

---

---

# *Formal Completion*



阿巴阿巴阿巴阿巴阿巴阿巴阿巴阿巴  
阿巴阿巴阿巴阿巴阿巴阿巴阿巴阿巴  
阿巴阿巴阿巴阿巴阿巴!

---

---

# Formal Completion

## 1 Formal completion of rings and modules

**Definition 1.** Let  $A$  be a ring and  $\mathcal{T}$  a topology on  $A$ . We say that  $(A, \mathcal{T})$  is a *topological ring* if the operations of addition and multiplication are continuous with respect to the topology  $\mathcal{T}$ .

Given a topological ring  $A$ . A *topological  $A$ -module* is a pair  $(M, \mathcal{T}_M)$  where  $M$  is an  $A$ -module and  $\mathcal{T}_M$  is a topology on  $M$  such that the addition and scalar multiplication is continuous. The morphisms of topological  $A$ -modules are the continuous  $A$ -linear maps. They form a category denoted by  $\mathbf{TopMod}_A$ .

**Definition 2.** Let  $A$  be a ring,  $I$  an ideal of  $A$  and  $M$  an  $A$ -module. The  *$I$ -adic topology* on  $M$  is the topology defined by the basis of open sets  $x + I^k M$  for all  $x \in M, k \geq 0$ .

**Example 3.** Let  $A = \mathbb{Z}$  be the ring of integers and  $p$  a prime number. The  $p$ -adic topology on  $\mathbb{Z}$  is defined by the metric

$$d(x, y) := \|x - y\|_p := p^{-v(x-y)},$$

where  $v$  is the valuation defined by the ideal  $p\mathbb{Z}$ .

Note that for  $I$ -adic topology, any homomorphism  $f : M \rightarrow N$  of  $A$ -modules is continuous since  $f(x + I^k N) \subset f(x) + I^k M$  for all  $x \in M$  and  $k \geq 0$ . Hence the forgotten functor  $\mathbf{TopMod}_A \rightarrow \mathbf{Mod}_A$  gives an equivalence of categories.

Let  $M$  be an  $A$ -module equipped with the  $I$ -adic topology. Note that  $M$  is Hausdorff as a topological space if and only if  $\bigcap_{n \geq 0} I^n M = \{0\}$ . In this case, we say that  $M$  is  *$I$ -adically separated*.

When  $M$  is  $I$ -adically separated, we can see that  $M$  is indeed a metric space. Fix  $r \in (0, 1)$ . For every  $x \neq y \in M$ , there is a unique  $k \geq 0$  such that  $x - y \in I^k M$  but  $x - y \notin I^{k+1} M$ . We can define a metric on  $M$  by

$$d(x, y) := r^k.$$

This metric induces the  $I$ -adic topology on  $M$ .

To analyze the  $I$ -adic separation property of  $M$ , the following Artin-Rees Lemma is particularly useful.

**Theorem 4** (Artin-Rees Lemma). Let  $A$  be a noetherian ring,  $I$  an ideal of  $A$ ,  $M$  a finite  $A$ -module and  $N$  a submodule of  $M$ . Then there exists an integer  $r$  such that for all  $n \geq 0$ , we have

$$(I^{r+n} M) \cap N = I^n (I^r M \cap N).$$

*Proof.* Let

$$A' := A \oplus IX \oplus I^2 X^2 \oplus \cdots \subset A[X]$$

be a graded  $A$ -algebra. Note that if  $I = (a_1, \dots, a_k)$ , then  $A' = A[a_1 X, \dots, a_k X]$ . Hence  $A'$  is a

noetherian ring. Let

$$M' := M \oplus IMX \oplus I^2MX^2 \oplus \dots$$

be a graded  $A'$ -module. Then  $M'$  is a finite  $A'$ -module since it is generated by  $M$  and  $M$  is finite over  $A$ . Let

$$N' := N \oplus (IM \cap N)X \oplus (I^2M \cap N)X^2 \oplus \dots$$

be a graded submodule of  $M'$ . Then  $N'$  is finite over  $A'$ . Suppose  $N' = \sum A'x_i$  with  $x_i \in I^{d_i}M \cap N$ . Choose  $r \geq d_i$  for all  $i$ . Then the degree  $n+r$  part of  $N'$  is equal to degree  $n$  part of  $A'$  timing the degree  $r$  part of  $N'$ . That is, for all  $n \geq 0$ ,  $I^{n+r}M \cap N = I^n(I^rM \cap N)$ .  $\square$

**Corollary 5.** Let  $A$  be a noetherian ring,  $I$  an ideal of  $A$ ,  $M$  a finite  $A$ -module and  $N$  a submodule of  $M$ . Then the subspace topology on  $N$  induced by  $N \subset M$  coincides with the  $I$ -adic topology on  $N$ .

*Proof.* This is a direct consequence of the Artin-Rees Lemma.  $\square$

**Corollary 6.** Let  $A$  be a noetherian ring,  $I$  an ideal of  $A$ , and  $M$  a finite  $A$ -module. Let  $N = \bigcap_{n \geq 0} I^n M$ . Then  $IN = N$ . In particular, if  $I \subset \text{rad}(A)$ , then  $M$  is  $I$ -adically separated.

*Proof.* We have that

$$N = I^{n+r}M \cap N = I^n(I^rM \cap N) = I^nN \subset IN \subset N.$$

The latter conclusion follows from the Nakayama's Lemma.  $\square$

**Definition 7.** Let  $A$  be a ring,  $I$  an ideal of  $A$  and  $M$  an  $A$ -module. We say that  $M$  is *complete (with respect to  $I$ -adic topology)* if  $M$  is  $I$ -adically separated and complete as a metric space with respect to the metric induced by the  $I$ -adic topology.

**Lemma 8.** Let  $A$  be a ring,  $I$  an ideal of  $A$  and  $M$  an  $A$ -module. Then the inverse limit

$$\widehat{M} := \varprojlim (\dots \rightarrow M/I^n M \rightarrow M/I^{n-1} M \rightarrow \dots \rightarrow M/IM)$$

exists in the category of  $A$ -modules. Moreover,  $\widehat{A}$  is an  $A$ -algebra and  $\widehat{M}$  is an  $\widehat{A}$ -module.

*Proof.* Let

$$\widehat{M} := \left\{ (x_n) \in \prod_{n \geq 0} M/I^n M \mid x_{n+1} \mapsto x_n \right\}.$$

We claim that  $\widehat{M}$  is that we desired. **Yang: To be completed.**  $\square$

**Definition 9** (Formal Completion). Let  $A$  be a ring,  $I$  an ideal of  $A$  and  $M$  an  $A$ -module. The *formal completion* of  $M$  with respect to  $I$ , denoted by  $\widehat{M}$ , is defined as

$$\widehat{M} := \varprojlim (\dots \rightarrow M/I^n M \rightarrow M/I^{n-1} M \rightarrow \dots \rightarrow M/IM),$$

where the maps are the natural projections  $M/I^n M \rightarrow M/I^{n-1} M$ .

**Example 10.** Let  $A = \mathbb{Z}$  be the ring of integers and  $I = p\mathbb{Z}$ . The formal completion of  $\mathbb{Z}$  with respect to  $p\mathbb{Z}$  is the ring of  $p$ -adic integers, denoted by  $\mathbb{Z}_p$ . The elements of  $\mathbb{Z}_p$  can be represented as infinite series of the form

$$a_0 + a_1p + a_2p^2 + \cdots,$$

where  $a_i \in \{0, 1, \dots, p-1\}$ .

**Example 11.** Let  $R$  be a ring,  $A = R[X_1, \dots, X_n]$  and  $I = (X_1, \dots, X_n)$ . The formal completion of  $A$  with respect to  $I$  is the ring of formal power series  $R[[X_1, \dots, X_n]]$ . The elements of  $R[[X_1, \dots, X_n]]$  can be represented as infinite series of the form

$$\sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n},$$

where  $a_{i_1, \dots, i_n} \in R$  and the multi-index  $(i_1, \dots, i_n)$  runs over all non-negative integers.

**Proposition 12.** The formal completion  $\widehat{M}$  of a  $A$ -module  $M$  is complete, and image of  $M$  is dense in  $\widehat{M}$ . Moreover,  $\widehat{M}$  is uniquely characterized by above properties.

*Proof.* Yang: To be completed. □

By the universal property of the inverse limit, we get a covariant functor from the category of  $A$ -modules to the category of topological  $\widehat{A}$ -modules, which sends an  $A$ -module  $M$  to  $\widehat{M}$  and a morphism  $f : M \rightarrow N$  to the induced morphism  $\widehat{f} : \widehat{M} \rightarrow \widehat{N}$ .

**Lemma 13.** Let

$$0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$$

be an exact sequence of finite  $A$ -modules. Then the sequence of  $\widehat{A}$ -modules

$$0 \rightarrow \widehat{M}_1 \rightarrow \widehat{M}_2 \rightarrow \widehat{M}_3 \rightarrow 0$$

is still exact.

*Proof.* Yang: To be completed. □

**Proposition 14.** Let  $\widehat{A}$  be completion of a noetherian ring  $A$  with respect to an ideal  $I$  and  $M$  a finite  $A$ -module. Then the natural map  $M \otimes_A \widehat{A} \rightarrow \widehat{M}$  is an isomorphism.

*Proof.* Since  $A$  is noetherian and  $M$  is finite, we have an exact sequence

$$A^m \rightarrow A^n \rightarrow M \rightarrow 0.$$

By Lemma 13, we have an exact sequence

$$\widehat{A}^m \rightarrow \widehat{A}^n \rightarrow \widehat{M} \rightarrow 0.$$

On the other hand, we have

$$A^m \otimes_A \widehat{A} \rightarrow A^n \otimes_A \widehat{A} \rightarrow M \otimes_A \widehat{A} \rightarrow 0$$

by right exactness of the tensor product. Since the inverse limit commutes with finite direct sums, we complete the proof by the Five Lemma.  $\square$

**Proposition 15.** Let  $A$  be a noetherian ring and  $I$  an ideal of  $A$ . Then the formal completion  $\hat{A}$  of  $A$  with respect to  $I$  is a flat  $A$ -module.

*Proof.* This is a direct consequence of Lemma 13 and Proposition 14.  $\square$

**Lemma 16.** Let  $\hat{A}$  be the formal completion of a noetherian ring  $A$  with respect to an ideal  $I$ . Suppose that  $I$  is generated by  $a_1, \dots, a_n$ . Then we have an isomorphism of topological rings

$$\hat{A} \cong A[[X_1, \dots, X_n]] / (X_1 - a_1, \dots, X_n - a_n).$$

*Proof.* Yang: To be completed.  $\square$

**Proposition 17.** Let  $A$  be a noetherian ring and  $I$  an ideal of  $A$ . Then the formal completion  $\hat{A}$  of  $A$  with respect to  $I$  is a noetherian ring.

*Proof.* Note that  $A[[X_1, \dots, X_n]]$  is noetherian by Hilbert's Basis Theorem. Then the conclusion follows from Lemma 16.  $\square$

**Proposition 18.** Let  $A$  be a noetherian ring and  $\mathfrak{m}$  a maximal ideal of  $A$ . Then the formal completion  $\hat{A}$  of  $A$  with respect to  $\mathfrak{m}$  is a local ring with maximal ideal  $\mathfrak{m}\hat{A}$ .

*Proof.* Yang: To be completed.  $\square$

## 2 Complete local rings

Let  $(A, \mathfrak{m}, \mathbf{k})$  be a noetherian complete local ring with respect to the  $\mathfrak{m}$ -adic topology. We say that  $A$  is *of equal characteristic* if  $\text{char } A = \text{char } \mathbf{k}$ , and *of mixed characteristic* if  $\text{char } A \neq \text{char } \mathbf{k}$ . In latter case,  $\text{char } \mathbf{k} = p$  and  $\text{char } A = 0$  or  $\text{char } A = p^k$ .

The goal of this subsection is the following structure theorem for noetherian complete local rings due to Cohen.

**Theorem 19** (Cohen Structure Theorem). Let  $(A, \mathfrak{m}, \mathbf{k})$  be a noetherian complete local ring of dimension  $d$ . Then

- (a)  $A$  is a quotient of a noetherian regular complete local ring;
- (b) if  $A$  is regular and of equal characteristic, then  $A \cong \mathbf{k}[[X_1, \dots, X_d]]$ ;
- (c) if  $A$  is regular, of mixed characteristic  $(0, p)$  and  $p \notin \mathfrak{m}^2$ , then  $A \cong D[[X_1, \dots, X_{d-1}]]$ , where  $(D, p, \mathbf{k})$  is a complete DVR;
- (d) if  $A$  is regular, of mixed characteristic  $(0, p)$  and  $p \in \mathfrak{m}^2$ , then  $A \cong D[[X_1, \dots, X_d]]/(f)$ , where  $(D, p, \mathbf{k})$  is a complete DVR and  $f$  a regular parameter.

To prove the Cohen Structure Theorem, we first list some preliminary results on complete local rings. They are independently important and can be used in other contexts.

**Theorem 20** (Hensel's Lemma). Let  $(A, \mathfrak{m}, \mathbf{k})$  be a complete local ring,  $f \in A[X]$  a monic polynomial and  $\bar{f} \in \mathbf{k}[X]$  its reduction modulo  $\mathfrak{m}$ . Suppose that  $\bar{f} = \bar{g} \cdot \bar{h}$  for some monic polynomials  $\bar{g}, \bar{h} \in \mathbf{k}[X]$  such that  $\gcd(\bar{g}, \bar{h}) = 1$ . Then the factorization lifts to a unique factorization  $f = g \cdot h$  in  $A[X]$  such that  $g$  and  $h$  are monic polynomials.

*Proof.* Lift  $\bar{g}$  and  $\bar{h}$  to monic polynomials  $g_1, h_1 \in A[X]$ . We inductively construct a sequence of monic polynomials  $g_n, h_n \in A[X]$  such that  $\Delta_n = f - g_n h_n \in \mathfrak{m}^n[X]$  and  $g_n - g_{n+1}, h_n - h_{n+1} \in \mathfrak{m}^n[X]$  for all  $n \geq 1$ . Suppose that  $g_n$  and  $h_n$  are constructed. Let  $g_{n+1} = g_n + \varepsilon_n$  and  $h_{n+1} = h_n + \eta_n$  for  $\varepsilon_n, \eta_n \in \mathfrak{m}^n[X]$ . Then we have

$$f - g_{n+1}h_{n+1} = \Delta_n - (\varepsilon_n h_n + \eta_n g_n) + \varepsilon_n \eta_n.$$

Hence we just need to choose  $\varepsilon_n$  and  $\eta_n$  such that

$$\varepsilon_n h_n + \eta_n g_n \equiv \Delta_n \pmod{\mathfrak{m}^{n+1}}, \quad \deg \varepsilon_n < \deg g_n, \quad \deg \eta_n < \deg h_n.$$

Since  $\gcd(\bar{g}, \bar{h}) = 1$ , there exist  $\bar{u}, \bar{v} \in \mathbf{k}[X]$  such that  $\bar{u}\bar{g} + \bar{v}\bar{h} = 1$  and  $\deg \bar{u} < \deg \bar{g}$ ,  $\deg \bar{v} < \deg \bar{h}$ . Lift  $\bar{u}$  and  $\bar{v}$  to  $u, v \in A[X]$  preserving the degrees. Then we have  $ug_n + vh_n \equiv 1 \pmod{\mathfrak{m}}$ . Let  $\varepsilon_n = u\Delta_n$  and  $\eta_n = v\Delta_n$ . Then we get the desired equation.  $\square$

**Proposition 21.** Let  $(A, \mathfrak{m}, \mathbf{k})$  be a noetherian complete local ring and  $M$  an  $A$ -module that is  $\mathfrak{m}$ -adically separated. Suppose  $\dim_{\mathbf{k}} M/\mathfrak{m}M < \infty$ . Then the basis of  $M \otimes_A \mathbf{k}$  as  $\mathbf{k}$ -vector space can be lifted to a generating set of  $M$  as an  $A$ -module.

*Proof.* Let  $t_1, \dots, t_n \in M$  such that their images in  $M/\mathfrak{m}M$  form a basis of  $M/\mathfrak{m}M$  as a  $\mathbf{k}$ -vector space. Then  $M = t_1A + \dots + t_nA + \mathfrak{m}M$ . For every  $x \in M$ , we can write

$$x = a_{0,1}t_1 + \dots + a_{0,n}t_n + m_1$$

for some  $a_{0,i} \in A$  and  $m_1 \in \mathfrak{m}M$ . Inductively, we have  $\mathfrak{m}^k M = t_1\mathfrak{m}^k + \dots + t_n\mathfrak{m}^k + \mathfrak{m}^{k+1}M$ . Suppose that we have constructed  $m_k \in \mathfrak{m}^k M$ . Then we can write

$$m_k = a_{k,1}t_1 + \dots + a_{k,n}t_n + m_{k+1}.$$

Note that  $\sum_{k \geq 0} a_{k,i}$  converges in  $A$ , denote its limit by  $a_i$ . Then we have

$$x - a_1t_1 - \dots - a_nt_n = \sum_{i=1}^n \sum_{r \geq k} a_{r,i}t_i + m_k \in \mathfrak{m}^k M$$

for all  $k$ . Since  $M$  is  $\mathfrak{m}$ -adically separated,  $x = a_1t_1 + \dots + a_nt_n$ . It follows that  $M = \sum At_i$ .  $\square$

The key to prove the Cohen Structure Theorem is the existence of coefficient rings.

**Definition 22** (Coefficient rings). Let  $(A, \mathfrak{m}, \mathbf{k})$  be a noetherian complete local ring.

When  $A$  is equal-characteristic, the coefficient ring (or coefficient field) is a homomorphism of rings  $\mathbf{k} \rightarrow A$  such that  $\mathbf{k} \rightarrow A \rightarrow A/\mathfrak{m}$  is an isomorphism.

When  $A$  is mixed-characteristic, the coefficient ring is a complete local ring  $(R, pR, \mathbf{k})$  with a local homomorphism of rings  $R \hookrightarrow A$  such that the induced homomorphism  $R/pR \rightarrow A/\mathfrak{m}$  is an isomorphism.

**Remark 23.** Recall that a homomorphism of local rings  $f : (A, \mathfrak{m}_A) \rightarrow (B, \mathfrak{m}_B)$  is said to be local if  $f^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$ .

**Theorem 24.** Every noetherian complete local ring  $(A, \mathfrak{m}, \mathbf{k})$  has a coefficient ring.

Assume the existence of coefficient rings, we can prove the Cohen Structure Theorem.

*Proof of Cohen Structure Theorem.* Let  $R$  be a coefficient ring of  $A$  and  $\mathfrak{m} = (f_1, \dots, f_d)$  a minimal generating set of  $\mathfrak{m}$ . Then we have a homomorphism of complete local rings

$$\Phi : R[[X_1, \dots, X_d]] \rightarrow A, \quad X_i \mapsto f_i.$$

Let  $\mathfrak{n}$  be the maximal ideal of  $R[[X_1, \dots, X_d]]$ . Then  $\mathfrak{n}A = \mathfrak{m}$ . By Proposition 21,  $A$  is generated by 1 as an  $R[[X_1, \dots, X_d]]$ -module. This implies that  $\Phi$  is surjective and (a) follows.

If  $A$  is regular of equal characteristic, then  $\mathfrak{m}$  is generated by a regular sequence. By consider the dimension of  $R[[X_1, \dots, X_d]]$  and  $A$ , we have that  $\Phi$  is an isomorphism. This proves (b).

Note that if  $A$  is regular of mixed characteristic  $(0, p)$  and  $p \notin \mathfrak{m}^2$ , then  $\mathfrak{m}$  is generated by  $p, f_1, \dots, f_{d-1}$ . Then consider the homomorphism of complete local rings

$$R[[X_1, \dots, X_{d-1}]] \rightarrow A, \quad X_i \mapsto f_i.$$

By the same argument as above, we have that it is an isomorphism. This proves (c).

For (d), we have that  $\ker \Phi$  is of height 1 by the dimension argument. Since regular local rings are UFDs, we can write  $\ker \Phi = (f)$  for some  $f \in R[[X_1, \dots, X_d]]$ . Then we finish.  $\square$

## 2.1 Existence of coefficient rings

*Proof of Theorem 24 in characteristic 0.* Note that for any  $n \in \mathbb{Z}$ ,  $n \notin \mathfrak{m}$ . Hence  $\mathbb{Q} \subset A$ . Let  $\Sigma := \{\text{subfield in } A\}$  and  $K$  a maximal element in  $\Sigma$  with respect to the inclusion. The set  $\Sigma$  is non-empty since  $\mathbb{Q} \in \Sigma$ . By Zorn's Lemma,  $K$  exists. Then  $K$  is a subfield of  $\mathbf{k}$  by  $K \hookrightarrow A \twoheadrightarrow A/\mathfrak{m} \cong \mathbf{k}$ . We claim that  $K$  is a coefficient field of  $A$ .

Suppose there is  $\bar{t} \in \mathbf{k} \setminus K$ . If  $\bar{t}$  is transcendental over  $K$ , lift  $\bar{t}$  to an element  $t \in A$ . Then for any polynomial  $f \neq 0 \in K[T]$ , we have  $f(\bar{t}) \neq 0 \in \mathbf{k}$ . Hence  $f(t) \notin \mathfrak{m}$ . This implies that  $1/f(t) \in A$ , whence  $K(t) \subset A$ . This contradicts the maximality of  $K$ . If  $\bar{t}$  is algebraic over  $K$ , let  $f \in K[T]$  be the minimal polynomial of  $\bar{t}$ . Then  $f$  is irreducible in  $K[T]$  and  $f(\bar{t}) = 0$ . Regard  $f$  as a polynomial in  $A[T]$  by  $K \hookrightarrow A$ . Note that  $\text{char } A = 0$  implies that  $f$  is separable. By Hensel's Lemma (Theorem 20), we can lift the root  $\bar{t}$  to an element  $t \in A$  such that  $f(t) = 0$ . Then  $K(t)$  is a field extension of

$K$  and  $K(t) \subset A$ . This contradicts the maximality of  $K$  again.  $\square$

The same strategy does not work when  $\text{char } k = p > 0$  since there might be inseparable extensions. To fix this, we need to introduce the notion of  $p$ -basis.

**Definition 25.** Let  $k$  be a field of characteristic  $p$ . A finite set  $\{t_1, \dots, t_n\} \subset k \setminus k^p$  is called  $p$ -independent if  $[k(t_1, \dots, t_n) : k] = p^n$ . A set  $\Theta \subset k \setminus k^p$  is called a  $p$ -independent if its any finite subset is  $p$ -independent. A  $p$ -basis for  $k$  is a maximal  $p$ -independent set  $\Theta \subset k \setminus k^p$ .

By definition, we have that  $k = k^p[\Theta]$  for any  $p$ -basis  $\Theta$  of  $k$ . For any  $a \in k$  and  $\theta \in \Theta$ , we can write  $a$  as a polynomial in  $\Theta$  with coefficients in  $k^p$ . The degree of  $\theta$  in such polynomial representation is at most  $p - 1$ . Such polynomial representation is unique by definition of  $p$ -independence.

Applying the Frobenius map  $n$  times, we have that  $k^{p^n} = k^{p^{n+1}}[\Theta^{p^n}]$ . This follows that  $k = k^{p^n}[\Theta]$  for all  $n$ . Moreover, for any  $a \in k$  and  $\theta \in \Theta$ , we can write  $a$  as a polynomial in  $\Theta$  with coefficients in  $k^{p^n}$  and the degree of  $\theta$  is at most  $p^n - 1$ . Such polynomial representation is unique.

Let  $k$  be a perfect field of characteristic  $p$ . If there is  $a \in k \setminus k^p$ , then  $k(a^{1/p})/k$  is an inseparable extension. This contradicts the perfectness of  $k$ . Hence  $k = k^p$  and  $k$  has no nonempty  $p$ -basis.

**Example 26.** Let  $k = \mathbb{F}_p(t_1, \dots, t_n)$ . Then  $k^p = \mathbb{F}_p(t_1^p, \dots, t_n^p)$ . The set  $\{t_1, \dots, t_n\}$  is a  $p$ -basis for  $k$ .

*Proof of Theorem 24 in characteristic  $p$ .* Choose  $\Theta \subset A$  such that its image in  $A/\mathfrak{m}$  is a  $p$ -basis for  $k$ . Let  $A_n := A^{p^n} = \{a^{p^n} : a \in A\}$  and  $K := \bigcap_{n \geq 0} (A_n[\Theta])$ . Then we claim that  $K$  is a coefficient field of  $A$ .

First we show that  $A_n[\Theta] \cap \mathfrak{m} \subset \mathfrak{m}^{p^n}$ . For every  $a \in A_n[\Theta]$ , if the degree of  $\theta$  in the polynomial representation of  $a$  is more than  $p^n - 1$ , we can write  $\theta^k = \theta^{ap^n} \cdot \theta^b$  for some  $b < p^n$ . Regard  $\theta^{ap^n} \in A^{p^n}$  as coefficients. Now assume that  $a \in A_n[\Theta] \cap \mathfrak{m}$ . Then consider the image of  $a$  in  $A/\mathfrak{m}$ . The image of  $a$  equals 0 implies every coefficient of  $a$  is in  $\mathfrak{m}$ . Such coefficients are of form  $b^{p^n}$  for some  $b \in A$ , whence  $b \in \mathfrak{m}$ . Hence  $a \in \mathfrak{m}^{p^n}$ . This implies that  $K \cap \mathfrak{m} = \bigcap_{n \geq 0} (A_n[\Theta] \cap \mathfrak{m}) \subset \bigcap_{n \geq 0} \mathfrak{m}^{p^n} = \{0\}$ . Then  $K$  is a field and hence a subfield of  $k$ .

For any  $\bar{a} \in k$ , note that  $k = k^p[\bar{\Theta}] = k^{p^2}[\bar{\Theta}] = \dots = k^{p^n}[\bar{\Theta}] = \dots$ . For every  $n$ , write

$$\bar{a} = \sum_{\mu_n} \bar{c}_{\mu_n}^{p^n} \mu_n =: P_{\bar{a},n}(\bar{c}_{\mu_n}),$$

where  $\mu_n$  runs over all monomials in  $\bar{\Theta}$  with degree at most  $p^n - 1$  and  $\bar{c}_{\mu_n} \in k$ . We call this representation the  $p^n$ -development of  $\bar{a}$  with respect to  $\bar{\Theta}$ . Plug the  $p^m$ -development of  $c_{\mu_n}$  into  $P_{\bar{a},n}$ , we get the  $p^{n+m}$ -development of  $\bar{a}$ . In formula, that is,

$$P_{\bar{a},n}(P_{\bar{a},m}(\bar{c}_{\mu_{n+m}})) = P_{\bar{a},n+m}(\bar{c}_{\mu_{n+m}}).$$

Lift  $\bar{c}_{\mu_n}$  to  $c_{\mu_n} \in A$  for all  $\mu_n$ . Let  $a_n := P_{\bar{a},n}(c_{\mu_n}) = \sum_{\mu_n} c_{\mu_n}^{p^n} \mu_n \in A_n[\Theta]$ . For  $m \geq n$ , we have  $a_n - a_m \in A_n[\Theta] \cap \mathfrak{m} \subset \mathfrak{m}^{p^n}$ . Hence  $a_n$  converges to an element  $a \in A$ . Now we show that  $a \in K$ . For every  $\mu_k$ , let  $b_{\mu_k,n} \in A$  be the element getting by plugging  $c_{\mu_{k+n}}$  into the  $P_{\bar{a},n}$ . Then  $b_{\mu_k,n}$



converges to an element  $b_{\mu_k} \in A$ . By construction, we have

$$a = \lim_{n \rightarrow \infty} P_{\bar{a}, n+k}(c_{\mu_{n+k}}) = \lim_{n \rightarrow \infty} P_{\bar{a}, k}(b_{\mu_k, n}) = P_{\bar{a}}(b_{\mu_k}) = \sum_{\mu_k} b_{\mu_k}^{p^k} \mu_k \in A_k[\Theta], \quad \forall k.$$

It follows that  $a \in K$ . □

**Lemma 27.** Let  $(A, \mathfrak{m}, k)$  be a noetherian complete local ring of mixed characteristic. Suppose that  $\mathfrak{m}^n = 0$  for some  $n \geq 1$ . Then there exists a complete local ring  $(R, pR, k)$  with  $R \subset A$ .

*Proof.* Fix a  $p$ -basis of  $k$  and lift it to  $\Theta \subset R$ . Let  $q = p^{n-1}$  and

$$\mathcal{M} := \left\{ \theta_1^{k_1} \cdots \theta_d^{k_d} \mid \theta_i \in \Theta, k_i \leq q-1 \right\}, \quad S := \left\{ \sum_{\mu \in \mathcal{M}, \text{ finite}} a_\mu \mu \mid a_\mu \in R^q \right\}.$$

For any  $a, b \in A$ , we claim that  $a \equiv b \pmod{\mathfrak{m}}$  if and only if  $a^q \equiv b^q \pmod{\mathfrak{m}^n}$ . If  $a \equiv b \pmod{\mathfrak{m}}$ , write  $a = b + m$  for some  $m \in \mathfrak{m}$ . Then  $a^p = b^p + pb^{q-1}m + \cdots + m^p$ . Hence  $a^p \equiv b^p \pmod{\mathfrak{m}^2}$ . Inductively, we have  $a^q \equiv b^q \pmod{\mathfrak{m}^n}$ . Conversely, if  $a^q \equiv b^q \pmod{\mathfrak{m}^n}$ , then  $a^q - b^q \in \mathfrak{m}^n \subset \mathfrak{m}$ . Note that the Frobenius map  $x \mapsto x^q$  is injective on  $A/\mathfrak{m}$ . It follows that  $a \equiv b \pmod{\mathfrak{m}}$ . By the claim,  $S$  maps to  $k^q[\Theta] = k$  bijectively.

Let

$$R := S + pS + p^2S + \cdots + p^{n-1}S.$$

We claim that  $R$  is a subring of  $A$ . If so,  $R/pR \cong k$  and we get a complete local ring  $(R, pR, k)$ .

Take  $a, b \in A$ . We have

$$a^q + b^q = (a + b)^q + pc \in A^q + pA.$$

Inductively, we have

$$a^q + b^q \in A^q + pA^q + \cdots + p^{n-1}A^q.$$

This implies that  $R$  is closed under addition. Note that  $\theta^a = \theta^{aq} \cdot \theta^b$  with  $b < q$ . Then for any  $\mu, \nu \in \mathcal{M}$ , we have  $\mu\nu \in S$ . Hence  $R$  is closed under multiplication. □

**Lemma 28.** Let  $k$  be a field of characteristic  $p$ . Then there exists a DVR  $(D, p, k)$  of mixed characteristic  $(0, p)$ .

*Proof.* Fix a well order  $\leq$  on  $k$  and for any  $a \in k$ , set  $k_a$  be the subfield of  $k$  generated by all elements  $b \in k$  such that  $b \leq a$ . Then  $k = \bigcup_{a \in k} k_a$ . We construct DVRs  $D_a$  with residue field  $k_a$  such that  $D_a \subset D_b$  for  $a \leq b$ . Begin from  $k_0 = \mathbb{F}_p$  and let  $D_0 = \mathbb{Z}_{(p)}$ . Suppose that  $D_a$  is constructed for all  $a < b$ . If  $k_b/k_a$  is transcendental, then let  $D_b$  be the localization of  $D_a[b]$  at the prime ideal generated by  $p$ .

If  $k_b/k_a$  is algebraic, then let  $\bar{f} \in k_a[T]$  be the monic minimal polynomial of  $b$ . Let  $K_a = \text{Frac}(D_a)$  and  $K_b = K_a[T]/(f)$ , where  $f$  is a monic lift of  $\bar{f}$  to  $D_a[T]$ . Note that  $f$  is irreducible since  $\bar{f}$  is irreducible. Let  $D_b$  be the integral closure of  $D_a$  in  $K_b$ . In general,  $D_b$  is a Dedekind domain.

Consider the prime factorization  $pD_b = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$  in  $D_b$ . For every  $i$ ,  $D_b/\mathfrak{p}_i$  is a field extension of  $\mathbf{k}_a$  and  $\bar{f}$  has a root in  $D_b/\mathfrak{p}_i$ . Suppose  $\deg \bar{f} = \deg f = d$ . It follows that  $[(D_b/\mathfrak{p}_i) : \mathbf{k}_a] = d$ . Note that we have  $\sum_{i=1}^k e_i f_i = [K_b : K_a] = d$ . Hence  $k = 1$  and  $e_1 = 1$ . It follows that  $pD_b$  is prime and  $D_b$  is a DVR with residue field  $\mathbf{k}_b$ .

Let  $D = \bigcup_{a \in \mathbf{k}} D_a$ . Then  $(D, pD, \mathbf{k})$  is the desired DVR.  $\square$

**Example 29.** Let  $\mathbf{k} = \mathbb{F}_p(t)$ . Then  $D = \mathbb{Z}[t]_{(p)}$  is a DVR satisfying the condition in Lemma 28.

Let  $\mathbf{k} = \overline{\mathbb{F}_p}$ . For any  $n \geq 1$ , let  $K_n = K_{n-1}(\zeta_{p^{n-1}})$  and  $K_0 = \mathbb{Q}$ . Let  $D_n := \mathcal{O}_{K_n, \mathfrak{p}_n}$  be the localization of the ring of integers of  $K_n$  at the prime  $\mathfrak{p}_n$  lying above  $\mathfrak{p}_{n-1}$ . Then  $D := \bigcup_n D_n$  is a DVR with residue field  $\mathbf{k}$ .

**Lemma 30.** Given  $\mathbf{k}$  a field of characteristic  $p$ , there exists a unique complete local ring  $(R, pR, \mathbf{k})$  of mixed characteristic  $(p^n, p)$ .

*Proof.* The existence follows from Lemma 28. To show the uniqueness, suppose that  $(R', pR', \mathbf{k})$  is another complete local ring of mixed characteristic  $(p^n, p)$ . Fix a  $p$ -basis of  $\mathbf{k}$  and lift it to  $\Theta \subset R$  and  $\Theta' \subset R'$  relatively. Let  $q = p^{n-1}$  and

$$\mathcal{M} := \left\{ \theta_1^{k_1} \cdots \theta_d^{k_d} \mid \theta_i \in \Theta, k_i \leq q-1 \right\}, \quad S := \left\{ \sum_{\mu \in \mathcal{M}, \text{ finite}} a_\mu \mu \mid a_\mu \in R^q \right\}.$$

Define  $\mathcal{M}', S'$  similarly with  $\Theta'$  and  $R'$ . Since  $S \rightarrow R \rightarrow \mathbf{k}$  and  $S' \rightarrow R' \rightarrow \mathbf{k}$  are bijections, we can define a bijective map  $\Phi : S \rightarrow S'$ .

Note that any element in  $S$  can be written as  $s + pr$  with  $s \in S$  and  $r \in R$  uniquely since  $S \rightarrow \mathbf{k}$  is bijective. Inductively, we can write any element in  $R$  as

$$r = s + ps_1 + p^2s_2 + \cdots + p^{n-1}s_{n-1},$$

where  $s_i \in S$ . The similarly for  $R'$ . Extend  $\Phi$  to  $R$  and we get a bijection between  $R$  and  $R'$ . Note that by construction,  $\Phi$  preserves addition and multiplication. Hence we get a ring isomorphism  $\Phi : R \rightarrow R'$ .  $\square$

*Proof of Theorem 24 in mixed characteristic.* Since  $A$  is complete, we have  $A = \varprojlim_n A/\mathfrak{m}^n$ . By Lemma 27, there is a complete local ring  $(R_n, pR_n, \mathbf{k})$  with  $R_n \subset A/\mathfrak{m}^n$ . By Lemma 30, such  $R_n$  is unique up to isomorphism. It follows that  $R_n \cong R_m/p^{k_n}$  for  $m \geq n$ . We get an inverse system

$$\cdots \rightarrow R_n \rightarrow R_{n-1} \rightarrow \cdots \rightarrow R_1 \cong \mathbf{k}.$$

Let  $R := \varprojlim_n R_n$ . Then  $(R, pR, \mathbf{k})$  is a complete local ring. The homomorphisms  $R_n \hookrightarrow A/\mathfrak{m}^n$  induce a homomorphism of complete local rings  $R \hookrightarrow A$ . This concludes the proof.  $\square$