THE STRUCTURE THEORY OF COMPLETE LOCAL RINGS

ZHAN JIANG

CONTENTS

1. COMPLETE LOCAL RINGS

1.1. **Local rings.** A local ring R contains a field iff $\mathrm{char}(R) = \mathrm{char}(K)$:

- If $\mathrm{char}(K) = 0$, then it's clearly that R does. Therefore R contains a copy of $\mathbb{Z}$. Every integer has a nonzero image in $R/\mathfrak{m}$, therefore they are units in R, then $\mathbb{Q}$ injects into R. If R contains a field of characteristic 0, then every prime integer is invertible, therefore $\mathrm{char}(K) = 0$.
- If $\mathrm{char}(K) = p$, $\mathrm{char}(R) = p$. Then R contains $\mathbb{Z}/p\mathbb{Z}$. If R contains a copy of $\mathbb{Z}/p\mathbb{Z}$, then $\mathrm{char}(K) = p$.

So we have following definition

Definition 1.1. A local ring $(R, \mathfrak{m}, K)$ is **equicharacteristic** if R contains a field. A local ring $(R, \mathfrak{m}, K)$ is **mixed characteristic** if it's not equicharacteristic.

Now we know that this definition is equivalent to the condition that R and K has the same characteristic. This suggests why we use the term "equicharacteristic".

Remark 1.2. The residue field K of a mixed characteristic local ring R always has characteristic p while R has characteristic either 0 or a power of p: If $\mathrm{char}(R) \neq 0$, then pick an integer a which is zero in R. If a has more than one prime factor, then write $a = bc$ where $b, c > 1$ are relatively prime integers. Then $bc = 0$ implies that one of them is in the maximal ideal. If both are in the maximal ideal, then $1 \in \mathfrak{m}$, a contradiction. Therefore one of them is not in $\mathfrak{m}$, which will be a unit. So we can pass to a smaller integer with less prime factors. Repeat this until we reach a integer of prime power. That will be the characteristic of R.

1.2. **Hensel's Lemma.**

Lemma 1.3 (Hensel)**.** *Let $(R, \mathfrak{m}, K)$ be a $\mathfrak{m}$-adically separated, complete quasilocal ring. Let $f \in R[x]$ be a monic polynomial of degree d and let $F = \overline{f}$ be the image of f in $K[x]$ (Here the map is induced by $R \to K$ modulo $\mathfrak{m}$).*

If $F = GH$ where G, H are polynomials in $K[x]$ and are monic of degree s, t respectively (Clearly $s + t = d$). And G and H are relatively prime in $K[x]$. Then there are unique monic polynomials $g, h \in R[x]$ of degree s, t respectively such that $f = gh$ and $\overline{g} = G, \overline{h} = H$.

Proof. Let F_n be the image of f in $(R/\mathfrak{m}^n)[x]$, we recursively construct monic polynomials $G_n, H_n \in (R/\mathfrak{m}^n)[x]$ of degree s, t respectively such that $F_n = G_n H_n$. We shall also show that $G_n(H_n)$ maps to $G_{n-1}(H_{n-1})$ and all of them are unique. Then $(G_1, G_2, ...)$ will define g and $(H_1, H_2, ...)$ will defien h. We have $f - gh \in \cap_i \mathfrak{m}^i = \{0\}$.

Now let $G_1 = G$ and $H_1 = H$ and assume that G_{n-1} and H_{n-1} are given. Construct two monic polynomials $G'_n, H'_n \in (R/\mathfrak{m}^n)[x]$ by lifting every coefficient of G_n and H_n respectively. Then G'_n has degree s and H'_n has degree t. And we have

$$F_n - G'_n H'_n = 0 \mod \mathfrak{m}^{n-1} R[x]$$

We want to show that there are unique $\widetilde{G}_n$ of degree at most $s-1$ and $\widetilde{H}_n$ of degree at most $t-1$ in $\mathfrak{m}^{n-1}R[x]$ such that

$$F_n - (G'_n + \widetilde{G}_n)(H'_n + \widetilde{H}_n) = 0$$

So let $D_n = F_n - G'_n H'_n \in \mathfrak{m}^{n-1}R[x]$, then we aim to find such polynomials such that

$$D_n - G'_n \widetilde{H}_n - \widetilde{G}_n H'_n - \widetilde{G}_n \widetilde{H}_n = 0$$

But note that we are working in $(R/\mathfrak{m}^n)[x]$ and $\widetilde{G}_n \widetilde{H}_n \in \mathfrak{m}^{2n-2} R[x]$. So we are looking for $\widetilde{G}_n$ and $\widetilde{H}_n$ such that

$$D_n = G'_n \widetilde{H}_n + \widetilde{G}_n H'_n$$

Now we have to use the condition that G and H are relatively prime in $K[x]$. So G, H generates the unit ideal in $K[x]$ and $((R/\mathfrak{m}^n)[x])_{\mathrm{red}}$ is $K[x]$. Therefore G'_n and H'_n shall generate the unit ideal as well. We can find $A, B \in (R/\mathfrak{m}^n)[x]$ such that $1 = AG'_n + BH'_n$. Then we have

$$D_n = (D_n A)G'_n + (D_n B)H'_n$$

Now divide $D_n A$ by H'_n, we have

$$D_n A = H'_n Q + \widetilde{H}_n$$

where $\deg(\widetilde{H}_n) \leq t - 1$. So

$$0 = H_{n-1} Q + \widetilde{H}_n \mod \mathfrak{m}^{n-1} R[x]$$

$\widetilde{H}_n$ has smaller degree than $H_{n-1}Q$, therefore $\widetilde{H}_n, Q$ must be zero, i.e. must be in $\mathfrak{m}^{n-1}R[x]$. Now we have

$$D_n = \widetilde{H}_n G'_n + (D_n B - Q G'_n) H'_n$$

where both D_n and $\widetilde{H}_n G'_n$ has degree $< n$, which forces $D_n B - Q G'_n$, which we denote $\widetilde{G}_n$, to be of degree $\leq s - 1$.

Now we want to show that $\widetilde{H}_n$ and $\widetilde{G}_n$ are unique. If we have a different choice for these two polynomial. Take the difference then we have $\alpha G'_n + \beta H'_n = 0$ with $\deg(\alpha) \leq t - 1$ and $\deg(\beta) \leq s - 1$. G'_n is a unit if we modulo H'_n, then α is divisible by H'_n, but H'_n is monic. This implies that $\alpha = 0$ therefore $\beta = 0$.

So we set $G_n = G'_n + \widetilde{G}_n$ and $H_n = H'_n + \widetilde{H}_n$. If we have a different choice for G_n and H_n, then their difference will be our $\widetilde{G}_n$ and $\widetilde{H}_m$, which will be unqiue, i.e. 0. So G_n and H_n are unique. □

1.3. **Complete local rings.** A local ring $(R, \mathfrak{m}, K)$ is complete if it's complete with respect to its maximal ideal $\mathfrak{m}$.

2. The Equicharacteristic Case

2.1. Coefficient fields.

2.1.1. *Char* = 0.

Definition 2.1. A field in a local ring such that maps onto the residue field is called a **coefficient field** of R.

We shall prove that a complete local ring always contains a coefficient field. Once R contains such a field, we can write $R = K \oplus_K \mathfrak{m}$. We shall prove the existence of a coefficient field in equicharacteristic case:

Theorem 2.2 (Char=0)**.** *Let $(R, \mathfrak{m}, K)$ be an equicharacteristic complete local ring of characteristic 0. Then R has a coefficient.*

Proof. Let Λ be the set of all subrings of R that happens to be fields. By hypothesis, Λ is not empty. The union of any chain of elements in Λ will again be a subring of R that is a field. By Zorn's lemma, Λ will have a maximal element, call it K_0.

Now we have a map $K_0 \subseteq R \to K$, this is an injection from K_0 to K. To finish the proof, we only need to show that this map is surjection. Denote the image of K_0 in K by K_1.

Suppose that the map is not surjection, pick an element $\alpha \in K - K_1$. There are two cases:

(1):Suppose α is transdental over K_1. Let a be the perimage of α in R. Then a is clearly transdental over K_0. Therefore $K_0[a]$ is a polynomial subring in R and every nonzero element is a unit in R: otherwise a would be algebraic over K_0. Then we have $K_0(a) \subseteq R$, which is a larger subfield of R containing K_0.

(2):Suppose α is algebraic over K_1. Let F be the minimal polynomial of α in K_1 and let f be the preimage of F with coefficients in K_0. Since $F(x) \in K[x]$ factors as $(x - t)H(x)$ and the two factors are relatively prime (Because $\mathrm{char}(K) = 0 \Rightarrow K$ is a perfect field). Now we can apply Hensel's lemma and conculde that $f(x) = (x - a)h(x)$ where a maps to α. Now we show that $K_0[a]$ maps onto $K_1[\alpha]$. We only need to show surjectivity. If $P(x) \in K_0[x]$ kills a then $f|P$ therefore $P(\alpha) = 0$. So $K_0[a] \cong K_1[\alpha]$. Therefore $K_0[a]$ is a larger subfield of R containing K_0. □

Remark 2.3. From the proof we see that any maximal subfield is a coefficient field. The proof also shows that in $\mathrm{char}(R) = \mathrm{char}(K) = p$ case, the maximal subfield can only be a purely inseperable algebraic extension of K.

2.1.2. *Char = p, K is perfect.* Now we want to write down the similar theorem for the case where R is characteristic p and K is perfet. We shall give a different prove. Note that the existence of a coefficient field already holds by the Remark 2.3 above.

Theorem 2.4 (Char = p, K is perfect)**.** *Let $(R, \mathfrak{m}, K)$ be an equicharacteristic complete local ring of prime characteristic $p > 0$. If K is perfect, then R has a unique coefficient field, which is $K_0 = \cap^n \mathcal{F}^n(R)$ where $\mathcal{F}$ is the Frobenius map.*

Proof. Let L be a coefficient field for R. Since F is an isomorphism on L. So $L \cong \mathcal{F}(L) \cong \mathcal{F}^2(L) \cong \cdots$. Therefore $L \subseteq K_0$. Once we show that K_0 is a field, by the construction of L, we know that $L = K_0$.

Now we want to show that K_0 is a field. First we show that $K_0 \cap \mathfrak{m} = \{0\}$: Pick $u \in K_0 \cap \mathfrak{m}$, then for any n we have $u = \mathcal{F}^n(v)$ for some $v \in \mathfrak{m}$. Therefore $u \in \mathfrak{m}^{p^n} \Rightarrow u \in \cap_n \mathfrak{m}^{p^n} = (0)$.

So every element of $K_0 - \{0\}$ is a unit of R, it follows that K_0 is a coefficient field. □

Remark 2.5. We can given an alternative argument without using Zorn's lemma: We can still show that K_0 is a field by the proof above, next we have to show that $K_0 \subseteq R \to K$ is surjection:

Proof of the Remark. For any element $\alpha \in K$, let $a_n \in R$ be the element maps to $\alpha^{1/p^n} \in K$, then $a_n^{p^n}$ maps to α. We claim that $\{a_n^{p^n}\}$ is a Cauchy sequence in R: Since r_n and r_{n+1}^p both maps to α^{1/p^n}, we have $r_n - r_{n+1}^p \in \mathfrak{m}$ so $r_n^{p^n} - r_{n+1}^{p^{n+1}} \in \mathfrak{m}^{p^n}$.

Denote the limit of the sequence above by a, then it's obvious that a maps to α. In order to show that $a \in L_0$, we need to show that $a \in R^{p^n}$ for every n. This comes from that we can pass to a subsequence and take p^nth root of the sequence $r_n, r_{n+1}^p, \ldots$. It's again Cauchy and has a limit b, but then $b^{p^n} = a$ so $a \in R^{p^n}$. □

2.1.3. *Char = p, K is not perfect.* Here we deal with the final case, the positive prime characteristic case with residue field not perfect. This time the coefficient is again not unqiue.

We have to use the technique of p-base, here is definition

Definition 2.6. Let K be a field of prime characteristic p. Finitely many elements $\lambda_1, \ldots, \lambda_n$ in $K - K^p$ are called **p-independent** if $[K^p[\lambda_1, \ldots, \lambda_n] : K^p] = p^n$. An infinitely subset of $K - K^p$ is **p-independent** if every finite subset is p-independent.

This is equivalent to TO BE ADDED

A maximal p-independent subset of $K - K^p$ is a p-base for K over K^p. Its existence is guranteed by Zorn's lemma: since the union of a chain of p-independent sets is still p-independent.

It's easy to see that $K = K^p[\Lambda]$. So Λ is a p-base iff every element of K is an unique polynomial in elements in Λ over K^p with exponents in every element is at most $p - 1$.

For any $q = p^n$, the set $\Lambda^q = \{\lambda^q : \lambda \in \Lambda\}$ is a p-base for K^q over K^{pq}. In particular, Λ^p is a p-base for K^p over K^{p^2} and by multiplying two bases we see that the monomials in the elements of Λ of degree at most $p^2 - 1$ are a basis for K over K^{p^2}. Inductively we see that monomials in the elements of Λ of degree at most $p^n - 1$ are a basis for K over K^{p^n}. Therefore $K = K^{p^n}[\Lambda]$.

Theorem 2.7. *Let $(R, \mathfrak{m}, K)$ be a complete local ring of prime characteristic p. Let Λ be a p-base for K and let T be a lifting of Λ to R. Then there is a unique coefficient field for R containing T, namely, $K_0 = \cap_n R_n[T]$ where $R_n = R^{p^n}$.*

Proof. Any coefficient field must contain some lifting of Λ. We note that K_0 is already a subring containing T. If L is a coefficient field containing T, then T is a p-base for L. Therefore for any n, $L = L^{p^n}[T] \subseteq R_n[T]$. So $L \subseteq K_0$. Once we show that K_0 is a coefficient field, the uniqueness will follow.

Call a polynomial is a p^n-polynomial if every variable has exponent at most $p^n - 1$. Therefore every element in $R_n[T]$ could be expressed as a p^n-polynomial in elements of T and every element in $K^{p^n}[\Lambda]$ is a p^n-polynomial in elements of Λ.

Next we observe that

$$R_n[T] \cap \mathfrak{m} \subseteq \mathfrak{m}^{p^n}$$

Any p^n-polynomial in $\mathfrak{m}$ will have zero image in K^{p^n}, therefore every coefficient of the polynomial is zero. Then every coefficient is in $\mathfrak{m}$ and is in $\mathfrak{m}^{p^n}$. Then the inclusion follows.

But now we see that $K_0 \cap \mathfrak{m} = \cap_n (R_n[T] \cap \mathfrak{m}) \subseteq \cap_n \mathfrak{m}^{p^n} = \{0\}$. We can conclude that K_0 injects into K. It sufficies to show that $K_o \to K$ is surjection.

Let $\alpha \in K$ be given. Since $K = K^{p^n}[\Lambda]$, we can map $R_n[T]$ onto K so we can choose $a_n \in R_n[T]$, but then $a_{n+1} - a_n \in R_n[T] \cap \mathfrak{m} \subseteq \mathfrak{m}^{p^n}$. So $a_1, a_2, \ldots$ form a Cauchy sequence and has a limit, call it a. Then a maps to α.

a is independent of the choice of the Cauchy sequence: If we have one more sequence $a_1', a_2', \ldots$ with $a_n' \in R_n[T]$ and each maps to α. Then $a_i - a_i' \in R_n[T] \cap \mathfrak{m} \subseteq \mathfrak{m}^{p^n}$. So they have the same limit.

Next we want to show that $a \in R_n[T]$ for every n, which will complete our proof. We fix n and write α as a p^n-polynomial in elements of Λ over K^{p^n}.

$$\alpha = \sum_{\mu} \beta_\mu^{p^n} \mu$$

where μ are monomials in Λ and $\beta_\mu \in K$. Replace each μ by corresponding monomial in T, which we denote $\widetilde{\mu}$. For each β_μ, we can construct a sequence $b_{k,\mu}$ as above.Then

$$a_k = \sum_\mu b_{k,\mu}^{p^n} \widetilde{\mu}$$

form a Cauchy sequence and converges to a as each a_k maps to α and $a_k \in R_k[T]$. But we also note that

$$\lim_k a_k = \sum_\mu (\lim_k b_{k,\mu})^{p^n} \widetilde{\mu}$$
$$a = \sum_\mu b_\mu^{p^n} \widetilde{\mu} \in R_n[T]$$

□

2.2. **Structure theorem.** Once we know that existence of a coefficient field in a complete local ring R, we can show that it is a holomorphic 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 following general result:

Proposition 2.8. *Suppose $I \subseteq R$ is a fintely generated ideal and R is I-adically complete. Let $\mathfrak{m}$ be an I-adically separated R-module. Let $u_1, ..., u_n \in M$ have images that span M/IM over R/I, then $u_1, ..., u_n$ spans $\mathfrak{m}$ over R.*

Proof. Since $\mathfrak{m} = Ru_1 + Ru_2 + \cdots + Ru_n + IM$, given any element $u \in M$, we can write

$$u = r_1^{(0)} u_1 + \cdots + r_n^{(0)} u_n + v^{(1)}$$

But we can also write $IM = Iu_1 + \cdots + Iu_n + I^2M$, so we can expand $v^{(1)} \in IM$ to

$$\begin{aligned} u &= r_1^{(0)} u_1 + \cdots + r_n^{(0)} u_n + v^{(1)} \\ &= (r_1^{(0)} + r_1^{(1)}) u_1 + \cdots + (r_n^{(0)} + r_n^{(1)}) u_n + v^{(2)}. \end{aligned}$$

Now we can replace $v^{(2)} \in I^2M$ be the expansion $I^2M = I^2u_1 + \cdots + I^2u_n + I^3M$. Therefore inductively we have

$$u = (r_1^{(0)} + \cdots + r_1^{(k)}) u_1 + \cdots + (r_n^{(0)} + \cdots + r_n^{(k)}) u_n + v^{(k+1)}$$

where $r_*^{(j)} \in I^j$ and $v^{j+1} \in I^{j+1}M$. For eveery j, we see that $\sum_{j=0}^\infty r_i^{(j)}$ represents an element s_i in R. We claim that $u = s_1u_1 + \cdots + s_nu_n$.

The point is that we have

$$u - (r_1^{(0)} + \cdots + r_1^{(k)}) u_1 - \cdots - (r_n^{(0)} + \cdots + r_n^{(k)}) u_n \in I^{k+1}M$$
$$s_1u_1 + \cdots + s_nu_n - (r_1^{(0)} + \cdots + r_1^{(k)}) u_1 - \cdots - (r_n^{(0)} + \cdots + r_n^{(k)}) u_n \in I^{k+1}M$$

So

$$u - s_1u_1 - \cdots - s_nu_n \in I^{k+1}M$$

for every k, hence the difference is in $\cap_k I^kM = \{0\}$. □

Remark 2.9. We tacitly used the fact that the infinite sum $r_i^{(k)} + r_i^{(k+1)} + \cdots \in I^kM$. This actually requires a proof, which we record here:

Since I is finitely generated (That's why we need this condition in the proposition) then I^k is generated by monomials in these generators of degree k. We denote these monomials $g_1, ..., g_m$. Then for every j we have

$$r_i^{(k+j)} = q_1^{(j)} g_1 + \cdots + q_m^{(j)} g_m$$

where $q_*^j \in I^j$ since $I^{k+j} = I^k(I^j)$. Thus

$$r_i^{(k)} + r_i^{(k+1)} + \cdots = (q_1^{(k)} + q_1^{(k+1)} + \cdots) g_1 + \cdots + (q_m^{(k)} + q_m^{(k+1)} + \cdots) g_m$$

Each infinite sum will converge to an element in R and the conclusion holds.

We have following proposition:

Proposition 2.10. *Let $(S, \mathfrak{n}, L) \to (R, \mathfrak{m}, K)$ be a local map of complete local rings. Suppose that $r_1, ..., r_k \in \mathfrak{m}$ together with $\mathfrak{n}R$ generate an $\mathfrak{m}$-primary ideal, then there is a unique continuous map $S[\![X_1, ..., X_k]\!] \to R$ induced by mapping X_i to r_i in $S[X_1, ..., X_n] \to R$.*

(1) If K is a finite algebraic extension over L, then R is module finite over the image of $S[\![X_1, ..., X_k]\!]$
(2) If $L \to K$ is an isomorphism and $\mathfrak{n}R + (r_1, ..., r_k)R = \mathfrak{m}$, then the map $S[\![X_1, ..., X_k]\!] \to R$ is a surjection.

Proof. (1): Let $\widetilde{R} = S[\![X_1, ..., X_k]\!]$ and $\widetilde{\mathfrak{m}} = (X_1, ..., X_k)\widetilde{R} + n\widetilde{R}$. We first show that R is module-finite over the image of $\widetilde{R}$: the image of $\widetilde{\mathfrak{m}}$, which we denote $\widetilde{\mathfrak{m}}R$, is $\mathfrak{m}$-primary, which contains a power of $\mathfrak{m}$. So $R/\widetilde{\mathfrak{m}}R$ is of finite length over K and it follows that $R/\widetilde{\mathfrak{m}}R$ is a finite-dimensional vector space over K. But since K is a finite extension of L. This continues to be a finite dimensional vector space over $L = \widetilde{R}/\widetilde{\mathfrak{m}}$. We can choose a finite set of generators for $R/\widetilde{\mathfrak{m}}R$ over $\widetilde{R}/\widetilde{\mathfrak{m}}$, and by Proposition 2.8 we see that this set will generate R over (the image of) $\widetilde{R}$.

(2):We can carry out the same argument and find that $R/\widetilde{\mathfrak{m}}R$ is a finite-dimensional vector space over $\widetilde{R}/\widetilde{\mathfrak{m}}$. But this time the dimension is 1. Therefore we can generate R over $\widetilde{R}$ by 1, which means that the map is surjection. □

Now R is complete and contains a coefficient field K_0 and let $r_1, ..., r_k$ be k elements in $\mathfrak{m}$. Then we can map $K_0[X_1, ..., X_k]$ to R by mapping X_i to r_i. Then this will induce a unique map $K_0[\![X_1, ..., X_k]\!] \to R$.

Now we are ready to prove the structure theorem for complete local rings:

Theorem 2.11. *Let $(R, \mathfrak{m}, K)$ be a complete local ring with coefficient field K_0. Let $f_1, ..., f_d$ be a system of parameters for R where $d = \dim(R)$. Extend them to be a set of generators $r_1, ..., r_d, r_{d+1}, ..., r_n$ for $\mathfrak{m}$ where n is the embedded dimension of R. Then*

(1) The unique map $K_0[\![X_1, ..., X_d]\!] \to R$ is injective and R is module-finite over the image.
(2) The unique map $K_0[\![X_1, ..., X_n]\!] \to R$ is surjective.

Proof. (1): Let $\widetilde{R} = K_0[\![X_1, ..., X_d]\!]$ and $\widetilde{\mathfrak{m}} = (X_1, ..., X_d)\widetilde{R}$. By Proposition 2.10 above, R is module-finite over the image of $\widetilde{R}$. We only need to show injectivity. Let I be the kernel of $\widetilde{R} \to R$, then killing I will lower the dimension, but the dimension of the image has to be $d = \dim(R)$. So I must be zero.

(2): This is a direct corollary of Proposition 2.10 □

Remark 2.12. From part (1) of the theorem above we see that the set of system of parameters $r_1, ..., r_d$ together with the coefficient field generates a formal power series ring inside R, therefore any former power series in $r_1, ..., r_d$ is zero iff all coefficients are zero. This fact is usually referred to as **analytic independence of a system of parameters**.

From the proof, we immediately have following corollary:

Corollary 2.13. *A complete regular local ring with a coefficient field is a formal power series ring over its coefficient field.*

Proof. Just notice that the set of system of parameters are also a set of generators of $\mathfrak{m}$. So the map $K_0[\![X_1, ..., X_d]\!] \to R$ is injective as well as surjective. □

3. The Weierstrass Perparation Theorem

3.1. **The theorem.** Let $(R, \mathfrak{m}, K)$ be a complete local ring and let x be a formal indeterminate over R. let $f = \sum_{i=0}^{\infty} a_i x^i \in R[\![x]\!]$. We have following definition

Definition 3.1. f is said to be **regular in x of order n** if $a_n \notin \mathfrak{m}$ while $a_i \in \mathfrak{m}$ for all $i < n$.

So basically, if f is regular in x of order n, then $f = \widetilde{f} + x^n u$ where $\widetilde{f}$ is a polynomial in $\mathfrak{m}[x]$ (all coefficients in $\mathfrak{m}$) and u is a unit in $R[\![x]\!]$.

Theorem 3.2 (Weierstrass Preparation Theorem)**.** *Let $(R, \mathfrak{m}, K)$ be a complete local ring and let x be a formal indeterminate over R. Let $f \in R[\![x]\!]$ be regular in x of order n. Then $R[\![x]\!]/fR[\![x]\!]$ is spanned by a free basis $1, x, ..., x^{n-1}$ over R. Every element $g \in R[\![x]\!]$ can be written uniquely in the form $qf + r$ where $q \in R[\![x]\!]$ and $r \in R[x]$ is a polynomial of degree at most $n - 1$.*

Proof. Let $\mathfrak{m} = R[\![x]\!]/(f)$ be a finitely generated module over $R[\![x]\!]$. First of all we note that $M/\mathfrak{m}M \cong K[\![x]\!]/(\overline{f})$ where $\overline{f}$ is the image of f under the map $R[\![x]\!] \to K[\![x]\!]$. Note that $\overline{f} = \overline{u}x^n$ where $\overline{u}$ continues to be a unit. So $K[\![x]\!]/(\overline{f}) \cong K[\![x]\!]/(x^n)$, which is a K-vector space where $1, x, ..., x^{n-1}$ form a K-basis.

Now we want to apply Proposition 2.8. In order to do that, we need M to be $\mathfrak{m}$-adically separated. But this follows from the fact that $\mathfrak{m}$ is finitely generated over $R[\![x]\!]$. Therefore it's (m, x)-adically separated and so $\mathfrak{m}$-adically separated. Now $1, x, ..., x^{n-1}$ spans $M/\mathfrak{m}M$ over $R/\mathfrak{m}$. So they will span M over R.

Next we want to show that $q'f + r'$ is another such representation. Then $(r' - r) = (q - q')f$, so we only need to show that if we have $r = qf$ where r is a polynomial of degree at most $n - 1$, then $q = 0$.

Suppose otherwise. Since some coefficient of q is not 0, we can choose t such that q is not 0 in $R[\![x]\!]/\mathfrak{m}^t R[\![x]\!]$. Choose such a t as small as possible and fix it. Now working in $R[\![x]\!]/\mathfrak{m}^t R[\![x]\!]$: assume that $q = ax^d$+higher degree terms. Note that every coefficient (including a) now in q will be in $\mathfrak{m}^{t-1}$. Also all terms of f of degree smaller than n will have coefficient in $\mathfrak{m}$, hence, they will kill q. Once we multiply by f there is one and only one nozero term of degree $n + d$. But then $\deg(qf) \geq d + n > n - 1$, a contradiction! □

Corollary 3.3. *Let $R[\![x]\!]$ and f be as stated in the above theorem and f is regular of order n in x. Then f has a unique multiple qf which is a monic polynomial in $R[x]$ of degree n. The q is a unit and qf has all non-leading coefficients in $\mathfrak{m}$.*

Proof. We apply the Weierstrss Preparation Theorem to $g = x^n$, we get $x^n = qf + r$, which is $x^n - r = qf$. The uniqueness part follows from the uniqueness of the theorem.

Now work in $R[\![x]\!]/\mathfrak{m}R[\![x]\!]$, then $x^h - \overline{r} = \overline{q}\overline{f}$. $\overline{f}$ is a unit u times x^h. So $\overline{r}$ is necessarily 0 and we have $x^h = x^h u\overline{q}$. Cancelling x^n we get $\overline{q}$ is a unit in $K[\![x]\!]$ and it follows that q is a unit in $R[\![x]\!]$. □

Remark 3.4. The polynomial qf is called **the unique monic associate of** f.

The result is usually applied to the formal power series ring in k variables $K[\![x_1, ..., x_k]\!]$: One may take $R = K[\![x_1, ..., x_{k-1}]\!]$ and let $x = x_n$. In this case f is regular in x_n if and only if it involves a term cx_k^n where $c \in K - \{0\}$. The regularity of f of order n in x_k is equivalent to the assertion that under the map $K[\![x_1, ..., x_k]\!] \to K[\![x_k]\!]$ which kills $x_1, ..., x_{k-1}$, the image of f is a unit times x^n.

Any nonzero element can be made regular in x_k by a change of variables:

- If K is infinite: We write f as $f_0 + f_1 + f_2 + \cdots$ where f_j is homogeneous in $x_1, ..., x_k$ of degree j. Let suppose $G = f_j$ involves x_k. Apply a degree-preserving map $x_i \mapsto x_i + \lambda_i x_k$ for $i < k$ and $x_k \mapsto \lambda_k x_k$, then the image of G will be a polynomial with a term $G(\lambda_1, ..., \lambda_k)x_k^j$. Notice that G is nonzero and K is infinite, we can choose some $\lambda_1, ..., \lambda_k$ such that $G(\lambda_1, ..., \lambda_k) \neq 0$.
- If K is finite, we will apply the map $x_i \mapsto x_i + x_k^{N_i}$ for $1 \leq i \leq k - 1$ and keeps x_k unchanged. Choose a monomial order $x_1^{a_1}x_2^{a_2} \cdots x_k^{a_k} < x_1^{b_1}x_2^{b_2} \cdots x_k^{b_k}$ if $a_1 = b_1, ..., a_i = b_i$ and $a_{i+1} < b_{i+1}$. Now let $x_1^{d_1} \cdots x_k^{d_k}$ be the smallest monomial with nonzero coefficient in f and let $d = \max\{d_1, ..., d_n\}$. Let $N_i = (kd)^{k-i}$. We claim that the image of f is regular in x_n: After killing $x_1, ..., x_{k-1}$ we get

  $$f(x_k^{N_1}, x_k^{N_2}, ..., x_k^{N_{k-1}}, x_k)$$

  And there is a term $x_k^{d_1N_1 + \cdots + d_{k-1}N_{k-1} + d_n}$ coming from the smallest term. We just need to show that this term won't be cancelled by other terms.

For any other term $x_1^{e_1}\cdots x_k^{e_k}$. The image of this is $x_k^{e_1N_1+\cdots+e_{k-1}N_{k-1}+e_n}$. So we just need to show that

$$e_1N_1+\cdots+e_{k-1}N_{k-1}+e_n > d_1N_1+\cdots+d_{k-1}N_{k-1}+d_n$$

Assume that $e_j = d_j$ for $j < i$ and $e_i > d_i$. Then it's equivalent to show that

$$(e_i-d_i)N_i+\sum_{j>i}(e_j-d_j)N_j > 0$$

which is

$$\begin{aligned}(e_i-d_i)N_i+\sum_{j>i}(e_j-d_j)N_j &> N_i-\sum_{j>i}d_jN_j\\ &> N_i-d\sum_{j>i}N_j\\ &= (kd)^{k-i}-d\sum_{j>i}(kd)^{k-j}\\ &= (kd)^{k-i}-d(kd)^{k-i-1}(k-i)\\ &> (kd)^{k-i}-(kd)(kd)^{k-i-1}=0\end{aligned}$$

So the image of f is regular in x_k.

3.2. **Application.** Now we are ready to prove that every power series ring in finitely many variables over a field is an UFD. In fact this is true for any regular local rings.

Theorem 3.5. *Let K be a field and let $R = K[\![x_1, ..., x_n]\!]$ be the formal power series ring in n variables over K. Then R is a UFD.*

Proof. Let $R_n = K[\![x_1, ..., x_n]\!]$ and $\mathfrak{m}_n$ be the ideal of R_n. If $n = 0$ then $R_n = K$ is a field and the conclusino follows. If $n = 1$, then R_n is a DVR therefore it's a UFD.

Suppose $n > 1$. It sufficies to prove that if $f \in \mathfrak{m}_n$ is irreducible then it's prime. Suppose that $f|gh$ where $g, h \in m$. If g or h is a unit, then the assumption is meaningless. We have an equation $qf = gh$. Since f is irreducible, we have that $q \in \mathfrak{m}$. We may make a change of variables so that f, q, g, h are regular in x_n. Then we can multiply both sides by some units to make f, g, h into their unique monic associated polynomials. Then we have the same equation with $f, g, h \in R_{n-1}[x_n]$.

We can divide gh by f in $R_{n-1}[x_n]$ and get $gh = qf + r$ where $\deg(r) < \deg(f)$. The Weierstrass Preparation Theorem guarantees that the representation is unique in $R_{n-1}[\![x_n]\!]$. Therefore $r = 0$ and q is also a polynomial in $R_{n-1}[x_n]$.

By induciton hypothesis, we know that R_{n-1} is UFD hence $R_{n-1}[x_n]$ is UFD. Once we know that f continues to be irreducible in $R_{n-1}[x_n]$, then we will have $f|g$ or $f|h$. If not, write $f = f_1f_2$ with $\deg(f_1) < \deg(f)$ and $\deg(f_2) < \deg(f)$. Modulo $\mathfrak{m}_{n-1}$ we have that $x_n^d = \overline{f}_1\overline{f}_2$. So each of them is a monic polynomial with all non-leading coefficients in $\mathfrak{m}_{n-1}$. Thus they are not units in R_n. A contradiction! □

4. The Mixed Characteristic Case

4.1. **Coefficient rings.**

Definition 4.1. A **coefficient ring** is either a field or a complete local ring (V, pV, K) where K has characteristic $p > 0$. If R is complete local, then V is a **coefficient ring** for R if $V \subseteq R$ is a coefficient ring, $V \to R$ is local and the induced map of residue fields is an isomorphism.

In the mixed characteristic case, there are basically two possibilities: R has characteristic 0 or R has characteristic p^n. The second case is where p is nilpotent, and it will be the essential case

4.2. **Char = p^n.** First of all we have a lemma holds for any local ring.

Lemma 4.2. *Let $(R, \mathfrak{m}, K)$ be local with K of prime characteristic p. If $r \equiv s \mod \mathfrak{m}$ and n is an integer. Then for any $N \geq n-1$, let $q = p^N$, we have $r^q \equiv s^q \mod \mathfrak{m}^n$*

Proof. This is true when $n = 1$ and we prove by induction. Assume that it's true for some $N \geq n-1$, we have to show that it's true for $N+1 \geq n$.

Since $r^q - s^q = t \in \mathfrak{m}^n$, we have that $r^{pq} = (s^q + t)^p = s^{pq} + ptw$ but then $pt \in \mathfrak{m}^{n+1}$. So $r^{pq} - s^{pq} \in \mathfrak{m}^{n+1}$. □

Notice that this lemma will be very useful when $\mathfrak{m}$ is nilpotent: We can choose n such that $\mathfrak{m}^n = 0$. Then $r^q = s^q$ if $r \equiv s \mod m$. Therefore R^q maps bijectively onto K^q.

Let Λ be a p-base for K over K^p and let T be a lifting of Λ in R. Then elements of K will be q-polynomials in elements of Λ over K^q. Let S_N be the set of q-polynomials in elements of T over R^q.

Now we have following theorem

Theorem 4.3. *Let $(R, \mathfrak{m}, K)$ be an Artinian local ring with $\mathrm{char}(K) = p$, i.e. $\mathfrak{m}^n = 0$. For any lifting T of a p-base Λ in K, there is a unique coefficient ring $V \subseteq R$ containing T.*

Proof. Let $V = S_N + pS_N + \cdots + p^{n-1}S_N$. We shall prove that this is a coefficient ring and it's unique.

First we show that it's a ring: Let V' be the addition closure of V, then V' is clearly a ring (multiplication is obvisouly closed in V). We prove that V is a ring by proving $V = V'$. In order to show that, we prove $p^jV = p^jV'$ by reverse induction on j.

This holds when $j = n$ as $p^n = 0$. Now assume $p^{j+1}V = p^{j+1}V'$. For any two elements $v_1, v_2 \in p^jS_N$, we want to show that there is some $v_3 \in p^jS_N$ such that $v_1 + v_2 - v_3 \in p^{j+1}V = p^{j+1}V'$ since $p^{j+1}V'$ is spanned by p^jS_N over $p^{j+1}V'$. Write

$$v_1 = p^j \sum_\mu r_{1,\mu}^q \mu$$
$$v_2 = p^j \sum_\mu r_{2,\mu}^q \mu$$

where $r_{*,\mu} \in R$ and $\mu \in S_N$. Let

$$v_3 = p^j \sum_\mu (r_{1,\mu} + r_{2,\mu})^q \mu$$

Then

$$v_1 + v_2 - v_3 = p^{j+1} \sum_\mu G_N(r_{1,\mu}, r_{2,\mu})\mu$$

where $G_N(x, y) := ((x+y)^q - x^q - y^q)/p$ in which $q = p^N$. Notice that S_N maps onto K and r^q only depends on the image of r in K by the lemma. We may choose all $r_{*,\mu}$ to be in S_N. Then $v_1 + v_2 - v_3 \in p^{j+1}V'$. So we have $V = V'$.

Now suppose $\widetilde{V}$ is another coefficient ring containing T and R^q, then since V is generated by T and R^q we must have $V \subseteq \widetilde{V}$. On the other hand, any element $u \in \widetilde{V}$ could be written as $u = s_1 + u_1$ where $s_1 \in S_N$ and $u_1 \in \mathfrak{m} \cap \widetilde{V} = p\widetilde{V}$. But then we can repeat this precedure and write $u_1 = p(s_2 + u_2)$. Therefore $\widetilde{V} \subseteq S_N + pS_N + \cdots + p^{n-1}S_N = V$. Therefore V is the only possible coefficient ring.

Finally we want to prove that V is a DVR. First we note that $V - pV$ has nonzero image in K therefore $V \cap m = pV$ and V is local with maximal ideal pV. We also know that $V/pV \cong K$ by the construction of V. So V is a coefficient ring for R □

From the proof we see that V is actually determined by S_N, or equivalently, by R^q and T. We make this more explicit by following theorem.

Theorem 4.4. *Let (V, pV, K) and (V', pV', K') be two coefficient rings of the same characteristic p^n. Let $\Lambda(\Lambda')$ be p-base for K over K^p(for K′ over K'^p) and let T(T′) be a lifting in R(R′). Suppose that there is an isomorphism $K \to K'$ such that maps Λ to Λ' and so it extens to a bijection from T to T′. Then it extends uniquely to an isomorphism from V to V′*

Proof. We notice that the map $K \to K'$ extends to a bijection $S_N \to S'_N$, but then we know $V = S_N + pS_N + \cdots + p^{n-1}S_N$. So the conclusion follows. □

4.3. **Char = 0.** Let (V, pV, K) be a coefficient rings. V is of characteristic p^n while K is of characteristic p. Then trivially we have $\mathrm{Ann}_V\, p^j V = p^{n-j}V, 0 \leq j \leq n$.

Suppose that there is another coefficient ring (W, pW, K) with the residue field, $\mathrm{char}(W) = p^k$ and $W \to V$ is an surjection. Then $V = W/p^n$. This comes from the fact that every ideal in W is of the form $p^s W$.

Lemma 4.5. *Let K be a field of characteristic $p > 0$ and let (V_t, pV_t, K) be a sequence of coefficient rings. Suppose that*

$$V_0 \twoheadleftarrow V_1 \twoheadleftarrow V_2 \twoheadleftarrow \cdots$$

is an inverse limit system of coefficient rings and surjective maps. Suppose that the characteristic of V_t is $p^{n(t)}$, then there are two cases:

- *$t(n)$ is eventually constant and the map is eventually an isomoprhism*
- *$t(n)$ goes to infinity and the inverse limit is a coefficient ring with characteristic 0.*

Proof. The first case is trivial by our observation above: if $V_{t+1} \to V_t$ is surjection and $n(t+1) = n(t)$. Then the map is necessarily isomoprhism. Now assume that $n(t)$ goes to infinity, we may pass to a subsequence and assume that $n(t)$ is strictly increasing.

We want to show that the maximal ideal of this local ring is generated by p. Every element in the inverse limit is a sequence $(v_1, v_2, ...)$ where $v_i \in V_i$. And it's obvious that one v_i is a unit iff all v_i's are units. So we assume that all v_i are not units, i.e. $v_i = pw_i$. Then this is an element in the maximal ideal, so we want to show that it is p times some element. Let $f_{i+1} : V_{i+1} \to V_i$ be the surjection. We do this by replace all w_i with $w'_i = f_{i+1}(w_{i+1})$.

We have to show two things:

- $v_i = pw'_i$: this comes from $v_i = f_{i+1}(pw_{i+1}) = pf_{i+1}(w_{i+1}) = pw'_i$
- $f_i(w'_i) = w'_{i-1}$: Since $pw_i = v_i = pw'_i$, we have $p(w_i - w'_i) = 0$ so $w_i - w'_i \in p^{n(i)-1}V_i$. Note that $n(i) - 1 \geq n(i-1)$ therefore this ideal is killed by f_i. Then $f_i(w_i) = f_i(w'_i)$

Now we can conclude that the inverse limit is a local ring (V, pV, K). The fact that the ring arises as an inverse limit implies that it's complete. □

Now we are ready to prove the existence of a coefficient ring:

Theorem 4.6 (I.S.Cohen)**.** *If $(R, \mathfrak{m}, K)$ is a complete local ring and K has a p-base Λ, then there is a unique coefficient ring containing the lifting T of Λ.*

Proof. We now only need to deal with $\mathrm{char}(R) = 0$. Any coefficient ring for R containing T maps onto a coefficient ring for $R_n = R/\mathfrak{m}^n$ containing the image of T. There is a unique coefficient ring $V_n \subseteq R_n$. We may choose q large enough such that this q works in the construction of V_n and V_{n+1}. Then the surjection $R_{n+1} \to R_n$ clearly induces surjection $V_{n+1} \to V_n$. Then the Limit $\mathrm{Lim}_n\, V_n$ is a coefficient ring for R. □

4.4. **Structure Theorem.** All the hard work has been done. Since we know the existence of a coefficient ring, we immediately have following:

Theorem 4.7. *A complete local ring $(R, \mathfrak{m}, K)$ of mixed characteristic is a holomorphic image of a complete regular local ring $V[\![X_1, ..., X_n]\!]$ where V is a coefficient ring.*

Proof. We know that R has a coefficient ring V or of the form V/p^nV. Let $p, r_1, ..., r_n$ be a set of generators for $\mathfrak{m}$. Then let $V[\![X_1, ..., X_n]\!] \to R$ by induced by $V[X_1, ..., X_n] \to R$ sending X_i to r_i. Then by Proposition 2.10, we see that the map is surjection. □

Theorem 4.8. *Let $(R, \mathfrak{m}, K)$ be a complete local ring of mixed characteristic. Let $r_1, ..., r_{d-1}$ be a system of parameters for R/pR. Then R is module-finite over the image of $V[\![X_1, ..., X_{d-1}]\!]$ where V is a coefficient ring.*

Proof. This is a corollary of Propisition 2.10. □

Unlike the equicharacteristic case, we don't always have that R is module-fintie over some formal power series ring. For example, $R = V[\![x]\!]/(px)$. V is the coefficient ring while R is not module-finite over V. But in some nice cases we do have following:

Theorem 4.9. *If p is part of a system of parameters for R, then V is a DVR and R is module-finite over $V[\![X_1, ..., X_{d-1}]\!]$.*

Proof. Again we only need to prove injectivity: If I is the kernel, then R/I will have smaller dimension than R, which is a contradiction! □

A regular local ring $(R, \mathfrak{m}, K)$ of mixed characteristic p is **unramified** if equivalently:

(1) $p \notin \mathfrak{m}^2$
(2) R/pR is regular

A quotient of a regular ring by an ideal I is regular iff I is generated by part of a minimal set of generators for the maximal ideal $\mathfrak{m}$: If I is generated by the correct set of elements, then every time we kill an element in I, both the Krull dimension and embedded dimension drops by 1. The result follows by induction. If R/I is regular. Suppose that $I \subseteq \mathfrak{m}^2$, then killing I drops the Krull dimension without changing the embedded dimension. Therefore there is an element in I not in $\mathfrak{m}^2$. Kill it then the result follows by induction on $\dim(R)$.

Note that in an unramified ring, suppose Q is a prime ideal of R. There are two cases: If $p \notin Q$, then R_Q is an equicharacteristic 0 regular local ring. If $p \in Q$, then R_Q is again unramified as R_Q/pR_Q is a localization of R/pR.

Now we are ready to give the structure theorem of complete regular local ring with mixed characteristic:

Theorem 4.10. *Let $(R, \mathfrak{m}, K)$ be a complete regular local ring of Krull dimension d with mixed characteristic. Then*

(1) R is unramified iff $R \cong V[\![X_1, ..., X_{d-1}]\!]$.
(2) R is ramified iff $R \cong V[\![X_1, ..., X_d]\!]/(p-a)$ where a is in the maximal ideal of $V[\![X_1, ..., X_d]\!]$ but not contained in $pV[\![X_1, ..., X_d]\!]$

Proof. The unramified case is equivalent to the "field" case.

Now assume that $p \in \mathfrak{m}^2$, we still have a surjection $\widetilde{R} = V[\![X_1, ..., X_d]\!] \to R$. The kernel is a height 1 ideal while $\widetilde{R}$ is regular hence UFD. So I is principal. Since $\widetilde{\mathfrak{m}}^2$ maps onto $\mathfrak{m}^2$, some elmenet must be mapped onto p, call it a. Then $p - a \in I$. If $a = pa'$, then $p - a = p(1 - a')$ where $1 - a'$ is a unit. So $p \in I \Rightarrow p = 0$ in R. A contradiction! So $a \notin p\widetilde{R}$. Then $p - a \in \widetilde{\mathfrak{m}} - \widetilde{\mathfrak{m}}^2$ so the ideal generated by $p - a$ is of height 1. Thus $R = \widetilde{R}/(p - a)$. □

4.5. **Remark.**

Theorem 4.11. *Let K be a field of characteristic $p > 0$. Then there exists a complete Noetherian valuation domain (V, pV, K) with residue class field K.*

Proof. TO BE ADDED □