The structure theory of complete local rings

Introduction

In the study of commutative Noetherian rings, localization at a prime followed by completion at the resulting maximal ideal is a way of life. Many problems, even some that seem "global," can be attacked by first reducing to the local case and then to the complete case. Complete local rings turn out to have extremely good behavior in many respects. A key ingredient in this type of reduction is that when R is local, $\widehat{R}$ is local and faithfully flat over R.

We shall study the structure of complete local rings. A complete local ring that contains a field always contains a field that maps onto its residue class field: thus, if (R, m, K) contains a field, it contains a field K_0 such that the composite map $K_0 \subseteq R \twoheadrightarrow R/m = K$ is an isomorphism. Then $R = K_0 \oplus_{K_0} m$, and we may identify K with K_0. Such a field K_0 is called a *coefficient field* for R.

The choice of a coefficient field K_0 is *not unique* in general, although in positive prime characteristic p it is unique if K is perfect, which is a bit surprising. The existence of a coefficient field is a rather hard theorem. Once it is known, one can show that every complete local ring that contains a field is a homomorphic image of a formal power series ring over a field. It is also a module-finite extension of a formal power series ring over a field. This situation is analogous to what is true for finitely generated algebras over a field, where one can make the same statements using polynomial rings instead of formal power series rings. The statement about being a module-finite extension of a power series ring is an analogue of the Noether normalization theorem. A local ring (R, m, K) that contains a field is called *equicharacteristic*, because R contains a field if and only if R and K have the same characteristic. (It is clear that if $K \subseteq R$ they must have the same characteristic. If K has characteristic 0, it is clear that R does, and contains a copy of $\mathbb{Z}$. Since no nonzero integer vanishes in R/m, every nonzero integer is a unit in R, which gives a unique map of $\mathbb{Q} = (\mathbb{Z} - \{0\})^{-1}\mathbb{Z}$ into R by the universal mapping property of localization. On the other hand, if R has positive prime characteristic $p > 0$, it clearly contains a copy of $\mathbb{Z}/p\mathbb{Z}$.)

Local rings that are not equicharacteristic are called *mixed characteristic*. The characteristic of the residue class field of such a ring is always a positive prime integer p. The characteristic of the ring is either 0, which is what it will be in the domain case, or else a power of p, p^k, with $k > 1$.

The term *discrete valuation ring*, abbreviated DVR, will be used for a local domain V, not a field, whose maximal ideal is principal, say tV, $t \neq 0$. It is then the case that every nonzero element of V is uniquely expressible in the form ut^n, where u is a unit, and every ideal is consequently principal. (Technically, these rings should be called *rank one* discrete valuation domains or Noetherian discrete valuation domains.)

A local domain of mixed characteristic will have characteristic 0, while its residue class field has positive prime characteristic p. An example is the ring of p-adic integers, which is the completion of the localization of the integers at the prime ideal generated by the positive prime integer p. A formal power series ring over the p-adic integers also has mixed characteristic.

The structure of complete local rings in mixed characteristic is more complicated, but the theory has been fully worked out: if $(R,\, m)$ has mixed characteristic, it is a homomorphic image of a formal power series ring over a complete discrete valuation ring (V, pV) whose maximal ideal is generated by a positive prime integer p. If a mixed characteristic local ring is a domain, it is module-finite over a formal power series ring over such a ring $V \subseteq R$ such that the induced map of residue class fields $V/pV \to R/m$ is an isomorphism. V is called a *coefficient ring for* R. When R is not a domain the statements are more complicated, but the situation is completely understood.

A local ring is regular if and only if its completion is regular: completing does not change the Krull dimension and does not change the embedding dimension. The associated graded ring of the maximal ideal is also unchanged. These facts are discussed in greater detail in the sequel. Complete regular local rings can be classified. A complete regular local ring that contains a field is simply the formal power series ring in finitely many variables over a field. The situation in mixed characteristic is more complicated, but also well understood. If V is a coefficient ring, the complete regular ring R of Krull dimension d is either a formal power series ring $V[[x_1, \ldots, x_{d-1}]]$, or it will have the form $T/(p-f)$, where $T = V[[x_1, \ldots, x_d]]$ has maximal ideal $m_T = (p, x_1, \ldots, x_d)T$, and $f \in m_T^2$.

An important property of complete local rings is that they satisfy Hensel's lemma. Let $(R,\, m,\, K)$ be complete local and let f be a monic polynomial over R. If $u \in R[x]$, we write $\overline{u}$ for the polynomial in $K[x]$ obtained by taking residue classes of coefficients of u modulo m. Suppose that $\overline{f}$ factors $\overline{f} = GH$ in $K[x]$, where G and H are relatively prime monic polynomials. Hensel's lemma asserts that this factorization lifts uniquely to $R[x]$. That is, there are monic polynomials $g,\, h \in R[x]$ such that $f = gh$ and $\overline{g} = G$ while $\overline{h} = H$.

This is a very powerful result. For example, consider the formal power series ring $\mathbb{C}[[z]]$ in one variable over the complex numbers, and consider the polynomial equation $x^2-(1+z)$. Mod the maximal ideal $zC[[z]]$, this equation becomes $x^2 - 1 = (x-1)(x+1)$. Hensel's lemma now implies that $x^2-(1+z)$ factors as $\big(x-\alpha(z)\big)\big(x-\beta(z)\big)$ where $\alpha(z), \beta(z) \in \mathbb{C}[[z]]$. Of course, these must be square roots of $1+z$, so that $\beta = -\alpha$. Hensel's lemma also implies that their constant terms must be 1 and -1. Lifting the factorization yields the existence of power series square roots for $1 + z$. Of course, we know this from Newton's binomial theorem, which gives an explicit formula for $(1 + z)^{1/2}$. But Hensel's lemma provides solutions to much more complicated problems for which no formula is readily available. This result is closely related to the implicit function theorem.

Here is a simple example of a local ring that contains a field but does not have a coefficient field. Let V be the localization of the polynomial ring $\mathbb{R}[t]$ in one variable over the real numbers $\mathbb{R}$ at the prime ideal $P = (t^2 + 1)$, and let $m = PV$. Then V/PV is the fraction field of $\mathbb{R}[t]/(t^2 + 1) \cong \mathbb{C}$, which is $\mathbb{C}$. But $S \subseteq \mathbb{R}(t)$ does not contain any element

whose square is -1: the square of a non-constant rational function is non-constant, and the square of a real scalar cannot be -1. Note that V is a DVR.

The completion of $\widehat{V}$ of V is also a DVR with residue class field $\mathbb{C}$, and so it must contain a square root of -1. Can you see what it is?

Hensel's Lemma and coefficient fields in equal characteristic 0

We begin our analysis of the structure of complete local rings by proving Hensel's lemma.

Theorem (Hensel's lemma). *Let (R, m, K) be a complete local ring and let f be a monic polynomial of degree d in $R[x]$. Suppose that $\overline{u}$ denotes the image of $u \in R[x]$ under the ring homomorphism $R[x] \twoheadrightarrow K[x]$ induced by $R \twoheadrightarrow K$. If $\overline{f} = GH$ where $G, H \in K[x]$ are monic of degrees s and t, respectively, and G and H are relatively prime in $K[x]$, then there are unique monic polynomials $g, h \in R[x]$ such that $f = gh$ and $\overline{g} = g$ while $\overline{h} = h$.*

Proof. Let F_n denote the image of f in $(R/m^n)[x]$. We recursively construct monic polynomials $G_n \in (R/m^n)[x]$, $H_n \in (R/m^n)[x]$ such that $F_n = G_n H_n$ for all $n \geq 1$, where G_n and H_n reduce to G and H, respectively, mod m, and show that F_n and G_n are unique. Note that it will follow that for all n, G_n has the same degree as G, namely s, and H_n has the same degree as H, namely t, where $s + t = d$. The uniqueness implies that mod m^{n-1}, G_n, H_n become G_{n-1}, H_{n-1}, respectively. This yields that the sequence of coefficients of x^i in the G_n is an element of $\varprojlim_n (R/m^n) = R$, since R is complete. Using the coefficients determined in this way, we get a polynomial g in $R[x]$, monic of degree s. Similarly, we get a polynomial $h \in R[x]$, monic of degree t. It is clear that $\overline{g} = G$ and $\overline{h} = H$, and that $f = gh$, since this holds mod m^n for all n: thus, every coefficient of $f - gh$ is in $\bigcap_n m^n = (0)$.

It remains to carry through the recursion, and we have $G_1 = G$ and $H_1 = H$ from the hypothesis of the theorem. Now assume that G_n and H_n have been constructed and shown unique for a certain $n \geq 1$. We must construct G_{n+1} and H_{n+1} and show that they are unique as well. It will be convenient to work mod m^{n+1} in the rest of the argument: replace R by R/m^{n+1}. Construct G^*, H^* in $R[x]$ by lifting each coefficient of G_n and H_n respectively, but such that the two leading coefficients occur in degrees s and t respectively and are both 1. Then, mod m^n, $F \equiv G^* H^*$, i.e., $\Delta = F - G^* H^* \in m^n R[x]$. We want to show that there are unique choices of $\delta \in m^n R[x]$ of degree at most $s-1$ and $\epsilon \in m^n R[x]$ of degree at most $t-1$ such that $F - (G^* + \delta)(H^* + \epsilon) = 0$, i.e., such that $\Delta = \epsilon G^* + \delta H^* + \delta\epsilon$. Since $\delta, \epsilon \in m^n R[x]$, $n \geq 1$, their product is in $m^{2n} R[x] = 0$, since $2n \geq n + 1$. Thus, our problem is to find such ϵ and δ with $\Delta = \epsilon G^* + \delta H^*$. Now, G and H generate the unit ideal in $K[x]$, and $R[x]_{\mathrm{red}} = K[x]$. It follows that G^* and H^* generate the unit ideal in $R[x]$, and so we can write $1 = \alpha G^* + \beta H^*$. Multiplying by Δ, we get $\Delta = \Delta\alpha G^* + \Delta\beta H^*$. Then $\Delta\alpha$ and $\Delta\beta$ are in $m^n R[x]$, but do not yet satisfy our degree requirements. Since H^* is monic, we can divide $\Delta\alpha$ by H^* to get a quotient γ and remainder ϵ, i.e., $\Delta\alpha = \gamma H^* + \epsilon$, where the degree of ϵ is $\leq t - 1$. If we consider this mod m^n, we have $0 \equiv \gamma H_n + \epsilon$, from which it follows that γ, $\epsilon \in m^n R[x]$. Then $\Delta = \epsilon G^* + \delta H^*$ where $\delta = \gamma G^* + \Delta\beta$. Since Δ and ϵG^* both have degree $< n$, so does δH^*, which implies that the degree of δ is $\leq s - 1$.

Finally, suppose that we also have $\Delta = \epsilon' G^* + \delta' H^*$ where ϵ' has degree $\leq t-1$ and δ' has degree $\leq s-1$. Subtracting, we get an equation $0 = \mu G^* + \nu H^*$ where the degree of $\mu = \epsilon - \epsilon'$ is $\leq t-1$ and the degree of $\nu = \delta - \delta'$ is $\leq s-1$. Since G^* is a unit considered mod H^*, it follows that $\mu \in (H^*)$, i.e., that H^* divides μ. But H^* is monic, and so this cannot happen unless $\mu = 0$: the degree of μ is too small. Similarly, $\nu = 0$. $\square$

Remark. This result does not need that R be Noetherian. The same proof, verbatim, shows that if (R, m) is a quasilocal ring that is m-adically separated and complete (so that $R \cong \varprojlim_n R/m^n$), the same result holds.

We can now deduce:

Theorem. *Let (R, m, K) be a complete local ring that contains a field of characteristic 0. Then R has a coefficient field. In fact, R will contain a maximal subfield, and any such subfield is a coefficient field.*

Proof. Let $\mathcal{S}$ be the set of all subrings of R that happen to be fields. By hypothesis, this set is nonempty. Given a chain of elements of $\mathcal{S}$, the union is again a subring of R that is a field. By Zorn's lemma, $\mathcal{S}$ will have a maximal element K_0. To complete the proof of the theorem, we shall show that K_0 maps isomorphically onto K. Obviously, we have a map $K_0 \subseteq R \twoheadrightarrow R/m = K$, and so we have a map $K_0 \to K$. This map is automatically injective: call the image K_0'. To complete the proof, it suffices to show that it is surjective.

If not, let θ be an element of K not in the image of K_0. We consider two cases: the first is that θ is transcendental over K_0'. Let t denote an element of R that maps to θ. Then $K_0[t]$ is a polynomial subring of R, and every nonzero element is a unit: if some element were in m, then working mod m we would get an equation of algebraic dependence for θ over K_0' in K. By the universal mapping property of localization, the inclusion $K_0[t] \subseteq R$ extends to a map $K_0(t) \subseteq R$, which is necessarily an inclusion. This yields a subfield of R larger than K_0, a contradiction.

We now consider the case where θ is algebraic over the image of K_0. Consider the minimal polynomial of θ over K_0', and let f be the corresponding polynomial with coefficients in $K_0[x] \subseteq R[x]$. Modulo m, this polynomial factors as $(x-\theta)H(x)$, where these are relatively prime because θ is separable over K_0': this is the only place in the argument where we use that the field has characteristic 0. The factorization lifts uniquely: we have $f = (x-t)h(x)$ where $t \in R$ is such that $t \equiv \theta \bmod m$. That is, $f(t) = 0$. We claim that the map $K_0[t] \subseteq R \twoheadrightarrow R/m$, whose image is $K_0'[\theta]$, gives an isomorphism of $K_0[t]$ with $K_0'[\theta]$: we only need to show injectivity. But if $P(x) \in K_0[x]$ is a polynomial such that $P(t)$ maps to 0, then f divides $P(x)$, which implies that $P(t) = 0$. Since $K_0[t] \cong K_0'[\theta]$ (both are $\cong K_0[t]/\big(f(t)\big)$), $K_0[t]$ is a field contained in R that is strictly larger than K_0, a contradiction. $\square$

Remark. If R is a complete local domain of positive prime characteristic $p > 0$, the same argument shows that R contains a maximal subfield K_0, and that K is purely inseparable and algebraic over the image of K_0.

Coefficient fields in characteristic p when the residue class field is perfect

We can get a similar result easily in characteristic $p > 0$ if $K = R/m$ is perfect, although the proof is completely different.

Theorem. *Let (R, m, K) be a complete local ring of positive prime characteristic p. Suppose that K is perfect. Let $R^{p^n} = \{r^{p^n} : r \in R\}$ for every $n \in \mathbb{N}$. Then $K_0 = \bigcap_{n=0}^{\infty} R^{p^n}$ is a coefficient field for R, and it is the only coefficient field for R.*

Proof. Consider any coefficient field L for R, assuming for the moment that one exists. Then $L \cong K$, and so L is perfect. Then

$$L = L^p = \cdots = L^{p^n} = \cdots,$$

and so for all n,

$$L \subseteq L^{p^n} \subseteq R^{p^n}.$$

Therefore, $L \subseteq K_0$. If we know that K_0 is a field, it follows that $L = K_0$, proving uniqueness.

It therefore suffices to show that K_0 is a coefficient field for K. We first observe that K_0 meets m only in 0. For if $u \in K_0 \cap m$, then u is a p^n th power for all n. But if $u = v^{p^n}$ then $v \in m$, so $u \in \cap_n m^{p^n} = (0)$.

Thus, every element of $K_0 - \{0\}$ is a unit of R. Now if $u = v^{p^n}$, then $1/u = (1/v)^{p^n}$. Therefore, the inverse of every nonzero element of K_0 is in K_0. Since K_0 is clearly a ring, it is a subfield of R.

Finally, we want to show that given $\theta \in K$ some element of K_0 maps to θ. Let r_n denote an element of R that maps to $\theta^{1/p^n} \in K$. Then $r_n^{p^n}$ maps to θ. We claim that $\{r_n^{p^n}\}_n$ is a Cauchy sequence in R, and so has a limit r. To see this, note that r_n and r_{n+1}^p both map to θ^{1/p^n} in K, and so $r_n - r_{n+1}^p$ is in m. Taking p^n powers, we find that

$$r_n^{p^n} - r_{n+1}^{p^{n+1}} \in m^{p^n}.$$

Therefore, the sequence is Cauchy, and has a limit $r \in R$. It is clear that r maps to θ. Therefore, it suffices to show that $r \in R^{p^k}$ for every k. But

$$r_k, r_{k+1}^p, \ldots, r_{k+h}^{p^h} \cdots$$

is a sequence of the same sort for the element θ^{1/p^k}, and so is Cauchy and has a limit s_k in R. But $s_k^{p^k} = r$ and so $r \in R^{p^k}$ for all k. $\square$

Coefficient fields and structure theorems

Before pursuing the issue of the existence of coefficient fields and coefficient rings further, we show that the existence of a coefficient field implies that the ring is a homomorphic image of a power series ring in finitely many variables over a field, and is also a module-finite extension of such a ring.

We begin as follows:

Proposition. *Let R be separated and complete in the I-adic topology, where I is a finitely generated ideal of R, and let M be an I-adically separated R-module. Let $u_1, \ldots, u_h \in M$ have images that span M/IM over R/I. Then $u_1, \ldots, u_h$ span M over R.*

Proof. Since $M = Ru_1 + \cdots + Ru_h + IM$, we find that for all n,

$$(*) \qquad I^n M = I^n u_1 + \cdots + I^n u_n + I^{n+1} M.$$

Let $u \in M$ be given. Then u can be written in the form $r_{01}u_1 + \cdots + r_{0h}u_h + v_1$ where $v_1 \in IM$. Therefore $v_1 = r_{11}u_1 + \cdots r_{1h}u_h + v_2$ where the $r_{1j} \in IM$ and $v_2 \in I^2M$. Then

$$u = (r_{01} + r_{11})u_1 + \cdots + (r_{0n} + r_{1h})u_h + v_2,$$

where $v_2 \in I^2M$. By a straightforward induction on n we obtain, for every n, that

$$u = (r_{01} + r_{11} + \cdots + r_{n1})u_1 + \cdots + (r_{0h} + r_{1h} + \cdots + r_{nh})u_h + v_{n+1}$$

where every $r_{jk} \in I^j$ and $v_{n+1} \in I^{n+1}M$. In the recursive step, the formula $(*)$ is applied to the element $v_{n+1} \in I^{n+1}M$. For every k, $\sum_{j=0}^{\infty} r_{jk}$ represents an element s_k of the complete ring R. We claim that

$$u = s_1u_1 + \cdots + s_hu_h.$$

The point is that if we subtract

$$(r_{01} + r_{11} + \cdots + r_{n1})u_1 + \cdots + (r_{0h} + r_{1h} + \cdots + r_{nh})u_n$$

from u we get $v_{n+1} \in I^{n+1}M$, and if we subtract it from

$$s_1u_1 + \cdots + s_hu_h$$

we also get an element of $I^{n+1}M$. Therefore,

$$u - (s_1u_1 + \cdots + s_hu_h) \in \bigcap_n I^{n+1}M = 0,$$

since M is I-adically separated. $\square$

Remark. We tacitly used in the argument above that if $r_{jk} \in I^j$ for $j \geq n+1$ then

$$r_{n+1,k} + r_{n+2,k} + \cdots + r_{n+t,k} + \cdots \in I^{n+1}.$$

This actually requires an argument. If I is finitely generated, then I^{n+1} is finitely generated by the monomials of degree $n+1$ in the generators of I, say, $g_1, \ldots, g_d$. Then

$$r_{n+1+t,k} = \sum_{\nu=1}^{d} q_{t\nu} g_\nu,$$

with every $q_{t\nu} \in I^t$, and

$$\sum_{t=0}^{\infty} r_{n+1+t,k} = \sum_{\nu=1}^{d} (\sum_{t=0}^{\infty} q_{t\nu}) g_\nu.$$

We also note:

Proposition. *Let $f : R \to S$ be a ring homomorphism, and supposed that S is J-adically complete and separated for an ideal $J \subseteq S$ and that $I \subseteq R$ maps into J. Then there is a unique induced homomorphism $\widehat{R}^I \to S$ that is continuous (i.e., preserves limits of Cauchy sequences in the appropriate ideal-adic topology).*

Proof. $\widehat{R}^I$ is the ring of I-adic Cauchy sequences mod the ideal of sequences that converge to 0. The continuity condition forces the element represented by $\{r_n\}_n$ to map to

$$\lim_{n\to\infty} f(r_n)$$

(Cauchy sequences map to Cauchy sequences: if $r_m - r_n \in I^N$, then $f(r_m) - f(r_n) \in J^N$, since $f(I) \subseteq J$). It is trivial to check that this is a ring homomorphism that kills the ideal of Cauchy sequences that converge to 0, which gives the required map $\widehat{R}^I \to S$. $\square$

A homomorphism of quasilocal rings $h : (A, \mu, \kappa) \to (R, m, K)$ is called a *local homomorphism* if $h(\mu) \subseteq m$. If A is a local domain, not a field, the inclusion of A in its fraction field is not local. If A is a local domain, any quotient map arising from killing a proper ideal is local. A local homomorphism induces a homomorphism of residue class fields $\kappa = A/\mu \to R/m = K$.

Proposition. *Let (A, μ, κ) and (R, m, K) be complete local rings, and $h : A \to R$ a local homomorphism. Suppose that $f_1, \ldots, f_n \in m$ together with μR generate an m-primary ideal. Then:*

(a) *There is a unique continuous homomorphism $h : A[[X_1, \ldots, X_n]] \to R$ extending the A-algebra map $A[X_1, \ldots, X_n]$ taking X_i to f_i for all i.*

(b) *If K is a finite algebraic extension of κ, then R is module-finite over the image of $A[[X_1, \ldots, X_n]]$.*

(c) *If $\kappa \to K$ is an isomorphism, and $\mu R + (f_1, \ldots, f_n)R = m$, then the map h described in (a) is surjective.*

Proof. (a) This is immediate from the preceding Proposition, since $(X_1, \ldots, X_n)$ maps into m.

(b) The expansion of the maximal ideal $\mathcal{M} = (\mu, X_1, \ldots, X_n)$ of $A[[X_1, \ldots, X_n]]$ to R is $\mu R + (f_1, \ldots, f_n)R$, which contains a power of m, say m^N. Thus, $R/\mathcal{M}R$ is a quotient of R/m^N and has finite length: the latter has a filtration whose factors are the finite-dimensional K-vector spaces m^i/m^{i+1}, $0 \leq i \leq N-1$. Since K is finite-dimensional over κ, it follows that $R/\mathcal{M}R$ is finite-dimensional over $A[[X_1, \ldots, X_n]]/\mathcal{M} = \kappa$. Choose elements of R whose images in $R/\mathcal{M}R$ span it over κ. By the earlier Theorem, these elements span R as an $A[[X_1, \ldots, X_n]]$-module. We are using that R is $\mathcal{M}$-adically separated, but this follows because $\mathcal{M}R \subseteq m$, and R is m-adically separated.

(c) We repeat the argument of the proof of part (b), noting that now $R/\mathcal{M}R \cong K \cong \kappa$, so that $1 \in R$ generates R as an $A[[X_1, \ldots, X_n]]$ module. But this says that R is a cyclic $A[[X_1, \ldots, X_n]]$-module spanned by 1, which is equivalent to the assertion that $A[[X_1, \ldots, X_n]] \to R$ is surjective. $\square$

We have now done all the real work needed to prove the following:

Theorem. *Let (R, m, K) be a complete local ring with coefficient field $K_0 \subseteq K$, so that $K_0 \subseteq R \twoheadrightarrow R/m = K$ is an isomorphism. Let $f_1, \ldots, f_n$ be elements of m generating an ideal primary to m. Let $K_0[[X_1, \ldots, X_n]] \to R$ be constructed as in the preceding Proposition, with X_i mapping to f_i and with $A = K_0$. Then:*

(a) *R is module-finite over $K_0[[X_1, \ldots, X_n]]$.*

(b) *Suppose that $f_1, \ldots, f_n$ generate m. Then the homomorphism $K_0[[x_1, \ldots, x_n]] \to R$ is surjective. (By Nakayama's lemma, the least value of n that may be used is the dimension as a K-vector space of m/m^2.)*

(c) *If $d = \dim(R)$ and $f_1, \ldots, f_d$ is a system of parameters for R, the homomorphism*

$$K_0[[x_1, \ldots, x_d]] \to R$$

is injective, and so R is a module-finite extension of a formal power series subring.

Proof. (a) and (b) are immediate from the preceding Proposition. For part (c), let $\mathfrak{A}$ denote the kernel of the map $K_0[[x_1, \ldots, x_d]] \to R$. Since R is a module-finite extension of the ring $K_0[[x_1, \ldots, x_d]]/\mathfrak{A}$, $d = \dim(R) = \dim(K_0[[x_1, \ldots, x_d]]/\mathfrak{A})$. But we know that $\dim(K_0[[x_1, \ldots, x_d]]) = d$. Killing a nonzero prime in a local domain must lower the dimension. Therefore, we must have that $\mathfrak{A} = (0)$. $\square$

Thus, when R has a coefficient field K_0 and $f_1, \ldots, f_d$ are a system of parameters, we may consider a formal power series

$$\sum_{\nu \in \mathbb{N}^d} c_\nu f^\nu,$$

where $\nu = (\nu_1, \ldots, \nu_d)$ is a multi-index, the $c_\nu \in K_0$, and f^ν denotes $f_1^{\nu_1} \cdots f_d^{\nu_d}$. Because R is complete, this expression represents an element of R. Part (c) of the preceding Theorem implies that this element is not 0 unless all of the coefficients c_ν vanish. This fact is sometimes referred to as the *analytic independence of a system of parameters*. The

elements of a system of parameters behave like formal indeterminates over a coefficient field. Formal indeterminates are also referred to as *analytic indeterminates*.

Regular rings in equal characteristic

We next want to prove that a local ring is regular if and only if its completion is regular, and that a complete regular local ring containing a coefficient field is a formal power series ring over a field. We first observe the following:

Lemma. *Let $R \to S$ be a map of rings such that S is flat over R. Then:*
(a) *For every prime Q of S, if Q lies over P in R then $R_P \to S_Q$ is faithfully flat.*
(b) *If S is faithfully flat over R, then for every prime P of R there exists a prime Q of S lying over P.*
(c) *If S is faithfully flat over R and $P_n \supset \cdots \supset P_0$ is a strictly decreasing chain of primes of R then there exists Q_n lying over P_n in S; moreover, for every choice of Q_n there is a (strictly decreasing) chain $Q_n \supset \cdots \supset Q_0$ such that Q_i lies over P_i for every i.*
(d) *If S is faithfully flat over R then* $\dim(R) \leq \dim(S)$.

Proof. (a) We first show that S_Q is flat over R_P. Recall that if W, M are R_P modules, $W \otimes_R M \to W \otimes_{R_P} M$ is an isomorphism. (Briefly, if $s \in R - P$, in $W \otimes_R M$ we have that $(1/s)w \otimes u = (1/s)w \otimes s(1/s)u = (1/s)sw \otimes (1/s)u = w \otimes (1/s)u$, so that inverses of elements of $R - P$ automatically pass through the tensor symbol in $W \otimes_R M$). Thus, to show that if $N \hookrightarrow M$ is an injection of R_P-modules then $S_Q \otimes_{R_P} M \to S_Q \otimes_{R_P} M$ is injective, it suffices to show that $S_Q \otimes_R N \to S_Q \otimes_R M$ is injective. But since S_Q is flat over S and S is flat over R, we have that S_Q is flat over R, and the needed injectivity follows.

Thus S_Q is flat over R_P. Since the maximal ideal PR_P maps into S_Q, faithful flatness is then clear.

(b) When S is faithfully flat over R, R injects into S and the contraction of IS to R is I for every ideal I of R. (If $\mathfrak{A}$ is the kernel of $R \to S$, when we apply $S \otimes_R \_$ to $\mathfrak{A} \hookrightarrow R$ we get an injection $\mathfrak{A} \otimes S \hookrightarrow S$ whose image is $\mathfrak{A}S$, which is (0). But then $\mathfrak{A} \otimes_R S = (0)$, which implies that $\mathfrak{A} = 0$. By base change, $(R/I) \otimes_R S = S/IS$ is faithfully flat over R/I for every ideal I of R, and so $R/I \to S/IS$ is injective, which means that $IS \cap R = I$.) Hence, for every prime P, the contraction of PS is disjoint from $R - P$, and so PS is disjoint from the image of $R - P$ in S. Thus, there is a prime ideal Q of S that contains PS and is disjoint from the image of $R - P$, and this means that Q lies over P in R.

(c) The existence of Q_n follows from part (b). By a straightforward induction on n, it suffices to show the existence of $Q_{n-1} \subseteq Q_n$ and lying over P_{n-1}. Then, once we have found $Q_i, \ldots, Q_n$, the problem of finding Q_{i-1} is of exactly the same sort. Consider the map $R_{P_n} \to R_{Q_n}$, which is faithfully flat by part (a). Thus, there exists a prime $\mathcal{Q}_{n-1}$ of R_{Q_n} lying over $P_{n-1}R_{P_n}$. Let Q_{n-1} be the contraction of $\mathcal{Q}_{n-1}$ to R. Since $\mathcal{Q}_{n-1} \subseteq Q_nR_{Q_n}$, we have that $Q_{n-1} \subseteq Q_n$. Since $\mathcal{Q}_{n-1}$ contracts to $P_{n-1}R_{P_n}$, it contracts to P_{n-1} in R, and so Q_{n-1} contracts to P_{n-1} as well.

(d) Given a finite strictly decreasing chain in R, there is a chain in S that lies over it, by part (c), and the inclusions are strict for the chain in S since they are strict upon contraction to R. It follows that $\dim(S) \geq \dim(R)$. $\square$

All of the completions referred to in the next result are m-adic completions.

Proposition. *Let (R, m, K) be a local ring and let $\widehat{R}$ be its completion.*

(a) *The maximal $m_{\widehat{R}}$ ideal of $\widehat{R}$ is the expansion of m to $\widehat{R}$. Hence, $m^n\widehat{R} = m_{\widehat{R}}^n$ for all n.*

(b) *The completion $\widehat{I}$ of any ideal I of R may be identified with $I\widehat{R}$. In particular, $m_{\widehat{R}}$ may be identified with $\widehat{m}$.*

(c) *Expansion and contraction gives a bijection between m-primary ideals of R and $\widehat{m}$-primary ideals of $\widehat{R}$. If $\mathfrak{A}$ is an m-primary ideal of R, $R/\mathfrak{A} \cong \widehat{R}/\widehat{\mathfrak{A}}$.*

(d) *$\dim(R) = \dim(\widehat{R})$, and every system of parameters for R is a system of parameters for $\widehat{R}$.*

(e) *The embedding dimension of R, which is $\dim_K(m/m^2)$, is the same as the embedding dimension of $\widehat{R}$.*

Proof. Part (b) is a consequence of the fact that completion is an exact functor on finitely generated R-modules that agrees with $\widehat{R} \otimes_R \_$: since we have an injection $I \to R$, we get injections $\widehat{I} \hookrightarrow \widehat{R}$ and $I \otimes_R \widehat{R} \hookrightarrow R \otimes_R \widehat{R} \cong \widehat{R}$. The image of $I \otimes_R \widehat{R}$ is $I\widehat{R}$, so that $I \otimes_R \widehat{R} \cong I\widehat{R} \cong \widehat{I} \hookrightarrow \widehat{R}$, as claimed. When $I = m$, the short exact sequence $0 \to m \to R \to K \to 0$ remains exact upon completion, and $\widehat{K} \cong K$, which shows that $m_{\widehat{R}} = m\widehat{R}$, proving (a). When $I = \mathfrak{A}$ is m-primary, we have that $0 \to \mathfrak{A} \to R \to R/\mathfrak{A}$ is exact, and so we get an exact sequence of completions

$$0 \to \widehat{\mathfrak{A}} \to \widehat{R} \to \widehat{R/\mathfrak{A}} \to 0.$$

Because there is a power of m contained in $\mathfrak{A}$, there is a power of m that kills $R/\mathfrak{A}$, and it follows that the natural map $R/\mathfrak{A} \hookrightarrow \widehat{R/\mathfrak{A}}$ is an isomorphism. The bijection between m-primary ideals of R and $\widehat{m}$-primary ideals of $\widehat{R}$ may be seen as follows: the ideals of R containing m^n correspond bijectively to the ideals of R/m^n, while the ideals of $\widehat{R}$ containing $\widehat{m}^n = m^n\widehat{R}$ correspond bijectively to the ideals of $\widehat{R}$ containing $\widehat{m}^n$. But $R/m^n \cong \widehat{R}/\widehat{m}^n$.

We have that $\dim(\widehat{R}) \geq \dim(R)$ since $\widehat{R}$ is faithfully flat over R. But if $x_1, \ldots, x_n$ is a system of parameters in R, so that $m^N \subseteq (x_1, \ldots, x_n)R$, then $\widehat{m}^n \subseteq (x_1, \ldots, x_n)\widehat{R}$. It follows that $\dim(\widehat{R}) \leq n = \dim(R)$, and so $\dim(\widehat{R}) = \dim(R) = n$, and it is now clear that the images of $x_1, \ldots, x_n$ in $\widehat{R}$ form a system of parameters.

Now, $\widehat{m}/\widehat{m}^2 \cong m\widehat{R}/m^2\widehat{R} \subseteq \widehat{R}/m^2\widehat{R} \cong R/m^2$, and it follows that $\widehat{m}/\widehat{m}^2 \cong m/m^2$, as required. $\square$

Remark. Let K be, for simplicity, an algebraically closed field, and let R be a finitely generated K-algebra, so that the maximal spectrum of R can be thought of as an closed algebraic set X in some $\mathbb{A}_k^N$. To get an embedding, one maps a polynomial ring over K onto R: the least integer N such that $K[x_1, \ldots, x_N]$ can be mapped onto on R as

a K-algebra is the smallest integer such that X can be embedded as a closed algebraic set in $\mathbb{A}^N_K$. In this context it is natural to refer to N as the embedding dimension of X, and by extension, of the ring R. We now let K be any field. It is natural to extend this terminology to complete rings containing a field: the integer $\dim_K(m/m^2)$ gives the least N such that $K[[x_1, \ldots, x_n]]$ can be mapped onto the complete local ring (R, m, K) when R contains a field (in which case, as we shall soon see, it has a coefficient field). The term *embedding dimension*, which is reasonably natural for complete equicharacteristic local rings, has been extended to all local rings.

Corollary. *A local ring R is regular if and only if $\widehat{R}$ is regular.*

Proof. By definition, R is regular if and only if it dimension and embedding dimension are equal. The result is therefore clear from parts (d) and (e) of the preceding Proposition. □

We now prove the following characterization of equicharacteristic regular local rings, modulo the final step of proving the existence of coefficient fields in general in characteristic $p > 0$.

Corollary. *Suppose that (R, m, K) be an equicharacteristic local ring. Then R is regular of Krull dimension n if and only if $\widehat{R}$ is isomorphic to a formal power series ring $K[[X_1, \ldots, X_n]]$.*

Proof. We assume the existence of coefficient fields in general for equicharacteristic complete local rings: we give the proof of the remaining case immediately following. By the preceding Corollary, we may assume that R is complete. It is clear that a formal power series ring is regular: we want to prove the converse. We have a field $K_0 \subseteq R$ such that $K_0 \subseteq R \twoheadrightarrow R/m = K$ is an isomorphism. Let $x_1, \ldots, x_n$ be a minimal set of generators of m. By the final Theorem of the preceding lecture, we have a map $K_0[[X_1, \ldots, X_n]] \to R$ sending X_i to x_i. By part (b) of the theorem, since the X_i generate m the map is surjective. By part (c) of the theorem, since $x_1, \ldots, x_n$ is a system of parameters the map is injective. Thus, the map is an isomorphism. □

Coefficient fields in characteristic p and p-bases

We now discuss the construction of coefficient fields in local rings (R, m, K) of prime characteristic $p > 0$ that contain a field when K need not be perfect, which is needed to complete the proof of the result given at the end of the previous section.

Let K be a field of characteristic $p > 0$. Finitely many elements $\theta_1, \ldots, \theta_n$ in $K - K^p$ are called *p-independent* if $[K^p[\theta_1, \ldots, \theta_n] : K^p] = p^n$. This is equivalent to the assertion that

$$K^p \subseteq K[\theta_1] \subseteq K^p[\theta_1, \theta_2] \subseteq \cdots \subseteq K^p[\theta_1, \theta_2, \ldots, \theta_n]$$

is a strictly increasing tower of fields. At each stage there are two possibilities: either θ_{i+1} is already in $K^p[\theta_1, \ldots, \theta_i]$, or it has degree p over it, since θ_{i+1} is purely inseparable of degree p over K^p. Every subset of a p-independent set is p-independent. An infinite subset of $K - K^p$ is called *p-independent* if every finite subset is p-independent.

A maximal p-independent subset of $K - K^p$ is called a *p-base* for K. Zorn's Lemma guarantees the existence of a p-base, since the union of a chain of p-independent sets is p-independent. If Θ is a p-base, then $K = K^p[\Theta]$, for an element of $K - K^p[\Theta]$ could be used to enlarge the p-base. The empty set is a p-base for K if and only if K is perfect.

It is easy to see that Θ is a p-base for K if and only if every element of K is uniquely expressible as a polynomial in the elements of Θ with coefficients in K^p such that the exponent on every θ is at most $p-1$, i.e., the monomials in the elements of Θ of degree at most $p-1$ in each element are a basis for K over K^p.

Now for $q = p^n$, the elements of $\Theta^q = \{\theta^q : \theta \in \Theta\}$ are a p-base for K^q over K^{pq}: in fact we have a commutative diagram:

$$\begin{array}{ccc} K & \xrightarrow{F^q} & K^q \\ \uparrow & & \uparrow \\ K^p & \xrightarrow[F^{pq}]{} & K^{pq} \end{array}$$

where the vertical arrows are inclusions and the horizontal arrows are isomorphisms: here, $F^q(c) = c^q$. In particular, Θ^p is a p-base for K^p, and it follows by multiplying the two bases together that the monomials in the elements of Θ of degree at most $p^2 - 1$ are a basis for K over K^{p^2}. By a straightforward induction, the monomials in the elements of Θ of degree at most $p^n - 1$ in each element are a basis for K over K^{p^n} for every $n \in \mathbb{N}$.

Theorem. *Let (R, m, K) be a complete local ring of positive prime characteristic p, and let Θ be a p-base for K. Let T be a subset of R that maps bijectively onto Θ, i.e., a lifting of the p-base to R. Then there is a unique coefficient field for R that contains T, namely, $K_0 = \bigcap_n R_n$, where $R_n = R^{p^n}[T]$. Thus, there is a bijection between liftings of the p-base Θ and the coefficient fields of R.*

Proof. Note that any coefficient field must contain some lifting of Θ. Observe also that K_0 is clearly a subring of R that contains T. It will suffice to show that K_0 is a coefficient field and that any coefficient field L containing T is contained in K_0. The latter is easy: the isomorphism $L \to K$ takes T to Θ, and so T is a p-base for L. Every element of L is therefore in $L^{p^n}[T] \subseteq R^{p^n}[T]$. Notice also that every element of $R^{p^n}[T]$ can be written as a polynomial in the elements of T of degree at most $p^n - 1$ in each element, with coefficients in R^{p^n}. The reason is that any $N \in \mathbb{N}$ can be written as $ap^n + b$ with $a, b \in \mathbb{N}$ and $b \leq p^n - 1$. So t^N can be rewritten as $(t^a)^{p^n} t^b$, and thus if t^N occurs in a term we can rewrite that term so that it only involves t^b by absorbing $(t^a)^{p^n}$ into the coefficient from R^{p^n}. Let us call a polynomial in the elements of T with coefficients in R^{p^n} *special* if the exponents are all at most $p^n - 1$. Thus, every element of $R^{p^n}[T]$ is represented by a special polynomial. We shall also say that a polynomial in elements of Θ with coefficients in K^{p^n} is *special* if all exponents on elements of T are at most $p^n - 1$. Note that special polynomials in elements of T with coefficients in R^{p^n} map mod m onto special polynomials in elements of Θ with coefficients in K^{p^n}.

We next observe that

$$R^{p^n}[T] \cap m \subseteq m^{p^n}.$$

Write the element of $u \in R^{p^n}[T] \cap m$ as a special polynomial in elements of T with coefficients in R^{p^n}. Then its image in K, which is 0, is a special polynomial in the elements of Θ with coefficients in K^{p^n}, and so cannot vanish unless every coefficient is 0. This means that each coefficient of the special polynomial representing u must have been in $m \cap R^{p^n} \subseteq m^{p^n}$. Thus,

$$K_0 \cap m = \bigcap_n (R^{p^n}[T] \cap m) \subseteq \bigcap_n m^{p^n} = (0).$$

We can therefore conclude that K_0 injects into K. It will suffice to show that $K_0 \to K$ is surjective to complete the proof.

Let $\lambda \in K$ be given. Since $K = K^{p^n}[\Theta]$, for every n we can choose an element of $R^{p^n}[T]$ that maps to λ: call it r_n. Then $r_{n+1} \in R^{p^{n+1}}[T] \subseteq R^{p^n}[T]$, and so $r_n - r_{n+1} \in R^{p^n} \cap m \subseteq m^{p^n}$ (the difference $r_n - r_{n+1}$ is in m because both r_n and r_{n+1} map to λ in K). This shows that $\{r_n\}_n$ is Cauchy, and has a limit r_λ. It is clear that $r_\lambda \equiv \lambda \bmod m$, since that is true for every r_n. Moreover, r_λ is independent of the choices of the r_n: given another sequence r'_n with the same property, $r_n - r'_n \in R^{p^n}[T] \cap m \subseteq m^{p^n}$, and so $\{r_n\}_n$ and $\{r'_n\}_n$ have the same limit. It remains only to show that for every n, $r_\lambda \in R^{p^n}[T]$. To see this, write λ as a polynomial in the elements of Θ with coefficients of the form c^{p^n}. Explicitly,

$$\lambda = \sum_{\mu \in \mathcal{F}} c_\mu^{p^n} \mu$$

where $\mathcal{F}$ is some finite set of monomials in the elements of θ. If $\mu = \theta_1^{k_1} \cdots \theta_s^{k_s}$, let $\mu' = t_1^{k_1} \cdots t_s^{k_s}$, where t_j is the element of T that maps to θ_j. For every $\mu \in \mathcal{F}$ and every $n \in \mathbb{N}$, choose $c_{\mu,n} \in R_n$ such that $c_{\mu,n}$ maps to c_μ mod m. Thus, $\{c_{\mu,n}\}_n$ is a Cauchy sequence converging to r_{c_μ}. Let

$$w_n = \sum_{\mu \in \mathcal{F}} c_{\mu,n}^{p^n} \mu'$$

for every $n \in \mathbb{N}$. Then $w_n \in R_n$ and $w_n \equiv \lambda \bmod m$. It follows that

$$\lim_{n \to \infty} w_n = r_\lambda,$$

but this limit is also

$$\sum_{\mu \in \mathcal{F}} r_{c_\mu}^{p^n} \mu' \in R_n.$$

□

Remark. This result shows that if (R, m, K) is a complete local ring that is not a field and K is not perfect, then the choice of a coefficient field is *never* unique. Given a lifting of a p-base T, where $T \neq \emptyset$ because K is not perfect, we can always change it by adding a nonzero element of m to one or more of the elements in the p-base.

The Weierstrass preparation theorem

Before proceeding further with the investigation of coefficient rings in mixed characteristic, we explore several consequences of the theory that we already have.

Theorem (Weierstrass preparation theorem). *Let (A, m, K) be a complete local ring and let x be a formal indeterminate over A. Let $f = \sum_{n=0}^{\infty} a_n x^n \in A[[x]]$, where $a_h \in A - m$ is a unit and $a_n \in m$ for $n < h$. (Such an element f is said to be regular in x of order h.) Then the images of $1, x, \ldots, x^{h-1}$ are a free basis over A for the ring $A[[x]]/fA[[x]]$, and every element $g \in A[[x]]$ can be written uniquely in the form $qf + r$ where $q \in A[[x]]$, and $r \in A[x]$ is a polynomial of degree $\leq h - 1$.*

Proof. Let $M = A[[x]]/(f)$, which is a finitely generated $A[[x]]$-module, and so will be separated in the $\mathcal{M}$-adic topology, where $\mathcal{M} = (m, x)A[[x]]$. Hence, it is certainly separated in the m-adic topology. Then $M/mM \cong K[[x]]/(\overline{f})$, where $\overline{f}$ is the image of f under the map $A[[x]] \twoheadrightarrow K[[x]]$ induced by $A \twoheadrightarrow K$: it is the result of reducing coefficients of f mod m. It follows that the lowest nonzero term of $\overline{f}$ has the form cx^h, where $c \in K$, and so $\overline{f} = x^h\gamma$ where γ is a unit in $K[[x]]$. Thus,

$$M/mM \cong K[[x]]/(\overline{f}) = K[[x]]/(x^h),$$

which is a K-vector space for which the images of $1, x, \ldots, x^{h-1}$ form a K-basis. By the Proposition on p. 6, $1, x, \ldots, x^{h-1}$ span $A[[x]]/(f)$ as an A-module. This means precisely that every $g \in A[[x]]$ can be written $g = qf + r$ where $r \in A[x]$ has degree at most $h - 1$.

Suppose that $g'f + r'$ is another such representation. Then $r' - r = (q - q')f$. Thus, it will suffice to show if $r = qf$ is a polynomial in x of degree at most $h - 1$, then $q = 0$ (and $r = 0$ follows). Suppose otherwise. Since some coefficient of q is not 0, we can choose t such that q is not 0 when considered mod $m^tA[[x]]$. Choose such a t as small as possible, and let d be the least degree such that the coefficient of x^d is not in m^t. Pass to R/m^t. Then q has lowest degree term ax^d, and both a and all higher coefficients are in m^{t-1}, or we could have chosen a smaller value of t. When we multiply by f (still thinking mod m^t), note that all terms of f of degree smaller than h kill q, because their coefficients are in m. There is at most one nonzero term of degree $h + d$, and its coefficient is not zero, because the coefficient of x^h in f is a unit. Thus, qf has a nonzero term of degree $\geq h + d > h - 1$, a contradiction. This completes the proof of the existence and uniqueness of q and r. □

Corollary. *Let $A[[x]]$ and f be as in the statement of the Weierstrass Preparation Theorem, with f regular of order h in x. Then f has a unique multiple fq which is a monic polynomial in $A[x]$ of degree h. The multiplier q is a unit, and qf has all non-leading coefficients in m. The polynomial qf called the unique monic associate of f.*

Proof. Apply the Weierstrass Preparation Theorem to $g = x^h$. Then $x^h = qf + r$, which says that $x^h - r = qf$. By the uniqueness part of the theorem, these are the only choices of q, r that satisfy the equation, and so the uniqueness statement follows. It remains only

to see that q is a unit, and that r has coefficients in m. To this end, we may work mod $mA[[x]]$. We use $\overline{u}$ for the class of $u \in A[[x]]$ mod $mA[[x]]$, and think of $\overline{u}$ as an element of $K[[x]]$.

Then $x^h - \overline{r} = \overline{q}\overline{f}$. Since $\overline{f}$ is a unit γ times x^h, we must have $\overline{r} = 0$. It follows that $x^h = x^h\overline{q}\gamma$. We may cancel x^h, and so $\overline{q}$ is a unit of of $K[[x]]$. It follows that q is a unit of $A[[x]]$, as asserted. $\square$

Discussion. This result is often applied to the formal power series ring in n-variables, $K[[x_1, \ldots, x_n]]$: one may take $A = K[[x_1, \ldots, x_{n-1}]]$ and $x = x_n$, for example, though, obviously, one might make any of the variable play the role of x. In this case, a power series f is regular in x_n if it involves a term of the form cx_n^h with $c \in K - \{0\}$, and if one takes h as small as possible, f is regular of order h in x_n. The regularity of f of order h in x_n is equivalent to the assertion that under the unique continuous $K[[x_n]]$-algebra map $K[[x_1, \ldots, x_n]] \to K[[x_n]]$ that kills $x_1, \ldots, x_{n-1}$, the image of f is a unit times x_n^h. A logical notation for the image of f is $f(0, \ldots, 0, x_n)$. The Weierstrass preparation theorem asserts that for any g, we can write $f = qg + r$ uniquely, where $q \in K[[x_1, \ldots, x_n]]$, and $r \in K[[x_1, \ldots, x_{n-1}]][x_n]$. In this context, the unique monic associate of f is sometimes call the *distinguished pseudo-polynomial* associated with f. If $K = \mathbb{R}$ or $\mathbb{C}$ one can consider instead the ring of convergent (on a neighborhood of 0) power series. One can carry through the proof of the Weierstrass preparation theorem completely constructively, and show that when g and f are convergent, so are q and r. See, for example, [O. Zariski and P. Samuel, *Commutative Algebra*, Vol. II, D. Van Nostrand Co., Inc., Princeton, 1960], pp. 139–146.

Any nonzero element of the power series ring (convergent or formal) can be made regular in x_n by a change of variables. The same applies to finitely many elements $f_1, \ldots, f_s$, since it suffices to make the product $f_1 \cdots f_s$ regular in x_n, (if the image of $f_1 \cdots f_s$ in $K[[x_n]]$ is nonzero, so is the image of every factor). If the field is infinite one may make use of a K-automorphism that maps $x_1, \ldots, x_n$ to a different basis for $Kx_1 + \cdots + Kx_n$. One can think of f as $f_0 + f_1 + f_2 + \cdots$ where every f_j is a homogeneous polynomial of degree j in $x_1, \ldots, x_n$. Any given form G occurring in $f_j \neq 0$ can be made into a monic polynomial by a suitable linear change of variables. (Let $d = \deg(G)$. Make a change of variables in which $x_n \mapsto \lambda_n x_n$ and $x_j \mapsto x_j + \lambda_j x_n$ for $1 \leq j \leq n-1$, where the λ_j are scalars in the field and $\lambda_n \neq 0$. All we need is for x_n^d to occur with nonzero coefficient in the image of G, which is $G(x_1 + \lambda_1 x_n, \ldots, x_{n-1} + \lambda_{n-1}x_n, \lambda_n x_n)$. But the coefficient of x_n^d in this homogeneous polynomial can be recovered by substituting $x_1 = \cdots = x_{n-1} = 0$ and $x_n = 1$, which gives $G(\lambda_1, \ldots, \lambda_n)$. Since the polynomial $x_n G$ is not identically 0, and since the field is infinite, there is a choice of the λ_j for which it does not vanish.)

If K is finite one can still get the image of f under an automorphism to be regular in x_n by mapping $x_1, \ldots, x_n$ to $x_1 + x_n^{N_1}, \ldots, x_{n-1} + x_n^{N_{n-1}}, x_n$, respectively, as in the proof of the Noether normalization theorem, although the details are somewhat more difficult. Consider the monomials that occur in f (there is at least one, since f is not 0), and totally order the monomials so that $x_1^{j_1} \cdots x_n^{j_n} < x_1^{k_1} \cdots x_n^{k_n}$ means that for some i, $1 \leq i \leq n$, $j_1 = k_1$, $j_2 = k_2$, $\ldots$, $j_{i-1} = k_{i-1}$, while $j_i < k_i$. Let $x_1^{d_1} \cdots x_n^{d_n}$ be the smallest monomial that occurs with nonzero coefficient in f with respect to this ordering, and let

$d = \max\{d_1, \ldots, d_n\}$. Let $N_i = (nd)^{n-i}$, and let θ denote the continuous K-automorphism of $K[[x_1, \ldots, x_n]]$ that sends $x_i \mapsto x_i + {x_n}^{N_i}$ for $1 \leq i \leq n-1$, and $x_n \mapsto x_n$. We claim that $\theta(f)$ is regular in x_n. The point is that the value of $\theta(f)$ after killing $x_1, \ldots, x_{n-1}$ is

$$f(x_n^{N_1}, x_n^{N_2}, \ldots, x_n^{N_{n-1}}, x_n),$$

and the term $c'x_1^{e_1} \cdots x_n^{e_n}$ where $c' \in K - \{0\}$ maps to

$$c' x_n^{e_1 N_1 + e_2 N_2 + \cdots + e_{n-1} N_{n-1} + e_n}.$$

In particular, there is a term in the image of $\theta(f)$ coming from the $x_1^{d_1} \cdots x_n^{d_n}$ term in f, and that term is a nonzero scalar multiple of

$$x_n^{d_1 N_1 + d_2 N_2 + \cdots + d_{n-1} N_{n-1} + d_n}.$$

It suffices to show that no other term cancels it, and so it suffices to show that if for some i with $1 \leq i \leq n$, we have that $e_j = d_j$ for $j < i$ and $e_i > d_i$, then

$$e_1 N_1 + e_2 N_2 + \cdots + e_{n-1} N_{n-1} + e_n > d_1 N_1 + d_2 N_2 + \cdots + d_{n-1} N_{n-1} + d_n.$$

The left hand side minus the right hand side gives

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

since $d_j = e_j$ for $j < i$. It will be enough to show that this difference is positive. Since $e_i > d_i$, the leftmost term is at least N_i. Some of the remaining terms are nonnegative, and we omit these. The terms for those j such $e_j < d_j$ are negative, but what is being subtracted is bounded by $d_j N_j \leq d N_j$. Since at most $n-1$ terms are being subtracted, the sum of the quantities being subtracted is strictly bounded by $nd \max_{j>i}\{dN_j\}$. The largest of the N_j is N_{i+1}, which is $(dn)^{n-(i+1)}$. Thus, the total quantity being subtracted is strictly bounded by $(dn)(dn)^{n-i-1} = (dn)^{n-i} = N_i$. This completes the proof that

$$e_1 N_1 + e_2 N_2 + \cdots + e_{n-1} N_{n-1} + e_n > d_1 N_1 + d_2 N_2 + \cdots + d_{n-1} N_{n-1} + d_n,$$

and we see that $\theta(f)$ is regular in x_n, as required.

If the Weierstrass Preparation Theorem is proved directly for a formal or convergent power series ring R over a field K (the constructive proofs do not use *a priori* knowledge that the power series ring is Noetherian), the theorem can be used to prove that the ring R is Noetherian by induction on n. The cases where $n = 0$ or $n = 1$ are obvious: the ring is a field or a discrete valuation ring. Suppose the result is known for the power series ring A in $n-1$ variables, and let R be the power series ring in one variable x_n over A. Let I be an ideal of R. We must show that I is finitely generated over R. If $I = (0)$ this is clear. If $I \neq 0$ choose $f \in I$ with $f \neq 0$. Make a change of variables such that f is regular in x_n over A. Then $I/fR \subseteq R/fR$, which is a finitely generated module over A. By the induction hypothesis, A is Noetherian, and so R/fR is Noetherian over A, and hence I/fR is a Noetherian A-module, and is finitely generated as an A-module. Lift these generators to I. The resulting elements, together with f, give a finite set of generators for I.

Although we shall later give a quite different proof valid for all regular local rings, we want to show how the Weierstrass preparation theorem can be used to prove unique factorization in a formal power series ring.

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

Proof. We use induction on n. If $n = 0$ then R is a field, and if $n = 1$, R is a discrete valuation ring. In particular, R is a principal ideal domain and, hence, a unique factorization domain.

Suppose that $n > 1$. It suffices to prove that if $f \in m$ is irreducible then f is prime. Suppose that f divides gh, where it may be assumed without loss of generality that g, $h \in m$. Then we have an equation $fw = gh$, and since f is irreducible, we must have that $w \in m$ as well. We may make a change of variables so that all of f, w, g and h are regular in x_n. Moreover, we can replace f, g, and h by monic polynomials in x_n over

$$A = K[[x_1, \ldots, x_{n-1}]]$$

whose non-leading coefficients are in $Q = (x_1, \ldots, x_{n-1})R$: we multiply each by a suitable unit. The equation will hold after we multiply w by a unit as well, although we do not know *a priori* that w is a polynomial in x_n. We can divide $gh \in A[x_n]$ by f which is monic in x_n to get a unique quotient and remainder, say $gh = qf + r$, where the degree of r is less the degree d of f. The Weierstrass preparation theorem guarantees a unique such representation in $A[[x_n]]$, and in the larger ring we know that $r = 0$. Therefore, the equation $gh = qf$ holds in $A[x_n]$, and this means that $q = w$ is a monic polynomial in x_n as well.

By the induction hypothesis, A is a UFD, and so $A[x_n]$ is a UFD. If f is irreducible in $A[x_n]$, we immediately obtain that $f \mid g$ or $f \mid h$. But if f factors non-trivially $f = f_1 f_2$ in $A[x_n]$, the factors f_1, f_2 must be polynomials in x_n of lower degree which can be taken to be monic. Mod Q, f_1, f_2 give a factorization of x^d, and this must be into two powers of x of lower degree. Therefore, f_1 and f_2 both have all non-leading coefficients in Q, and, in particular their constant terms are in Q. This implies that neither f_1 nor f_2 is a unit of R, and this contradicts the irreducibility of f in R. Thus, f must be irreducible in $A[x_n]$ as well. $\square$

The mixed characteristic case

Consider a complete local ring (R, m, K). If K has characteristic 0, then $\mathbb{Z} \to R \to K$ is injective, and $\mathbb{Z} \subseteq R$. Moreover, no element of $W = \mathbb{Z} - \{0\}$ is in m, since no element of W maps to 0 in $R/m = K$, and so every element of $\mathbb{Z} - \{0\}$ has an inverse in R. By the universal mapping property of localization, we have a unique map of $W^{-1}\mathbb{Z} = \mathbb{Q}$ into R, and so R is an equicharacteristic 0 ring. We already know that R has a coefficient field. We also know this when R has prime characteristic $p > 0$, i.e., when $\mathbb{Z}/p\mathbb{Z} \subseteq R$.

We now want to develop the structure theory of complete local rings when R need not contain a field. From the remarks above, we only need to consider the case where K has prime characteristic $p > 0$, and we shall assume this in the further development of the theory. The coefficient rings that we are about to describe also exist in the complete separated quasi-local case, but, for simplicity, we only treat the Noetherian case.

We shall say that V is a *coefficient ring* if it is a field or if it is complete local of the form (V, pV, K), where K has characteristic $p > 0$. If R is complete local we shall say that V is a coefficient ring for R if V is a coefficient ring, $V \subseteq R$ is local, and the induced map of residue fields is an isomorphism. We shall prove that coefficient rings always exist.

In the case where the characteristic of K is $p > 0$, there are three possibilities. It may be that $p = 0$ in R (and V), in which case V is a field: we have already handled this case. It may be that p is not nilpotent in V: in this case it turns out that V is a Noetherian discrete valuation domain (DVR), like the p-adic integers. Finally, it may turn out that p is not zero, but is nilpotent. Although it is not obvious, we will prove that in this case, and when V is a field of characteristic $p > 0$, V has the form W/p^nW where $n \geq 1$ and W is a DVR with maximal ideal pW.

We first note:

Lemma. *Let (R, m, K) be local with K of prime characteristic $p > 0$. If $r, s \in R$ are such that $r \equiv s$ mod m, and $n \geq 1$ is an integer, then for all $N \geq n - 1$, with $q = p^N$ we have that $r^q \cong s^q$ mod m^n.*

Proof. This is clear if $n = 1$. We use induction. If $n > 1$, we know from the induction hypothesis that $r^q \equiv y^q \bmod m^N$ if $N \geq n - 2$, and it suffices to show that $r^{pq} \equiv y^{pq} \bmod m^{N+1}$. Since $r^q = s^q + u$ with $u \in m^N$, we have that $r^{pq} = (s^q + u)^p = s^{pq} + puw + u^p$, where puw is a sum of terms from the binomial expansion each of which has the form $\binom{pq}{j} s^j u^{p-j}$ for some j, $1 \leq j \leq p - 1$, and in each of these terms the binomial coefficient is divisible by p. Since $u \in m^N$ and $p \cdot 1_R \in m$, $puw \in m^{N+1}$, while $u^p \in m^{Np} \subseteq m^{N+1}$ as well. $\square$

Recall that a p-base for a field K of prime characteristic $p > 0$ is a maximal set of elements Λ of $K - K^p$ such that for every finite subset of distinct elements $\lambda_1, \ldots, \lambda_h$ of Λ, $[K(\lambda_1, \ldots, \lambda_h) : K] = p^h$. K has a p-base by Zorn's lemma. The empty set is a p-base for K if and only if K is perfect. The set of monomials in the the elements of the p-base Λ such that every exponent is at most $p-1$ is a K^p-basis for K over K^p, and, more generally, $(*)$ for every $q = p^N$, the set of monomials in the elements of Λ such that every exponent is at most $q - 1$ is a basis for K over $K^q = \{a^q : a \in K\}$. See pp. 11 and 12.

The following Proposition, which constructs coefficient rings when the maximal ideal of the ring is nilpotent, is the heart of the proof of the existence of coefficient rings. Before giving the proof, we introduce the following notation, which we will use in another argument later. Let x, y be indeterminates over $\mathbb{Z}$. Let q be a power of p, a prime. Then $(x + y)^q - x^q - y^q$ is divisible by p in $Z[x, y]$, since the binomial coefficients that occur are all divisible by p, and we write $G_q(x, y) \in \mathbb{Z}[x, y]$ for the quotient, so that $(x + y)^q = x^q + y^q + pG_q(x, y)$.

Proposition. *Suppose that (R, m, K) is local where K has characteristic $p > 0$, and that $m^n = 0$. Choose a p-base Λ for K, and a lifting of the p-base to R: that is, for every $\lambda \in \Lambda$ choose an element $\tau_\lambda \in R$ with residue λ. Let $T = \{\tau_\lambda : \lambda \in \Lambda\}$. Then R has a unique coefficient ring V that contains T. In fact, suppose that we fix any sufficiently large power $q = p^N$ of p (in particular, $N \geq n - 1$ suffices) and let S_N be the set of all expressions of the form $\sum_{\mu \in \mathcal{M}} r_\mu^q \mu$, where the $\mathcal{M}$ is a finite set of mutually distinct monomials in*

the elements of T such that the exponent on every element of T is $\leq q-1$ and every $r_\mu^q \in R^q = \{r^q : r \in R\}$. Then we may take

$$V = S_N + pS_N + p^2S_N + \cdots + p^{n-1}S_N,$$

which will be the same as the smallest subring of R containing R^q and T.

Before giving the proof, we note that it is not true in general that R^q is closed under addition, and neither is S_N, but we will show that for large N, V is closed under addition and multiplication, and this will imply at once that it is the smallest subring of R containing R^q and T.

Proof of the Proposition. We first note if $r \equiv s \bmod m$ then $r^q \equiv s^q \bmod m^n$ if $N \geq n-1$, by the preceding Lemma. Therefore R^q maps bijectively onto $K^q = \{a^q : a \in K\}$ when we take residue classes mod m. By the property (*) of p-bases, the residue class map $R \to K$ sends S_N bijectively onto K.

Suppose that W is a coefficient ring containing T. For each $r \in R$, if $w \equiv r \bmod m$, then $w^q = r^q$. Thus, $R^q \subseteq W$. Then $S_N \subseteq W$, and so $V \subseteq W$. Now consider any element $w \in W$. Since S_n contains a complete set of representatives of elements of K, every element of W has the form $\sigma_0 + u$ where $u \in m \cap W = pW$, and so $w = \sigma_0 + pw_1$. But we may also write w_1 in this way and substitute, to get an expression $w = \sigma_0 + p\sigma_1 + p^2w_2$, where σ_0, $\sigma_1 \in S_n$ and $w_2 \in W$. Continuing in this way, we find, by a straightforward induction, that

$$W = S_N + pS_N + \cdots + p^jS_N$$

for every $j \geq 1$. We may apply this with $j = n$ and note that $p^n = 0$ to conclude that $W = V$. Thus, if there is a coefficient ring, it must be V. However, at this point we do not even know that V is closed under addition.

We next claim that V is a ring. Let V' be the closure of V under addition. Then we can see that V' is a ring, since, by the distributive law, it suffices to show that the product of two elements $p^ir^q\mu$ and $p^jr'^q\mu'$ has the same form. The point is that $\mu\mu'$ can be rewritten in the form $\nu^q\mu''$ where μ'' has all exponents $\leq q-1$, and $p^{i+j}(rr'\nu)^q\mu''$ has the correct form. Thus, V' is the smallest ring that contains R^q and T.

We next prove that V itself is closed under addition. We shall prove by reverse induction on j that $p^jV = p^jV'$ for all j, $0 \leq j \leq n$. The case that we are really aiming for is, of course, where $j = 0$. The statement is obvious when $j = n$, since $p^nV' = 0$. Now suppose that $p^{j+1}V = p^{j+1}V'$. We shall show that $p^jV = p^jV'$, thereby completing the inductive step. Since p^jV' is spanned over $p^{j+1}V' = p^{j+1}V$ by p^jS_n, it will suffice to show that given any two elements of p^jS_n, their sum differs from an element of p^jS_n by an element of $p^{j+1}V' = p^{j+1}V$. Call the two elements

$$v = p^j \sum_{\mu \in \mathcal{M}} r_\mu^q \mu$$

and

$$v' = p^j \sum_{\mu \in \mathcal{M}} r'_m u^q \mu,$$

where $r_\mu, r'_m u \in R$ and $\mathcal{M}$ is a finite set of monomials in elements of T, with exponents $\leq q-1$, large enough to contain all those monomials that occur with nonzero coefficient in the expressions for v and v'. Since S_n gives a complete set of representatives of K and r^q only depends on what r is mod m, we may assume that all of the r_μ and r'_μ are elements of S_n. Let

$$v'' = p^j \sum_{\mu \in \mathcal{M}} (r_\mu + r'_\mu)^q \mu.$$

Then

$$v'' - v - v' = p^j \sum_{\mu \in \mathcal{M}} pG_q(r_\mu, r'_\mu)\mu = p^{j+1} \sum_{\mu \in \mathcal{M}} G_q(r_\mu, r'_\mu)\mu \in p^{j+1}V',$$

as required, since all the r_μ, $r'_\mu \in S_N$ and V' is a ring. This completes the proof that $V' = V$, and so V is a subring of R.

We have now shown that V is a subring of R, and that it is the only possible coefficient ring. It is clear that $pV \subseteq m$, while an element of $V - pV$ has nonzero image in K: its constant term in S_N is nonzero, and S_N maps bijectively to K. Thus, $m \cap V = pV$, and we know that $V/pV \cong K$, since S_N maps onto K. It follows that pV is a maximal ideal of V generated by a nilpotent, and so pV is the only prime ideal of V. Any nonzero element of the maximal ideal can be written as $p^t u$ with t as large as possible (we must have that $t < n$), and then u must be a unit. Thus, every nonzero element of V is either a unit, or a unit times a power of p. It follows that every nonzero proper ideal is generated by p^k for some positive integer k, where k is as small as possible such that p^k is in the ideal. It follows that V is a principal ideal ring. Thus, V is a Noetherian local ring, and, in fact, an Artin local ring. $\square$

Theorem. *Let K, K' be isomorphic fields of characteristic $p > 0$ and let $g : K \to K'$ be the isomorphism. Let (V, pV, K) and (V', pV', K') be two coefficient rings of the same characteristic, $p^n > 0$. We shall also write a' for the image of $a \in K$ under g. Let Λ be a p-base for K and let $\Lambda' = g(\Lambda)$ be the corresponding p-base for K'. Let T be a lifting of Λ to V and let T' be a lifting of Λ' to T'. We have an obvious bijection $\widetilde{g} : T \to T'$ such that if $\tau \in T$ lifts $\lambda \in \Lambda$ then $\widetilde{g}(\tau) \in T'$ lifts $\lambda' = g(\lambda)$. Then $\widetilde{g}$ extends uniquely to an isomorphism of V with V' that lifts $g : K \to K'$.*

Proof. As in the proof of the Proposition on pp. 18–19 showing the existence of a coefficient ring when $m^n = 0$, we choose $N \geq n-1$ and let $q = p^N$. For every element $a \in K$ there is a unique element $\rho_a \in V^q$ that maps to $a^q \in K^q$. Similarly, there is a unique element $\rho'_{a'} \in V'^q$ that maps to a'^q for every $a' \in K'$. If there is an isomorphism $V \cong V'$ as stated, it must map $\rho_a \to \rho'_{a'}$ for every $a \in K$. Said otherwise, we have an obvious bijection $V^q \to V'^q$, and $\widetilde{g}$ must extend it. Just as in the proof of the Proposition, we can define $S_N = S$ to consist of linear combinations of distinct monomials in T such that in every monomial, every exponent is $\leq q-1$, and such that every coefficient is in V^q. Then S will map bijectively onto K. We define $S'_N = S' \subseteq V'$ analogously. Since S' maps bijectively onto K', we have an obvious bijection $\widetilde{g} : S \to S'$. We use σ' for the element of S' corresponding to $\sigma \in S$.

Every element $v \in V$ must have the form $\sigma_0 + pv_1$ where σ_0 is the unique element of S that has the same residue as v modulo pV. Continuing this way, as in the proof of the previous Proposition, we get a representation

$$v = \sigma_0 + p\sigma_1 + p^2\sigma_2 + \cdots + p^{n-1}\sigma_{n-1}$$

for the element $v \in V$, where the $\sigma_j \in S$. We claim this is unique. Suppose we have another such representation

$$v = \sigma_0^* + p\sigma_1^* + \cdots + p^{n-1}\sigma_{n-1}^*.$$

Suppose that $\sigma_i = \sigma_i^*$ for $i < j$. We want to show that $\sigma_j = \sigma_j^*$ as well. Working in $V/p^{j+1}V$ we have that $\sigma_j p^j = \sigma_{j+1} p^j$, i.e., that $(\sigma_j - \sigma_j^*)$ kills p^j working mod p^{j+1}. By part (a) of the Lemma that follows just below, we have that $\sigma_j - \sigma_j^* \in pV$, and so σ_j and σ_j^* represent the same element of $K = V/pV$, and therefore are equal.

Evidently, any isomorphism $V \cong V'$ satisfying the specified conditions must take

$$\sigma_0 + p\sigma_1 + \cdots + p^{n-1}\sigma_{n-1}$$

to

$$\sigma_0' + p\sigma_1' + \cdots + p^{n-1}\sigma_{n-1}'.$$

To show that this map really does give an isomorphism of V with V' one shows simultaneously, by induction on j, that addition is preserved in p^jV, and that multiplication is preserved when one multiplies elements in p^hV and p^iV such that $h + i \geq j$. For every element $a \in K$, let σ_a denote the unique element of S that maps to a. Note that we may write ρ_a as σ_a^q, since σ_a has residue a mod pV.

Now,

$$p^j\rho_a\mu + p^j\rho_b\mu = p^j(\sigma_a^q + \sigma_b^q)\mu = p^j\big((\sigma_a + \sigma_b)^q - pG_q(\sigma_a, \sigma_b)\big),$$

where $G_q(x, y) \in \mathbb{Z}[x, y]$ is such that $(x + y)^q = x^q + y^q + pG_q(x, y)$. Since $\sigma_a + \sigma_b$ has residue $a + b$ mod pV, we have that $(\sigma_a + \sigma_b)^q = \rho_{a+b}$, and it follows that

$$p^j\rho_a\mu + p^j\rho_b\mu = p^j\rho_{a+b}\mu - p^{j+1}G_q(\sigma_a, \sigma_b)\mu.$$

We have similarly that

$$p^j\rho'_{a'}\mu + p^j\rho'_{b'}\mu' = p^j\rho'_{a'+b'}\mu' - p^{j+1}G_q(\sigma'_{a'}, \sigma'_{b'})\mu',$$

and it follows easily that addition is preserved by our map $p^jV \to p^jV'$: note that $p^{j+1}G_q(\sigma_a, \sigma_b)\mu$ maps to $p^{j+1}G_q(\sigma'_{a'}, \sigma'_{b'})\mu'$ because all terms are multiples of p^{j+1} (the argument here needs the certain multiplications are preserved as well addition).

Once we have that our map preserves addition on terms in p^jV, the fact that it preserves products of pairs of terms from $p^hV \times p^iV$ for $h + i \geq j$ follows from the distributive law, the fact that addition in p^jV is preserved, and the fact that there is a unique way of writing $\mu_1\mu_2$, where μ_1 and μ_2 are monomials in the elements of T with all exponents $\leq q - 1$, in the form $\nu^q\mu_3$ where all exponents in μ_3 are $\leq q - 1$, and

$$(p^h\rho_a\mu_1)(p^i\rho_b\mu_2) = p^{h+i}(\sigma_a\sigma_b\nu)^q\mu_3$$

in V, while

$$(p^h\rho'_{a'}\mu'_1)(p^i\rho'_{b'}\mu'_2) = p^{h+i}(\sigma'_{a'}\sigma'_{b'}\nu')^q\mu'_3$$

in V'. $\square$

Lemma. *Let K be a field of characteristic $p > 0$ and let (V, pV, K), (W, pW, K) and (V_n, pV_n, K), $n \in \mathbb{N}$, be coefficient rings.*

(a) *If $p^t = 0$ while $p^{t-1} \neq 0$ in V, which is equivalent to the statement that p^t is the characteristic of V, then $\mathrm{Ann}_V p^j V = p^{t-j}V$, $0 \leq j \leq t$. Moreover, if $p^s = 0$ while $p^{s-1} \neq 0$ in W, and $W \twoheadrightarrow V$ is a surjection, then $V = W/p^tW$.*

(b) *Suppose that*

$$V_0 \twoheadleftarrow V_1 \twoheadleftarrow \cdots \twoheadleftarrow V_n \twoheadleftarrow \cdots$$

is an inverse limit system of coefficient rings and surjective maps, and that the characteristic of V_n is $p^{t(n)}$ where $t(n) \geq 1$. Then either $t(n)$ is eventually constant, in which case the maps $h_n : V_{n+1} \twoheadrightarrow V_n$ are eventually all isomorphisms, and the inverse limit is isomorphic with V_n for any sufficiently large n, or $t(n) \to \infty$ as $n \to \infty$, in which case the inverse limit is a complete local principal ideal V with maximal ideal pV and residue class field K. In particular, the inverse limit V is a coefficient ring.

Proof. (a) Every ideal of V (respectively, W) has the form p^kV (respectively, p^W)for a unique integer k, $0 \leq k \leq t$ (respectively, $0 \leq k \leq s$) The first statement follows because $k+j \geq n$ iff $k \geq n-j$. The second statement follows because V must have the form S/p^kS for some k, $0 \leq k \leq S$, and the characteristic of S/p^kS is p^k, which must be equal to p^t.

(b) If $t(n)$ is eventually constant it is clear that all the maps are eventually isomorphisms. Therefore, we may assume that $t(n) \to \infty$ as $n \to \infty$. By passing to an infinite subsequence of the V_n we may assume without loss of generality that $t(n)$ is strictly increasing with n. We may think of an element of the inverse limit as a sequence of elements $v_n \in V_n$ such that v_n is the image of v_{n+1} for every n. It is easy to see that one of the v_n is a unit if and only if all of them are. Suppose on the other hand that none of the v_n is a unit. Then each v_n can be written as pw_n for $w_n \in V_n$. The problem is that while pw_{n+1} maps to pw_n, for all n, it is not necessarily true that w_{n+1} maps to w_n.

Let h_n be the map $V_{n+1} \to V_n$. For all n, let $w'_n = h_n(w_{n+1})$. We will show that for all n, $v_n = pw'_n$ and that $h_n(w'_{n+1}) = w'_n$ for all n. Note first that $h_n(pw_{n+1}) = pw_n = v_n$, and it is also pw'_n. This establishes the first statement. Since $p(w_{n+1} - w'_{n+1}) = 0$, it follows that $w_{n+1} - w'_{n+1} = p^{t(n+1)-1}\delta$, by part (a). Then

$$w'_n = h_n(w_{n+1}) = h_n(w'_{n+1}) + p^{t(n+1)-1}h_n(\delta) = h_n(w'_{n+1}),$$

as required, since $p^{t(n+1)-1}$ is divisible by $p^{t(n)}$, the characteristic of V_n.

It follows that the inverse limit has a unique maximal ideal generated by p. No nonzero element is divisible by arbitrarily high powers of p, since the element will have nonzero image in V_n for some n, and its image in this ring is not divisible by arbitrarily high powers of p. It follows that every nonzero element can be written as a power of p times a unit, and no power of p is 0, because the ring maps onto V/p^t for arbitrarily large values of t. It is forced to be an a principal ideal domain in which every nonzero ideal is generated by a power of p. The fact that the ring arises as an inverse limit implies that it is complete. $\square$

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

Proof. It suffices to prove that there exists a Noetherian valuation domain (V, pV, K): its completion will then be complete with the required properties. Choose a well-ordering of K in which 0 is the first element. We construct, by transfinite induction, a direct limit system of Noetherian valuation domains $\{V_a, pV_a, K_a\}$ indexed by the well-ordered set K and injections $K_a \hookrightarrow K$ such that

(1) $K_0 \cong \mathbb{Z}/p\mathbb{Z}$

(2) The image of K_a in K contains a.

(3) The diagrams

$$\begin{array}{ccccc} V_b & \twoheadrightarrow & K_b & \hookrightarrow & K \\ \uparrow & & \uparrow & & \| \\ V_a & \twoheadrightarrow & K_a & \hookrightarrow & K \end{array}$$

commute for all $a \leq b \in K$.

Note the given a direct limit system of Noetherian valuation domains and injective local maps such that the same element, say, t (in our case $t = p$) generates all of their maximal ideals, the direct limit, which may be thought of as a directed union, of all of them is a Noetherian discrete valuation domain such that t generates the maximal ideal, and such that the residue class field is the directed union of the residue class fields. Every element of any of these rings not divisible by t is a unit (even in that ring): thus, if W is the directed union, pW is the unique maximal ideal. Every nonzero element of the union is a power of t times a unit, since that is true in any of the valuation domains that contain it, and it follows that every nonzero ideal is generated by the smallest power of p that it contains. The statement about residue class fields is then quite straightforward.

Once we have a direct limit system as described, the direct limit will be a discrete Noetherian valuation domain in which p generates the maximal ideal and the residue class field is isomorphic with K.

It will therefore suffice to construct the direct limit system.

We may take $V_0 = \mathbb{Z}_P$ where $P = p\mathbb{Z}$. We next consider an element $b \in K$ which is the immediate successor of $a \in K$. We have a Noetherian discrete valuation domain (V_a, pV_a, K_a) and an embedding $K_a \hookrightarrow K$. We want to enlarge V_a suitably to form V_b. If b is transcendental over K_a we simply let V_b be the localization of the polynomial ring $V_a[x]$ in one variable over V_a at the expansion of pV_a: the residue class field may be identified with $K_a(x)$, and the embedding of $K_a \hookrightarrow K$ may be extended to the simple transcendental extension $K_a(x)$ so that x maps to $b \in K$.

If b is already in the image of K_a we may take $V - b = V_a$. If instead b is algebraic over the image of K_a, but not in the image, then it satisfies a minimal monic polynomial $g = g(x)$ of degree at least 2 with coefficients in the image of K_a. Lift the coefficients to V_a so as to obtain a monic polynomial $G = G(x)$ of the same degree over V_a. We shall show that $V_b = V_a[x]/\big(G(x)\big)$ has the required properties. If G were reducible over the

fraction field of V_a, by Gauss' Lemma it would be reducible over V_a, and then g would be reducible over the image of K_a in K. If follows that $\big(G(x)\big)$ is prime in $V_a[x]$m and so V_b is a domain that is a module-finite extension of V_a. Consider a maximal ideal m of V_b. Then the chain $m \supset (0)$ in V_b lies over a chain of distinct primes in V_a: since V_a has only two distinct primes, we see that m lies over pV_a and so $p \in m$. But

$$V_b/pV_a \cong \mathrm{Im}\,(K_a)[x]/g(x) \cong \mathrm{Im}\,(K_a)[b],$$

and so p must generate a unique maximal ideal in V_b, and the residue class field behaves as we require as well.

Finally, if b is a limit ordinal, we first take the direct limit of the system of Noetherian discrete valuation domains indexed by the predecessors of b, and then enlarge this ring as in the preceding paragraph so that the image of its residue class field contains b. □

Corollary. *If p is a positive prime integer and K is field of characteristic p, there is, up to isomorphism, a unique coefficient ring of characteristic $p > 0$ with residue class field K and characteristic p^t, and it has the form V/p^tV, where (V, pV, K) is a Noetherian discrete valuation domain.*

Proof. By the preceding Theorem, we can construct V so that it has residue field K. Then V/p^tV is a coefficient ring with residue class field K of characteristic p, and we already know that such all rings are isomorphic, which establishes the uniqueness statement. □

Corollary. *Let p be a positive prime integer, K a field of characteristic p, and suppose that (V, pV, K) and (W, pW, K) are complete Noetherian discrete valuation domains with residue class field K. Fix a p-base Λ for K. Let T be a lifting of Λ to V and T' a lifting to W. Then there is a unique isomorphism of V with W that maps each element of T to the element with the same residue in Λ in T'.*

Proof. By our results for the case where the maximal ideal is nilpotent, we get a unique such isomorphism $V/p^nV \cong W/p^nW$ for every n, and this gives an isomorphism of the inverse limit systems

$$V/pV \twoheadleftarrow V/p^2V \twoheadleftarrow \cdots \twoheadleftarrow V/p^nV \twoheadleftarrow \cdots$$

and

$$W/pW \twoheadleftarrow W/p^2W \twoheadleftarrow \cdots \twoheadleftarrow W/p^nW \twoheadleftarrow \cdots$$

that takes the image of T in each V/p^nV to the image of T' in the corresponding W/p^nW. This induces an isomorphism of the inverse limits, which are V and W, respectively. □

Theorem (I. S. Cohen). *Every complete local ring (R, m, K) has a coefficient ring. If the residue class field has characteristic $p > 0$, there is a unique coefficient ring containing a given lifting T to R of a p-base Λ for K.*

Proof. We may assume that K has characteristic $p > 0$: we already know that there is a coefficient field if the characteristic of K is 0.

Any coefficient ring for R containing T must map onto a coefficient ring for R/m^n containing the image of T. Here, there is a unique coefficient ring V_n, which may be described, for any sufficiently large $q = p^N$, as the smallest subring containing all qth powers and the image of T . We may take q large enough that it may be used in the description of coefficient rings V_{n+1} for R_{n+1} and V_n for R_n, and it is then clear that $R_{n+1} \twoheadrightarrow R_n$ induces $V_{n+1} \twoheadrightarrow V_n$. If we construct $\varprojlim_n V_n$ and $\varprojlim_n R_n$ as sequences of elements $\{r_n\}_n$ such that r_{n+1} maps to r_n for all n, it is clear that $\varprojlim_n V_n \subseteq \varprojlim_n R_n$. By part (b) of the Lemma on p. 2, $V = \varprojlim_n V_n$ is a coefficient ring, and so V is a coefficient ring for R. $\square$

Corollary. *Every complete local ring (R, m, K) is a homomorphic image of a complete regular local ring. In the equicharacteristic case, this may be taken to be a formal power series ring over a field. If R does not contain a field, we may take the regular ring to be formal power series over a Noetherian discrete valuation ring that maps onto a coefficient ring for R.*

Proof. We already know this in the equicharacteristic case. In the remaining cases, K has characteristic p and R has a coefficient ring which is either a Noetherian discrete valuation ring (V, pV, K) or of the form V/p^nV for such a ring V. Let $p, u_1, \ldots, u_s$ be generators for the maximal ideal of R, and map $V[X_1, \ldots, X_s] \to R$ as a V-algebra such that $X_j \mapsto u_j$, $1 \leq j \leq s$, which induces a map $V[[X_1, \ldots, X_s]] \to R$. By part (c) of the second Proposition on p. 7, this map is surjective. $\square$

Corollary. *Let (R, m, K) be a complete local ring of mixed characteristic $p > 0$. Let (V, pV, K) be a coefficient ring for R, and let $x_1, \ldots, x_{d-1} \in R$ have images that are a system of parameters for R/pR. Map $V[[X_1, \ldots, X_{d-1}]] \to R$ as V-algebras by sending X_j to x_j, $1 \leq j \leq d-1$. Then R is module-finite over the image of $V[[X_1, \ldots, X_{d-1}]]$, and if R is a domain, or, more generally, if p is part of a system of parameters for R (equivalently, p is not in any minimal prime of R such that $\dim(R/P) = \dim(R)$), then V is a Noetherian discrete valuation domain, and R is a module-finite extension of $V[[X_1, \ldots, X_{d-1}]]$.*

Proof. That R is module-finite over the image is immediate form part (b) of the second Proposition on p. 7. If p is part of a system of parameters, then $\dim(R) = d$. It follows that the kernel of the map from the domain $V[[X_1, \ldots, X_{d-1}]]$ to R is (0), or else R will be module-finite over a domain of dimension $d - 1$. $\square$

Note, however, that $R = V[[x]]/px$ is not module-finite over a formal power series ring over a coefficient ring. V is a coefficient ring, but p is not part of a system of parameters. R is one dimensional, and it is not module-finite over V.

A regular local ring (R, m, p) of mixed characteristic p is called *unramified* if, equivalently:

(1) $p \notin m^2$.

(2) R/pR is also regular.

A quotient of a regular local ring by an ideal J is regular if and only if J is generated by part of a minimal set of generators for the maximal ideal of the regular local ring.

(The "if" direction is clear: we may kill the generators of J one at a time. Each time, since the ring is a domain, the Krull dimension drops by exactly one, and so does the imbedding dimension. For the "only if" direction, note that if $J \subseteq m^2$ in nonzero, killing J decreases the Krull dimension without decrreasing the embedding dimension, and so the quotient ring cannot be regular. If $J \not\subseteq m^2$ then J contains an element x_1 that is part of a minimal set of generators for m. The result know follows by induction on $\dim(R)$ by passing to $J/x_1R \subseteq R/x_1R$. We have that R/x_1R is still regular, and the new quotient is still $\cong R/J$.) In particular, R/pR is regular if and only if p is part of a minimal set of generators for m, and this holds if and only if $p \notin m^2$. Note that if Q is a prime ideal of an unramified regular local ring of mixed characteristic, then if $p \notin Q$ we have that R_Q is an equicharacteristic 0 regular local ring, while if $p \in Q$ then R_Q is again unramified, because R_Q/pR_Q is a localization of R/pR and therefore is again regular.

Theorem. *Let (R, m, K) be a complete regular local ring of Krull dimension d. If R is equicharacteristic then $R \cong K[[X_1, \ldots, X_d]]$. If R is mixed characteristic with K of characteristic $p > 0$ then R is unramified if and only if $R \cong V[[X_1, \ldots, X_{d-1}]]$, a formal power series ring, where (V, pV, K) is a coefficient ring (and so is a complete Noetherian discrete valuation domain). If R is mixed characteristic with K of characteristic $p > 0$ then R is ramified regular iff $R \cong T/(p - G)$ where V is a coefficient ring that is a Noetherian discrete valuation domain, $T = V[[x_1, \ldots, x_d]]$ is a formal power series ring with maximal ideal m_T, and and $G \in m_T^2 - pT$.*

Proof. In the unramified case, p may be extended to a minimal set of generators for m, say $p, x_1, \ldots, x_{d-1}$. We are now in the situation of both preceding corollaries: we get a map $V[[X_1, \ldots, X_{d-1}]] \to R$ such that the residue field of V maps onto that of R, while the images of $p, x_1, \ldots, x_{d-1}$ generate m. This implies that the map is onto. But, as in preceding Corollary, the map is injective. Thus, $R \cong V[[X_1, \ldots, X_{d-1}]]$. Conversely, with (V, pV, K) a Noetherian complete discrete valuation domain, $V[[X_1, \ldots, X_{d-1}]]$ is a complete regular local ring of mixed characteristic and $p \notin m^2$.

Now suppose that $p \in m^2$. Choose a minimal set of generators $x_1, \ldots, x_d$ for m. The we still get a surjection $V[[X_1, \ldots, X_d]] \twoheadrightarrow R$. Since R is regular it is a domain, and the kernel must be a height one prime of $T = V[[x_1, \ldots, x_d]]$, since $\dim(R) = d$. But $V[[x_1, \ldots, x_d]]$ is regular, and therefore a UFD, and so this height one prime P is principal. Since $p \in m^2$ and m_T^2 maps onto m^2, we get an element of $\mathrm{Ker}\,(T \twoheadrightarrow R)$ of the form $p - G$, where $G \in m_T^2$. The element G cannot be divisible by p: if it were, $G = pG_0$ with $G_0 \in m$, and then $p - G = p(1 - G_0)$ generates pT, since $1 - G_0$ is a unit, while $p \neq 0$ in R. Conversely, if $G \in m_T^2$ and $G \notin pT$, then $p - G \in m_T - m_T^2$, and so it is part of a minimal set of generators for m_T. Therefore $R = T/(p - G)$ is regular. Since $G \notin pT$, $p - G$ and p are not associates, and, in particular, p is not a multiple of $p - G$. Since p is nonzero in R, R is of mixed characteristic. Since $G \in m_T^2$, p is in the square of the maximal ideal of R, i.e., R is a ramified regular local ring. $\square$

Corollary. *Every complete local ring (R, m, K) is a homomorphic image of a complete regular local ring. In the equicharacteristic case, this may be taken to be a formal power series ring over a field. If R does not contain a field, we may take the regular ring to be*

formal power series over a Noetherian discrete valuation ring that maps onto a coefficient ring for R.

Proof. We already know this in the equicharacteristic case. In the remaining cases, K has characteristic p and R has a coefficient ring which is either a Noetherian discrete valuation ring (V, pV, K) or of the form V/p^nV for such a ring V. Let $p, u_1, \ldots, u_s$ be generators for the maximal ideal of R, and map $V[X_1, \ldots, X_s] \to R$ as a V-algebra such that $X_j \mapsto u_j$, $1 \leq j \leq s$, which induces a map $V[[X_1, \ldots, X_s]] \to R$. By part (c) of the second Proposition on p, 7, this map is surjective. □

Corollary. *Let (R, m, K) be a complete local ring of mixed characteristic $p > 0$. Let (V, pV, K) be a coefficient ring for R, and let $x_1, \ldots, x_{d-1} \in R$ have images that are a system of parameters for R/pR. Map $V[[X_1, \ldots, X_{d-1}]] \to R$ as V-algebras by sending X_j to x_j, $1 \leq j \leq d-1$. Then R is module-finite over the image of $V[[X_1, \ldots, X_{d-1}]]$, and if R is a domain, or, more generally, if p is part of a system of parameters for R (equivalently, p is not in any minimal prime of R such that $\dim(R/P) = \dim(R)$), then V is a Noetherian discrete valuation domain, and R is a module-finite extension of $V[[X_1, \ldots, X_{d-1}]]$.*

Proof. That R is module-finite over the image is immediate form part (b) of the second Proposition on the third page of the Lecture Notes of January 12. If p is part of a system of parameters, then $\dim(R) = d$. It follows that the kernel of the map from the domain $V[[X_1, \ldots, X_{d-1}]]$ to R is (0), or else R will be module-finite over a domain of dimension $d-1$. □

Note, however, that $R = V[[x]]/(px)$ is not a module-finite extension of a formal power series ring over a coefficient ring. V is a coefficient ring, but p is not part of a system of parameters. R is one dimensional, and it is not module-finite over the image of V.