

Functorial Cohen Rings

by

Wayne Allen Whitney

A.B. (Harvard University) 1994

M.A. (University of California, Berkeley) 1999

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Mathematics

in the

GRADUATE DIVISION

of the

UNIVERSITY of CALIFORNIA, BERKELEY

Committee in charge:

Professor Hendrik Lenstra, Chair

Professor Arthur Ogus

Professor Terry Speed

Fall 2002

Functorial Cohen Rings

Copyright 2002
by
Wayne Allen Whitney

Abstract

Functorial Cohen Rings

by

Wayne Allen Whitney

Doctor of Philosophy in Mathematics

University of California, Berkeley

Professor Hendrik Lenstra, Chair

Let S be a commutative ring. A field k with an S -algebra structure induces a functor Q_k from the category of complete local commutative S -algebras to the category of sets. This functor is given by sending a local ring A with residue field QA to $\text{Hom}_S(k, QA)$, the set of morphisms in the category of fields with S -algebra structure. The functor Q_k is shown to be representable if and only if the module of Kähler differentials $\Omega_{k/S}$ is zero. The crux of the proof of this theorem is the development of a functorial construction of the Cohen ring of a field equipped with a p -basis. This represents an expansion and modernization of the earlier work of Cohen.

Contents

1	Preliminaries	1
1.1	Introduction	1
1.2	Conventions	2
1.3	Differential bases	2
1.4	Completeness	3
1.5	Completion	4
2	Cohen rings	6
2.1	Two categories	7
2.2	Two subrings	7
2.3	Properties of the subring $F(A)$	8
2.4	Iterates of F	9
2.5	Projection onto \mathbf{P}_k	11
2.6	The structure of \mathbf{P}_k	11
2.7	Populating the categories	13
2.8	The construction	14
3	Main theorem	16
3.1	Characteristic 0	16
3.2	The unit	18
3.3	Main proof	19
	Bibliography	21

Acknowledgements

I wish to thank Professor Hendrik Lenstra for all of his ideas, feedback, and support, without which this dissertation would not exist. I also wish to thank Professor Arthur Ogus for his guidance early in my graduate career. Finally, I would like to thank my colleague Dr. James Borger for his frequent suggestions and encouragement.

Chapter 1

Preliminaries

All rings and algebras are commutative with unit.

A “Cohen ring” is a complete discrete valuation ring for which a prime number p is a uniformizer. For any field k of positive characteristic p , there is a Cohen ring $C(k)$ with residue field k , unique up to isomorphism [5, 0.19.8.5, p. 111]. However, $C(k)$ is not a functor in k , as for imperfect k the ring $C(k)$ is not unique up to unique isomorphism. This deficit may be repaired by introducing an appropriate auxiliary ring S and passing to S -algebras, which leads to the somewhat broader result presented here.

1.1 Introduction

Let S be a ring, and consider two categories of S -algebras: the category \mathbf{C} of complete local S -algebras with continuous homomorphisms, and the category \mathbf{F} of S -algebras which are fields. (Note that the definition of complete here is broader than the usual one, see Section 1.4 for details.) There is an obvious functor $Q : \mathbf{C} \rightarrow \mathbf{F}$ which associates to a local ring its residue field. The functor Q has a right adjoint, given by considering a field to be a discrete complete local ring with maximal ideal 0 . In this generality, Q does not admit a left adjoint.

However, Q does have a “partial” left adjoint in the following sense: for a field k in \mathbf{F} , define the functor $Q_k : \mathbf{C} \rightarrow \mathbf{Sets}$ by $A \mapsto \text{Hom}_{\mathbf{F}}(k, QA)$. Were Q to have a left adjoint, Q_k would be representable for all k ; instead the following theorem holds.

Theorem 1.1. *With S , k , and Q_k as above, the functor Q_k is representable if and only if the module of Kähler differentials $\Omega_{k/S}$ is zero.*

Note that $\Omega_{k/S}$ is zero if and only if the morphism $S \rightarrow k$ is “formally unramified” [5, 0.20.7.4, p. 148].

The connection between Theorem 1.1 and Cohen rings is that for k of positive characteristic and for certain S , the object representing Q_k is a Cohen ring $C(k)$.

Recall that this means there is a natural system of bijections $l_A : \text{Hom}_{\mathbb{C}}(C(k), A) \rightarrow \text{Hom}_{\mathbb{F}}(k, QA)$ as A ranges over the objects of \mathbb{C} . In fact, it will turn out that l_A may be taken to be q_A , the map induced by the functor Q . Cohen proved that when $S = \mathbb{Z}$ and A is Noetherian, the map q_A is surjective [3, Corollary 1, p. 82]. Theorem 1.1 is an extension of this classical result.

The proof of Theorem 1.1 will be fairly elementary and will assume only basic notions of commutative algebra and category theory, such as Kähler differentials and adjoint functors. In particular, familiarity with Cohen rings is not required. Unusual or non-standard notions are discussed later in this chapter.

The strategy for proving Theorem 1.1 will be to first consider the situation that k has positive characteristic p and is equipped with a p -basis. A functorial construction of the Cohen ring $C(k)$ equipped with a lifted p -basis occupies Chapter 2. The remainder of the proof of Theorem 1.1 lies in Chapter 3 and consists of some category theory and differential theory.

1.2 Conventions

The set \mathbb{N} is the set of non-negative integers.

A ring A admits a unique homomorphism $\mathbb{Z} \rightarrow A$, and the “characteristic” of A is the nonnegative integer generator of the kernel of this map, written $\text{char } A$.

A basis of a vector space V over a field k is a map from a set U to V , such that the induced map $\bigoplus_U k \rightarrow V$ is an isomorphism. To translate this notion to the more usual notion of a basis as a subset of V , consider the image of the map $U \rightarrow V$.

1.3 Differential bases

For a field k , the k -module of Kähler differentials over \mathbb{Z} is denoted Ω_k and is equipped with a universal derivation $d : k \rightarrow \Omega_k$. A “differential basis” of k is a map $T : U \rightarrow k$ such that $d \circ T$ is a basis of Ω_k as a k -module [4, Section 7.4, p. 190]. The notion of differential basis reduces to two more familiar notions according to characteristic, as follows [4, Theorem 16.14, p. 398].

Given a set U , let $\Pi(U)$ denote the free commutative monoid on U , written multiplicatively; the elements of $\Pi(U)$ are monomials in U . For $n \in \mathbb{N}$, let $\Pi_n(U)$ denote the subset of $\Pi(U)$ of elements where the degree of any $u \in U$ is less than n . For a field k of positive characteristic p , a “ p -basis” of k is a map $T : U \rightarrow k$ such that the induced map $\Pi_p(U) \rightarrow k$ is a basis of k as a k^p -module. For fields of positive characteristic p , the notion of p -basis coincides with the notion of differential basis.

For a set U , the ring $\mathbb{Z}[U]$ is the polynomial ring on U with coefficients in \mathbb{Z} , and the field $\mathbb{Q}(U)$ is the field of rational functions on U with coefficients in \mathbb{Q} . The field $\mathbb{Q}(U)$ is the field of quotients of $\mathbb{Z}[U]$. Let k be a field of characteristic 0. A map $U \rightarrow k$ induces a homomorphism $\mathbb{Z}[U] \rightarrow k$, and if this homomorphism is injective, it

further induces a map $\mathbb{Q}(U) \rightarrow k$. A “transcendence basis” of k is a map $T : U \rightarrow k$ which induces a map $\mathbb{Q}(U) \rightarrow k$, and for which k is algebraic over the image of $\mathbb{Q}(U)$. For a field k of characteristic 0, the notion of transcendence basis coincides with the notion of differential basis.

Let A be a local ring with residue field k , and let $T : U \rightarrow k$ be a differential basis of k . A “lifted differential basis” of A is a map $T_A : U \rightarrow A$ for which composition with the natural surjection $A \rightarrow k$ gives the differential basis T . The notions of “lifted p -basis” and “lifted transcendence basis” are defined analogously.

Since the map defining a differential basis T is necessarily injective, it will occasionally be convenient to abuse notation and denote the image of this map by T also. The same applies to lifted differential bases.

1.4 Completeness

For convenience, a local ring A may be written as (A, \mathfrak{m}) where \mathfrak{m} is the maximal ideal of A .

The standard notion of completeness is as follows: the completion \hat{A} of a local ring (A, \mathfrak{m}) is defined as $\hat{A} = \text{projlim}_{n \rightarrow \infty} A/\mathfrak{m}^n$, and A is complete if the natural map $A \rightarrow \hat{A}$ is an isomorphism. This notion works well for Noetherian rings, but for non-Noetherian rings it suffers from a number of deficits. For example, the ring \hat{A} need not be complete [2, Exercise 3.2.12, p. 283–284].

Therefore this paper will use a more refined notion of complete. The basic idea is that a complete local ring is a topological ring which is a projective limit of “tractable” discrete local rings. The usual notion of tractable is that the maximal ideal is nilpotent. However, this paper will use a slightly broader notion, simply because all of the results may be proven for this broader notion with little extra effort.

If V is a subset of a ring A and $n \in \mathbb{N}$, then the subset $V^{[n]}$ of A is defined to be the image of V under the n -th power map of A . In the case of a field k of characteristic p , it is common to write k^p instead of $k^{[p]}$, as done earlier.

For an ideal \mathfrak{J} of A and for $n \in \mathbb{N}$, define $\mathfrak{J}^{(n)}$ to be the ideal generated by $\mathfrak{J}^{[n]}$. Note that if A is a \mathbb{Q} -algebra, then $\mathfrak{J}^{(n)}$ coincides with \mathfrak{J}^n , although this fact will not be used. The ideal \mathfrak{J} is “weakly nilpotent” if there exists $n \in \mathbb{N}$ with $\mathfrak{J}^{(n)} = 0$. As $\mathfrak{J}^{(n)}$ is always a subset of \mathfrak{J}^n , a nilpotent ideal is weakly nilpotent. Conversely, if \mathfrak{J} is finitely generated and weakly nilpotent, it is nilpotent.

Example 1.2. An ideal which is weakly nilpotent but not nilpotent.

Let k be a field of positive characteristic p , let X be an infinite set, and let $x : \mathbb{N} \rightarrow X$ be an injective map. That is, x is an infinite sequence in X without repetition. Consider the polynomial ring $k[X]$, and let \mathfrak{m} be the ideal of $k[X]$ generated by the elements of X . Then for each $n \in \mathbb{N}$, the product $\prod_{i=1}^n x(i)$ is an element of \mathfrak{m}^n but does not lie in $\mathfrak{m}^{(p)}$. Therefore the ideal $\mathfrak{m}/\mathfrak{m}^{(p)}$ of the ring $k[X]/\mathfrak{m}^{(p)}$ is not nilpotent, but it is obviously weakly nilpotent.

A “complete” local ring is a topological local ring A for which there exists a directed system of ideals \mathfrak{J}_i in A such that each quotient $A_i = A/\mathfrak{J}_i$ is discrete with weakly nilpotent maximal ideal and such that the natural map $A \rightarrow \text{projlim}_i A_i$ is an isomorphism of topological rings. Here the projective limit is endowed with the product topology. Such a collection of ideals \mathfrak{J}_i , or equivalently quotients A_i , will be called “structural”. Morphisms of complete local rings are required to be continuous, which forces them to be local as well.

1.5 Completion

The motivation for passing to a definition of a complete local ring using topological rings is to permit a satisfactory notion of completing a local ring. In addition to the category \mathbf{C} of complete local S -algebras with continuous morphisms, consider the category \mathbf{L} of local S -algebras with local morphisms. As morphisms in \mathbf{C} are local, there is a forgetful functor from \mathbf{C} to \mathbf{L} which simply drops the topology on the rings. The following lemma describes completion in terms of this forgetful functor.

Lemma 1.3. *There is a completion functor $A \mapsto \hat{A}$ from \mathbf{L} to \mathbf{C} which is left adjoint to the forgetful functor $\mathbf{C} \rightarrow \mathbf{L}$.*

Proof. Let (A, \mathfrak{m}) be an object of \mathbf{L} , let $A_n = A/\mathfrak{m}^{(n)}$, and let $\mathfrak{m}_n = \mathfrak{m}/\mathfrak{m}^{(n)}$. Define the ring \hat{A} as $\text{projlim}_{n \rightarrow \infty} A_n$. Since the projective system A_n is countable and has surjective transition maps, the natural map $\hat{A} \rightarrow A_n$ is surjective for each n . Then the ring \hat{A} is complete, as the maximal ideal $\hat{\mathfrak{m}}$ of \hat{A} is weakly nilpotent. Let $\hat{\mathfrak{m}}$ be the kernel of the natural map $\hat{A} \rightarrow A/\mathfrak{m}$. The ring \hat{A} is local, as any $a \in \hat{A} \setminus \hat{\mathfrak{m}}$ has image in $A_n \setminus \mathfrak{m}_n$ which is invertible, and these inverses form a compatible sequence of elements defining $a^{-1} \in \hat{A}$. The S -algebra structure on \hat{A} is given by composing the structure map $S \rightarrow A$ with the natural $A \rightarrow \hat{A}$. Thus \hat{A} is an object of \mathbf{C} . The operation $A \mapsto \hat{A}$ forms a functor from \mathbf{L} to \mathbf{C} , as any local map $A \rightarrow B$ induces a map $A_n \rightarrow B_n$ for each positive $n \in \mathbb{N}$, where B_n is defined analogously to A_n .

It remains to show that $A \mapsto \hat{A}$ is left adjoint to the forgetful functor from \mathbf{C} to \mathbf{L} . That is, if B is any object of \mathbf{C} , it is required to show that $\text{Hom}_{\mathbf{C}}(\hat{A}, B) \cong \text{Hom}_{\mathbf{L}}(A, B)$. To see this, let (B_i, \mathfrak{n}_i) be a structural system of quotients of B . That is, each B_i is a discrete quotient of B , each \mathfrak{n}_i is weakly nilpotent, and the natural map $B \rightarrow \text{projlim}_i B_i$ is an isomorphism.

Giving a local map $A \rightarrow B$ is equivalent to giving a compatible sequence of local maps $A \rightarrow B_i$. As \mathfrak{n}_i is weakly nilpotent, let $n_i \in \mathbb{N}$ be the smallest integer such that $\mathfrak{n}_i^{(n_i)} = 0$. Then any local map $A \rightarrow B_i$ factors through A_{n_i} , since $\mathfrak{n}_i^{(n_i)} = 0$. Thus giving a local map $A \rightarrow B$ is equivalent to giving a compatible family of local maps $A_{n_i} \rightarrow B_i$.

On the other hand, giving a continuous local map $\hat{A} \rightarrow B$ is equivalent to giving a compatible family of continuous local maps $\hat{A} \rightarrow B_i$. A continuous local map $\hat{A} \rightarrow B_i$

is required to factor through the map $\hat{A} \rightarrow A_{m_i}$ for some $m_i \in \mathbb{N}$, since the kernel of the map $\hat{A} \rightarrow B_i$ must be open. In fact, m_i may be taken to be n_i , since it is certainly permissible to increase m_i , and if $m_i > n_i$, any map $A_{m_i} \rightarrow B_i$ factors through A_{n_i} . Also, any map from $A_{n_i} \rightarrow B_i$ is automatically continuous, as both rings are discrete. Thus giving a continuous local map $\hat{A} \rightarrow B$ is also equivalent to giving a compatible family of local maps $A_{n_i} \rightarrow B_i$.

This shows that $\text{Hom}_{\mathbf{C}}(\hat{A}, B) \cong \text{Hom}_{\mathbf{L}}(A, B)$, so the functor $A \mapsto \hat{A}$ is left adjoint to the forgetful functor $\mathbf{C} \rightarrow \mathbf{L}$. \square

Note that if $B = \hat{A}$, then B is complete, but as discussed already [2, Exercise 3.2.12, p. 283–284], it need not be the case that $B = \hat{B}$. This is not unexpected, as applying the forgetful functor to B in order to construct \hat{B} involves the loss of information.

Chapter 2

Cohen rings

Let k be a field of positive characteristic p equipped with a p -basis $T : U \rightarrow k$, and let S be $\mathbb{Z}[U]$, the polynomial ring on U with integer coefficients. This makes k into an object of \mathbf{F} , the category of S -algebras which are fields. As T induces a basis of Ω_k , it follows that $\Omega_{k/S}$ is zero, so this situation meets the hypotheses of Theorem 1.1. This chapter will prove a key piece of Theorem 1.1 under these conditions.

Recall from Chapter 1 the category \mathbf{C} of complete local S -algebras with continuous morphisms and the residue field functor $Q : \mathbf{C} \rightarrow \mathbf{F}$. Let \mathbf{C}_k be the the “fiber” of Q over k . That is, an object of \mathbf{C}_k consists of an object A of \mathbf{C} equipped with an isomorphism $QA \cong k$. A morphism in \mathbf{C}_k is a morphism in \mathbf{C} whose image under Q makes a commutative triangle with the given isomorphisms with k . In practical terms, it is convenient to think of \mathbf{C}_k as the category of objects of \mathbf{C} whose residue field “is” k , and this abuse of language will sometimes be used. The functor $Q : \mathbf{C} \rightarrow \mathbf{F}$ obviously induces a functor $Q : \mathbf{C}_k \rightarrow \mathbf{F}$.

Now if Q_k is representable by an object C of \mathbf{C} , it is reasonable to expect that $QC \cong k$. In fact, this is proven in Chapter 3; for now, this expectation is purely motivational. Then choosing an isomorphism $QC \cong k$ makes C into an object of \mathbf{C}_k . Moreover, Theorem 1.1 implies that C is an initial object of \mathbf{C}_k , as all morphisms between two objects of \mathbf{C}_k have the same image under Q . For these reasons, constructing an initial object in \mathbf{C}_k will be the approach to proving Theorem 1.1 for k and S .

As alluded to in Section 1.1, for the above choice of S , the initial object of \mathbf{C}_k will be a Cohen ring, called a “Cohen S -algebra” for short. This chapter will prove the following result.

Theorem 2.1. *With k , S , and \mathbf{C}_k as above, a Cohen S -algebra $C(k)$ exists in \mathbf{C}_k . Moreover, any Cohen S -algebra $C(k)$ is an initial object of \mathbf{C}_k .*

Note that the category of local S -algebras is equivalent to the category of local rings A equipped with a lifted p -basis T_A , where a morphism $A \rightarrow B$ is required to carry T_A to T_B . This more concrete point of view will be taken.

2.1 Two categories

Since a Cohen S -algebra $C(k)$, if it exists, is a complete discrete valuation ring, it is the inverse limit of its quotients $C(k)/p^n C(k)$ for $n \in \mathbb{N}$. The strategy for constructing $C(k)$ will be to first construct $C(k)/p^n C(k)$ for each n , as these rings are Artinian and hence simpler.

Let \mathbf{N}_k be the subcategory of \mathbf{C}_k of discrete local rings with weakly nilpotent maximal ideal. To be completely explicit, an object of \mathbf{N}_k consists of the data of

- a local ring A with weakly nilpotent maximal ideal \mathfrak{m} ,
- a surjective homomorphism $\varphi : A \rightarrow k$,
- a lifted p -basis T_A of A .

The surjection φ induces the requisite isomorphism $QA \cong k$, and the lifted p -basis T_A induces the S -algebra structure. For convenience, the statement $A \in \mathbf{N}_k$ (or $(A, \mathfrak{m}) \in \mathbf{N}_k$) means that the triple (A, φ, T_A) is an object of \mathbf{N}_k .

As to the morphisms in \mathbf{N}_k , they are ring homomorphisms which respect the given structure. Explicitly, a morphism from (A, φ_A, T_A) to (B, φ_B, T_B) is a map $f : A \rightarrow B$ such that $\varphi_A = \varphi_B f$ and $fT_A = T_B$.

Note that if $C(k)$ is a Cohen S -algebra, then the quotients $C(k)/p^n C(k)$ are objects of \mathbf{N}_k . They have an additional notable property: their maximal ideals are generated by p . With that in mind, define the category \mathbf{P}_k to be the full subcategory of \mathbf{N}_k of objects (A, \mathfrak{m}) with $\mathfrak{m} = pA$.

Example 2.2. An object of \mathbf{P}_k .

Let T be a set, and let $k = \mathbb{F}_p(T)$ with the p -basis given by T . For any $n \in \mathbb{N}$, let $A = \mathbb{Z}[T]_{(p)}/(p^n)$ with the obvious surjection $A \rightarrow k$ and the lifted p -basis given by T . Then A is an object of \mathbf{P}_k .

2.2 Two subrings

It would be possible to construct $C(k)$ directly from \mathbf{P}_k , if \mathbf{P}_k were known to have sufficiently many objects. However, directly constructing members of \mathbf{P}_k is some trouble. Instead, a way to pass from \mathbf{N}_k to \mathbf{P}_k will be developed, and then members of \mathbf{N}_k will be constructed.

To begin, let $A \in \mathbf{N}_k$ and consider two ways of passing to a subring of A . First, let $E(A) = A^{[p]} + pA$.

Lemma 2.3. *For a ring A , the subset $E(A) = A^{[p]} + pA$ is in fact a ring, namely the subring generated by $A^{[p]}$ and pA .*

Proof. Recall that in characteristic p , taking p -th powers is a ring homomorphism. Let $\bar{A} = A/pA$; then $\bar{A}^{[p]}$ is a subring of \bar{A} . As $E(A)$ is the preimage of $\bar{A}^{[p]}$ under the residue map $A \rightarrow \bar{A}$, it follows that $E(A)$ is a ring. \square

Note, however, that $E(A)$ is not an object of \mathbf{N}_k when k is imperfect, because the residue field of $E(A)$ is k^p . To enlarge the subring $E(A)$, let $F(A) = E(A)[T_A]$, regarding T_A as a subset of A .

Lemma 2.4. *For $A \in \mathbf{N}_k$, the object $(F(A), \varphi|_{F(A)}, T_A)$ is again in \mathbf{N}_k .*

Proof. First, T_A is contained in $F(A)$ by definition, and certainly T_A is a lifted p -basis for $F(A)$.

Second, the image of $F(A)$ under φ is all of k , as follows. By definition, $F(A)$ is the smallest subring of A containing $E(A)$ and T_A . Then $\varphi(F(A))$ is the smallest subring of k containing $\varphi(E(A))$ and $\varphi(T_A)$. But $\varphi(E(A))$ is just k^p , and $\varphi(T_A)$ is just T . So $\varphi(F(A))$ equals $k^p[T]$, which is k .

Lastly, if \mathfrak{m} is the kernel of φ , then $\mathfrak{m} \cap F(A)$ is the kernel of $\varphi|_{F(A)}$. Since $(\mathfrak{m} \cap F(A))^{(n)} \subseteq \mathfrak{m}^{(n)}$ for any $n \in \mathbb{N}$, the weak nilpotency of \mathfrak{m} implies the weak nilpotency of $\mathfrak{m} \cap F(A)$. \square

Corollary 2.5. *If $A \in \mathbf{P}_k$, then $F(A)$ equals A .*

Proof. The residue field map $A \rightarrow k$ maps $F(A)$ surjectively onto k by Lemma 2.4. This implies $A = F(A) + pA$, as pA is the maximal ideal of A . However, pA is contained in $F(A)$, so A equals $F(A)$. \square

The lemma and corollary show that F is an operation from \mathbf{N}_k to itself which fixes \mathbf{P}_k . Moreover, F is functorial since it is defined only in terms of addition and multiplication, without choices. That is, if $f : A \rightarrow B$ is a morphism in \mathbf{N}_k , then $f(F(A))$ is contained in $F(B)$ and $f|_{F(A)}$ is again a morphism in \mathbf{N}_k . Furthermore, F preserves both injections and surjections, as may be seen by inspection.

2.3 Properties of the subring $F(A)$

The ring $F(A)$ is closer to being to an object of \mathbf{P}_k , in that the maximal ideal of $F(A)$ is closer to being the principal ideal generated by p . The following lemma makes this statement precise.

For an A -ideal \mathfrak{J} , define $g(\mathfrak{J})$ to be the A -ideal $\mathfrak{J}^{(p)} + p\mathfrak{J}$.

Lemma 2.6. *Let $(A, \mathfrak{m}) \in \mathbf{N}_k$, and suppose $\mathfrak{m} \subseteq pA + \mathfrak{J}$ for an ideal \mathfrak{J} of A . Then it follows that $\mathfrak{m} \cap F(A) \subseteq pF(A) + (g(\mathfrak{J}) \cap F(A))$.*

Proof. Recall that $F(A) = E(A)[T_A]$. It will be fruitful to work modulo pA , so let a $\bar{\cdot} : A \rightarrow A/pA$ be the natural map. Note that $\bar{A} = A/pA$ equipped with $T_{\bar{A}} = \overline{T_A}$ is again an object of \mathbf{N}_k , and that the operations E and F commute with $\bar{\cdot}$. Also note that the hypothesis on \mathfrak{m} implies that $\bar{\mathfrak{m}} \subseteq \bar{\mathfrak{J}}$.

An arbitrary element a of $E(\bar{A})[T_{\bar{A}}]$ may be written as a sum of products of elements of $E(\bar{A})$ and $T_{\bar{A}}$. However, since $T_{\bar{A}}^{[p]} \subseteq E(\bar{A})$, each product has the simple form am , where $a \in E(\bar{A})$ and $m \in \Pi_p(T_{\bar{A}})$. Noting that $E(\bar{A}) = \bar{A}^{[p]}$ gives that a can be written as $a = \sum_{m \in \Pi_p(T_{\bar{A}})} a_m^p m$, where $a_m \in \bar{A}$ and $a_m = 0$ for all but finitely many m .

Then $a \in \bar{\mathfrak{m}}$ if and only if the image of a in k is 0. Since the image of $\Pi_p(T_{\bar{A}})$ in k is a basis of k over k^p , it follows that $a \in \bar{\mathfrak{m}}$ if and only if $a_m^p \in \bar{\mathfrak{m}}$ for all m . Also, $\bar{\mathfrak{m}}$ is a prime ideal, so equivalently $a \in \bar{\mathfrak{m}}$ if and only if $a_m \in \bar{\mathfrak{m}}$ for all m ; that is, $\bar{\mathfrak{m}} \cap F(\bar{A}) \subseteq \bar{\mathfrak{m}}^{(p)}$. Moreover, as $\bar{\mathfrak{m}} \subseteq \bar{\mathfrak{J}}$, it follows that $\bar{\mathfrak{m}} \cap F(\bar{A}) \subseteq \bar{\mathfrak{J}}^{(p)}$.

Now lift this result back to the ring A . The preimage of $\bar{\mathfrak{m}} \cap F(\bar{A})$ is just $\mathfrak{m} \cap F(A)$, as $pA \subseteq \mathfrak{m} \cap F(A)$; the preimage of $\bar{\mathfrak{J}}^{(p)}$ is $\mathfrak{J}^{(p)} + pA$. Thus, lifting gives that $\mathfrak{m} \cap F(A) \subseteq \mathfrak{J}^{(p)} + pA$.

To finish, note that $A = F(A) + \mathfrak{m}$, since the rings A and $F(A)$ coincide modulo \mathfrak{m} . This equality and the facts $\mathfrak{m} \subseteq pA + \mathfrak{J}$ and $pA \subseteq F(A)$ imply that $A \subseteq F(A) + \mathfrak{J}$. Substituting this last inequality for A in the statement $\mathfrak{m} \cap F(A) \subseteq \mathfrak{J}^{(p)} + pA$ shows that $\mathfrak{m} \cap F(A) \subseteq pF(A) + g(\mathfrak{J})$. Finally, taking the intersection with $F(A)$ gives that $\mathfrak{m} \cap F(A) \subseteq pF(A) + (g(\mathfrak{J}) \cap F(A))$, the desired result. \square

Example 2.7. An object B of \mathbf{N}_k for which B is not in \mathbf{P}_k but $F(B)$ is in \mathbf{P}_k .

Let A be an object of \mathbf{P}_k , for instance as in Example 2.2. Let M be an A module which is killed by p , for example $M = A/pA$. Let $B = A \oplus M$ with the ring structure $(a_1, m_1) \cdot (a_2, m_2) = (a_1 a_2, a_1 m_2 + a_2 m_1)$. Then B is local with maximal ideal $\mathfrak{n} = pA \oplus M$ and residue field k . Consider A as a subset of B via the map $a \mapsto (a, 0)$. For an element (a, m) of B , note that $(a, m)^p = (a^p, pa^{p-1}m) = a^p$. This shows that the weak nilpotency of \mathfrak{m} implies the weak nilpotency of \mathfrak{n} . Lastly, B inherits a lifted p -basis T_B from A , so B is an object of \mathbf{N}_k . Note that B is not in \mathbf{P}_k as \mathfrak{n} is not equal to pB .

As observed, $B^{[p]}$ is a subset of A , and by construction pB equals pA . Since T_B has image in A , it follows that $F(B)$ is contained in A . On the other hand, Corollary 2.5 indicates that $F(A) = A$. Since $F(B)$ contains $F(A)$, it follows that $F(B) = A$.

2.4 Iterates of F

Next consider $F^i(A)$, the i -fold iterate of the functor F on A . Evidently $F^i(A)$ is a subring of A and an object of \mathbf{N}_k , and the maximal ideal of $F^i(A)$ is $\mathfrak{m} \cap F^i(A)$.

Corollary 2.8. For $(A, \mathfrak{m}) \in \mathbf{N}_k$ and $n \in \mathbb{N}$, the maximal ideal $\mathfrak{m} \cap F^n(A)$ of the ring $F^n(A)$ is contained in $pF^n(A) + (g^n(\mathfrak{m}) \cap F^n(A))$.

Proof. For a subring B of A , let g_B denote the operation g on B -ideals. Then for an A -ideal \mathfrak{J} , note that $g_B(\mathfrak{J} \cap B) \subseteq g_A(\mathfrak{J})$. The result therefore follows from induction on Lemma 2.6, where $\mathfrak{J} = \mathfrak{m}$ initially. \square

It is obvious that $g(\mathfrak{m}^n) \subseteq \mathfrak{m}^{n+1}$ for positive n , so if \mathfrak{m} is nilpotent, it is immediate that $g^N(\mathfrak{m}) = 0$ for some $N \in \mathbb{N}$. However, this still holds with only the hypothesis that \mathfrak{m} is weakly nilpotent.

Lemma 2.9. *For $(A, \mathfrak{m}) \in \mathbf{N}_k$, there exists an $N \in \mathbb{N}$ such that $g^N(\mathfrak{m}) = 0$.*

Proof. It will again be convenient to work in A/pA , so let $\bar{} : A \rightarrow A/pA$ be the natural map. Recall that $\bar{A} \in \mathbf{N}_k$, and note that g commutes with $\bar{}$.

In \bar{A} the operation g is just $g(\mathfrak{J}) = \mathfrak{J}^{(p)}$. Moreover, taking p -th powers is a ring homomorphism in \bar{A} , so it follows that $(\mathfrak{J}^{(p^n)})^{(p)} = \mathfrak{J}^{(p^{n+1})}$, and thus $g^n(\mathfrak{J}) = \mathfrak{J}^{(p^n)}$. Therefore, as $\bar{\mathfrak{m}}$ is weakly nilpotent, there exists an $N_1 \in \mathbb{N}$ with $g^{N_1}(\bar{\mathfrak{m}}) = 0$.

Lifting this back to A gives that $g^{N_1}(\mathfrak{m}) \subseteq pA$. For a principal ideal $\mathfrak{J} = aA$, note that $\mathfrak{J}^{(p)} = a^pA$. This shows that $g(p^nA) = p^{n+1}A$ for all positive $n \in \mathbb{N}$, and it follows by induction that $g^n(pA) = p^{n+1}A$ for $n \in \mathbb{N}$. As $p \in \mathfrak{m}$ and \mathfrak{m} is weakly nilpotent, there exists $N_2 \in \mathbb{N}$ such that $p^{N_2} = 0$. Take $N = N_1 + N_2 - 1$ and observe that $g^N(\mathfrak{m}) = 0$, as desired. \square

Corollary 2.10. *For $(A, \mathfrak{m}) \in \mathbf{N}_k$, there exists an $N \in \mathbb{N}$ such that $F^N(A) \in \mathbf{P}_k$.*

Proof. By Lemma 2.9, there exists an $N \in \mathbb{N}$ such that $g^N(\mathfrak{m}) = 0$. Then Corollary 2.8 indicates that $\mathfrak{m} \cap F^N(A)$, the maximal ideal of $F^N(A)$, is contained in $pF^N(A)$. But $p \in \mathfrak{m} \cap F^N(A)$, so it follows that $\mathfrak{m} \cap F^N(A) = pF^N(A)$. Then by definition $F^N(A)$ is in \mathbf{P}_k . \square

Example 2.11. For any $n \in \mathbb{N}$, an object B of \mathbf{N}_k for which $F^n(B)$ is not in \mathbf{P}_k but $F^{n+1}(B)$ is in \mathbf{P}_k .

Again let A be an object of \mathbf{P}_k and let M be an A -module killed by p . For k in \mathbb{N} , let S^kM denote the k -th symmetric power of M , the quotient of $M^{\otimes k}$ by the standard action of the symmetric group S_k . Note that $S^0M = A$. Then let $B = \bigoplus_{i=0}^{p^n} S^iM$, equipped with multiplication given by the tensor product and module multiplication maps $S^jM \times S^kM \rightarrow S^{j+k}M$. Note that B is a ring containing A as a subring, that B is local with maximal ideal $\mathfrak{n} = pA \oplus \bigoplus_{i=1}^{p^n} S^iM$ which is weakly nilpotent, and that B inherits a lifted p -basis from A . Thus B is an object of \mathbf{N}_k .

Let D be any subring of B containing A , with lifted p -basis $T_D = T_A$, and calculate $F(D)$ as follows. Corollary 2.5 indicates that $F(A) = A$, and $F(D)$ contains $F(A)$, so $F(D)$ contains A . Therefore $F(D)$ is the subring of D generated by A , $D^{[p]}$, pD , and T_D . But pD equals pA and T_D is contained in A , so this reduces to $F(D) = A[D^{[p]}]$.

Since multiplication in B respects the grading, it follows by induction that

$$F^j(B) = A \oplus \bigoplus_{i=1}^{p^{n-j}} (S^iM)^{[p^j]}$$

where $(S^i M)^{[p^j]}$ sits in degree ip^j . In particular, $F^n(B)$ equals $A \oplus M^{[p^n]}$ and has maximal ideal $pA \oplus M^{[p^n]}$, which is not generated by p . However, $F^{n+1}(B)$ equals A .

2.5 Projection onto \mathbf{P}_k

The functor F characterizes \mathbf{P}_k in the following sense.

Lemma 2.12. *A ring $A \in \mathbf{N}_k$ is in \mathbf{P}_k if and only if $F(A) = A$.*

Proof. If $A \in \mathbf{P}_k$, then Corollary 2.5 states that $F(A) = A$. Suppose conversely that $F(A) = A$. By Corollary 2.10, there exists an $N \in \mathbb{N}$ such that $F^N(A) \in \mathbf{P}_k$. But $F(A) = A$ implies that $F^N(A) = A$, so A is in fact in \mathbf{P}_k . \square

Rather than dealing with the iterates of F directly, it will be convenient to simply consider a “projection” functor from \mathbf{N}_k to \mathbf{P}_k .

Theorem 2.13. *The limit of the iterates F^i is a functor $G : \mathbf{N}_k \rightarrow \mathbf{P}_k$, which preserves injections and surjections and is a “projection”. That is, if I is the inclusion functor from $\mathbf{P}_k \rightarrow \mathbf{N}_k$, then GI is the identity functor on \mathbf{P}_k . Moreover, G is right adjoint to I .*

Proof. First note that for any ring $A \in \mathbf{N}_k$, by Corollary 2.10 there is some $N \in \mathbb{N}$ for which $F^N(A) \in \mathbf{P}_k$, and then by Lemma 2.12, it follows that $F^i(A) = F^N(A)$ for all $i \geq N$. Thus the limit of the $F^i(A)$ is just $F^N(A)$, so define $G(A) = F^N(A)$. Moreover, for any finite collection of objects of \mathbf{N}_k there is some single $N \in \mathbb{N}$ for which $G = F^N$ on those objects. This defines G on morphisms and shows that G is a functor. And since F preserves injections and surjections, G does as well.

In the language of the current lemma, Lemma 2.12 states that $FI = I$. It follows that GI is the identity functor on \mathbf{P}_k .

For the adjointness, it is necessary to give, for any object $A \in \mathbf{P}_k$ and $B \in \mathbf{N}_k$, a natural isomorphism between $\text{Hom}_{\mathbf{N}_k}(IA, B)$ and $\text{Hom}_{\mathbf{P}_k}(A, GB)$. Note that G gives a map from $\text{Hom}_{\mathbf{N}_k}(IA, B)$ to $\text{Hom}_{\mathbf{P}_k}(GIA, GB)$, and since GI is the identity on \mathbf{P}_k , this is the desired map. The map is surjective, as for any morphism $\psi : A \rightarrow GB$, and for $i : GB \rightarrow B$ the natural inclusion, it holds that $G(i\psi) = \psi$. And the map is injective as the functor G on morphisms is restriction to a subring, but as GI is the identity on \mathbf{P}_k , in the case of the object IA , this restriction operation is trivial. \square

2.6 The structure of \mathbf{P}_k

The functor G will be useful in elucidating the structure of the category \mathbf{P}_k . This category is highly constrained, as this section will demonstrate.

Lemma 2.14. *Let $A \in \mathbf{P}_k$ and $B \in \mathbf{N}_k$. If $f : B \rightarrow A$ is an injective map in \mathbf{N}_k , then it is surjective.*

Proof. As $A \in \mathbf{P}_k$, the maximal ideal of A is pA . Identify B with its image in A ; then as the residue fields of A and B coincide, A equals $B + pA$. Since $p^n B \subseteq B$, this gives by induction that $A = B + p^n A$ for all $n \in \mathbb{N}$. But as pA is weakly nilpotent, p^n equals 0 for some $n \in \mathbb{N}$, which gives that $A = B$. \square

Corollary 2.15. *If $A \in \mathbf{N}_k$ and $B \subseteq A$ with $B \in \mathbf{P}_k$, then B equals $G(A)$.*

Proof. Theorem 2.13 shows that $G(B) \subseteq G(A)$, as G preserves inclusions, and that $G(B) = B$. Since $G(A) \in \mathbf{P}_k$, Lemma 2.14 shows that B equals $G(A)$. \square

Note that for $(A, \mathfrak{m}) \in \mathbf{N}_k$, the characteristic of A is a positive power of p : the characteristic is positive, as \mathfrak{m} is weakly nilpotent, and any prime different from p does not divide the characteristic, as such a prime is invertible in k .

Lemma 2.16. *For A in \mathbf{P}_k , every ideal of A is generated by a power of p .*

Proof. Let $\text{char } A = p^n$, where $n \in \mathbb{N}$. It suffices to show that any non-zero element $a \in A$ has the form $p^i u$, where $0 \leq i < n$ and u is a unit in A . So let $a \in A$ with $a \neq 0$. As $p^n = 0$, the element a is not in $p^n A$. Since $a \in p^0 A$, there is a maximal $i \in \mathbb{N}$ such that $a \in p^i A$. Then $a = p^i x$ for $x \in A$. But x is not an element of pA , as if it were, a would be an element of $p^{i+1} A$, contradicting the maximality of i . Thus x is a unit, as desired. \square

In fact, char characterizes objects of \mathbf{P}_k .

Lemma 2.17. *Let $f : A \rightarrow B$ be a morphism in \mathbf{P}_k . If $\text{char } A = \text{char } B$, then f is an isomorphism.*

Proof. Let $\text{char } A = p^n$. The kernel of f is $p^i A$ for some $i \in \mathbb{N}$ with $i \leq n$, by Lemma 2.16. But $p^i = 0$ in B and $\text{char } B = p^n$, so i is at least n . Thus $i = n$ and f is injective. Then by Lemma 2.14, f is an isomorphism. \square

Moreover, any two objects of \mathbf{P}_k are “comparable”, in that there is a morphism between them. This will be shown using products in \mathbf{N}_k .

Lemma 2.18. *If (A, \mathfrak{m}_A) and (B, \mathfrak{m}_B) are objects in \mathbf{N}_k , then the ring theoretic fiber product $C = A \times_k B$ has a natural \mathbf{N}_k -structure for which it is the product of A and B in \mathbf{N}_k .*

Proof. Let φ_A and φ_B be the specified surjections $A \rightarrow k$ and $B \rightarrow k$, respectively. Recall that $C = A \times_k B$ is the subring of $A \times B$ consisting of elements (a, b) such that $\varphi_A(a) = \varphi_B(b)$. Thus if π_1 and π_2 are the two projections from $A \times B$, the two maps $\varphi_A \pi_1$ and $\varphi_B \pi_2$ coincide, and this defines a map $\varphi_C : C \rightarrow k$. This map is surjective because both φ_A and φ_B are, so the kernel \mathfrak{m}_C is a maximal ideal.

Let $T_C : U \rightarrow A \times B$ be the map $T_A \times T_B$. The image of T_C lies in C as $\varphi_A T_A = \varphi_B T_B = T$. This also shows that $\varphi_C T_C = T$, so T_C is a lifted p -basis.

To show that $C \in \mathbf{N}_k$ it remains only to verify that \mathfrak{m}_C is weakly nilpotent. Note that \mathfrak{m}_C is a subset of $\mathfrak{m}_A \times \mathfrak{m}_B$. If $\mathfrak{m}_A^{(n)} = 0$ and $\mathfrak{m}_B^{(m)} = 0$, set $N = \max(n, m)$. Then as multiplication in $A \times B$ is component-wise, $(\mathfrak{m}_A \times \mathfrak{m}_B)^{(N)}$ is zero, and \mathfrak{m}_C is weakly nilpotent.

Lastly, since morphisms in \mathbf{N}_k are required to commute with the specified surjections to k , the fact that C is the fibered product in the category of rings is precisely the property required for C to be the product in \mathbf{N}_k . \square

Now it is possible to show that taking the characteristic defines a faithful functor from \mathbf{P}_k to the category associated to the ordered set of positive integers.

Theorem 2.19. *For two objects (A, \mathfrak{m}_A) and (B, \mathfrak{m}_B) of \mathbf{P}_k , the cardinality of the set $\text{Hom}_{\mathbf{P}_k}(A, B)$ is 1 if $\text{char } A \geq \text{char } B$ and 0 otherwise.*

Proof. Let $\text{char } A = p^n$ and $\text{char } B = p^m$. Obviously if $\text{char } A < \text{char } B$, there are no maps from A to B . When $\text{char } A > \text{char } B$, any map $f : A \rightarrow B$ would have kernel containing $p^m A$ and therefore factor through the natural map $A \rightarrow A/p^m A$. So it suffices to consider the case that $\text{char } A = \text{char } B$ and show that $\text{Hom}_{\mathbf{P}_k}(A, B)$ has a unique element.

Let $A \times_k B$ be the product of A and B in \mathbf{N}_k , and let $D = G(A \times_k B)$. Then Theorem 2.13 shows that $D \in \mathbf{P}_k$, and that D has natural surjections $\pi_1 : D \rightarrow A$ and $\pi_2 : D \rightarrow B$. Moreover, D also has characteristic p^n by construction, so by Lemma 2.17, the maps π_1 and π_2 are isomorphisms. Thus $\pi_2 \pi_1^{-1}$ is a map from A to B , so the cardinality of $\text{Hom}_{\mathbf{P}_k}(A, B)$ is at least 1.

Lastly, let $f : A \rightarrow B$ be any map. The map f is determined by its graph Γ , the subring of $A \times_k B$ given by $\{(a, b) \mid b = f(a)\}$. The lifted p -basis $T_{A \times_k B}$ has image in Γ , since $f T_A$ equals T_B , so set $T_\Gamma = T_{A \times_k B}$. This makes Γ into an object of \mathbf{N}_k . Note that $\pi_1 : \Gamma \rightarrow A$ is an isomorphism, so moreover Γ is in \mathbf{P}_k . However, by Corollary 2.15, the \mathbf{N}_k -object $A \times_k B$ has a unique \mathbf{P}_k -subobject, so there is a unique map $f : A \rightarrow B$. \square

2.7 Populating the categories

At this point, the only remaining obstacle to constructing a Cohen S -algebra $C(k)$ is the possibility that the categories \mathbf{N}_k and \mathbf{P}_k have too few objects. The following lemma will allow the construction of sufficient objects.

Lemma 2.20. *Let X be a set, and let $\mathbb{Z}[X]$ denote the polynomial ring on X . If $\mathfrak{J} \subseteq \mathbb{Z}[X]$ is an ideal such that $\mathfrak{J} \cap \mathbb{Z} = p\mathbb{Z}$, then $\mathfrak{J}^n \cap \mathbb{Z}$ equals $p^n \mathbb{Z}$ for all $n \in \mathbb{N}$.*

Proof. Note that $p^n \in \mathfrak{J}^n$, so it suffices to show that $p^{n-1} \notin \mathfrak{J}^n$.

First consider the case that X is finite and \mathfrak{J} is maximal. Then $\mathbb{Z}[X]/\mathfrak{J}$ is a finite field [1, Corollary 5.24, p. 67]. Therefore there exists a monic polynomial $f \in \mathbb{Z}[t]$

of positive degree such that $\mathbb{Z}[X]/\mathfrak{J}$ is isomorphic to $\mathbb{Z}[t]/(p, f)$. Set $A = \mathbb{Z}[t]/(f)$, so $\mathbb{Z}[X]/\mathfrak{J}$ is isomorphic to A/pA . The induced morphism $\mathbb{Z}[X] \rightarrow A/pA$ may be lifted to a morphism $\varphi : \mathbb{Z}[X] \rightarrow A$, since $\mathbb{Z}[X]$ is a polynomial ring. It follows that $\varphi(\mathfrak{J}) \subseteq pA$.

Because f is monic of positive degree, A is a \mathbb{Z} module of finite rank. This implies that $(p^n A) \cap \mathbb{Z} = p^n \mathbb{Z}$ and therefore $p^{n-1} \notin p^n A$. The image $\varphi(\mathfrak{J}^n)$ is contained in $p^n A$, so p^{n-1} is not in $\varphi(\mathfrak{J}^n)$ and therefore p^{n-1} is not in \mathfrak{J}^n .

Next consider the case that X is finite and \mathfrak{J} is arbitrary. Then there exists a maximal ideal \mathfrak{m} of $\mathbb{Z}[X]$ which contains \mathfrak{m} . Now $\mathfrak{m} \cap \mathbb{Z}$ contains $p\mathbb{Z}$, and as 1 is not an element of \mathfrak{m} , it follows that $\mathfrak{m} \cap \mathbb{Z} = p\mathbb{Z}$. Then by the previous case, p^{n-1} is not in \mathfrak{m}^n . But \mathfrak{J}^n is a subset of \mathfrak{m}^n , so indeed p^{n-1} is not in \mathfrak{J}^n .

Lastly, allow X to be arbitrary, and suppose $p^{n-1} \in \mathfrak{J}^n$. Then p^{n-1} has an expression as a finite linear combination of n -fold products of elements of \mathfrak{J} . That is, if X_0 is the set of elements of X which appear in this expression, X_0 is finite. It follows that $p^{n-1} \in (\mathfrak{J} \cap \mathbb{Z}[X_0])^n$. This, however, contradicts the previous case for the ring $\mathbb{Z}[X_0]$, so $p^{n-1} \notin \mathfrak{J}^n$. \square

Corollary 2.21. *For any field k of positive characteristic p and any positive $n \in \mathbb{N}$, there exist objects of \mathbf{N}_k and \mathbf{P}_k of characteristic p^n .*

Proof. In Lemma 2.20, take $X = k$, and take \mathfrak{J} to be the kernel of the natural map from $\mathbb{Z}[X]$ to k . As $\text{char } k = p$, it is clear that $\mathfrak{J} \cap \mathbb{Z} = p\mathbb{Z}$, so Lemma 2.20 indicates that $\mathfrak{J}^n \cap \mathbb{Z} = p^n \mathbb{Z}$. In other words, if $A = \mathbb{Z}[X]/\mathfrak{J}^n$, then A has characteristic p^n . The ring A is also equipped with a natural surjection onto k , and the choice of $T_A = T$, via the inclusion of X into A , is a lifted p -basis. As the maximal ideal of A is $\mathfrak{J}/\mathfrak{J}^n$, it is clearly weakly nilpotent. Thus A is an object of \mathbf{N}_k of characteristic p^n , and then $G(A)$ is an object of \mathbf{P}_k of characteristic p^n . \square

Corollary 2.21 shows that \mathbf{P}_k is, in fact, equivalent to the category associated to the ordered set of positive integers.

2.8 The construction

It is now possible to give the proof of Theorem 2.1.

Proof. For each positive $n \in \mathbb{N}$, let C_n be an object of \mathbf{P}_k of characteristic p^n , whose existence was shown in Corollary 2.21. Theorem 2.19 shows that these objects are unique up to unique isomorphism and form a projective system in only one way. Define the ring $C(k)$ as $\text{projlim}_{n \rightarrow \infty} C_n$. Note the transition maps in this projective system are surjective because the map $C_n \rightarrow C_n/p^{n-1}C_n$ is surjective, and $C_n/p^{n-1}C_n$ is isomorphic to C_{n-1} .

Observe that $C(k)$ is a Cohen ring as follows. The system of maps $T_{C_n} : U \rightarrow C_n$ is compatible, so it yields a map $T_{C(k)} : U \rightarrow C(k)$. Since the limit defining $C(k)$ is

countable with surjective transition maps, it is clear that $C(k)$ comes with a surjective structure map φ to k , and that $T_{C(k)}$ is a lifted p -basis. It is also clear that $C(k)$ is local with maximal ideal $\mathfrak{m} = \ker \varphi$: any $x \notin \mathfrak{m}$ has image $x_n \in C_n$ which is a unit; as x_n has a unique inverse in C_n , the x_n^{-1} define an inverse $x^{-1} \in C(k)$.

The maximal ideal \mathfrak{m} of $C(k)$ is generated by p : note that for any $n \in \mathbb{N}$, multiplication by p defines an isomorphism of additive groups from C_n to pC_{n+1} . Since pC_{n+1} is the maximal ideal of C_{n+1} , the limit of the pC_{n+1} is just \mathfrak{m} . Then taking the limit of the system of isomorphisms gives that multiplication by p is an isomorphism from $C(k)$ to \mathfrak{m} , that is, that $\mathfrak{m} = pC(k)$.

To show that $C(k)$ is a discrete valuation ring, it suffices to show that any non-zero ideal \mathfrak{J} of $C(k)$ is generated by p^n for some n . In the rings C_n , every ideal is generated by a power of p , by Lemma 2.16. Note that if $p^n \notin \mathfrak{J}$ for all $n \in \mathbb{N}$, then the image of \mathfrak{J} in C_n is 0 for all $n \in \mathbb{N}$, so that \mathfrak{J} is zero. So let n be the smallest element of \mathbb{N} such that $p^n \in \mathfrak{J}$. Now $C(k)/p^n C(k)$ is in \mathbf{P}_k , so $C(k)/p^n C(k)$ is isomorphic to C_n . Then $\mathfrak{J}/p^n C(k)$ is an ideal of C_n , which can only be the zero ideal, as $p^m \notin \mathfrak{J}$ for $m < n$. That is, \mathfrak{J} equals $p^n C(k)$.

This shows the existence of a Cohen S -algebra $C(k)$ in \mathbf{C}_k . To show that $C(k)$ is initial, first consider the case that (A, \mathfrak{m}) is an object of \mathbf{N}_k . Then the characteristic of A is p^n for some $n \in \mathbb{N}$, and therefore any ring map $C(k) \rightarrow A$ factors through $C(k)/p^n C(k)$, which is isomorphic to C_n . So it suffices to show that there is a unique continuous local map from C_n to A .

Note that any map from C_n to A must be injective, as C_n and A have the same characteristic, and every ideal of C_n is generated by an integer by Lemma 2.16. Then the image of such a map is in \mathbf{P}_k , and by Corollary 2.15, the image must be $G(A)$. Lastly, Theorem 2.19 shows that there is a unique map from C_n to $G(A)$. Such a map is continuous since both C_n and A are discrete.

This completes the argument when A is in \mathbf{N}_k . For general $A \in \mathbf{C}_k$, since A is complete, it is the inverse limit of discrete local rings (A_i, \mathfrak{m}_i) with A_i in \mathbf{N}_k . Then giving a morphism $C(k) \rightarrow A$ is equivalent to giving a compatible system of morphisms $C(k) \rightarrow A_i$. As there is a unique morphism $C(k) \rightarrow A_i$ for each i , there is a unique system of morphisms, which must be compatible. Hence there is a unique morphism $C(k) \rightarrow A$, as desired.

This shows that $C(k)$ is an initial object of \mathbf{C}_k . To see that any Cohen ring D in \mathbf{C}_k is initial, note that the quotient $D_n = D/p^n D$ is an object of \mathbf{P}_k for any positive $n \in \mathbb{N}$. Therefore D_n is isomorphic to C_n by Theorem 2.19. Since D is isomorphic to $\text{projlim}_n D_n$, this shows that D is isomorphic to $C(k)$, and hence D is initial. \square

Example 2.22. A Cohen S -algebra.

Let T be a set, and let $k = \mathbb{F}_p(T)$ with the p -basis given by T . From Example 2.2, the ring $\mathbb{Z}[T]_{(p)}/(p^n)$, with lifted p -basis given by T , lies in \mathbf{P}_k and has characteristic p^n . Thus $C(k)$ is the completion of $\mathbb{Z}[T]_{(p)}$ with the lifted p -basis given by T .

Chapter 3

Main theorem

Most of the hard work of proving Theorem 1.1 has already gone into the proof of Theorem 2.1. All that is now required is a characteristic 0 analogue to Theorem 2.1 and some differential theory and category theory.

3.1 Characteristic 0

Let k be a field of characteristic 0, let $T : U \rightarrow k$ be a transcendence basis of k over \mathbb{Q} , and let $S = \mathbb{Z}[U]$. The categories \mathbf{C} and \mathbf{F} are the usual categories of S -algebras, and the transcendence basis T makes k into an object of \mathbf{F} . Again, let \mathbf{C}_k be the fiber of Q at k . Under these conditions, the following theorem analogous to Theorem 2.1 holds.

Theorem 3.1. *With k , S , and \mathbf{C}_k as above, k is an initial object in \mathbf{C}_k .*

Proof. The field k is made into an object of \mathbf{C}_k by equipping it with the identity map $k \rightarrow k$. Let A be an object of \mathbf{C}_k . It will be convenient to identify QA with k via the specified isomorphism $QA \cong k$. Then a morphism $k \rightarrow A$ in \mathbf{C}_k is simply a morphism in \mathbf{C} whose image under Q is the identity on k .

Note that k is an algebraic extension of $\mathbb{Q}(U)$ since T is a transcendence basis. The theorem states that there is a unique map $k \rightarrow A$ in \mathbf{C} whose image under Q is id_k . This will be shown by proving an analogous result for any intermediate field l with $\mathbb{Q}(U) \subseteq l \subseteq k$, namely that there is a unique map $l \rightarrow A$ in \mathbf{C} whose image under Q is the inclusion $l \rightarrow k$. Obviously when $l = k$, this is the theorem.

Any non-zero element of $\mathbb{Z}[U]$ has an invertible image in A , since its image in k is invertible. This shows that the $\mathbb{Z}[U]$ -algebra structure on A induces a unique $\mathbb{Q}(U)$ -algebra structure. In particular, the result holds for $l = \mathbb{Q}(U)$.

Now suppose l is monogenic over $\mathbb{Q}(U)$, that is, that $l = \mathbb{Q}(U)[\alpha]$ for some $\alpha \in l$. First consider the case that A is discrete with weakly nilpotent maximal ideal \mathfrak{m} . There exists a minimal $n \in \mathbb{N}$ such that $\mathfrak{m}^{(n)} = 0$; proceed by induction on n . If n

equals 1, then \mathfrak{m} equals 0 and $A = k$, and obviously the inclusion $l \rightarrow k$ is the unique map $l \rightarrow A$ lying over the inclusion $l \rightarrow k$. Now assume that $n > 1$ and the result holds for any discrete ring (A', \mathfrak{n}) in \mathbf{C}_k with $\mathfrak{n}^{(n-1)} = 0$. Let $\mathfrak{J} = \mathfrak{m}^{(n-1)}$ and consider the ring $B = A/\mathfrak{J}$. As this ring meets the induction hypothesis, there is a unique map $l \rightarrow B$ lying over the map $l \rightarrow k$. It remains to show this map $l \rightarrow B$ extends uniquely to a map $l \rightarrow A$.

In A , the ideal \mathfrak{J} satisfies $\mathfrak{J}^{(2)} = 0$, as $2(n-1) \geq n$. Let $f \in \mathbb{Q}(U)[t]$ be the minimal polynomial of α over $\mathbb{Q}(U)$. Note that $f'(\alpha) \neq 0$ as l over $\mathbb{Q}(U)$ is a separable extension. Let V be the set of preimages in A of the image of α in B , and let β be an element of V . Since V is an \mathfrak{J} -coset, V equals $\beta + \mathfrak{J}$.

Let $i \in \mathfrak{J}$ and calculate $f(\beta+i)$ by Taylor's formula: $f(\beta+i) = f(\beta) + f'(\beta)i + \gamma i^2$ for some $\gamma \in A$. But as $i^2 = 0$, this reduces to $f(\beta+i) = f(\beta) + f'(\beta)i$. Now the image in l of $f'(\beta)$ is just $f'(\alpha)$, which is non-zero. Hence $f'(\beta)$ is invertible in A . So $f(\beta+i) = 0$ if and only if $i = -f(\beta)/f'(\beta)$. Note that $f(\beta)$ is in \mathfrak{J} , as the image of β in B is a root of f in B .

Thus, f has a unique root in A lying over the image of α in B , so there is a unique extension of the structure map $\mathbb{Q}(U) \rightarrow A$ to a map $l \rightarrow A$ lying over the inclusion $l \rightarrow k$. By induction, this proves the result for l when A is discrete and \mathfrak{m} is weakly nilpotent.

Now consider the case of arbitrary A . Since A is complete, A is the inverse limit of a system of discrete rings (A_i, \mathfrak{m}_i, k) with \mathfrak{m}_i weakly nilpotent. Thus giving a map to A is equivalent to giving a compatible system of maps to the A_i . By the previous case, for each i there is a unique map $l \rightarrow A_i$ lying over the inclusion $l \rightarrow k$. These maps are compatible as they are unique. Therefore, there is a unique map $l \rightarrow A$ lying over the inclusion $l \rightarrow k$, and the result holds for l .

Lastly, as k over $\mathbb{Q}(U)$ is algebraic, k is the direct limit of the field extensions of $\mathbb{Q}(U)$ in k of finite degree. Moreover, as any field extension in characteristic 0 of finite degree admits a primitive element, k is the direct limit of the monogenic extensions of $\mathbb{Q}(U)$. Thus giving a map $k \rightarrow A$ is equivalent to giving a compatible series of maps $l_i \rightarrow A$, as l_i varies over the monogenic extensions of $\mathbb{Q}(U)$ lying within k . But as just shown, for any monogenic l_i , there is a unique map $l_i \rightarrow A$ lying over the inclusion $l_i \rightarrow k$. These maps form a compatible system as they are unique. Therefore, there is a unique map $k \rightarrow A$ lying over the identity map $k \rightarrow k$, as desired. \square

In fact, Theorem 2.1 is easily combined with Theorem 3.1 to prove the following case of Theorem 1.1.

Theorem 3.2. *Let k be a field equipped with a differential basis $T : U \rightarrow k$, and let $S = \mathbb{Z}[U]$. Then the functor $Q_k : \mathbf{C} \rightarrow \mathbf{F}$ on S -algebras given by $A \mapsto \text{Hom}_{\mathbf{F}}(k, QA)$ is representable.*

Proof. If k has positive characteristic p , let $C(k)$ be a Cohen S -algebra, and if k has characteristic 0, let $C(k)$ equal k . It suffices to show that the map $q_A :$

$\text{Hom}_{\mathbb{C}}(C(k), A) \rightarrow \text{Hom}_{\mathbb{F}}(k, QA)$ induced by Q is bijective. Equivalently, it suffices to show that for any $a \in \text{Hom}_{\mathbb{F}}(k, QA)$, the inverse image $q_A^{-1}(a)$ has a unique element.

First consider the case that a is an isomorphism, and make $C(k)$ into an object of \mathbb{C}_k via a . By Theorems 2.1 and 3.1, there is a unique map $C(k) \rightarrow A$ in \mathbb{C}_k . This means precisely that $q_A^{-1}(a)$ has a unique element, as desired.

For the general case, let $\varphi : A \rightarrow QA$ be the residue field map, and let B be $\varphi^{-1}(a(k))$. Then B is a subring of A and an object of \mathbb{C} , and the map a induces an isomorphism $b : k \rightarrow QB$. Now any map from $C(k)$ to A lying over a must factor through B . More specifically, if $q_B : \text{Hom}_{\mathbb{C}}(C(k), B) \rightarrow \text{Hom}_{\mathbb{F}}(k, QB)$ is the map induced by Q , then $q_A^{-1}(a)$ and $q_B^{-1}(b)$ are in bijection. But $q_B^{-1}(b)$ has a unique element, as b is an isomorphism. Therefore $q_A^{-1}(a)$ has a unique element, and $C(k)$ represents the functor Q_k . \square

3.2 The unit

A categorical result will be used to prove Theorem 1.1 from Theorem 3.2, as follows.

To say that an object C of \mathbb{C} represents the functor $Q_k : \mathbb{C} \rightarrow \mathbf{Sets}$ given by $A \mapsto \text{Hom}_{\mathbb{F}}(k, QA)$ is to say that there exists a system of bijections

$$l_A : \text{Hom}_{\mathbb{C}}(C, A) \xrightarrow{\sim} \text{Hom}_{\mathbb{F}}(k, QA)$$

for all $A \in \mathbb{C}$, where the l_A are functorial in A . Such a system of bijections gives rise to a “unit map” $u : k \rightarrow QC$ in \mathbb{F} , defined as $u = l_C(\text{id}_C)$. The unit map has the following important property: let $q_A : \text{Hom}_{\mathbb{C}}(C, A) \rightarrow \text{Hom}_{\mathbb{F}}(QC, QA)$ be the map given by Q , and let $u_A : \text{Hom}_{\mathbb{F}}(QC, QA) \rightarrow \text{Hom}_{\mathbb{F}}(k, QA)$ be the map given by precomposition with u . Then l_A equals $u_A q_A$ by Yoneda’s Lemma.

In the case of the functor Q_k on \mathbb{C} , the unit map u is always an isomorphism.

Lemma 3.3. *Suppose that for some $k \in \mathbb{F}$, the functor Q_k is representable by an object $C \in \mathbb{A}$. Then the unit map $u : k \rightarrow QC$ is an isomorphism.*

Proof. Consider the field k as a complete local ring with maximal ideal 0 , and consider the associated bijection $l_k : \text{Hom}_{\mathbb{C}}(C, k) \rightarrow \text{Hom}_{\mathbb{F}}(k, k)$. Since l_k is surjective, there exists a map $\varphi : C \rightarrow k$ such that $l_k(\varphi) = \text{id}_k$. Recall that $l_k = u_k q_k$, and that by definition u_k acts on a map by precomposing with u . This gives that $q_k(\varphi) \circ u = \text{id}_k$. Now id_k is surjective, so $q_k(\varphi)$ is surjective. But $q_k(\varphi)$ is a field homomorphism, so it is injective. Thus $q_k(\varphi)$ is an isomorphism, and therefore u is an isomorphism. \square

The lemma shows that to attempt to represent Q_k , it suffices to consider candidate rings C with residue field isomorphic to k . Also, instead of dealing with an abstract system of bijections l_A , it suffices to consider whether the map $q_A : \text{Hom}(C, A) \rightarrow \text{Hom}(k, QA)$ induced by Q is an isomorphism for all A .

3.3 Main proof

It is now possible to prove Theorem 1.1.

Proof. First suppose that Q_k is representable on \mathbf{C} , and let $A = k \oplus \Omega_{k/S}$. The k -module A has a ring structure given by $(x_1, m_1) \cdot (x_2, m_2) = (x_1 x_2, x_1 m_2 + x_2 m_1)$. Let $d : k \rightarrow \Omega_{k/S}$ be the universal derivation. Then A admits two ring homomorphisms from k , namely the map $f_1(x) = (x, 0)$ and the map $f_2(x) = (x, dx)$. Consider A to be an S -algebra via f_1 ; this makes A into an object of \mathbf{C} .

By Lemma 3.3, any object C representing Q_k has $QC \cong k$, and the map $q_A : \text{Hom}_{\mathbf{C}}(C, A) \rightarrow \text{Hom}_{\mathbf{F}}(k, QA)$ induced by Q is a bijection. Let $\varphi : C \rightarrow k$ be the residue field map. Then $f_1\varphi$ and $f_2\varphi$ are two elements of $\text{Hom}_{\mathbf{C}}(C, A)$, and q_A sends both $f_1\varphi$ and $f_2\varphi$ to id_k in $\text{Hom}_{\mathbf{F}}(k, QA)$. Since q_A is injective, this shows $f_1\varphi = f_2\varphi$. As φ is surjective, this means $f_1 = f_2$ and $d = 0$. But the image of d generates $\Omega_{k/S}$ as a k -module, so $\Omega_{k/S}$ is 0.

Now assume $\Omega_{k/S} = 0$. Recall that the sequence of homomorphisms $\mathbb{Z} \rightarrow S \rightarrow k$ gives rise to the four term exact sequence of differentials

$$\Omega_S \otimes_S k \rightarrow \Omega_k \rightarrow \Omega_{k/S} \rightarrow 0$$

where $\Omega_S = \Omega_{S/\mathbb{Z}}$ [5, 0.20.5.7, p. 131]. Since $\Omega_{k/S} = 0$, the first map in the exact sequence is a surjection. This implies that there exists a subset U of S such that the map $T : U \rightarrow k$ is a differential basis of k .

So let $P = \mathbb{Z}[U]$ be the polynomial ring on U , and consider the categories \mathbf{F}_P and \mathbf{C}_P of P -algebras, defined analogously to \mathbf{F} and \mathbf{C} but with P in the role of S . Now S is a P -algebra, and the structure map $P \rightarrow S$ induces faithful functors $\mathbf{C} \rightarrow \mathbf{C}_P$ and $\mathbf{F} \rightarrow \mathbf{F}_P$, so that \mathbf{C} and \mathbf{F} may be considered subcategories of \mathbf{C}_P and \mathbf{F}_P .

By Theorem 3.2, the functor Q_k on \mathbf{C}_P is representable by a ring $C_P(k)$. From this ring the representing object of Q_k on \mathbf{C} may be constructed. First consider the discrete ring $C_P(k) \otimes_P S$. Note that $C_P(k)$ has residue field k , and that k is an S -algebra, so there is a natural surjective map $C_P(k) \otimes_P S \rightarrow k$. Call its kernel \mathfrak{m} , and let $C(k)$ be the completion of $(C_P(k) \otimes_P S)_{\mathfrak{m}}$, as in Lemma 1.3. The ring $C(k)$ is a complete local S -algebra, so $C(k)$ is an object of \mathbf{C} . In the category of local P -algebras, there is a natural map $C_P(k) \rightarrow (C_P(k) \otimes_P S)_{\mathfrak{m}}$ given by $p \mapsto p \otimes 1$. Then since $C_P(k)$ is its own completion, this gives a map $C_P(k) \rightarrow C(k)$ in \mathbf{C}_P .

To show that $C(k)$ represents Q_k it suffices to show that for any object A of \mathbf{C} , the map $q_A : \text{Hom}_{\mathbf{C}}(C(k), A) \rightarrow \text{Hom}_{\mathbf{F}}(k, QA)$ is bijective. Let $A \in \mathbf{C}$ and let ψ_1 and ψ_2 be two elements of $\text{Hom}_{\mathbf{C}}(C(k), A)$ for which $q_A(\psi_1) = q_A(\psi_2)$. Considering ψ_1 and ψ_2 as P -maps shows that ψ_1 and ψ_2 have the same image in $\text{Hom}_{\mathbf{C}_P}(C_P(k), A)$, as $C_P(k)$ represents Q_k on \mathbf{C}_P . As ψ_1 and ψ_2 are both S -maps, they have the same image in $\text{Hom}(S, A)$, namely the structure map of A . Thus ψ_1 and ψ_2 have the same image in $\text{Hom}_S(C_P(k) \otimes_P S, A)$. Since ψ_1 and ψ_2 are maps $C(k) \rightarrow A$, their image

in $\text{Hom}_S(C_P(k) \otimes_P S, A)$ in fact lies in the subset $\text{Hom}_S((C_P(k) \otimes_P S)_{\mathfrak{m}}, A)$. Then Lemma 1.3 shows that ψ_1 and ψ_2 coincide.

Now let $A \in \mathbf{C}$ and let $\psi : k \rightarrow QA$ be an arbitrary S -map. Considering ψ as a P -map shows that there exists a continuous P -map $C_P(k) \rightarrow A$ which lifts ψ . Both A and k are S -algebras, so this gives an S -map $C_P(k) \otimes_P S \rightarrow A$ which lifts ψ . Since ψ is injective, \mathfrak{m} is also the kernel of the induced map $C_P(k) \otimes_P S \rightarrow QA$. Therefore the map $C_P(k) \otimes_P S \rightarrow A$ gives a local map $(C_P(k) \otimes_P S)_{\mathfrak{m}} \rightarrow A$. Then Lemma 1.3 gives a continuous S -map $C(k) \rightarrow A$ lifting $\psi : k \rightarrow QA$, as desired.

This shows that $q_A : \text{Hom}_S(C(k), A) \rightarrow \text{Hom}_S(k, QA)$ is a bijection, so $C(k)$ represents the functor Q_k . That, in turn, shows that the object $C(k)$ does not depend on the choice of differential basis $U \rightarrow k$. \square

Example 3.4. The ring $C(k)$ when $S \rightarrow k$ is surjective.

Suppose the structure map $S \rightarrow k$ is surjective with kernel \mathfrak{n} , which clearly implies $\Omega_{k/S} = 0$. For a complete local ring A , any structure map $S \rightarrow A$ for which there exists an S -map $k \rightarrow QA$ must factor through $S_{\mathfrak{n}}$. Moreover, giving a local map $S_{\mathfrak{n}} \rightarrow A$ is equivalent to giving a continuous map from the completion $\hat{S}_{\mathfrak{n}}$ to A , by Lemma 1.3. On the other hand, $\hat{S}_{\mathfrak{n}}$ is an object of \mathbf{C}_k since the structure map $S \rightarrow k$ induces an isomorphism $Q\hat{S}_{\mathfrak{n}} \cong k$. Therefore $\hat{S}_{\mathfrak{n}}$ is an initial object of \mathbf{C}_k and $C(k)$ equals $\hat{S}_{\mathfrak{n}}$.

Bibliography

- [1] Atiyah, M. and Macdonald, I. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., New York, 1969.
- [2] Bourbaki, N. *Éléments de mathématique. Algèbre commutative. Chapitre 1 à 4*. Masson, Paris, 1985.
- [3] Cohen, I. On the structure and ideal theory of complete local rings, *Trans. Amer. Math. Soc.* **59** (1946), 54–106.
- [4] Eisenbud, D. *Commutative algebra with a view toward algebraic geometry*. Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.
- [5] Grothendieck, A. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. I. *Inst. Hautes Études Sci. Publ. Math.* **20** (1964), 1–259.
- [6] Nagata, M. On the structure of complete local rings, *Nagoya Math. J.* **1** (1950), 63–70.
- [7] Nagata, M. Corrections to my paper “On the structure of complete local rings”, *Nagoya Math. J.* **5** (1953), 145–147.