Complete Local Rings
Alexandre Daoud

1 Setting the Scene

In this project we aim to build an understanding of the theory behind completion of rings. We shall discuss local rings that are complete and conclude by stating (and proving a special case thereof) the Cohen structure theorem which concerns the classification of complete local Noetherian rings. A good understanding of elementary ring and module theory is assumed. Henceforth, all rings are assumed commutative with unity.

We begin by stating some important preliminary definitions:

Definition 1.1. Let R be a ring. We say that R is a **local ring** if it contains a unique maximal ideal $\mathfrak{m} \triangleleft R$.

Definition 1.2. Let R be a ring. We define the **ring of formal power series** in X over R to be

$$R[[X]] = \left\{ \sum_{i=0}^{\infty} r_i X^i \;\middle|\; r_i \in R \right\}$$

Given any $a = \sum_{i=0}^{\infty} a_i X^i$ and $b = \sum_{i=0}^{\infty} b_i X^i$, we define their sum as

$$\sum_{i=0}^{\infty} a_i X^i + \sum_{i=0}^{\infty} a_i X^i = \sum_{i=0}^{\infty} (a_i + b_i) X^i$$

and their product as

$$\left(\sum_{i=0}^{\infty} a_i X^i \right) \left(\sum_{i=0}^{\infty} a_i X^i \right) = \sum_{i=0}^{\infty} c_i X^i, \quad c_k = \sum_{i+j=k} a_i b_j$$

It is readily verified that the ring of formal power series over R is indeed a ring (completely analogously to the argumentation for a polynomial ring). We can also generalise this definition to that of formal power series in n indeterminates $X_1, \ldots, X_n$.

We shall soon see that the ring of formal power series over R can be constructed as the completion of the ring of polynomials over R with respect to some ideal.

Definition 1.3. Let $\{ G_i \}_{i \in I}$ be a family of algebraic structures (such as groups, rings or modules etc) indexed by some directed partially ordered[1] set I. Furthermore, let

$$\sigma_{ji} : G_j \to G_i, \quad i \leq j$$

be a collection of morphisms between the G_i. We say that (G_i, σ_{ji}) is an **inverse system** when the following conditions hold:

1. σ_{ii} is the identity morphism
2. Given any $i, j, k \in I$ such that $i \leq j \leq k$ we have $\sigma_{ki} = \sigma_{ji} \circ \sigma_{kj}$

Definition 1.4. Let (G_i, σ_{ji}) be an inverse system. We define the **inverse limit** (or **projective limit**) of the system as

$$\varprojlim_{i \in I} G_i = \left\{ g \in \prod_{i \in I} G_i \;\middle|\; g_i = \sigma_{ji}(g_j) \; \forall i \in I \right\}$$

In some sense, the inverse limit of an inverse system is defined to be the set of all sequences in the direct product which are 'coherent' with respect to the transition morphisms σ_{ji}.

The inverse limit can be defined in a much more abstract and general manner in the context of category theory. The above definition, however, will be sufficient for the purposes of our discussion.

2 Completion

Definition 2.1. Let R be a ring. A sequence of ideals

$$R = \mathfrak{m}_0 \supseteq \mathfrak{m}_1 \supseteq \dots$$

is called a **descending filtration of ideals** of R. We shall denote such a sequence by $\{ \mathfrak{m}_i \}$.

Definition 2.2. Let R be a ring and $\{ \mathfrak{m}_i \}$ a descending filtration. We define the **completion** of R with respect to the filtration $\{ \mathfrak{m}_i \}$ to be

$$\hat{R} = \varprojlim R/\mathfrak{m}_i$$

where the transition morphisms between the $R/\mathfrak{m}_i$ are reduction modulo $\mathfrak{m}_i$.

Example 2.3. Let R be a ring filtered by the ideals $\mathfrak{m}^i$ for some $\mathfrak{m} \triangleleft R$. We call $\{ \mathfrak{m}_i = \mathfrak{m}^i \}$ the **$\mathfrak{m}$-adic** filtration of R. The completion of R with respect to $\mathfrak{m}$, denoted $\hat{R}_{\mathfrak{m}}$, is the completion of R with respect to the $\mathfrak{m}$-adic filtration. Furthermore, if there exists an isomorphism $R \xrightarrow{\sim} \hat{R}_{\mathfrak{m}}$, we say that R is **complete** with respect to $\mathfrak{m}$.

[1] If $(I, \leq)$ is a partial ordering then I is **directed** if, given any $a, b \in I$, there exists a $c \in I$ such that $a \leq c$ and $b \leq c$.

Lemma 2.4. *Let R be a ring and $\mathfrak{m} \lhd R$ a maximal ideal. Then $R/\mathfrak{m}^k$ is a local ring for all $k \geq 1$.*

Proof. Let $M \lhd R/\mathfrak{m}^k$ be a prime ideal. Then M is of the form $P/\mathfrak{m}^k$ where $\mathfrak{m}^k \subseteq P \subseteq R$ and P is some prime ideal of R. It is easy to see by the definition of a prime ideal that if $\mathfrak{m}^k \subseteq P$ then $\mathfrak{m} \subseteq P$. But $\mathfrak{m}$ is maximal in R and thus $P = \mathfrak{m}$. It follows that $\mathfrak{m}/\mathfrak{m}^k$ is the unique prime ideal of $R/\mathfrak{m}^k$. Now, Krull's Theorem implies that $R/\mathfrak{m}^k$ has at least one maximal ideal. Since any maximal ideal is necessarily a prime ideal, $\mathfrak{m}/\mathfrak{m}^k$ is the unique maximal ideal and $R/\mathfrak{m}^k$ is a local ring. □

Proposition 2.5. *Let R be a ring and $\mathfrak{m} \lhd R$ a maximal ideal. Then $\hat{R}_\mathfrak{m}$ is a local ring.*

Proof. We first observe that since $\mathfrak{m}$ is a maximal ideal, $R/\mathfrak{m}$ is a field. We claim that

$$M = \{ (g_1, g_2, g_3, \dots) \in \hat{R}_\mathfrak{m} \mid g_1 = 0 \}$$

is the unique maximal ideal of $\hat{R}_\mathfrak{m}$. Indeed, consider the mapping

$$\begin{aligned} \phi : \hat{R}_\mathfrak{m} &\to R/\mathfrak{m} \\ g &\mapsto \pi_1(g) \end{aligned}$$

where π_i is the projection onto the i^{th} coordinate. This map is clearly surjective whose kernel is exactly M. Hence $\hat{R}_\mathfrak{m}/M \cong R/\mathfrak{m}$ whence M is maximal.

It remains to show that M is the unique such maximal ideal. To this end, we shall show that any element outside of M is a unit. Fix some $g = (g_1, g_2, \dots) \in \hat{R}_\mathfrak{m} \backslash M$. Clearly, $g_1 \not\equiv 0 \pmod{\mathfrak{m}}$ whence $g_i \not\equiv 0 \pmod{\mathfrak{m}^i}$ for all $i \geq 1$. By the previous lemma, $R/\mathfrak{m}^i$ is a local ring with maximal ideal $\mathfrak{m}/\mathfrak{m}^i$. By an isomorphism theorem we have

$$\frac{R/\mathfrak{m}^i}{\mathfrak{m}/\mathfrak{m}^i} \cong R/\mathfrak{m}$$

where $\mathfrak{m}/\mathfrak{m}^i$ is the kernel of the transition homomorphism $R/\mathfrak{m}^i \to R/\mathfrak{m}$. It follows that $g_i \notin \mathfrak{m}/\mathfrak{m}^i$ and thus g_i is a unit. Hence each g_i possesses an inverse $g_i^{-1} \in R/\mathfrak{m}^i$. We claim that $(g_1^{-1}, g_2^{-1}, \dots)$ is an element of the inverse limit. Multiplying the condition $g_j \equiv g_i \pmod{\mathfrak{m}^i}$ through by the corresponding inverses, we get $g_j^{-1} \equiv g_i^{-1} \pmod{\mathfrak{m}^i}$ and hence the inverse sequence is indeed in the inverse limit. We see that any element outside of M is a unit and thus M is the unique maximal ideal, making $\hat{R}_\mathfrak{m}$ a local ring. □

The above proposition gives us a simple way to construct complete local rings out of a ring and one of its maximal ideals - a powerful tool as we shall see later on.

We now make good on our promise in the previous section and show that the ring of formal power series can be obtained in the form of a completion.

Proposition 2.6. *Let R be a ring and $S = R[X_1, \dots, X_n]$. Then $\hat{S}_{(X_1,\dots,X_n)} \cong R[[X_1, \dots, X_n]]$.*

Proof. We shall only consider the case of one indeterminate X. The generalisation to n indeterminates follows easily. We have the natural homomorphisms

$$\begin{aligned} R[[X]] &\to R/(X)^i \\ f &\to f + (X^i) \end{aligned}$$

which induces a homomorphism $\psi : R[[X]] \to \hat{R}_{(X)}$. To show that this is an isomorphism, we shall construct its inverse.

Fix some $f = \sum_{i=0}^{\infty} a_i X^i \in R[[X]]$. We need to find a function ψ^{-1} such that

$$\psi^{-1}(f + (X), f + (X^2), \dots) = f(X)$$

Define $f_i(X)$ to be the 'cutoff' polynomial of f up to (but not including) the i^{th} power. Then

$$(f_1(X), f_2(X), \dots) = (a_0, a_0 + a_1 X, \dots) = (f + (X), f + (X^2), \dots) = \psi(f)$$

We can now define the inverse ψ^{-1} in terms of these cutoff polynomials:

$$\begin{aligned} \psi^{-1} : \hat{R}_{(X)} &\to R[[X]] \\ (f_1(X), f_2(X), \dots) &\mapsto f_1(X) + (f_2(X) - f_1(X)) + \dots \end{aligned}$$

Indeed, we have

$$\begin{aligned} \psi^{-1}(f + (X), f + (X^2), \dots) &= \psi^{-1}(f_1(X), f_2(X), \dots) \\ &= f_1(X) + (f_2(X) - f_1(X)) + (f_3(X) - f_2(X)) + \dots \\ &= a_0 + (a_0 + a_1(X) - a_0) + (a_0 + a_1 X + a_2 X^2 - a_0 - a_1(X)) + \dots \\ &= a_0 + a_1(X) + a_2 X^2 + \dots = f(X) \end{aligned}$$

□

Example 2.7. Another example is the p-adic completion of the integers:

$$\mathbb{Z}_p = \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/(p^n)$$

which consists of infinite sequences that can be represented as formal power series in p:

$$a_0 + a_1 p + a_2 p^2 + \dots \in \mathbb{Z}_p$$

where $a_i \in \mathbb{F}_p$. Since (p) is maximal in $\mathbb{Z}$, we see that $\mathbb{Z}_p$ is a complete local ring.

There exists a rich theory of p-adic numbers and p-adic analysis which reveals their usefulness, the majority of which is outside the scope of this project. For completeness sake, we note that $\mathrm{Frac}(\mathbb{Z}_p) = \mathbb{Q}_p$ is the (topological) completion of $\mathbb{Q}$ with respect to the so-called p-adic norm. In fact, Ostrowski's theorem shows that the p-adic completions are the only such completions of $\mathbb{Q}$, along with the standard real numbers $\mathbb{R}$. The interested reader is invited to read Koblitz [3] which provides a rigorous account of the aforementioned details.

3 Krull's Intersection Theorem

A natural question to ask is whether passing to the completion preserves the information of the original ring. Let R be a ring, $\mathfrak{m} \lhd R$ an ideal and consider the ring homomorphism

$$\begin{aligned} \phi : R &\to \hat{R}_{\mathfrak{m}} \\ r &\mapsto (r + \mathfrak{m}, r + \mathfrak{m}^2, \dots) \end{aligned}$$

The kernel of this mapping is clearly $\bigcap_{i=1}^{\infty} \mathfrak{m}^i$. For ϕ to be injective (and thus, information-preserving), we would require that $\bigcap_{i=1}^{\infty} \mathfrak{m}^i = \{ 0 \}$. In this section we shall see that this is the case when R is Noetherian and either an integral domain or a local ring (although these may not be necessary conditions).

We begin by generalising our notion of filtrations.

Definition 3.1. Let R be a ring. A sequence of additive subgroups

$$R = R_0 \supseteq R_1 \supseteq \dots$$

such that $R_m R_n \subseteq R_{m+n}$ is called a **descending filtration**. Furthermore if M is a module over R and

$$M = M_0 \supseteq M_1 \supseteq \dots$$

is a sequence of submodules of M such that $R_m M_n \subseteq M_{m+n}$ then such a sequence is a descending filtration of M.

Example 3.2. As before, we have the $\mathfrak{m}$-adic filtration where $R_n = \mathfrak{m}^n$ for some ideal $\mathfrak{m}$ of R. Similarly, we can filter any module M with the filtration $M_n = \mathfrak{m}^n M$.

Definition 3.3. Let M be a module over a ring R that is filtered by $\{ M_n \}$. Suppose that $\mathfrak{m} \triangleleft R$ is an ideal. We say that $\{ M_n \}$ is an **$\mathfrak{m}$-filtration** if $\mathfrak{m} M_n \subseteq M_{n+1}$ for all $n \in \mathbb{N}$. If, furthermore, we have $\mathfrak{m} M_n = M_{n+1}$ for sufficiently large n then $\{ M_n \}$ is **$\mathfrak{m}$-stable**.

Example 3.4. The $\mathfrak{m}$-adic filtration is clearly $\mathfrak{m}$-stable.

Definition 3.5. Let R be a ring. We say that R is a **graded** ring if there exists a family of additive subgroups $\{ R_n \}$ such that $R_m R_n \subseteq R_{m+n}$ and $R = \oplus_{n \in \mathbb{N}} R_n$. If M is an R-module, we say that M is a graded module if there exists a family of submodules $\{ M_n \}$ such that $M = \oplus_{n \in \mathbb{N}} M_n$ and $A_n M_m \subseteq M_{n+m}$

Example 3.6. Let R be a ring. Then the polynomial ring $R[X_1, \dots, X_n]$ is graded with R_n the set of all homogeneous polynomials of degree n.

Lemma 3.7. *Let R be a Noetherian ring and $\mathfrak{m} \triangleleft R$ an ideal. Define a graded ring*

$$R^* = \bigoplus_{n \in \mathbb{N}} \mathfrak{m}^n$$

Then R^* is Noetherian.

Proof. Since R is Noetherian we must have that $\mathfrak{m} = (m_1, \dots, m_n)$ for some $m_1, \dots, m_n$. It is easy to see that $R[X_1, \dots, X_n]$ surjects onto R^*. Indeed, the map sending X_i to m_i is surjective since $m_1, \dots, m_n$ are generators for $\mathfrak{m}$. Appealing to Hilbert's Basis Theorem, we see that R^* is Noetherian. □

Lemma 3.8. *Let R be a Noetherian ring and $\mathfrak{m} \triangleleft R$ an ideal. Suppose that M is a finitely-generated R-module and $\{ M_n \}$ an $\mathfrak{m}$-filtration of M. Define $M^* = \oplus_{n \in \mathbb{N}} M_n$ to be a graded R^*-module. Then the following are equivalent:*

1. *M^* is a finitely generated R^*-module*
2. *$\{ M_n \}$ is $\mathfrak{m}$-stable*

Proof. Define $N_n = \oplus_{n \in \mathbb{N}} M_i$. Clearly, N_n is finitely generated for all n. Now consider

$$M_n^* = N_n \oplus \mathfrak{m} M_n \oplus \mathfrak{m}^2 M_n \oplus \dots$$

This is clearly an R^*-submodule of M. Indeed, M_n^* is a subgroup of M_n by the fact that $\{ M_n \}$ is an $\mathfrak{m}$-filtration. M_n^* also satisifes the conditions of a graded R^* module by definition.

Since N_n is finitely generated, M_n^* is also finitely generated. We now observe that M^* is simply the union over all such M_n^*. This is clear since the direct sum must be non-zero for only finitely many coordinates. Since R^* is Noetherian, we have that M^* is finitely generated if and only if the ascending chain of M_n^* terminates. This is equivalent to saying $M^* = M_{n_0}^*$ for some $n_0 \in \mathbb{N}$. But then $M_{n_0+r} = \mathfrak{m}^r M_{n_0}$ for all $r \geq 0$. This is equivalent to $\{ M_n \}$ being $\mathfrak{m}$-stable. □

Proposition 3.9 (Artin-Rees Lemma)**.** *Let R be a Noetherian ring and $\mathfrak{m} \lhd R$ an ideal. Suppose that M is a finitely generated module over R and that $\{ M_n \}$ is a $\mathfrak{m}$-stable filtration of M. Then given any R-submodule of M, say N, we have that $\{ N \cap M_n \}$ is an $\mathfrak{m}$-stable filtration of N.*

Proof. It is clear that

$$\mathfrak{m}(N \cap M_n) \subseteq \mathfrak{m}N \cap \mathfrak{m}M_n \subseteq N \cap M_{n+1}$$

whence $N \cap M_n$ is an $\mathfrak{m}$-filtration. It thus defines a graded R^*-submodule of M and we may apply Lemma 3.8 to see that $N \cap M_n$ is $\mathfrak{m}$-stable. □

Theorem 3.10 (Krull's Intersection Theorem)**.** *Let R be a Noetherian ring and $\mathfrak{m} \lhd R$ an ideal. Suppose that M is a finitely generated R-module. Then there exists an element $r \in \mathfrak{m}$ such that*

$$(1 - r)\left(\bigcap_{i=1}^{\infty} \mathfrak{m}^i M\right) = 0$$

Furthermore, if R is an integral domain or a local ring and $\mathfrak{m}$ a proper ideal, then

$$\bigcap_{i=1}^{\infty} \mathfrak{m}^i = 0$$

Proof. We first observe that $\{ \mathfrak{m}^n M \}$ is an $\mathfrak{m}$-stable filtration of M. It is clear that $N = \bigcap_{i=1}^{\infty} \mathfrak{m}^i M$ is an R-submodule of M. It then follows from the Artin-Rees Lemma that $\{ N \cap \mathfrak{m}^i M \}$ is an $\mathfrak{m}$-stable filtration of N. In particular, there exists a k such that for all $n \geq k$

$$N \cap \mathfrak{m}^{k+1} M = \mathfrak{m}(N \cap \mathfrak{m}^k M)$$

But N is contained in both $\mathfrak{m}^{k+1}M$ and $\mathfrak{m}^k M$ whence $N = \mathfrak{m}N$. Appealing to Nakayama's Lemma, we see that there must exist some $r \in \mathfrak{m}$ such that $(1 - r)N = 0$.

To prove the second statement, we may consider R as a module over itself. We have

$$(1 - r)\bigcap_{i=1}^{\infty} \mathfrak{m}^i = 0.$$

Since $\mathfrak{m}$ is a proper ideal, we know that $r \neq 1$ whence $1 - r \neq 0$. Now, in the case that R is an integral domain, we must therefore have that $\bigcap_{i=1}^{\infty} \mathfrak{m}^i = 0$. If R is a local ring then $\mathfrak{m}$ and, in particular, r are necessarily contained in the unique maximal ideal, say M. It is easy to see that $1 - r$ is then a unit. Indeed, if $1 - r$ was not a unit then necessarily, $1 - r \in M$. But then $1 \in M$ which is a contradiction. Since a unit can never be a zero divisor, we see that $\bigcap_{i=1}^{\infty} \mathfrak{m}^i = 0$. □

We can now return to the discussion at the beginning of this section. Krull's Intersection Theorem now implies that the kernel of the mapping from R to $\hat{R}_{\mathfrak{m}}$ is zero if R is Noetherian and either an integral domain or a local ring. For brevity's sake, we shall call such a ring **embeddable** (by no means a canonical name). As its name would suggest, an embeddable ring can be embedded in its completion. Therefore, the information contained in an embeddable ring is preserved when passing to its completion.

4 The Noetherian Property

It is all well and good that we can embed certain rings in their completions; however one may question the usefulness of completions if they did not preserve 'nice' properties of rings. In this section, we aim to show that the Noetherian property of a ring is also preserved when passing to the completion.

We begin by generalising the Hilbert basis theorem to formal power series.

Theorem 4.1 (Formal Hilbert Basis Theorem)**.** *Let R be a Noetherian ring. Then $R[[X_1, \ldots, X_n]]$ is Noetherian.*

Proof. We prove the theorem for the case of one indeterminate X. The general case then follows easily by induction. If $f = a_n X^n + a_{n+1} X^{n+1} + \cdots \in R[[X]]$ is a power series, we shall say that the degree of f is n and that its anti-leading coefficient is a_n. If $f = 0$ then we shall consider the degree of f to be infinite and its anti-leading coefficient to be 0.

Let $I \triangleleft R[[X]]$ be an ideal. We need to show that I is finitely generated. Fix an $f_1 \in I$ of minimal degree (we can clearly do this since the degree must be positive). We first define a sequence of power series $\{ f_n \mid n \in \mathbb{N} \} \subseteq I$ inductively. Suppose that we have already chosen elements $f_1, \ldots, f_{i-1}$. Denote their degrees by d_i and their anti-leading coefficients by a_i. Now if $(f_1, \ldots, f_{i-1}) \neq I$ then choose an $f_i \in I \backslash (f_1, \ldots, f_{i-1})$ of minimal degree. If this process terminates then clearly, I is finitely generated. If not, then consider the ideal $(a_1, \ldots, a_i) \triangleleft R$ generated by the anti-leading coefficients of the first i functions in the sequence. We have that

$$(a_1) \subseteq (a_1, a_2) \subseteq \cdots \subseteq (a_1, \ldots, a_i) \subseteq \ldots$$

is an ascending chain of ideals in R. But R is Noetherian so this chain must stabilise at say $i = n$. We claim that I is generated by $f_1, \ldots, f_n$.

Fix some $g \in I$. Let a_g be its anti-leading coefficient and d_g its degree. It is clear that $a_g \in (a_1, \ldots, a_n)$. Hence we may write $a_g = \sum_{i=1}^{n} r_i^{(0)} a_i$ for some $r_i^{(0)} \in R$. First suppose that $d_g \geq d_n$. Define the power series

$$g_0 = \sum_{i=1}^{n} r_i^{(0)} X^{d_g - d_i} f_i$$

We observe that g_0 also has degree d_g and anti-leading coefficient a_g. It thus follows that the degree of $g - g_0$ is greater than d_g. Now, g and g_0 are both in I so we must have that $g - g_0 \in I$. We see that the anti-leading coefficient of $g - g_0$ is in the ideal generated by $a_1, \ldots, a_n$. We can then repeat this process to produce a power series g_1 with anti-leading

coefficient and degree equal to those of $g - g_0$. Continuing in this fashion, we inductively define a sequence of power series $g_0, \ldots, g_m$ such that

$$g_m = \sum_{i=1}^{n} r_i^{(m)} X^{d_g+m-d_i} f_i$$

for some $r_i^{(m)} \in R$. Now, $g - \sum_{i=1}^{m} g_i$ has degree greater than $d_g + m$ and we clearly see that

$$g = \sum_{i=0}^{\infty} g_i = \sum_{i=0}^{\infty} \sum_{j=1}^{n} r_j^{(i)} X^{d_g+i-d_j} f_j$$

Since the inner sum is finite, we may swap the summations to see that g is finitely generated by the $f_1, \ldots, f_n$.

Now suppose that $d_g < d_n$. We know that $a_g \in (a_1, \ldots, a_n)$ and there must exist some $1 \leq k \leq n$ such that $a_g \in (a_1, \ldots, a_k)$. Hence $d_g \geq d_k$. We may write $a_g = \sum_{i=1}^{k} r_i^{(0)} a_i$ for some $r_i^{(0)} \in R$. Now define

$$h = \sum_{i=1}^{k} r_i^{(0)} X^{d_g-d_i} f_i$$

which has the same anti-leading coefficient and degree as g. We see that $g - h$ has degree greater than d_g. Again, we inductively define a sequence in this fashion until we reach a power series of degree d_n. We can then apply the result from the previous case to see that $g \in (f_1, \ldots, f_n)$.

□

Proposition 4.2. *Let R be a Noetherian ring and $\mathfrak{m} \triangleleft R$ an ideal. Then the completion $\hat{R}_{\mathfrak{m}}$ is Noetherian.*

Proof. Fix generators of $\mathfrak{m}$, say $m_1, \ldots, m_n \in R$. We claim that there exists a well-defined and surjective homomorphism

$$\phi : R[[X_1, \ldots, X_n]] \to \hat{R}_{\mathfrak{m}}$$

that sends each X_i to m_i. We can clearly map $R[X_1, \ldots, X_n]/(X_1, \ldots, X_n)^i$ to $R/\mathfrak{m}^i$ by sending X_i to m_i. This map induces a homomorphism of inverse limits:

$$\phi : \varprojlim_{n \in \mathbb{N}} R[X_1, \ldots, X_n]/(X_1, \ldots, X_n)^n \to \varprojlim_{n \in \mathbb{N}} R/\mathfrak{m}^n$$

which gives us our well-defined homomorphism $\phi : R[[X_1, \ldots, X_n]] \to \hat{R}_{\mathfrak{m}}$. It remains to show that ϕ is surjective. To this end, fix an $r \in \hat{R}_{\mathfrak{m}}$. Then r is a sequence of coherent elements $r_k \in R/\mathfrak{m}^k$. Consider r_1, we may lift this element of $R/\mathfrak{m}$ to an element of R in the form

$$\overline{r_1} = a + b_1$$

where $a \in R$ and b_1 is a degree one polynomial in the $m_1, \ldots, m_n$. In fact, we may even consider a as a degree zero polynomial b_0 in the $m_1, \ldots, m_n$. Hence we may write $\overline{r_1} =$

$\sum_{i=0}^{1} b_i$. Since the r_k are coherent with resepect to the transition morphisms, we may build lifts of each r_k in the form

$$\overline{r_k} = \sum_{i=0}^{k} b_k$$

where b_k is a degree k polynomial in the $m_1, \ldots, m_n$. Writing $b_k = f_k(m_1, \ldots, m_n)$, we easily see that

$$r = \phi\left(\sum_{i=1}^{\infty} f_i(X_1, \ldots, X_n)\right)$$

Indeed, we may consider the above modulo $\mathfrak{m}^k$ to retrieve each r_k. We have shown that ϕ is surjective which means that

$$R[[X_1, \ldots, X_n]]/\ker\phi \cong \hat{R}_{\mathfrak{m}}$$

Now, $R[[X_1, \ldots, X_n]]$ is Noetherian by the Formal Hilbert Basis Theorem and any quotient of a Noetherian ring is necessarily Noetherian. We thus see that $\hat{R}_{\mathfrak{m}}$ is Noetherian. □

Clearly, the completion of Noetherian rings is quite well behaved. Combining the results of the past two sections, we see that a Noetherian ring that is local or an integral domain can be embedded in its Noetherian completion.

5 Hensel's Lemma

We now turn our sights towards a useful result for complete local Noetherian rings. Hensel's Lemma is an example of solving global problems by reducing them to local ones. In fact, discussing the behaviour locally may give us more information about the problem than we could ever have by only looking at the problem globally. As an example, consider a complete local Noetherian ring R with maximal ideal $\mathfrak{m}$. Suppose we have a polynomial $f(x) \in R[X]$ whose image in $R/\mathfrak{m}[X]$ has a root in $R/\mathfrak{m}$. Then such a root can be lifted to a root in R. By $\overline{f}(X)$ we shall mean the image of $f(X)$ under the canonical map $R[X] \to (R/\mathfrak{m})[X]$

Theorem 5.1 (Hensel's Lemma)**.** *Let R be a local Noetherian ring that is complete with respect to its unique maximal ideal $\mathfrak{m}$. Denote its residue field $k = R/\mathfrak{m}$. Furthermore, let $f(X) \in R[X]$ be a monic polynomial such that $\deg f \geq 1$. Suppose G, H are coprime monic polynomials in $k[x]$ such that $\overline{f} = GH$. Then there exists monic polynomials $g, h \in R[X]$ such that $\overline{g} = G, \overline{h} = H$ and $f = gh$.*

Proof. Let $d_G = \deg G$ so that $\deg H = d_H = n - d_G$. We shall first construct a sequence of monic polynomials $g_i, h_i \in R[X]$ satisfying the congruence $f \equiv g_i h_i \pmod{\mathfrak{m}^i[x]}$ for all $i \geq 1$. Furthermore, we shall require that these g_i and h_i satisfy $\overline{g_i} = G$ and $\overline{h_i} = H$.

We proceed by induction. Suppose that G, H are as hypothesised. We may lift the coefficients of G and H to elements in R, being careful to choose 1 as a lift for the coset $1+\mathfrak{m}$ in order to preserve monicity. This gives us polynomials $g_1, h_1 \in R[X]$ such that $\overline{g_1} = G$ and $\overline{h_1} = H$ and $f \equiv g_1 h_1 \pmod{\mathfrak{m}^i[X]}$. Clearly, $\deg g_1 = d_G$ and $\deg h_1 = d_H$. Now suppose

we have constructed functions satisfying such criteria up to i. We shall construct g_{i+1}, h_{i+1}. Since G, H are coprime to each other we can find polynomials $a, b \in k[x]$ such that

$$ag_i + bh_i \equiv 1 \pmod{\mathfrak{m}[X]} \tag{1}$$

By the inductive hypothesis, we have that $f \equiv g_i h_i \pmod{\mathfrak{m}^i[X]}$ which means that $f - g_i h_i \in \mathfrak{m}^i[X]$. Denote this polynomial by z. We may multiply Equation 1 by z to get

$$z \equiv zag_i + zbh_i \pmod{\mathfrak{m}^{i+1}[X]}$$

Applying the division algorithm to za and the monic polynomial h_i we get two polynomials $c, d \in R[X]$ such that $za = ch_i + d$ with $\deg d < \deg h_i = n - \deg g_i$. It is easy to see that $za \in \mathfrak{m}^i[X]$ hence

$$ch_i + d \equiv 0 \pmod{\mathfrak{m}^i[X]}$$

It follows that $c, d \in \mathfrak{m}^i[X]$. Indeed, we may apply the division algorithm to 0 to see that $0 \equiv 0h_i + 0 \pmod{\mathfrak{m}^i[X]}$. But the division algorithm in $R/\mathfrak{m}^i[X]$ produces a unique quotient and remainder so we must have that $c, d \equiv 0 \pmod{\mathfrak{m}^i[X]}$ whence $c, d \in \mathfrak{m}^i[X]$. Hence

$$\begin{aligned} z &\equiv (ch_i + d)g_i + zbh_i \pmod{\mathfrak{m}^{i+1}[X]} \\ &\equiv ch_i g_i + dg_i + zbh_i \end{aligned}$$

Now set $e = cg_i + zb$ so we have

$$z \equiv dg_i + eh_i \pmod{\mathfrak{m}^{i+1}[X]} \tag{2}$$

Since $\deg z, \deg dg_i < n$ we must have $\deg eh_i < n$. But $\deg h_i = d_H = n - d_G$ which implies that $\deg e < d_G$. It then follows that $\deg(g_i + e) = d_G$ and $\deg(h_i + d) = d_H$ and the two polymonials are still monic. Hence $g_i + e$ and $h_i + d$ are good candidates for g_{i+1} and h_{i+1} respectively. We just need to check that $f \equiv g_{i+1}h_{i+1} \pmod{\mathfrak{m}^{i+1}[X]}$ and that $\overline{g_{i+1}} = G$ and $\overline{h_{i+1}} = H$. Indeed,

$$\begin{aligned} g_{i+1}h_{i+1} &= (g_i + e)(h_i + d) \\ &= g_i h_i + eh_i + dg_i + ed \\ &\equiv g_i h_i + z \pmod{\mathfrak{m}^{i+1}[X]} \\ &= f \end{aligned}$$

where we have used the fact that $ed \in \mathfrak{m}^{2i}[X]$ which implies that $ed \equiv 0 \pmod{\mathfrak{m}^{i+1}[X]}$. Now, $d, e \in \mathfrak{m}^i$ so, clearly, $\overline{g_{i=1}} = G$ and $\overline{h_{i+1}} = H$.

We would now like to show that such a sequence of polynomials g_i and h_i are unique up to congruence modulo $\mathfrak{m}^i[X]$. More concretely, if $\overline{g'} = G$ and $\overline{h'} = H$ for some polynomials $g', h' \in R[X]$ and $f \equiv g'h' \pmod{\mathfrak{m}^i[X]}$ then $g' \equiv g_i \pmod{\mathfrak{m}^i[X]}$ and $h' \equiv h_i \pmod{\mathfrak{m}^i[X]}$. Suppose this is true for i. We shall prove that this is true for $i + 1$. Let $g', h' \in R[X]$ be monic polynomials of degree d_G and $d_H = n - d_G$ respectively such that $f \equiv g'h' \pmod{\mathfrak{m}^i[X]}$ and $\overline{g'} = G, \overline{h'} = H$. By the induction hypothesis, we know that $g' \equiv g_i \pmod{\mathfrak{m}^i[X]}$ and $h' \equiv h_i \pmod{\mathfrak{m}^i[X]}$. Denote $e' = g' - g_i$ and $d' = h' - h_i$. Reducing modulo $\mathfrak{m}^i[X]$ we see that $d', e' \in \mathfrak{m}^i[X]$. Now,

$$\begin{aligned} 0 &\equiv f - g'h' \pmod{\mathfrak{m}^{i+1}[X]} \\ &\equiv f - (e' + g_i)(d' + h_i) \\ &\equiv f - d'e' - d'g_i - e'h_i - g_i h_i \\ &\equiv z - d'g_i - e'h_i \end{aligned}$$

So that we have $z \equiv d'g_i + e'h_i \pmod{\mathfrak{m}^{i+1}[X]}$. Subtracting this from Equation 2 yields

$$0 \equiv (d - d')g_i + (e - e')h_i \pmod{\mathfrak{m}^{i+1}[X]} \tag{3}$$

Denote $\delta = d - d'$ and $\varepsilon = e - e'$. These are polynomials of degrees d_G and $n - d_G$ respectively. Multiplying Equation 3 by the polynomial a we have

$$0 \equiv a\delta g_i + a\varepsilon h_i \pmod{\mathfrak{m}^{i+1}[X]}$$

Equation 1 implies that $ag_i + bh_i - 1 = m$. Inserting this into the previous equation and rearranging, we have

$$\delta \equiv (\delta b - \varepsilon a)h_i - \delta m \pmod{\mathfrak{m}^{i+1}[X]}$$

Now, $\delta \in \mathfrak{m}^i[X]$ and $\mathfrak{m} \in \mathfrak{m}[X]$ whence $\delta \equiv (\delta b - \varepsilon a)h_i \pmod{\mathfrak{m}^{i+1}[X]}$. δ is thus a polynomial multiple of h_i in $R/\mathfrak{m}^i[X]$. But $\deg \delta < n - d_G$ and $\deg h_i = n - d_G$. Our only option is that $\delta \equiv 0 \pmod{\mathfrak{m}^{i+1}[X]}$. A similar argument shows that $\varepsilon \equiv 0 \pmod{\mathfrak{m}^{i+1}[X]}$. We now see that

$$\begin{aligned} g' &\equiv g_i + e' \equiv g_i + e \equiv g_{i+1} \pmod{\mathfrak{m}^{i+1}[X]} \\ h' &\equiv h_i + d' \equiv h_i + d \equiv h_{i+1} \pmod{\mathfrak{m}^{i+1}[X]} \end{aligned}$$

as required.

We now complete the proof by showing that there exist two polynomials $g, h \in R[X]$ such that $f = gh$ and $\overline{g} = G$ and $\overline{h} = H$. Indeed, let $1 \leq i < j$, then $f \equiv g_j h_j \pmod{\mathfrak{m}^j}$ whence $f - g_j h_j \in \mathfrak{m}^j[X] \subseteq \mathfrak{m}^i[X]$ and thus $f \equiv g_j h_j \pmod{\mathfrak{m}^i}$. It follows from the uniqueness shown above that $g_j \equiv g_i \pmod{\mathfrak{m}^i[X]}$ and $h_j \equiv h_i \pmod{\mathfrak{m}^j[X]}$. Let $a_{k,j}$ and $b_{l,j}$ be the k^{th} and l^{th} coefficients of g_j and h_j respectively, where $0 \leq k \leq d_G$ and $0 \leq l \leq d_H$. Clearly, we must have that

$$a_{k,j} \equiv a_{k,i} \pmod{\mathfrak{m}^i}$$

for all k. Hence, for fixed k, the sequence of coefficients $a_{k,j}$ (indexed over j) are coherent. Since R is complete, this sequence of coefficients defines an element of the inverse limit, say $\tilde{a}_k$. Similarly, we have $\tilde{b}_j$ is an element of the inverse limit. These elements of R then give us polynomials in $R[X]$:

$$\begin{aligned} g &= \tilde{a}_0 + \tilde{a}_1 X + \cdots + \tilde{a}_{d_G} X^{d_G} \\ h &= \tilde{b}_0 + \tilde{b}_1 X + \cdots + \tilde{b}_{d_H} X^{d_H} \end{aligned}$$

It follows from the fact that $\overline{g_i} = G$ for all i that $\overline{g} = G$. Similarly, $\overline{h} = H$. Now, we have that $f - g_i h_i \equiv 0 \pmod{\mathfrak{m}^i[X]}$ for all $i \geq 1$ and thus

$$f - gh \in \bigcap_{i=1}^{\infty} \mathfrak{m}^i[X]$$

But R is a local Noetherian ring and $\mathfrak{m} \lhd R$ is proper. By Krull's Intersection Theorem, we must have that $\bigcap_{i=1}^{\infty} \mathfrak{m}^i = \{ 0 \}$. We thus see that $f = gh$ as required. □

It turns out that Hensel's Lemma holds for a much wider class of rings than just complete local Noetherian rings. Any local ring that satisfies the conclusion of Hensel's Lemma is referred to as **Henselian**. Indeed, any complete local Noetherian ring is Henselian.

Corollary 5.2. *Let R be a local Noetherian ring that is complete with respect to its maximal ideal $\mathfrak{m}$. Suppose that $f(x) \in R[X]$ is a polynomial. If its image in the residue field $\overline{f}[X] \in k[x]$ has a simple root α then $f(X)$ has a simple root a such that $\overline{a} = \alpha$.*

Proof. Since α is a simple root of $\overline{f}[X]$ we may write $\overline{f}[X] = (X - \alpha)H(X)$ for some $H(X)$ coprime to $X - \alpha$. By Hensel's Lemma, $f(X)$ splits into two polynomials $f = gh$ such that $\overline{g} = X - \alpha$ and $\overline{h} = H$. This implies that $g = X - a$ for some $a \in R$ such that $\overline{a} = \alpha$. If h were not coprime to g then we could write $f(X) = (x - a)^2 h_2(X)$ for some $h_2(X) \in R[X]$. But then we would have $\overline{f}(X) = (x-\alpha)^2\overline{h_2}(X)$ which contradicts the fact that α is a simple root of $\overline{f}(X)$. □

Example 5.3. Consider the polynomial ring $\mathbb{R}[z]$. We may complete this with respect to its maximal ideal (z) (this is indeed maximal since $\mathbb{R}$ is a field) to get $\mathbb{R}[[z]]$ also with maximal ideal (z). We note that the residue field $\mathbb{R}[[z]]/(z) \cong \mathbb{R}$. Consider the polynomial $f(X) = X^2 - (1 + z) \in (\mathbb{R}[[z]])[X]$. Now $\overline{f}(X) = (X - 1)(X + 1) \in \mathbb{R}[X]$. Appealing to Hensel's Lemma, we see that there exist two power series $\alpha(z), \beta(z) \in \mathbb{R}[[z]]$ such that

$$X^2 - (1 + z) = (X - \alpha(z))(X - \beta(z))$$

Clearly, $\alpha(z)$ and $\beta(z)$ are square roots of $1+z$ so we must have that $\alpha(z) = -\beta(z)$. Hensel's Lemma also implies that the constant terms of these power series are 1 and -1 respectively.

The above example is quite a striking result. It implies there exist purely algebraic methods of obtaining power series expansions for certain functions. The resulting power series from the previous example coincides with the one obtained by the Taylor expansion of $\sqrt{1 + z}$. Indeed, way may proceed algorithmically with the proof of Hensel's lemma to construct the coefficients of each term in the power series $\alpha(z)$.

6 Cohen's Structure Theorem

In this section we aim to prove a special case of the Cohen Structure Theorem - a fundamental result that characterises complete local Noetherian rings. In order to do so, we begin by introducing some new ideas.

Definition 6.1. Let R be a ring and $\mathfrak{m} \triangleleft R$ an ideal. We define the **associated graded ring** of the filtration $\{\, \mathfrak{m}^i \,\}$ as

$$\mathrm{gr}_{\mathfrak{m}}(R) = \bigoplus_{i=0}^{\infty} \mathfrak{m}^i/\mathfrak{m}^{i+1}$$

with multiplication defined by the map

$$\begin{aligned} \mathfrak{m}^n/\mathfrak{m}^{n+1} \times \mathfrak{m}^m/\mathfrak{m}^{m+1} &\to \mathfrak{m}^{n+m}/\mathfrak{m}^{n+m+1} \\ (x + \mathfrak{m}^{n+1}, y + \mathfrak{m}^{m+1}) &\mapsto xy + \mathfrak{m}^{n+m+1} \end{aligned}$$

Definition 6.2. Consider the following diagram

$$G_0 \xrightarrow{\phi_1} G_1 \xrightarrow{\phi_2} G_2 \xrightarrow{\phi_3} \ldots \xrightarrow{\phi_n} G_n$$

where the G_i are groups (or modules) and the ϕ_j are morphisms between them. Then we say that such a diagram is an **exact sequence** if $\ker \phi_{i+1} = \operatorname{im} \phi_i$ for all $i = 1, \ldots, n - 1$. If G_1, G_2 and G_3 are groups (modules) and $f : G_1 \to G_2$ is injective and $g : G_2 \to G_3$ is surjective then the following diagram

$$0 \longrightarrow G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3 \longrightarrow 0$$

is called a **short** exact sequence.

Proposition 6.3 (short five lemma)**.** *Consider the commutative diagram with short exact rows*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \theta} & & \\ 0 & \longrightarrow & D & \xrightarrow{h} & E & \xrightarrow{i} & F & \longrightarrow & 0 \end{array}$$

If ϕ and θ are isomorphisms then so is ψ.

Proof. Proof omitted. The reader is invited to check any standard text on homological algebra for a rigorous treatment of this proof and of exact sequences in general. □

Lemma 6.4. *Let R and S be complete local rings that are complete with respect to their respective maximal ideals $\mathfrak{m}$ and $\mathfrak{n}$. Suppose that $\phi : R \to S$ is a homomorphism such that $\phi(\mathfrak{m}^i) \subseteq \mathfrak{n}^i$ for all $i \geq 1$. If the induced homomorphism of graded rings $\mathrm{gr}(\phi) : \mathrm{gr}_{\mathfrak{m}}(R) \to \mathrm{gr}_{\mathfrak{n}}(S)$ is surjective then so is ϕ.*

Proof. Consider the following commutative diagram

$$\begin{array}{ccccccccc} & & & & 0 & & 0 & & \\ & & & & \downarrow & & \downarrow & & \\ & & & & \ker\phi_{i+1} & \longrightarrow & \ker\phi_i & & \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathfrak{m}^i/\mathfrak{m}^{i+1} & \longrightarrow & R/\mathfrak{m}^{i+1} & \longrightarrow & R/\mathfrak{m}^i & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{gr}_i(\phi)} & & \downarrow{\scriptstyle \phi_{i+1}} & & \downarrow{\scriptstyle \phi_i} & & \\ 0 & \longrightarrow & \mathfrak{n}^i/\mathfrak{n}^{i+1} & \longrightarrow & S/\mathfrak{n}^{i+1} & \longrightarrow & S/\mathfrak{n}^i & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \\ & & & & 0 & & 0 & & \end{array}$$

where $\mathrm{gr}_i(\phi)$ is the induced map between the i^{th} decompositions in the associated graded ring and ϕ_i is map between the i^{th} coordinates of the inverse limits. Consider the third row of the above diagram. By an isomorphism theorem, we have that

$$\frac{R/\mathfrak{m}^{i+1}}{\mathfrak{m}^i/\mathfrak{m}^{i+1}} \cong R/\mathfrak{m}^i$$

and hence the third row is a short exact sequence. The same argumentation shows that the fourth row is also a short exact sequence. Now let $s \in S$. We need to exhibit an $r \in R$ such that $\phi(r) = s$. By definition, s is a sequence of coherent elements $s_i \in S/\mathfrak{n}^i$. Hence it suffices to show that there exists an $r_i \in R/\mathfrak{m}^i$ such that $\phi_i(r_i) = s_i$ and $r_{i+1} \equiv r_i \pmod{\mathfrak{m}^i}$.

We proceed by induction. Clearly, the surjectivity of $gr_0(\phi)$ implies that ϕ_1 is surjective. Now assume that ϕ_n is surjective. Since $\mathrm{gr}_n(\phi)$ is surjective, the short five lemma implies that ϕ_{n+1} is surjective. Hence given $s_{n+1} \in S/\mathfrak{n}^{n+1}$ there exists $r_{n+1} \in R/\mathfrak{m}^{n+1}$ such that $\phi_{n+1}(r_{n+1}) = s_{n+1}$. r_{n+1} may not reduce to r_n modulo $\mathfrak{m}^n$ but the difference between

them is an element of $\ker \phi_n$. From the diagram, we see that the third and fourth columns are short exact sequences. The short five lemma then implies that $\ker \phi_{i+1}$ surjects onto $\ker \phi_i$. We may thus modify r_{i+1} by an element of $\ker \phi_{i+1}$ to obtain the condition $r_{i+1} \equiv r_i \pmod{\mathfrak{m}^i}$. □

Definition 6.5. Let R be a local ring with unique maximal ideal $\mathfrak{m}$. Let $\varphi : R \to R/\mathfrak{m}$ be the canonical map from R to its residue field. If there exists a field $K \subseteq R$ such that φ maps K isomorphically to $R/\mathfrak{m}$ then K is said to be a **coefficient field** of R. In other words, if R has a coefficient field then R contains a copy of its residue field.

We now proceed to show that any complete local Noetherian ring that contains a field and whose residue field is perfect necessarily has a coefficient field. We accomplish this first by proving the case where the residue field has characteristic 0 and then the case where the characteristic is $p > 0$.

Lemma 6.6. *Let R be a local Noetherian ring that is complete with respect to its unique maximal ideal $\mathfrak{m}$. If $\operatorname{char}(R) = \operatorname{char}(R/\mathfrak{m}) = 0$ and R contains a field then R has a coefficient field.*

Proof. We must show that R contains a field that is isomorphic to its residue field. Consider the set

$$S = \{\, K \subseteq R \mid K \text{ is a field} \,\}$$

S is clearly non-empty by hypothesis. Let $\mathcal{C} \subseteq S$ be a chain in S. Then clearly the union of the elements in $\mathcal{C}$ is again a field contained in R and is thus in S. Appealing to Zorn's Lemma, there exists a maximal field $K \subseteq R$.

Now consider the mapping

$$\varphi : R \to k = R/\mathfrak{m}$$

which maps R onto its residue field k. We claim that φ maps K isomorphically to k. Since K is a field, we must have that $\varphi|_K$ is injective. Hence it remains to show that $\varphi|_K$ is surjective. Suppose that $\varphi(K) \subsetneq k$. Fix some $y \in k \backslash \varphi(K)$. Since φ is surjective, there is an $x \in R$ with $\varphi(x) = y$.

Suppose that y is not a root of a monic polynomial in $\varphi(K)[X]$. Then x is not the root of a monic polynomial in $K[X]$. Now consider the homomorphism

$$\begin{aligned} \psi : K[X] &\to R \\ X &\mapsto x \end{aligned}$$

Since K is a field, the kernel of ψ is either zero or the ideal generated by some monic polynomial. But x is not the root of any monic polynomial in $K[X]$ hence we must have that $\ker \psi = \{\, 0 \,\}$ whence ψ is injective. Hence R contains a copy of $K[X]$, which we denote $K[x]$. Now the map sending $K[x]$ to k is clearly injective since y is not the root of any monic polynomial in $\varphi(K)[X]$. It follows that if $p \in K[x]$ is non-zero then $p \not\equiv 0 \pmod{\mathfrak{m}}$. Hence $p \notin \mathfrak{m}$. But R is local so p must be a unit in R. We then have that the field of rational functions $\operatorname{Frac}(K[x]) = K(x)$ is contained in R. But $K \subsetneq K(x)$ which contradicts the maximality of K.

Conversely, suppose that y is a root of a monic polynomial in $\varphi(K)[X]$. Let $f \in \varphi(K)[X]$ be its minimal polynomial. f is irreducible over $\varphi(K)[X]$ and its inverse image, say F, is irreducible over $K[X]$. Now, $\text{char}(k) = 0$ hence f is seperable whence $f'(y) \neq 0$. This implies that y is a simple root of $f(X)$. Applying Corollary 5.2 we see that F has a simple root, say $x \in R$. Now consider the homomorphism

$$\begin{aligned} \psi : K[X]/F &\to R \\ X &\mapsto x \end{aligned}$$

We claim that ψ is injective. This becomes quite obvious from the following diagram:

$$\begin{array}{ccc} K[X]/F & \xrightarrow{\psi} & R \\ & \searrow & \downarrow \varphi \\ & & k \end{array}$$

Indeed, $\varphi \circ \psi$ is injective since $0 + F$ is the only element of $K[X]/F$ that can map to 0 in k. Hence ψ must be injective. We thus see that R contains a copy of $K[X]/F$. Now F is irreducible over K and $K[X]/F$ must be a field. It clearly contains (and is not equal to) K which contradicts the maximality of K in R.

Both cases yield contradictions so our only option is that $\varphi(K) = k$. □

Lemma 6.7. *Let R be a local Noetherian ring that is complete with respect to its unique maximal ideal $\mathfrak{m}$. If $\text{char}(R) = \text{char}(R/\mathfrak{m}) = p > 0$ and $R/\mathfrak{m}$ is perfect then R has a unique coefficient field.*

Proof. Let R^{p^n} denote the set

$$R^{p^n} = \{\, r^{p^n} \mid r \in R \,\}$$

We claim that $K = \bigcap_{i=0}^{\infty} R^{p^i}$ is a coefficient field for R. We must first show that K is itself a field. Suppose that $a \in K \cap \mathfrak{m}$. Then, by definition of K, a is a $(p^n)^{th}$ power of some element, say $b \in R$. It then follows that $b \in \mathfrak{m}$. From this we see that $a \in \bigcap_{i=0}^{\infty} \mathfrak{m}^{p^n}$. Krull's Intersection Theorem then implies that $a = 0$. Since $K \cap \mathfrak{m} = \{\, 0 \,\}$, we see that $K \setminus \{\, 0 \,\}$ are all units of R. Let $x \in K \setminus \{\, 0 \,\}$. Then $x = y^{p^n}$ for some n. Taking the inverse of both sides, we see that $x^{-1} = (y^{-1})^{p^n}$ and thus $x^{-1} \in K$. K is hence a field.

As in the proof of the previous lemma, in order to show that K is a coefficient field, it suffices to show that $\varphi : R \to R/\mathfrak{m}$ maps K onto the residue field. To this end, fix $y \in k = R/\mathfrak{m}$. We need to find an $x \in K$ such that $\varphi(x) = y$. Since φ is surjective and k is perfect, we can find an $x_n \in R$ such that $\varphi(x_n) = y^{1/p^n}$. Raising both sides to the $(p^n)^{th}$ power, we have $\varphi(x_n^{p^n}) = y$. Observe that both x_n and x_{n+1}^p map to y^{1/p^n} under φ. Thus, $x_n \equiv x_{n+1}^p \pmod{\mathfrak{m}}$. Raising this to the $(p^n)^{th}$ power, we have

$$x_n^{p^n} \equiv x_{n+1}^{p^{n+1}} \pmod{\mathfrak{m}^{p^n}}$$

We see that the sequence $x_i^{p^i}$ defines an element of the inverse limit[2], say $x \in R$. Furthermore, $\varphi(x) = y$ by construction. It remains to show that $x \in K$. By the definition of K,

[2]in fact, this sequence is a Cauchy sequence - the entire theory of complete local rings can be constructed through topological means by taking the powers of $\mathfrak{m}$ to be a basis of neighbourhoods of 0

we just need to show that $x \in R^{p^i}$ for all i. Clearly, we can play the same game as above to construct an element of the inverse limit that maps to y^{1/p^i} for all i. Hence for all i, we can find a z_i such that $z_i^{p^i} = x$ and the lemma is proven.

It remains to show the uniqueness of K. Suppose that L is any other coefficient field of R. Then $L \cong k$ and L is perfect. By definition of a perfect field, the Frobenius endomorphism on L is an automorphism whence $L = L^p = L^{p^2} = \dots$. This implies that $L = L^{p^n} \subseteq R^{p^n}$ for all $n \geq 0$ and thus $L \subseteq K$. But K is a field and $K \cong k \cong L$ so we must have that $L = K$. Hence K is the unique coefficient field of R. □

Theorem 6.8 (Cohen's Structure Theorem)**.** *Let R be a local Noetherian ring that is complete with respect to its unique maximal ideal $\mathfrak{m}$. Let $k = R/\mathfrak{m}$ be its residue field. If R contains a field and k is perfect then $R \cong k[[X_1, \dots, X_n]]/I$ for some ideal I.*

Proof. Since k is perfect, Lemmas 6.6 and 6.7 imply that R has a coefficient field, say K. Now R is Noetherian which means $\mathfrak{m}$ is finitely generated, say by $m_1, \dots, m_n$. We claim that the map

$$\begin{aligned} \phi : K[[X_1, \dots, X_n]] &\to R \\ X_i &\mapsto m_i \end{aligned}$$

is well-defined and surjective. Applying the same reasoning as for Proposition 4.2, we see that ϕ is well-defined. Now, for surjectivity, we consider the induced map of associated graded rings $\mathrm{gr}(\phi) : \mathrm{gr}(K[[X_1, \dots, X_n]]) \to \mathrm{gr}(R)$. This map is surjective because $K \cong k$ and

$$\begin{aligned} \mathrm{gr}_i(\phi) : \frac{(X_1, \dots, X_n)^i}{(X_1, \dots, X_n)^{i+1}} &\to \frac{\mathfrak{m}^i}{\mathfrak{m}^{i+1}} \\ X_i &\mapsto m_i \end{aligned}$$

is surjective since the m_i generate $\mathfrak{m}$. Now by Lemma 6.4, ϕ is surjective hence

$$k[[X_1, \dots, x_n]]/\ker(\phi) \cong R$$

thereby proving Cohen's Structure Theorem. □

In fact, Cohen's Structure Theorem holds for any complete local Noetherian ring that contains a field, regardless of whether or not that field is perfect. Since R contains a field K, it can be shown that $\mathrm{char}(R) = \mathrm{char}(K)$. For this reason, the case where R contains a field is sometimes called the **equicharacteristic** Cohen Structure Theorem.

If R does not contain a field then we may refer to the **mixed characteristic** Cohen Structure Theorem which states that a complete local Noetherian ring R that does not contain a field is isomorphic to $D[[X_1, \dots, X_n]]/I$ where D is some discrete valuation ring and I is an ideal.

References

[1] M.F Atiyah, I.G. MacDonald, *Introduction To Commutative Algebra*, Addison-Wesley, 1969

[2] David Eisenbud, *Introduction to Commutative Algebra with a View Towards Algebraic Geometry*, Springer-Verlag, 1995

[3] Neal Koblitz, *p-adic Numbers, p-adic Analysis and Zeta-Functions*, second edition, Springer, 1984.

[4] I. S. Cohen, *On the structure and ideal theory of complete local rings*, Trans. AMS **59** (1946), 54-106

[5] Robert Ash, *A Course in Commutative Algebra*, `http://www.math.uiuc.edu/~r-ash/ComAlg.html` [Accessed 11/01/16]

[6] Florian Bouyer, *Commutative Algebra II*, `https://www2.warwick.ac.uk/fac/sci/maths/people/staff/bouyer/commutative_algebra_ii.pdf` [Accessed 11/01/16]

[7] CRing Project, *Completions*, `https://math.berkeley.edu/~amathew/chcompletion.pdf` [Accessed 11/01/16]

[8] Daniel Murfet, *Hensel's Lemma*, `http://therisingsea.org/notes/HenselsLemma.pdf` [Accessed 11/01/16]

[9] Tamás Szamuely, *First Steps in Local Algebra*, `http://www.renyi.hu/~szamuely/localg.pdf` [Accessed 11/01/16]

[10] Mel Hochster, *The structure theory of complete local rings*, `http://www.math.lsa.umich.edu/~hochster/615W10/supStructure.pdf` [Accessed 11/01/16]