FIRST STEPS IN LOCAL ALGEBRA

These are notes for the beginning of a second course in commutative algebra taught at Central European University in 2010. The course continued with the homological theory (Cohen-Macaulay rings, regular rings, Koszul complexes etc.) All rings are assumed to be commutative with unit and all modules unitary.

1. Completions

Definition 1.1. Let A be a ring, and $I \subset A$ an ideal. The *completion* of A with respect to I is

$$\widehat{A} := \{(a_n) \subset \prod_{n=1}^{\infty} (A/I^n) \,:\, a_n = a_{n+1} \bmod I^n \text{ for all } n\,\}.$$

This is again a ring with the obvious operations. There is a natural map $A \to \widehat{A}$ given by $a \mapsto (a \bmod I^n)$; if it is an isomorphism, we say that A is *complete* with respect to I.

The *associated graded ring* is

$$\mathrm{gr}_\bullet(A) := \bigoplus_{n=0}^{\infty} I^n/I^{n+1}.$$

Here $I^0 := A$, and ring operations are again defined in the obvious way.

Recall that a graded ring is a ring R together with a family of additive subgroups R_n for each $n \geq 0$ such that $R_n R_m \subset R_{n+m}$ and $R = \bigoplus_n R_n$.

Example 1.2. The basic example is that of the polynomial ring $A = k[x_1, \ldots, x_n]$, k a field, and $I = (x_1, \ldots, x_n)$. Then $\widehat{A}$ is the formal power series ring $k[[x_1, \ldots, x_n]]$ and $\mathrm{gr}_\bullet(A) = A$.

Observe that we get the same result if instead of A we start with the localization $A_I = k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}$. One of the main goals of these notes is to show that all regular local rings containing a field behave in a similar way.

Completion is a special case of the inverse limit construction in category theory. Recall that an *inverse system* of groups (rings, modules, etc.) indexed by $\mathbf{N}$ together with its natural ordering is given by a group (ring, module...) G_n for each $n \geq 0$ and a morphism $\phi_n : G_{n+1} \to G_n$ for each $n > 0$. The *inverse limit* of the system is defined by

$$\lim_{\leftarrow} G_n := \{(g_n) \subset \prod_{n=1}^{\infty} G_n \,:\, g_n = \phi_n(g_{n+1}) \text{ for all } n\,\}.$$

Important inverse systems of modules over a fixed ring A are given by chains of submodules $M^0 \supset M^1 \supset M^2 \supset \dots$ of a fixed A-module M. The modules in the inverse system are the quotients M/M^n and the maps the natural projections. We call the inverse limit the completion of M with respect to the chain (M^n) and denote it by $\widehat{M}$. For instance, we may take $M^n := I^n M$ for an ideal $I \subset A$; in this case we call $\widehat{M}$ the *I-adic completion of M*. The case $M = A$ gives back the completion $\widehat{A}$ defined above.

There are natural surjective projections $p_n : \widehat{M} \to M/M^n$ for each n; set $\widehat{M^n} := \ker(p_n)$. The p_n induce isomorphisms $\widehat{M}/\widehat{M^n} \cong M/M^n$, so that the completion of $\widehat{M}$ with respect to the chain $(\widehat{M^n})$ is isomorphic to $\widehat{M}$.

The next observation shows that we have a certain freedom in choosing the inverse system defining a completion.

Proposition 1.3. *Let M be an A-module, and $M^0 \supset M^1 \supset M^2 \supset \dots$, $N^0 \supset N^1 \supset N^2 \supset \dots$ two chains of submodules such that for each M^n there exists N^m with $N^m \subset M^n$ and conversely, for each N^n there exists M^m with $M^m \subset N^n$. Then there is a canonical isomorphism*

$$\lim_{\leftarrow} M/M^n \cong \lim_{\leftarrow} M/N^n.$$

Proof. In the special case when the N^n can be identified with a subsequence of the M^n there is a natural map $\lim_{\leftarrow} M/M^n \to \lim_{\leftarrow} M/N^n$ given by restriction to subsequences which is plainly an isomorphism.

In the general case we can find strictly increasing maps $\alpha, \beta : \mathbf{N} \to \mathbf{N}$ such that for each M^n we have $N^{\alpha(n)} \subset M^n$ and for each N^n we have $M^{\beta(n)} \subset N^n$. There are natural maps $\lim_{\leftarrow} M/N^{\alpha(n)} \to \lim_{\leftarrow} M/M^n$ and $\lim_{\leftarrow} M/M^{\beta(n)} \to \lim_{\leftarrow} M/N^n$ induced by the natural projections. Composing with the isomorphisms constructed in the special case we get maps $\lim_{\leftarrow} M/N^n \to \lim_{\leftarrow} M/M^n$ and $\lim_{\leftarrow} M/M^n \to \lim_{\leftarrow} M/N^n$ which are plainly inverse to each other. □

Remark 1.4. In the above situation we may equip M with a topology in which we declare the M^n to be a basis of open neighbourhoods of 0. In the case $M^n = I^n M$ this is called the I-adic topology. A sequence $(m_n) \subset M$ is a Cauchy sequence for this topology if $m_i - m_j \in M^n$ for i, j larger than an index N depending on n; it converges to $m \in M$ if $m - m_i \in M^n$ for i larger than an index N depending on n. In the completion $\widehat{M}$ every Cauchy sequence is convergent.

The condition of the above proposition says that the topologies generated by the submodules M^n and N^n are equivalent. Thus the completion depends only on the topology of the module.

We conclude this section with a seemingly obvious fact.

Proposition 1.5. *Let A be a local ring with maximal ideal M. The M-adic completion $\widehat{A}$ is a local ring with maximal ideal $\widehat{M}$, the kernel of the natural projection $\widehat{A} \to A/M$.*

Proof. Given $m \in \widehat{M}$, the element $1+m$ is a unit in $\widehat{A}$. Indeed, the series $1-m+m^2-m^3+m^4+\dots$ is an inverse for $1+m$ and converges in $\widehat{A}$ (its 'tails' give an element in the inverse limit).

By definition $\widehat{A}/\widehat{M} \cong A/M$ is a field, so $\widehat{M}$ is a maximal ideal. Now given $m \in \widehat{M}$ and a maximal ideal $M' \subset \widehat{A}$, we have $m \in M'$. Indeed, otherwise $(m, M') = \widehat{A}$ so there exist $a \in \widehat{A}$ and $b \in M'$ with $am + b = 1$, but this contradicts the fact proven above that $1 - am$ is a unit. So $\widehat{M} \subset M'$, whence $\widehat{M} = M'$. □

Remark 1.6. The above proof shows that more generally if A is any ring and $\widehat{A}$ its completion with respect to an ideal $I \subset A$, then $\widehat{I} := \ker(\widehat{A} \to A/I)$ is contained in all maximal ideals of $\widehat{A}$, i.e. in its *Jacobson radical*.

2. The exactness property of completion

In this section the base ring A will always be Noetherian. The main result is:

Proposition 2.1. *Let*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

be an exact sequence of finitely generated A-modules, with A a Noetherian ring. Then for an ideal $I \subset A$ the natural sequence of I-adic completions

$$0 \to \widehat{M_1} \to \widehat{M_2} \to \widehat{M_3} \to 0$$

is exact.

Corollary 2.2. *We have canonical isomorphisms $\widehat{A}/\widehat{I} \cong A/I$ and $\widehat{I^n}/\widehat{I^{n+1}} \cong I^n/I^{n+1}$ for all $n > 0$. In other words, $\mathrm{gr}_\bullet(A) \cong \mathrm{gr}_\bullet(\widehat{A})$.*

Here, in contrast to the notation of Proposition 1.5, the notation $\widehat{I^n}$ stands for the I-adic completion of the A-module I^n.

Proof. Apply the proposition with $M_1 = I^{n+1}$, $M_2 = I^n$ (also for $n = 0$, where $I^0 = A$) and observe that $\widehat{I^n/I^{n+1}} = I^n/I^{n+1}$. □

Corollary 2.3. *If $J = (a_1, \dots, a_n) \subset A$ is any ideal, then its I-adic completion as an A-module satisfies $\widehat{J} \cong J\widehat{A}$.*

Proof. Applying the proposition to the exact sequence

$$0 \to J \to A \to A/J \to 0$$

shows $\widehat{A/J} \cong \widehat{A}/\widehat{J}$. Next, consider the exact sequence

$$A^n \xrightarrow{\phi} A \to A/J \to 0$$

where $\phi(t_1, \dots t_n) := \Sigma\, a_i t_i$. Applying the proposition again gives the exact sequence

$$\widehat{A}^n \xrightarrow{\widehat{\phi}} \widehat{A} \to \widehat{A}/\widehat{J} \to 0$$

so we conclude $\widehat{J} = \mathrm{Im}\,(\widehat{\phi})$. But $\widehat{\phi}$ is given by $\phi(\widehat{t_1}, \dots \widehat{t_n}) := \Sigma a_i \widehat{t_i}$ (or in other words $\widehat{\phi} = \phi \otimes \mathrm{id}_{\widehat{A}}$), so $\mathrm{Im}\,(\widehat{\phi}) = J\widehat{A}$. □

The next corollary shows that complete Noetherian rings are close to power series rings.

Corollary 2.4. *Let A be a Noetherian ring, $I = (a_1, \dots, a_n)$ an ideal of A. Then the I-adic completion $\widehat{A}$ satisfies*

$$\widehat{A} \cong A[[x_1, \dots, x_n]]/(x_1 - a_1, \dots x_n - a_n).$$

Proof. Consider the polynomial ring $B := A[x_1, \dots, x_n]$ and define an A-homomorphism $B \to A$ by sending x_i to a_i. It is surjective with kernel $J := (x_1 - a_1, \dots, x_n - a_n)$, and the ideal $(x_1, \dots, x_n) \subset B$ maps onto I in A. Applying Proposition 2.1 to the $(x_1, \dots, x_n)$-adic completion of

$$0 \to J \to B \to A \to 0$$

shows $\widehat{A} \cong \widehat{B}/\widehat{J}$. By Corollary 2.3 we have $\widehat{J} \cong J\widehat{B}$, so it remains to observe that $\widehat{B} \cong A[[x_1, \dots, x_n]]$. □

Example 2.5. Take $A = \mathbf{Z}$, $I = (p)$. The completion $\mathbf{Z}_p := \varprojlim \mathbf{Z}/p^n\mathbf{Z}$ is the *ring of p-adic integers*; by the corollary it is isomorphic to $\mathbf{Z}[[x]]/(x - p)$. The latter may actually be taken as a quick, albeit unorthodox, definition of p-adic integers.

The *proof of Proposition 2.1* will be given in two steps.

Step 1: We prove the exactness of the sequence of inverse limits

$$0 \to \varprojlim M_1/(I^n M_2 \cap M_1) \to \varprojlim M_2/I^n M_2 \to \varprojlim M_3/I^n M_3 \to 0.$$

Step 2: We prove that for each $m > 0$ there exists $n > 0$ with $I^n M_2 \cap M_1 \subset I^m M_1$.

Since obviously $I^m M_1 \subset I^m M_2 \cap M_1$, Step 2 implies that the condition of Proposition 1.3 is satisfied and therefore the completion of M_1 with respect to the chain $(I^n M_2 \cap M_1)$ is isomorphic the I-adic completion of M_1. Therefore the proposition will follow from Step 1. □

Step 1 follows by applying the following general lemma to the exact sequences

$$0 \to M_1/(I^n M_2 \cap M_1) \to M_2/I^n M_2 \to M_3/I^n M_3 \to 0.$$

Lemma 2.6. *Let $(G_n^1), (G_n^2)$ and (G_n^3) be inverse systems of groups such that there are commutative diagrams with exact rows*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_{n+1}^1 & \longrightarrow & G_{n+1}^2 & \longrightarrow & G_{n+1}^3 & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \phi_n^1} & & \downarrow{\scriptstyle \phi_n^2} & & \downarrow{\scriptstyle \phi_n^3} & & \\ 1 & \longrightarrow & G_n^1 & \longrightarrow & G_n^2 & \longrightarrow & G_n^3 & \longrightarrow & 1 \end{array}$$

for each $n > 0$. If moreover the maps ϕ_n^1 are surjective for all n, then the induced sequence

$$1 \to \varprojlim G_n^1 \to \varprojlim G_n^2 \to \varprojlim G_n^3 \to 1$$

of inverse limits is exact.

Proof. Left exactness of the sequence is immediate from the definition of the inverse limit. For surjectivity on the right we have to show that every sequence $(g_n^3) \in \varprojlim G_n^3$ is the image of a sequence $(g_n^2) \in \varprojlim G_n^2$. We use induction on n. We pick g_0^2 mapping to g_0^3 and assume that g_n^2 has been constructed. We lift g_{n+1}^3 to $g_{n+1}^2 \in G_{n+1}^2$ arbitrarily. The quotient $\phi_n^2(g_{n+1}^2)(g_n^2)^{-1}$ maps to 1 in G_n^3, hence it comes from some $g_n^1 \in G_n^1$. As ϕ_n^1 is surjective, we find $g_{n+1}^1 \in G_n^1$ mapping to g_n^1. Then $(g_{n+1}^1)^{-1} g_{n+1}^2$ still maps to g_{n+1}^3 in G_{n+1}^3 but moreover it maps to g_n^2 in G_n^2. □

We prove **Step 2** in a more precise form:

Proposition 2.7. (Artin–Rees lemma) *Let A be a Noetherian ring, $I \subset A$ an ideal and M a finitely generated module. Given a submodule $M_1 \subset M$, there exists $k > 0$ such that*

$$I^n M \cap M_1 = I^{n-k}(I^k M \cap M_1)$$

for all $n > k$.

Proof. Consider the infinite direct sums

$$B_I(A) := \bigoplus_{n=0}^{\infty} I^n, \qquad B_I(M) := \bigoplus_{n=0}^{\infty} I^n M.$$

Then $B_I(M)$ is a graded module over the graded ring $B_I(A)$, which means that $I^n(I^k M) \subset I^{n+k} M$ for all $n, k \geq 0$. A system of generators of M over A also generates $B_I(M)$ over $B_I(A)$, so $B_I(M)$ is a finitely generated $B_I(A)$-module. Moreover, a finite system of generators of I generates $B_I(A)$ as an *A-algebra*, so $B_I(A)$ is Noetherian by the Hilbert basis theorem.

Now $B_1 := \bigoplus_{n=0}^{\infty}(I^nM \cap M_1)$ is a $B_I(A)$-submodule of $B_I(M)$, hence finitely generated because $B_I(A)$ is Noetherian. So there is $k > 0$ such that all generators are contained in the direct sum of the $I^jM \cap M_1$ with $j \leq k$. By decomposing the generators $m_1, \ldots, m_r$ in their homogeneous components we may assume that for each $1 \leq j \leq r$ there exists $0 \leq \alpha(j) \leq k$ such that $m_j \in I^{\alpha(j)}M \cap M_1$. Then given $m \in I^nM \cap M_1$ for $n > k$, we may write

$$m = \sum_{j=1}^{r} i_j^{n-\alpha(j)} m_j = \sum_{j=1}^{r} i_j^{n-k}(i_j^{k-\alpha(j)} m_j)$$

for some $i_1, \ldots, i_r \in I$. But $i_j^{k-\alpha(j)} m_j \in I^kM \cap M_1$ for all j, so we conclude $m \in I^{n-k}(I^kM \cap M_1)$. This shows $I^nM \cap M_1 \subset I^{n-k}(I^kM \cap M_1)$, and the other inclusion is evident. □

The Artin–Rees lemma has another important consequence:

Corollary 2.8. (Krull intersection theorem) *If A is a Noetherian local ring with maximal ideal M, then*

$$\bigcap_{n=1}^{\infty} M^n = (0).$$

Proof. Write N for the intersection on the left hand side. As N is an ideal, we have $MN \subset N$. On the other hand, applying the Artin–Rees lemma to $N \subset A$ gives a k for which

$$N = M^{k+1} \cap N = M(M^k \cap N) \subset MN.$$

Thus $MN = N$, so $N = (0)$ by Nakayama's lemma. □

Corollary 2.9. *If A is a Noetherian local ring with maximal ideal M, the natural map $A \to \widehat{A}$ is injective.*

Proof. The kernel is $\bigcap_{n=1}^{\infty} M^n$. □

3. Power series rings

In this section we establish some basic properties of power series rings.

Proposition 3.1. *Let A be a Noetherian ring. Then the formal power series ring $A[[x]]$ is also Noetherian.*

Proof. This is similar to the proof of the Hilbert basis theorem. Fix an ideal $I \subset A$ and write I_r for the ideal in A generated by the leading coefficients a_r of power series of the form $a_r x^r + a_{r+1}x^{r+1} + \dots$ contained in I. Then $I_0 \subset I_1 \subset I_2 \subset \dots$ is an ascending chain, so there is n for which $I_n = I_{n+1} = I_{n+2} = \dots$ Choose finite sets of generators m_{ij} for the ideals I_j with $j \leq n$ and power series $s_{ij} \in I$ with leading coefficient $m_{ij} \in I_j$. Given a power series $s = a_r x + a_{r+1}x^{r+1} + \dots$ in I, we express it as an $A[[x]]$-linear combination of the s_{ij}. If $r \leq n$, we find $b_i \in A$ such that $a_r = \Sigma\, b_i m_{ir}$, so after subtracting finitely many A-linear combinations of the s_{ij} we may assume $r > n$. But then $a_r = \Sigma\, b_i^r m_{in}$ for some $b_i^r \in A$ and therefore $s - \Sigma\, b_i^r x^{r-n} s_{in}$ begins with a term $a_{r+1}x^{r+1}$. Therefore

$$s = \sum_i \left(\sum_{r=n+1}^{\infty} b_i^r x^{r-n} \right) s_{in}$$

where the coefficient in parentheses is an element of $A[[x]]$. □

Corollary 3.2. *If A is Noetherian, the power series ring $A[[x_1, \dots, x_n]]$ is Noetherian. In particular, this holds for the ring $k[[x_1, \dots, x_n]]$ over a field k.*

Combining with Corollary 2.4 we also get:

Corollary 3.3. *If A is a Noetherian ring, any completion $\widehat{A}$ of A by an ideal is Noetherian.*

The next property is more difficult to prove.

Theorem 3.4. *If k is a field, the power series ring $k[[x_1, \dots, x_n]]$ is a UFD.*

The result is easy for $n = 1$: the ring $k[[x]]$ is a principal ideal ring, and in fact all ideals are of the form (x^m) for some m (i.e. $k[[x]]$ is a discrete valuation ring). Indeed, a power series $\Sigma\, a_i x^i$ with $a_0 \neq 0$ is always a unit (we may assume $a_0 = 1$, and then $1 - h + h^2 - h^3 + \dots$ is an inverse for $1 + h$), and therefore every power series is x^m times a unit for some $m \geq 0$.

For the proof in the case $n > 1$, we write

$$k[[x_1, \dots, x_n]] = k[[x_1, \dots, x_{n-1}]][[x_n]].$$

Here $A = k[[x_1, \dots, x_{n-1}]]$ is a complete local ring with respect to its maximal ideal $(x_1, \dots, x_{n-1})$. The key property is:

Proposition 3.5. ('Euclidean division') *Let A be a Noetherian complete local ring with maximal ideal M, and let $f = \Sigma a_i x^i \in A[[x]] \setminus MA[[x]]$. Write n for the smallest index i for which $a_i \notin M$. Then for every $g \in A[[x]]$ we find $q \in A[[x]]$ and $r \in A[x]$ such that $\deg r < n$ and*

$$g = qf + r.$$

Moreover the q and r with this property are unique.

The following elegant proof of the proposition was stolen from lecture notes by Hochster. It is based on the following topological version of Nakayama's lemma.

Lemma 3.6. *Let A be a complete local ring with maximal ideal M, and N an A-module such that*

$$\bigcap_j M^j N = 0.$$

Assume there exist $n_1, \ldots, n_r \in N$ whose images generate the A/M-vector space N/MN. Then the n_i generate the A-module N.

Proof. By assumption,

$$N = An_1 + \ldots An_r + MN, \tag{1}$$

whence

$$M^j N = M^j n_1 + \cdots + M^j n_r + M^{j+1} N \tag{2}$$

for all $j \geq 0$. Given an element $n \in N$, we may write it as a sum

$$n = \left(\sum_{i=0}^{j} a_{i1} \right) n_1 + \cdots + \left(\sum_{i=0}^{j} a_{ir} \right) n_r + p_{j+1} \tag{3}$$

where $a_{il} \in M^i N$ for all i, l and $p_{j+1} \in M^{j+1} N$. This is easily proven by induction on j: for $j = 0$ it follows from (1) and once it is proven for $j-1$, we get it for j by applying (2) to p_j. The coefficients in brackets converge to elements $a_1, \ldots, a_r \in A$. For all $j \geq 0$ we have

$$n - (a_1 n_1 + \ldots a_r n_r) = p_{j+1} - \left(\sum_{i=j+1}^{\infty} a_{i1} \right) n_1 - \cdots - \left(\sum_{i=j+1}^{\infty} a_{ir} \right) n_r$$

by (3). Here the right hand side is in $M^{j+1} N$ and this holds for all j, so $n - (a_1 n_1 + \ldots a_r n_r) = 0$ by assumption. □

Proof of Proposition 3.5. Apply the lemma with $N = A[[x]]/(f)$. The ring $A[[x]]$ is Noetherian by Proposition 3.1, and it is local with maximal ideal (M, x) (because every element of $A[[x]] \setminus (M, x)$ has an inverse by a similar argument as above). Thus the intersection of the powers of (M, x) is trivial by the Krull intersection theorem, and therefore so is the intersection of the powers $M^j A[[x]]$. Passing to the quotient N we see that the assumption of the lemma is satisfied. Set $k := A/M$ and write $\bar{f}$ for the image of f in $A[[x]]/MA[[x]] = k[[x]]$. We have $\bar{f} = x^n \bar{u}$ where $\bar{u}$ is a unit. Hence $k[[x]]/(\bar{f}) \cong k[[x]]/(x^n)$ and is generated as a k-vector space by $1, x, \ldots, x^{n-1}$. But then by the lemma $A[[x]]/(f)$ is generated as an A-module by $1, x, \ldots, x^{n-1}$ which means exactly the existence of an Euclidean division $g = qf + r$ as in the proposition for

all $g \in A[[x]]$. It is enough to prove uniqueness for $g = 0$ where it is obvious. □

Corollary 3.7. (Weierstrass Preparation Theorem) *For f as above there exists a unique decomposition*

$$f = pu$$

where u is a unit in $A[[x]]$ and $p = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ is a polynomial with $b_i \in M$.

The polynomials p with the property of the corollary are called *Weierstrass polynomials*.

Proof. Apply the proposition to $g = x^n$:

$$x^n = qf + r$$

with $\deg r < n$. As $a_i \in M$ for $i < n$, the coefficients of r must lie in M, and so $x^n - r$ is a Weierstrass polynomial. Looking at the coefficient of x^n on both sides we obtain $1 = c_0 a_n + m$ where $c_0 = q(0)$ and $m \in M$. It follows that c_0 is a unit in A and hence q is a unit in $A[[x]]$ (same argument as above). Thus $f = q^{-1}(x^n - r)$ is a decomposition of the required shape.

For uniqueness, let $f = pu$ be a decomposition and write $p = x^n - r$. Then $x^n = u^{-1}f + r$ is a result of Euclidean division of x^n by f, so we conclude by the uniqueness statement of the proposition. □

Proof of Theorem 3.4. For simplicity we treat only the case of infinite k. Under this assumption for each $f \in k[[x_1, \ldots, x_n]]$ we may find an invertible linear transformation of coordinates after which we have $f(0, \ldots, 0, x_n) \neq 0$, or in other words $f \in A[[x_n]] \setminus MA[[x_n]]$, where $A = k[[x_1, \ldots, x_{n-1}]]$ and $M = (x_1, \ldots x_n)$.

As the ring is Noetherian, we have a decomposition $f = f_1 \ldots f_r$ where the f_i are irreducible so it is enough to prove uniqueness up to multiplication by units. To begin with, we must have $f_i(0, \ldots, 0, x_n) \neq 0$ for all i and therefore we may apply the Weierstrass Preparation Theorem to each f_i: $f_i = p_i u_i$ with some Weierstrass polynomials p_i and units u_i. We also have a Weierstrass decomposition $f = pu$. By the uniqueness of Weierstrass decompositions we must have $p = p_1 \ldots p_r$. On the other hand, the ring $A[x_n]$ is a UFD because A is a UFD by induction on n, and then so is the polynomial ring $A[x_n]$. Therefore there is a factorization into irreducibles $p = q_1 \ldots q_s$ in $A[x_n]$. But the p_i are irreducible in $A[[x_n]]$ because the f_i are. Therefore they are irreducible in $A[x_n]$, so by unique factorization in $A[x_n]$ we have $r = s$ and the p_i differ from the q_i only by units in $A[x_n]$. Therefore the f_i equal the q_i up to units in $A[[x_n]]$. □

4. Regular local rings

Recall that the (Krull) dimension of a ring A is the maximal r for which there is a strictly increasing chain of prime ideals $P_0 \subset P_1 \subset \cdots \subset P_r$ in A. A Noetherian local integral domain A of finite dimension d is *regular* if its maximal ideal M can be generated by d elements.

Remarks 4.1.

1. In fact, the property that A is an integral domain is a consequence of the other assumptions; we omit the proof.
2. It is a consequence of Krull's Hauptidealsatz that M cannot be generated by less than d elements.

If M is the maximal ideal of the local ring A, then M/M^2 is a vector space over the residue field $\kappa := A/M$ and by Nakayama's lemma a system of elements $m_1, \ldots, m_n$ generate the ideal M if and only if their images generate the κ-vector space M/M^2. Thus A is regular of dimension d if and only if $\dim {}_\kappa M/M^2 = d$.

For a regular local ring a minimal system of generators of M is called a *system of parameters*. This name is explained by the following partial case of Cohen's structure theorem.

Theorem 4.2. *Let A be a complete Noetherian local ring that contains a subfield k mapping isomorphically onto its residue field. Then A is a quotient of some power series ring $k[[x_1, \ldots, x_d]]$.*

If moreover A is regular of dimension d, then $A \cong k[[x_1, \ldots, x_d]]$.

Remarks 4.3.

(1) All the assumptions are satisfied by the completion of the local ring of a smooth point on an algebraic variety over an algebraically closed field.
(2) We shall see later that the assumptions are satisfied for any complete regular local ring containing a field.
(3) The ring $k[[x_1, \ldots, x_d]]$ is indeed regular, for its maximal ideal can be generated by d elements and it has dimension d. For the latter fact, the inequality $\dim k[[x_1, \ldots, x_d]] \geq d$ is obvious, and the reverse inequality can be proven by induction on d using Krull's Hauptidealsatz.

Lemma 4.4. *Let $\phi : A \to B$ be a homomorphism of complete local rings such that $\phi(M_A^n) \subset M_B^n$ for all $n \geq 1$, where M_A (resp. M_B) is the maximal ideal of A (resp. B).*

If the induced homomorphism $\mathrm{gr}_\bullet(A) \to \mathrm{gr}_\bullet(B)$ is injective (resp. surjective), then so is ϕ.

Proof. Consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_A^n/M_A^{n+1} & \longrightarrow & A/M_A^{n+1} & \longrightarrow & A/M_A^n & \longrightarrow & 0 \\ & & {\scriptstyle \mathrm{gr}_n(\phi)}\downarrow & & {\scriptstyle \phi_{n+1}}\downarrow & & {\scriptstyle \phi_n}\downarrow & & \\ 0 & \longrightarrow & M_B^n/M_B^{n+1} & \longrightarrow & B/M_B^{n+1} & \longrightarrow & B/M_B^n & \longrightarrow & 0 \end{array}$$

The injectivity of $\mathrm{gr}_n(\phi)$ shows the injectivity of ϕ_n for all n by induction on n, whence also the injectivity of ϕ. For surjectivity, given $(b_n) \in B = \widehat{B}$ with $b_n \in B/M_B^n$, we have to find $a_n \in A/M_A^n$ with $\phi_n(a_n) = b_n$ and $a_{n+1} \bmod M_A^n = a_n$. We do this by induction on n: by surjectivity of $\mathrm{gr}_n(\phi)$ and the diagram the surjectivity of ϕ_n implies that of ϕ_{n+1}, so we may lift b_{n+1} to $a_{n+1} \in A/M_A^{n+1}$. This a_{n+1} may not map to a_n in A/M_A^n but the difference lies in $\ker(\phi_n)$. Again by surjectivity of $\mathrm{gr}_n(\phi)$ and the diagram the map $\ker(\phi_{n+1}) \to \ker(\phi_n)$ is surjective, and we may therefore modify a_{n+1} by an element of $\ker(\phi_{n+1})$. □

Proof of Theorem 4.2. Let $t_1, \ldots, t_d$ be a system of generators for the maximal ideal M of A. There is a unique k-algebra homomorphism $\lambda : k[[x_1, \ldots, x_d]] \to A$ sending x_i to t_i. Indeed, for all n there is a unique homomorphism $\lambda : k[[x_1, \ldots, x_d]]/(x_1, \ldots, x_d)^n \to A/M^n$ sending the image of x_i to that of t_i; as A is complete, these assemble to a homomorphism λ as required. As $A/M \cong k$ and the t_i generate M, the induced map $\mathrm{gr}_\bullet(\lambda)$ is surjective, so λ is surjective by the lemma.

If moreover A is regular, we may choose $d = \dim A$. As moreover A is then an integral domain, the kernel of λ is a prime ideal, so since A and $k[[x_1, \ldots, x_d]]$ are both of dimension d, we must have $\ker(\lambda) = 0$.

□

We can use the theorem to expand elements of regular local rings in power series. To do so, we use first the fact, to be proven later in the course, that A is regular if and only if $\widehat{A}$ is. By Corollary 2.9 the natural map embeds A in $\widehat{A}$, so the theorem implies:

Corollary 4.5. *Given a regular local ring A of dimension d containing a field k mapping onto its residue field there is an injective homomorphism $A \hookrightarrow k[[x_1, \ldots, x_n]]$. It is determined by the choice of a regular system of parameters $t_1, \ldots, t_d$ in A. In other words, each element of A has a 'power series expansion' in the t_i.*

Remark 4.6. For $d = 1$ there is an easy direct proof of the corollary. In this case A is a discrete valuation ring, i.e. the maximal ideal M is principal. Fix a generator t of M and pick $a \in A$. Set $a_0 := a \bmod M$ and $b_0 = a - a_0$. Then $b_0 = b_1 t$ with a unique $b_1 \in A$ and we set $a_1 := b_1 \bmod M$. Continuing the process we get $a = a_0 + a_1 t + \ldots a_n t^n + b_n$ with $b_n \in M^n$ for each n, whence the required map $A \mapsto k[[t]]$; it is injective by the Krull intersection theorem.

For general d the obvious generalization of the above procedure still yields *some* power series expansion of a with respect to a regular system of parameters $t_1, \ldots, t_d$ but its uniqueness is not a priori clear.

5. Unique factorization

Our aim is to prove:

Proposition 5.1. *Let A be a Noetherian local ring. If $\widehat{A}$ is a UFD, then so is A.*

Combinied with Theorem 4.2 and Theorem 3.4 this will imply:

Corollary 5.2. *If A is a regular local ring containing a subfield mapping isomorphically onto its residue field, then A is a UFD.*

Remark 5.3. Theorem 7.2 below will allow us to replace the condition 'A contains a subfield mapping isomorphically onto its residue field' by 'A contains a field'. This is the traditional way to prove that regular local rings 'coming from geometry' are UFD's. In fact, Auslander and Buchsbaum proved by homological methods that every regular local ring is a UFD.

For the proof of the proposition we first need:

Lemma 5.4. *If A is a Noetherian local ring and $J \subset A$ is an ideal, then $J\widehat{A} \cap A = J$.*

Proof. Given $a \in J\widehat{A} \cap A$ and $n > 0$, we find $j \in J$ and $m_n \in \widehat{M^n}$ with $a = j + m_n$ using the isomorphism $\widehat{A}/\widehat{M^n} \cong A/M^n$. The same isomorphism shows that $\widehat{M^n} \cap A = M^n$, so $m_n = a - j \in M^n$. Therefore a is contained in the intersection of the ideals $J + M^n$ for all n. Applying the Krull intersection theorem to A/J we see that this implies $a \in J$, so we have proven $J\widehat{A} \cap A \subset J$. The reverse inclusion is obvious. □

Proof of Proposition 5.1. Recall that a ring is a UFD if and only if

(i) its principal ideals satisfy the ascending chain condition, and
(ii) if $a \mid bc$ with a irreducible, then $a \mid b$ or $a \mid c$.

As our A is Noetherian, it will suffice to prove condition (ii), which we do in the following slightly more general form:

(ii') if $a \mid bc$ and a, b have no common factors, then $a \mid c$.

As $\widehat{A}$ is a UFD by assumption and hence satisfies (ii'), it will be enough to prove two things:

(1) If $a \mid b$ in $\widehat{A}$, then $a \mid b$ in A.
(2) If a, b have no common factors in A, they have no common factors in $\widehat{A}$.

To prove (1), it suffices to note that $a \mid b$ in $\widehat{A}$ means $b \in a\widehat{A}$, but $a\widehat{A} \cap A = aA$ by the lemma, and we are done.

To prove (2) we assume $a = da'$, $b = db'$ in $\widehat{A}$ with a non-unit d, and prove that a, b have a common factor in A. In any case we have $ab' = ba'$ and we may assume a', b' have no common factor. Using the Krull intersection theorem in $\widehat{A}$ we find n such that $a' \notin \widehat{M}^n$; we may assume n is minimal. As in the lemma, write $a' = a_n + m_n$, $b' = b_n + p_n$ with $a_n, b_n \in A$, $m_n, p_n \in \widehat{M}^n$; here $a_n \notin \widehat{M}^n$. Now $ab_n - ba_n \in (a,b)\widehat{M}^n \cap A = (a,b)M^n$ by the lemma, so $ab_n - ba_n = at_n + bs_n$ with $s_n, t_n \in M^n$. Therefore $a(b_n - t_n) = b(a_n + s_n)$ and also $a'(b_n - t_n) = b'(a_n + s_n)$ as A is a domain and $ab' = ba'$. As a' and b' have no common factor, a' must divide $a_n + s_n$. But neither a' nor $a_n + s_n$ are in $\widehat{M}^n$; on the other hand, $a' \in \widehat{M}^{n-1}$ by assumption. This can only happen if a' and $a_n + s_n$ differ by a unit of $\widehat{A}$: $(a_n + s_n)\widehat{A} = a'\widehat{A}$. In particular, $a_n + s_n$ divides a in $\widehat{A}$, hence also in A by (1). Their quotient must be a non-unit h because a and a' differ by a non-unit in $\widehat{A}$. But the equation $a(b_n - t_n) = b(a_n + s_n)$ implies $h(b_n - t_n) = b$ (again since A is a domain) and we have found a nontrivial common factor of a and b. □

The above proof, which is pure juggling, is due to Mumford. One can also give a more conceptual proof using some nontrivial theorems of commutative algebra.

6. Hensel's lemma

The simplest form of Hensel's lemma is:

Proposition 6.1. *Let A be a complete local ring with maximal ideal M and residue field k. Let $f \in A[T]$ be a polynomial, and write $\bar{f}$ for the image of f in $k[T]$. Assume that $\bar{a} \in k$ satisfies $\bar{f}(\bar{a}) = 0$ but $\bar{f}'(\bar{a}) \neq 0$. Then there exists a unique $a \in A$ reducing to $\bar{a}$ modulo M with $f(a) = 0$.*

As A is complete with respect to M, it suffices to construct for each $n \geq 0$ elements $a_n \in A/M^n$ satisfying $a_1 = \bar{a}$, $f(a_n) = 0$ and a_n mapping to a_{n-1} in A/M^{n-1}. We shall do this by applying

Proposition 6.2. *Let B be a ring, $I \subset B$ an ideal satisfying $I^2 = 0$, and $f \in B[T]$ a polynomial. If $b \in B$ is such that $f(b) \in I$ but $f'(b)$ is a unit in B, there exists a unique $c \in B$ with $f(c) = 0$ and $c \equiv b$ mod I.*

By the above arguments, if we apply the proposition inductively with $B = A/M^n$, $I = M^{n-1}/M^n$ and b a lift of a_{n-1} to A/M^n, Proposition 6.1 follows. Indeed, since b maps to $\bar{a}$ modulo M by construction, $f'(b)$ maps to $f'(\bar{a})$ modulo M, and so $f'(b)$ is a unit but $f(b) \in M^{n-1}/M^n$.

We prove Proposition 6.2 in an even more general form:

Proposition 6.3. *Let B be a ring, $I \subset B$ an ideal satisfying $I^2 = 0$. Assume moreover given a commutative diagram*

$$\begin{array}{ccc} S & \xrightarrow{\bar{\lambda}} & B/I \\ \uparrow & & \uparrow \\ R & \xrightarrow{\mu} & B \end{array} \tag{4}$$

where $S = R[T]/(f)$ with some $f \in R[T]$, and write t for the image of T in S. If there is a lifting b of $\bar{\lambda}(t)$ to B such that $f'(b)$ is a unit in B, then $\bar{\lambda}$ lifts to a unique map $\lambda : S \to B$ making the diagram commute.

Here by abuse of notation we have denoted by f' the derivative of the image of f in $B[T]$ via μ.

To get the previous proposition, we apply this with $R = B$, $\mu = \mathrm{id}_B$ and $\bar{\lambda}$ the map $B[T]/(f) \to B/I$ induced by sending $t = T \bmod (f)$ to b, and then set $c := \lambda(t)$.

Proof. Lift $\bar{\lambda}(t)$ to $b \in B$ as postulated. To define λ, we have to find $h \in I$ such that $f(b+h) = 0$, for then $T \mapsto b+h$ determines λ uniquely. The Taylor formula with difference h is of the shape $f(b+h) = f(b)+f'(b)h$ because $I^2 = 0$ and $h \in I$. But $f'(b)$ is a unit in B, and therefore the equation $0 = f(b) + f'(b)h$ can be solved uniquely in h. □

Remarks 6.4.

(1) Hensel's lemma (Proposition 6.1) is often stated without the uniqueness of the lifting $a \in A$. However, it can be checked directly that existence implies uniqueness.

(2) The property of the above proposition (sometimes called the infinitesimal lifting property) was used by Grothendieck to define smoothness in algebraic geometry. He defined an R-algebra S to be *formally smooth (resp. formally étale)* if for any diagram of the shape (4) where $I \subset B$ is an ideal with $I^2 = 0$ there exists a lifting (resp. a unique lifting) $\lambda : S \to B$ of $\bar{\lambda}$ making the diagram commute.

The proposition thus says in particular that R-algebras of the form $S = R[T]/(f)$ with $(f, f') = (1)$ are formally étale (because in this case the image of f' is a unit in S). There is a more or less straightforward generalization for R-algebras of the form $S = R[T_1, \ldots, T_n]/(f_1, \ldots, f_n)$ where the Jacobian determinant of the f_i maps to a unit in S; they are also formally étale. If $S = R[T_1, \ldots, T_n]/(f_1, \ldots, f_m)$ with $m \leq n$ such the maximal minors of the Jacobian give units in S, then S is formally smooth. This is the algebraic version of the Jacobian criterion of smoothness in geometry.

Proposition 6.3 in particular applies when $R = K$ is a field and $S = L$ is a finite separable extension, by the theorem of the primitive element.

As an infinite separable algebraic extension is a union of finite separable extensions, uniqueness of the lifting in Proposition 6.3 implies:

Corollary 6.5. *Let $L|K$ be a separable algebraic field extension. Assume moreover given a commutative diagram*

$$\begin{array}{ccc} L & \xrightarrow{\bar{\lambda}} & B/I \\ \uparrow & & \uparrow \\ K & \longrightarrow & B \end{array}$$

where B is a ring, $I \subset B$ an ideal satisfying $I^2 = 0$. Then $\bar{\lambda}$ lifts to a map $\lambda : L \to B$ making the diagram commute.

The same holds if instead of $I^2 = 0$ we assume that B is complete with respect to I.

Here the second statement reduces to the first in the same way as Proposition 6.1 reduces to Proposition 6.2.

7. Coefficient fields

Definition 7.1. Let A be a local ring with maximal ideal M and residue field k. A field contained in A is a *coefficient field* of A if it is mapped isomorphically onto k by the natural projection $A \to k$.

Assume moreover that A is an integral domain. We say that A is *equi-characteristic* if $\mathrm{char}(A) = \mathrm{char}(k)$. This holds if and only if A contains a field. Sufficiency is obvious, and so is necessity in positive characteristic. For necessity in characteristic 0, observe that the subring $\mathbf{Z} \subset A$ generated by 1 must meet M trivially, and therefore all of its elements are units in A, i.e. A contains $\mathbf{Q}$.

Theorem 7.2. (Cohen) *If A is an equi-characteristic complete local ring, then A has a coefficient field.*

Combining with Theorem 4.2 we obtain:

Corollary 7.3. *Let A be an equi-characteristic complete Noetherian local ring with residue field k. Then A is a quotient of some power series ring $k[[x_1, \ldots, x_d]]$.*

If moreover A is regular of dimension d, then $A \cong k[[x_1, \ldots, x_d]]$.

Proof of Theorem 7.2 in characteristic 0. Let $k' \subset k$ be the a maximal subfield such that the identity map of k' lifts to a map $k' \to A$. By the arguments preceding the theorem and Zorn's lemma such a k' exists and contains the prime field $\mathbf{Q}$. Assume $k' \neq k$. If k contains an element $\bar{x}$ transcendental over k', then lifting $\bar{x}$ to $x \in A$ we see that the ring $k'[x]$ meets M trivially (otherwise we would have $k'[x] \cap M = (f)$ for a polynomial $f \in k'[T]$ and $\bar{x}$ would be algebraic over k'). Therefore $k'(x) \subset A$ and the map $k'(\bar{x}) \to A$ sending $\bar{x}$ to x lifts the identity of $k'(\bar{x})$, contradicting the maximality of k'. Hence $k|k'$ is an algebraic

extension, and also separable as we are in characteristic 0. Now an application of Corollary 6.5 with $L = k$, $K = k'$ and $B = A$ again contradicts the maximality of k'.

Proof of Theorem 7.2 in characteristic $p > 0$. This case follows as above from the following proposition applied to $B = A$, $L = k$ and the map $k \to A/M$:

Proposition 7.4. *Let B be a ring, $I \subset B$ an ideal satisfying $I^2 = 0$, and L a field of characteristic $p > 0$. Then any nonzero map $\bar{\lambda} : L \to B/I$ lifts to a map $\lambda : L \to B$.*

The same holds if instead of $I^2 = 0$ we assume that B is complete with respect to I.

Proof. Define a map $\lambda_p : L^p \to B$ as follows. Given $a \in L$, lift $\bar{\lambda}(a)$ to $b \in B$, and set $\lambda_p(a^p) := b^p$. This does not depend on the choice of b because if b' is another lifting, then $b - b' \in I$, so that $b^p - (b')^p = (b-b')^p = 0$ because $p \geq 2$ and $I^2 = 0$. The map λ_p is the unique lifting of $\bar{\lambda}|_{L^p}$ to a map $L^p \to B$, and identifies L^p with a subfield of B.[1] By Zorn's lemma there exists a maximal subfield $L' \subset B$ containing L^p; it is also a maximal subfield in L such that $\bar{\lambda}|_{L'}$ lifts to a map $L' \to B$. We know that $L^p \subset L'$ and now show that $L' = L$. Assume not, and pick $\alpha \in L' \setminus L$. Then $\alpha^p \in L^p$, and $x^p - \alpha^p$ is the minimal polynomial of α over L'. Moreover, any lifting β of $\bar{\lambda}(\alpha)$ to B satisfies $\beta^p = \lambda_p(\alpha^p)$ by uniqueness of λ_p. Therefore sending α to β defines an extension of $\bar{\lambda}|_{L'}$ to $L'(\alpha) = L'[x]/(x^p - \alpha^p)$, contradicting the maximality of L'.

To get the second statement, we apply the first part inductively to B/I^{n+1} in place of B and I^n/I^{n+1} in place of I, assuming that a lifting to B/I^n has already been constructed. □

Finally, we briefly discuss the Cohen structure theorem for complete local domains of mixed characteristic, i.e. of characteristic 0, and with residue field of characteristic $p > 0$. For proofs of unproven statements, see e.g. Matsumura's book.

There are two basic facts that go beyond the equicharacteristic case.

Fact 7.5. *Given a field k of characteristic $p > 0$, there exists a complete discrete valuation ring A_0 of characteristic 0 with residue field k and maximal ideal generated by p.*

Such an A_0 is often called a *Cohen ring*. In the case where k is perfect, the ring A_0 is unique up to unique isomorphism and depends functorially on k: it is the ring of *Witt vectors* of k. In the non-perfect case, however, unicity does not hold.

Fact 7.6. *Let A be a complete local domain of characteristic 0, with maximal ideal M and residue field k of characteristic $p > 0$. Given a*

[1] For L perfect the proof stops here.

Cohen ring A_0 with residue field k, the identity morphism of k can be lifted to a homomorphism $A_0 \to A$.

Note that since A is an integral domain of characteristic 0 and the only nonzero prime ideal of A_0 is (p), a morphism $A_0 \to A$ must be injective. Furthermore, identifying A_0 with a subring of A, the element p must be contained in M, whence $M \cap A_0 = (p)$.

Granted these facts, we may state the Cohen structure theorem in the mixed characteristic case.

Theorem 7.7. *For $A_0 \subset A$ as above, there is a surjective homomorphism $A_0[[x_1, \dots, x_n]] \twoheadrightarrow A$ for some $n > 0$.*

If moreover A is regular of dimension $d+1$ and $p \in M \setminus M^2$, there is such a map with $n = d$, inducing an isomorphism $A \cong A_0[[x_1, \dots, x_d]]$.

Proof. We can choose a generating system for M of the form $p, t_1, \dots, t_n$. In the regular $(d+1)$-dimensional case we may moreover arrange $n = d$ in view of the assumption $p \notin M^2$. The proof then proceeds in exactly the same way as that of Theorem 4.2. □

If A is regular but $p \in M^2$, there is no such isomorphism with a power series ring. The best one can get is an embedding $A_0[[x_1, \dots, x_d]] \hookrightarrow A$ such that A is finitely generated as a module over its image.

8. Cohen rings

In this section we prove the statement of Fact 7.5 in the case the field k is perfect. Under this assumption, the Cohen ring with residue field k is unique up to unique isomorphism.

Following Lazard and Serre, we prove a more general statement involving not necessarily local or Noetherian rings. Call an integral domain B of characteristic $p > 0$ *perfect* if the map $x \mapsto x^p$ is an automorphism of B. A *strict p-ring* is a ring A complete with respect to the ideal pA such that p is not a zero-divisor in A and $\bigcap_n p^n A = (0)$.

Theorem 8.1. *(1) Given a perfect ring B of characteristic p, there exists a strict p-ring A with $A/pA \cong B$.*

(2) Given strict p-rings A_i for $i = 1, 2$ such that $B_i := A_i/pA_i$ is a perfect ring, every homomorphism $\bar{\phi} : B_1 \to B_2$ lifts to a unique morphism $\phi : A_1 \to A_2$ inducing $\bar{\phi}$ modulo the pA_i.

Notice that statement (2) implies the uniqueness of the ring A in (1) up to unique isomorphism. In the case when the ring B in (1) is a field, we obtain Fact 7.5 in the perfect residue field case.

Example 8.2. Given a ring R and a prime number p, denote by $R[x^{p^{-\infty}}]$ the R-algebra generated by indeterminates $x^{p^{-i}}$ for $i \geq 0$

subject to the sole relations $(x^{p^{-i-1}})^p = x^{p^{-i}}$. It is the union of the polynomial rings $R[x, x^{p^{-1}}, \dots, x^{p^{-n}}]$ for all n.

For $R = \mathbf{F}_p$ we obtain the perfect ring $\mathbf{F}_p[x^{p^{-\infty}}]$. If we complete $\mathbf{Z}[x^{p^{-\infty}}]$ with respect to the ideal $p\mathbf{Z}[x^{p^{-\infty}}]$, we obtain a strict p-ring $\mathbf{Z}(x, p^{-\infty})$ with perfect residue ring $\mathbf{F}_p[x^{p^{-\infty}}]$.

Performing a similar construction for a family of variables $\{x_\alpha\}$ ($\alpha \in \Lambda$) we obtain a strict p-ring $\mathbf{Z}(\{x_\alpha\}, p^{-\infty})$ with perfect residue ring $\mathbf{F}_p[\{x_\alpha^{p^{-\infty}}\}]$. Note that given a perfect ring B and elements $b_\alpha \in B$ for all $\alpha \in \Lambda$, it makes sense to substitute $x_\alpha = b_\alpha$ in every $F \in \mathbf{F}_p[\{x_\alpha^{p^{-\infty}}\}]$, since for all n there is a unique $c_\alpha \in B$ with $c_\alpha^{p^n} = b_\alpha$.

The proof of the theorem will be based on the following lemma.

Lemma 8.3. *Given a strict p-ring A, the natural map $\pi : A \to A/pA$ has a unique multiplicative retraction, i.e. a map $\rho : A/pA \to A$ satisfying $\pi \circ \rho = \mathrm{id}$ and $\rho(\bar{a}\bar{b}) = \rho(\bar{a})\rho(\bar{b})$ for $\bar{a}, \bar{b} \in A/pA$. Moreover, $\rho(\bar{a})$ is the unique element of A with the properties*

$$\bar{a} = \rho(\bar{a}) \bmod pA, \quad \rho(\bar{a}) \in \bigcap_{n=0}^{\infty} A^{p^n}. \tag{5}$$

The element $\rho(\bar{a}) \in A$ is often called the *Teichmüller representative* of $\bar{a} \in A/pA$.

Proof. Given $\bar{a} \in A/pA$, we show that there is a unique $\rho(\bar{a}) \in A$ satisfying the properties (5). This will define the required multiplicative retraction, since for $\bar{b} \in A/pA$ the product $\rho(\bar{a})\rho(\bar{b})$ lifts $\bar{a} \cdot \bar{b}$ and is contained in A^{p^n} for all $n > 0$.

First we show that for all $i \geq 0$ there is a unique element $a_i \in A/p^{i+1}A$ mapping to $\bar{a} \bmod pA$ that is in the image of $A^{p^i} \bmod p^{i+1}A$. Indeed, since A/pA is perfect, we find $x \in A$ with $\bar{a} = x^{p^i} \bmod pA$. For such an x we have $(x + py)^{p^i} = x^{p^i} \bmod p^{i+1}$, hence the class

$$a_i := x^{p^i} \bmod p^{i+1}A$$

does not depend on x. Moreover, since obviously $x^{p^i} \in A^{p^{i-1}}$, by uniqueness we must have

$$x^{p^i} \bmod p^i A = a_i \bmod p^i A/p^{i+1}A = a_{i-1}.$$

Therefore, since A is a strict p-ring, the sequence (a_i) defines an element of $\varprojlim A/p^{i+1}A = A$ mapping to $\bar{a}$ modulo pA. Denote it by $\rho(\bar{a})$.

Now fix $n > 0$ and let $\bar{b}_n \in A/pA$ be the unique element with $\bar{b}_n^{p^n} = \bar{a}$. As above, we find a unique $b_n \in A$ satisfying $\bar{b}_n = b_n \bmod pA$ and such that $b_n \bmod p^{i+1}A$ is in the image of A^{p^i} for all i. But then $b_n^{p^n} \bmod p^{i+1}A$ also comes from A^{p^i} for all i and maps to $\bar{a} \bmod pA$. By uniqueness of the a_i we must have $\rho(\bar{a}) = b_n^{p^n}$. It follows that $\rho(\bar{a}) \in A^{p^n}$ for all n, as required. □

Since A is a strict p-ring, the lemma implies:

Corollary 8.4. *Each $a \in A$ can be uniquely written as a converging sum*

$$a = \sum_{i=0}^{\infty} \rho(\bar{a}_i) p^i$$

with suitable $\bar{a}_i \in A/pA$.

Proof of Theorem 7.5 (2). Consider the multiplicative retractions $\rho_i : A_i/pA_i \to A_i$ given by Lemma 8.3. The characterizing property (5) of the $\rho_i(\bar{a}_i)$ implies that we must have $\phi \circ \rho_1 = \rho_2 \circ \bar{\phi}$. As the A_i are strict p-rings, the only possible definition of ϕ is then by the formula

$$\phi\left(\sum_{i=0}^{\infty} \rho_1(\bar{a}_i) p^i\right) = \sum_{i=0}^{\infty} \rho_2(\bar{\phi}(\bar{a}_i)) p^i.$$

We have to show that this gives a ring homomorphism. Consider two families of variables x_i and y_i indexed by nonnegative integers. The elements

$$x := \sum_{i=0}^{\infty} x_i p^i, \quad y := \sum_{i=0}^{\infty} y_i p^i$$

make sense in the strict p-ring $\mathbf{Z}(\{x_i, y_i\}, p^{-\infty})$ of Example 8.2 whose residue ring is $\mathbf{F}_p[x_i^{p^{-\infty}}, y_i^{p^{-\infty}}]$. Note that $x_i = \rho(x_i)$ and similarly for the y_i, where ρ is the multiplicative retraction of $\mathbf{Z}(\{x_i, y_i\}, p^{-\infty})$. By the previous corollary we find elements $\bar{s}_i \in \mathbf{F}_p[x_i^{p^{-\infty}}, y_i^{p^{-\infty}}]$ such that

$$x + y = \sum_{i=0}^{\infty} \rho(\bar{s}_i) p^i.$$

Now given elements

$$a := \sum_{i=0}^{\infty} \rho_1(\bar{a}_i) p^i, \quad b := \sum_{i=0}^{\infty} \rho_1(\bar{b}_i) p^i$$

in A_1, the maps $x_i \mapsto \rho_1(\bar{a}_i)$, $y_i \mapsto \rho_1(\bar{b}_i)$ induce an $\mathbf{Z}$-algebra homomorphism $\mathbf{Z}[x_i^{p^{-\infty}}, y_i^{p^{-\infty}}] \to A_1$. Passing to p-adic completions we obtain an induced homomorphism $\mathbf{Z}(\{x_i, y_i\}, p^{-\infty}) \to A_1$ of strict p-rings sending x to a and y to b. Modulo p it becomes the natural homomorphism $\mathbf{F}_p[x_i^{p^{-\infty}}, y_i^{p^{-\infty}}] \to A_1/pA_1$ induced by sending $x_i \mapsto \bar{a}_i$, $y_i \mapsto \bar{b}_i$. This homomorphism sends $\bar{s}_j$ to $\bar{s}_j(\{\bar{a}_i\}, \{\bar{b}_i\})$ (we have already noted that this makes sense). Therefore we must have

$$a + b = \sum_{j=0}^{\infty} \rho_1(\bar{s}_j(\{\bar{a}_i\}, \{\bar{b}_i\})) p^j.$$

Now by the first part of the proof we have

$$\phi(a) = \sum_{i=0}^{\infty} \rho_2(\bar{\phi}(\bar{a}_i))p^i, \quad \phi(b) = \sum_{i=0}^{\infty} \rho_2(\bar{\phi}(\bar{b}_i))p^i$$

and therefore

$$\begin{aligned}\phi(a+b) &= \sum_{j=0}^{\infty} \rho_2(\bar{\phi}(s_j(\{\bar{a}_i\},\{\bar{b}_i\})p^j = \sum_{j=0}^{\infty} \rho_2(s_j(\{\bar{\phi}(\bar{a}_i)\},\{\bar{\phi}(\bar{b}_i)\})p^j \\ &= \phi(a) + \phi(b)\end{aligned}$$

since $\bar{\phi}$ is a homomorphism of perfect rings. The proof of multiplicativity is similar. □

Now it remains to give the *proof of Theorem 7.5 (1).* Notice that Example 8.2 gives the answer for perfect rings of the form $\mathbf{F}_p[\{x_\alpha^{p^{-\infty}}\}]$. But since every perfect ring is a quotient of some $\mathbf{F}_p[\{x_\alpha^{p^{-\infty}}\}]$ with a suitable system $\{x_\alpha\}$ of indeterminates, the statement follows from:

Lemma 8.5. *Assume given a surjective homomorphism $\bar{\phi} : B_1 \twoheadrightarrow B_2$ of perfect rings of characteristic $p > 0$. If there exists a strict p-ring A_1 with $A_1/pA_1 \cong B_1$, there is also a strict p-ring A_2 with $A_2/pA_2 \cong B_2$.*

Proof. Consider the subset

$$I := \left\{ \sum_{i=0}^{\infty} \rho_1(\bar{c}_i)p^i \ : \ c_i \in \ker(\bar{\phi}) \right\} \subset A_1$$

where ρ_1 is the multiplicative retraction. By an argument analogous to the verification of additivity in the previous proof we see that the fact that $\ker(\bar{\phi})$ is an ideal in B_1 implies that I is an ideal in A_1. Defining $A_2 := A_1/I$ we certainly have $A_2/pA_2 \cong B_2$. The retraction ρ_1 induces a multiplicative retraction $\rho_2 : B_2 \to A_2$, and the p-adic filtration on A_1 induces one on A_2. Moreover, we may write each element of A_2 uniquely as a converging sum

$$\sum_{i=0}^{\infty} \rho_2(\bar{a}_i)p^i$$

with $\bar{a}_i \in B_2$. This implies that A_2 is a strict p-ring. □

Remark 8.6. By the representation as in Corollary 8.4 we may identify the elements of a strict p-ring A with perfect residue field k with infinite sequences of elements of k, i.e. elements of the direct product $k^{\mathbf{N}}$. In fact, the map $A \to k^{\mathbf{N}}$ given by

$$\sum_{i=0}^{\infty} \rho(\bar{a}_i)p^i \mapsto (\bar{a}_i^{p^i})$$

is a bijection and and by transport of structure we obtain a ring structure on $k^{\mathbf{N}}$ (different from the usual one) that equips it with the structure of a strict p-ring. The advantage of this normalization is that given $(\bar{a}_i), (\bar{b}_i) \in k^{\mathbf{N}}$, the addition and multiplication maps are given by

$$(\bar{a}_i) + (\bar{b}_i) = (\sigma_i((\bar{a}_i), (\bar{b}_i))), \quad (\bar{a}_i) \cdot (\bar{b}_i) = (\pi_i((\bar{a}_i), (\bar{b}_i)))$$

where $\sigma_i, \pi_i \in \mathbf{Z}[\{x_i\}, \{y_i\}]$ are polynomials that can be determined explicitly. This is an improvement with respect to the previous construction where we had to use elements of $\mathbf{Z}(\{x_i, y_i\}, p^{-\infty})$. For a proof see e.g. Serre, Corps locaux, §II.6.

We denote by $W(k)$ the set $k^{\mathbf{N}}$ equipped with the above ring structure; it is the ring of *Witt vectors* of k. There are two important operations on $W(k)$ that are useful for applications:

$$F : (\bar{a}_i) \mapsto (\bar{a}_i^p)$$
$$V : (\bar{a}_i) \mapsto (0, \bar{a}_1, \bar{a}_2, \dots)$$

called the Frobenius and the Verschiebung (German for 'shifting'), respectively. Thus V shifts each sequence to the right, adding a zero on the left; it is additive but not multiplicative. On the other hand, F is a ring homomorphism. It is straightforward to check from the construction that $FV = VF$ is the multiplication-by-p map.