is called a *local homomorphism* if $h(\mu) \subseteq m$. If A is a local domain, not a field, the inclusion of A in its fraction field is not local. If A is a local domain, any quotient map arising from killing a proper ideal is local. A local homomorphism induces a homomorphism of residue class fields $\kappa = A/\mu \to R/m = K$.

Proposition. *Let A be a Noetherian ring that is complete and separated with respect to an ideal μ, which may be 0, let (R, m, K) be a complete local ring, and let $h : A \to R$ be a homomorphism, so that R is an A-algebra and μ maps into m. Thus, if (A, μ) is local, we are requiring that $A \to R$ be local. Suppose that $f_1, \dots, f_n \in m$ together with μR generate an m-primary ideal. Then:*

(a) *There is a unique continuous homomorphism $h : A[[X_1, \dots, X_n]] \to R$ extending the A-algebra map $A[X_1, \dots, X_n]$ taking X_i to f_i for all i.*

(b) *If K is module-finite over the image of A, then R is module-finite over the image of $A[[X_1, \dots, X_n]]$ under the map discussed in part (a).*

(c) *If the composite map $A \to R \twoheadrightarrow K$ is surjective, and $\mu R + (f_1, \dots, f_n)R = m$, then the map h described in (a) is surjective.*

Proof. (a) This is immediate from the preceding Proposition, since $(X_1, \dots, X_n)$ maps into m.

(b) $A[[X_1, \dots, X_n]]$ is complete and separated with respect to the the $\mathfrak{A}$-adic topology, where $\mathfrak{A} = (\mu, X_1, \dots, X_n)A[[X_1, \dots, X_n]]$. Given a Cauchy sequence of power series $\{f_k\}_k$, it is easy to see that the sequence of coefficients of a fixed monomial $X_1^{\nu_1} \cdots X_n^{\nu_n} = X^\nu$ is a Cauchy sequence in A in the μ-adic topology, and so has a limit $a_\nu \in A$. The only possible limit for the Cauchy sequence $\{f_k\}_k$ is the power series

$$\sum_{\nu \in \mathbb{N}^n} a_\nu X^\nu,$$

and it is easy to verify that this is the limit.

The expansion of the ideal $\mathfrak{A}$ of $A[[X_1, \dots, X_n]]$ to R is $\mu R + (f_1, \dots, f_n)R$, which contains a power of m, say m^N. Thus, $R/\mathcal{M}R$ is a quotient of R/m^N and has finite length: the latter has a filtration whose factors are the finite-dimensional K-vector spaces m^i/m^{i+1}, $0 \le i \le N-1$. Since K is module-finite over the image of A, it follows that $R/\mathfrak{A}R$ is module finite over over $A[[X_1, \dots, X_n]]/\mathfrak{A} = A/\mu$. Choose elements of R whose images in $R/\mathfrak{A}R$ span it over A/μ. By the Proposition stated on p. 2, these elements span R as an $A[[X_1, \dots, X_n]]$-module. We are using that R is $\mathfrak{A}$-adically separated, but this follows because $\mathfrak{A}R \subseteq m$, and R is m-adically separated.

(c) We repeat the argument of the proof of part (b), noting that now $R/\mathfrak{A}R \cong K \cong A/\mu$, so that $1 \in R$ generates R as an $A[[X_1, \dots, X_n]]$ module. But this says that R is a cyclic $A[[X_1, \dots, X_n]]$-module spanned by 1, which is equivalent to the assertion that $A[[X_1, \dots, X_n]] \to R$ is surjective. $\square$

We have now done all the real work needed to prove the following:

Theorem. *Let (R, m, K) be a complete local ring with coefficient field $K_0 \subseteq K$, so that $K_0 \subseteq R \twoheadrightarrow R/m = K$ is an isomorphism. Let $f_1, \dots, f_n$ be elements of m generating* *an ideal primary to m. Let $K_0[[X_1, \dots, X_n]] \to R$ be constructed as in the preceding Proposition, with X_i mapping to f_i and with $A = K_0$. Then:*

(a) *R is module-finite over $K_0[[X_1, \dots, X_n]]$.*

(b) *Suppose that $f_1, \dots, f_n$ generate m. Then the homomorphism $K_0[[x_1, \dots, x_n]] \to R$ is surjective. (By Nakayama's lemma, the least value of n that may be used is the dimension as a K-vector space of m/m^2.)*

(c) *If $d = \dim(R)$ and $f_1, \dots, f_d$ is a system of parameters for R, the homomorphism*

$$K_0[[x_1, \dots, x_d]] \to R$$

is injective, and so R is a module-finite extension of a formal power series subring.

Proof. (a) and (b) are immediate from the preceding Proposition. For part (c), let $\mathfrak{A}$ denote the kernel of the map $K_0[[x_1, \dots, x_d]] \to R$. Since R is a module-finite extension of the ring $K_0[[x_1, \dots, x_d]]/\mathfrak{A}$, $d = \dim(R) = \dim(K_0[[x_1, \dots, x_d]]/\mathfrak{A})$. But we know that $\dim(K_0[[x_1, \dots, x_d]]) = d$. Killing a nonzero prime in a local domain must lower the dimension. Therefore, we must have that $\mathfrak{A} = (0)$. $\square$

Thus, when R has a coefficient field K_0 and $f_1, \dots, f_d$ are a system of parameters, we may consider a formal power series

$$\sum_{\nu \in \mathbb{N}^d} c_\nu f^\nu,$$

where $\nu = (\nu_1, \dots, \nu_d)$ is a multi-index, the $c_\nu \in K_0$, and f^ν denotes $f_1^{\nu_1} \cdots f_d^{\nu_d}$. Because R is complete, this expression represents an element of R. Part (c) of the preceding Theorem implies that this element is not 0 unless all of the coefficients c_ν vanish. This fact is sometimes referred to as the *analytic independence of a system of parameters*. The elements of a system of parameters behave like formal indeterminates over a coefficient field. Formal indeterminates are also referred to as *analytic indeterminates*.