NOTES ON COMMUTATIVE ALGEBRA

TAMÁS SZAMUELY

CONTENTS

1. DIMENSION OF RINGS, RINGS OF LOW DIMENSION

All rings are supposed to be commutative and have a unit element. We start with the following basic definition.

Definition 1.1. Let A be a ring and $P \subseteq A$ be a prime ideal. Define the *height* of P by

$$\mathrm{ht}(P) := \sup\{r \in \mathbb{N} \mid \exists P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_r \subsetneq P \text{ chain of prime ideals in } P\}$$

The *Krull dimension* of the ring A is

$$\dim(A) := \sup\{\mathrm{ht}(P) \mid P \subseteq A \text{ prime}\}$$

In particular, when A is a *local* ring, i.e. it has a unique maximal ideal P, we have $\dim(A) = \mathrm{ht}(P)$.

We shall prove later that over a field k both the polynomial ring $k[x_1, \ldots, x_n]$ and the power series ring $k[[x_1, \ldots, x_n]]$ have Krull dimension n. In both cases $(x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \ldots, x_n)$ is a chain of prime ideals of maximal length. Note, however, that whereas $k[x_1, \ldots, x_n]$ is a finitely generated k-algebra and n is its minimal number of generators, this is not the case for $k[[x_1, \ldots, x_n]]$.

Remarks 1.2.
1. For A the coordinate ring of an affine variety X the chain $P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_r$ corresponds to a chain of irreducible subvarieties $Z_1 \supsetneq Z_2 \supsetneq \cdots \supsetneq Z_r$ contained in X. The dimension is thus the length of the longest such chain. This is a non-linear version of the definition of the dimension of a vector space V as the length of a maximal chain of subspaces in V.
2. Recall that for a prime ideal $P \subset A$ the map $Q \mapsto QA_P$ induces a bijection between prime ideals $Q \subset P$ and the prime ideals of the localization A_P. This implies $\mathrm{ht}(P) = \mathrm{ht}(PA_P) = \dim(A_P)$.

Let us look at examples of rings of low Krull dimension. Obviously, a field has Krull dimension 0. More generally, we have:

Proposition 1.3. *A Noetherian local ring A is of Krull dimension 0 if and only if it is Artinian.*

Examples of such rings other than fields include the rings $\mathbf{Z}/p^n\mathbf{Z}$ for p a prime number and $n > 1$ as well as $k[t]/(t^n)$ for t a field and $n > 1$. The maximal ideals are generated by p and t, respectively.

For use in the proof below we recall the following lemma.

Lemma 1.4. *The set of nilpotent elements in a ring A is an ideal, and equals the intersection of the prime ideals in A.*

The above ideal is called the *nilradical* of A.

Proof. The first statement is clear as the radical $\sqrt{I}$ of any ideal is again an ideal. For the second one, note first that a nilpotent element is contained in every prime ideal. Conversely, assume $f \in A$ is not nilpotent. We find a prime ideal not containing f. Consider the partially ordered set of ideals in A that do not contain any power of f. This set is not empty (it contains (0)) and satisfies the condition of Zorn's lemma, so it has a maximal element P. We contend that P is a prime ideal. Assume $x, y \in A \backslash P$; we have to show that $xy \notin P$. The ideals $P+(x)$, $P+(y)$ strictly contain P, hence by maximality of P both contain some power of f. But $(P + (x))(P + (y)) \subset P + (xy)$, and therefore $P + (xy)$ also contains some power of f, hence cannot equal P. This means $xy \notin P$. □

Proof of Proposition 1.3. Assume A is of Krull dimension 0. Then by Lemma 1.4 the maximal ideal P consists of nilpotent elements. Since A is Noetherian, P is finitely generated so for a generating system $y_1, \ldots, y_k$ there is a big enough exponent N such that $y_i^N = 0$ for all i. Hence all products of $k \cdot N$ elements in P are zero,i.e. $P^{kN} = 0$. Now we have a finite descending filtration $A \supseteq P \supseteq P^2 \supseteq P^3 \supseteq \cdots \supseteq$

$P^{kN} = 0$ of A where every quotient is a finite dimensional vector space over the field A/P, hence an Artinian A-module. Since an extension of Artinian modules is again Artinian, we are done by induction.

Conversely, assume A is Artinian, and $Q \subset P$ is a prime ideal in A. We show $Q = P$; for this we may replace A by A/Q and assume moreover that A is an integral domain. Suppose there were a nonzero element $x \in P$. As A is Artinian, the chain $(x) \supset (x^2) \supset (x^3) \supset \cdots$ must stabilize, i.e we find n such that $(x^n) = (x^{n+1})$. In particular, $x^n = rx^{n+1}$ for some $r \in A$. Since A is an integral domain, this implies $rx = 1$ which is impossible for $x \in P$. □

Remark 1.5. In fact, the proposition is true without assuming A local; see e.g. the book of Atiyah–MacDonald.

Next an important class of local rings of dimension 1.

Definition 1.6. A ring A is a *discrete valuation ring* if A is a local principal ideal domain which is not a field.

Basic examples of discrete valuation rings are localizations of $\mathbf{Z}$ or $k[x]$ at a (principal) prime ideal as well as power series rings in one variable over a field.

In the proposition below we prove that discrete valuation rings are of Krull dimension 1 and much more. Observe first that if A is a local ring with maximal ideal P, then the A-module P/P^2 is in fact a vector space over the field $\kappa(P) = A/P$, simply because multiplication by P maps P into P^2.

Proposition 1.7. *For a local domain A with maximal ideal P and fraction field K the following conditions are equivalent:*

(1) *A is a discrete valuation ring.*
(2) *A is Noetherian of Krull dimension 1 and P/P^2 is of dimension 1 over $\kappa(P)$.*
(3) *The maximal ideal P is principal, and after fixing a generator t of P every element $x \neq 0$ in K can be written uniquely in the form $x = ut^n$ with u a unit in A and $n \in \mathbf{Z}$.*

For the proof we need the following well-known lemma which will be extremely useful in other situations as well:

Lemma 1.8 (Nakayama)**.** *Let A be a local ring with maximal ideal P and M a finitely generated A-module. If $PM = M$, then $M = 0$.*

Proof. Assume $M \neq 0$ and let $m_0, \ldots, m_n$ be a minimal system of generators of M over A. By assumption m_0 is contained in PM and hence we have a relation $m_0 = p_0 m_0 + \ldots, p_n m_n$ with all the p_i elements of P. But here $1 - p_0$ is a unit in A (as

otherwise it would generate an ideal contained in P) and hence by multiplying the equation by $(1-p_0)^{-1}$ we may write m_0 as a linear combination of the other terms, which is in contradiction with the minimality of the system. □

Nakayama's lemma is often used through the following corollary.

Corollary 1.9. *Let A, P, M be as in the lemma and assume given elements $t_1, \dots, t_m \in M$ whose images in the A/P-vector space M/PM form a generating system. Then they generate M over A.*

Proof. Let T be the A-submodule generated by the t_i; we have $M = T + PM$ by assumption. Hence $M/T = P(M/T)$ and the lemma gives $M/T = 0$. □

Before proving the proposition we need another easy lemma which we'll prove in a much more general form later (see Remark 5.17 below).

Lemma 1.10. *Let A be a Noetherian integral domain and $t \in A$ an element which is not a unit. Then $\cap_n (t^n) = (0)$.*

Proof. The case $t = 0$ is obvious. Otherwise suppose $a \in \cap_n (t^n)$ is a nonzero element. Then $a = a_1 t$ for some $a_1 \in A$. Since $a \in (t^2)$, there is a_2 such that $a = a_2 t^2$, so since A is a domain we have $a_1 = a_2 t$. Repeating the argument we obtain an increasing chain of ideals $(a_1) \subset (a_2) \subset (a_3) \subset \cdots$ with $a_i = a_{i+1} t$. Here the inclusions are strict because an equality $(a_i) = (a_{i+1})$ would imply that for some s we have $a_{i+1} = a_i s = a_{i+1} t s$ which is impossible as t is not a unit. This contradicts the assumption that A is Noetherian. □

Proof of Proposition 1.7. To prove $(1) \Rightarrow (2)$, assume A is a discrete valuation ring and P is generated by t. Since A is a principal ideal domain, every nonzero prime ideal is generated by some prime element p. But (p) is contained in the maximal ideal $P = (t)$, which means that t divides p. But this is only possible if $(p) = (t) = P$, so A is of Krull dimension 1. Also, the image of t is a basis of the vector space P/P^2, whence (2). Next, assume (2) and apply Corollary 1.9 with $M = P$. It follows that the maximal ideal P of A is generated by some element t. To prove (3), it will suffice to show that it holds for every nonzero element $a \in A$ with $n \geq 0$. To find n, observe that by Corollary 1.10 there is a unique $n \geq 0$ for which $a \in P^n \setminus P^{n+1}$ which means that a can be written in the required form. Moreover, if $a = ut^n = vt^n$, then $u = v$ since A is a domain. Finally, assume (3) and take a nonzero ideal I of A. Note that condition (3) also implies $\cap_n (t^n) = (0)$, and therefore there is an $n > 0$ that is maximal with the property that $I \subset (t^n)$. By maximality of n we find an element $a \in I$ not contained in (t^{n+1}), whence $(t^n) = (a) \subset I$, from which $I = (t^n)$ follows. □

We now explain the origin of the name "discrete valuation ring".

Definition 1.11. For any field K, a *discrete valuation* is a surjection $v : K \to \mathbf{Z} \cup \{\infty\}$ with the properties

$$v(xy) = v(x) + v(y),$$
$$v(x + y) \geq \min\{v(x), v(y)\},$$
$$v(x) = \infty \text{ if and only if } x = 0.$$

The elements $x \in K$ with $v(x) \geq 0$ form a subring $A \subset K$ called the *valuation ring* of v.

Proposition 1.12. *A domain A is a discrete valuation ring if and only if it is the valuation ring of some discrete valuation $v : K \to \mathbf{Z} \cup \{\infty\}$, where K is the fraction field of A.*

Proof. Assume first A is a discrete valuation ring. Define a function $v : K \to \mathbf{Z} \cup \{\infty\}$ by mapping 0 to ∞ and any $x \neq 0$ to the integer n given by Proposition 1.7 (3). It is immediate to check that v is a discrete valuation with valuation ring A. Conversely, given a discrete valuation v on K, the elements of A with $v(a) > 0$ form an ideal $P \subset A$ with the property that $a \in P \setminus \{0\}$ if and only if $a^{-1} \notin A$. It follows that $A \setminus P = \{a \in A : v(a) = 0\}$ is the set of units in a and hence A is local with maximal ideal P. Note that if t is an element of P with $v(t) = 1$, then for every $p \in P$ we have $v(p/t) = v(p) - 1 \geq 0$, so that $p/t \in A$ and therefore $(t) = P$. Similarly, if $a \in K$ is a nonzero element with $v(a) = n$, we have $v(a/t^n) = 0$ and condition (3) of the above proposition follows. □

Examples 1.13.

(1) The discrete valuation corresponding to $k[[t]]$ is the function $k((t)) \to \mathbf{Z} \cup \{\infty\}$ sending a power series to the order of its zero or pole at 0.
(2) The ring $\mathbf{Z}_{(p)}$ is the valuation ring of the discrete valuation $\mathbf{Q} \to \mathbf{Z} \cup \{\infty\}$ sending 0 to ∞ and a rational number $a/b \neq 0$ to the unique integer n such that $a/b = p^n(a'/b')$ with a', b' prime to p. This defines an infinite number of different discrete valuations on $\mathbf{Q}$, one for each prime p.
(3) Similarly, one can consider the discrete valuation on $k(t)$ sending 0 to ∞ and a rational function $p/q \neq 0$ to the unique integer n such that $p/q = t^n(p'/q')$ with $p'(0) \neq 0$, $q'(0) \neq 0$. Its valuation ring is the localization $k[t]_{(t)} \subset k(t)$.

    More generally, for each $a \in k$ the localization $k[t]_{(t-a)} \subset k(t)$ is a discrete valuation ring corresponding to the discrete valuation taking the 'order of zero or pole' of a function at $t = a$.

There is another very useful characterization of discrete valuation rings which uses the notion of integral closure. We begin by some reminders. Recall that given an extension of rings $A \subset B$, an element $b \in B$ is said to be *integral* over A if it is a

root of a *monic* polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$. There is the following characterization of integral elements:

Lemma 1.14. *Let $A \subset B$ an extension of rings. The following are equivalent for an element $b \in B$:*

(1) *The element b is integral over A.*
(2) *The subring $A[b]$ of B is finitely generated as an A-module.*
(3) *There is a subring C of B containing b which is finitely generated as an A-module.*
(4) *There exists a faithful $A[b]$-module C that is finitely generated as an A-module.*

Recall that an A-module C is faithful if there is no nonzero $a \in A$ with $aC = 0$.

Proof. For the implication $(1) \Rightarrow (2)$ note that if b satisfies a monic polynomial of degree n, then $1, b, \ldots, b^{n-1}$ is a basis of $A[b]$ over A. The implication $(2) \Rightarrow (3)$ is trivial, and $(3) \Rightarrow (4)$ follows because if C is a subring as in (3) and $a \in A[b]$ satisfies $aC = 0$, then $a = a \cdot 1 = 0$. Now only $(4) \Rightarrow (1)$ remains. For this let $c_1, \ldots, c_m$ be a system of A-module generators for C and consider the A-module endomorphism of C given by multiplication by b. For all i we have $bc_i = a_{i1}c_1 + \cdots + a_{im}c_m$ with some $a_{ij} \in A$. It follows that the system of homogeneous equations

$$a_{i1}c_1 + \ldots (a_{ii} - b)c_i + \cdots + a_{im}c_m = 0$$

for $i = 1, \ldots, m$ has a nontrivial solution in the c_i, hence by Cramer's rule the determinant of the coefficient matrix annihilates the c_i and therefore equals 0 by faithfulness of C. This determinant is, up to sign, a monic polynomial in $A[x]$ evaluated at $x = b$. □

Corollary 1.15. *Those elements of B which are integral over A form a subring in B.*

Proof. Given two elements $b_1, b_2 \in B$ integral over A, the elements $b_1 - b_2$ and $b_1 b_2$ are both contained in the subring $A[b_1, b_2]$ of B. This subring is a finitely generated A-module since $A[b_1]$ and $A[b_2]$ are, so condition (3) holds. □

If all elements of B are integral over A, we say that the extension $A \subset B$ is *integral*.

Corollary 1.16. *Given a tower of extensions $A \subset B \subset C$ with $A \subset B$ and $B \subset C$ integral, the extension $A \subset C$ is also integral.*

Proof. Each $c \in C$ satisfies a monic polynomial equation $c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0$ with $b_i \in B$ and is therefore integral over the A-subalgebra $A[b_0, \ldots, b_{n-1}] \subset B$. This is a finitely generated A-module because the b_i are integral over A, hence so is the A-subalgebra $A[b_0, \ldots, b_{n-1}, c] \subset C$. □

For later use we note the following fact.

Lemma 1.17. *If $A \subset B$ is an integral extension of integral domains, then A is a field if and only if B is a field.*

Proof. Assume first A is a field. If $b \in B$ is a nonzero element, it satisfies a monic polynomial equation

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$$

with $a_i \in A$ and $a_0 \neq 0$ (this latter fact uses that B is an integral domain). But then $(-a_0^{-1})(b^{n-1} + b_{n-1}b^{n-2} + \cdots + a_1)$ is an inverse for b, which shows that B is a field.

For the converse, suppose B is a field and given $a \in A$, pick $b \in B$ with $ab = 1$. Since B is integral over A, we also find $a_i \in A$ with $b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$ by Lemma 1.14. Multiplying by a^{n-1} we obtain $b = -a_{n-1} - \cdots - a_1 a^{n-2} - a_0 a^{n-1} \in A$ as required. □

If A is a domain with fraction field K and L is an extension of K, the *integral closure* of A in L is the subring of L formed by elements integral over A. We say that A is *integrally closed* if its integral closure in the fraction field K is just A. By Corollary 1.16 the integral closure of a domain A in some extension L of its fraction field is integrally closed.

Example 1.18. A unique factorization domain A is integrally closed. Indeed, we may write every element of the fraction field K in the form a/b with a, b coprime. If it satisfies a monic polynomial equation $(a/b)^n + a_{n-1}(a/b)^{n-1} + a_1(a/b) + a_0 = 0$ with coefficients in A, then after multiplying with b^n we see that a^n should be divisible by b, which is only possible when b is a unit.

In particular, the ring **Z** is integrally closed.

Now we can state:

Proposition 1.19. *A local domain A is a discrete valuation ring if and only if A is Noetherian, integrally closed and its Krull dimension is 1.*

Integrally closed Noetherian domains of Krull dimension 1 are usually called *Dedekind domains.* So the proposition says that a local Dedekind domain is the same thing as a discrete valuation ring.

For the proof recall the following lemma which is a starting point of the theory of associated primes.

Lemma 1.20. *Let A be a Noetherian ring, M a nonzero A-module and I a maximal element in the system of ideals of A that are annihilators of nonzero elements of M. Then I is a prime ideal.*

Recall that the annihilator of $m \in M$ is the ideal $\{a \in A : am = 0\} \subset A$. A maximal element I as in the lemma exists because A is Noetherian.

Proof. Suppose I is the annihilator of $m \in M$ and $ab \in I$ but $a \notin I$. Then $am \neq 0$ and its annihilator J contains b. But I is also contained in J, and hence $I = J$ by maximality of I. We conclude that $b \in I$. □

Proof of Proposition 1.19. Necessity of the conditions has already been checked. For sufficiency, let P be the maximal ideal of A and fix a nonzero $x \in P$. Applying the lemma to the A-module $A/(x)$ and using the fact that P is the only nonzero prime ideal of A we find $a \in A$ such that P is the annihilator of a mod (x) in $A/(x)$ (note that the annihilator of 1 mod (x) is nonzero). We next show that we may find $y \in P$ such that $ay \notin xP$. Indeed, assume for contradiction that $aP \subseteq xP$. In the fraction field K of A we then have $(a/x)P \subset P$, so P is a faithful $A[a/x]$-module (as both $A[a/x]$ and P are subrings of K). As A is Noetherian, P is finitely generated as an A-module, so by Lemma 1.14 the element $a/x \in K$ is integral over A. But A is integrally closed, so $a/x \in A$ and therefore $a \in (x)$. But then the annihilator of a in $A/(x)$ is A and not P.

Finally, we show that for y as above we have $P = (y)$ and hence the criterion of Proposition 1.7 (2) holds. Since $ay \in (x)$ by definition of P but $ay \notin xP$, we must have $ay = xu$ with a unit $u \in A \setminus P$ and hence there is an equality of ideals $(x) = (ay)$. So $aP \subset (x)$ means that for every $p \in P$ we have $ap = ayb$ for some $b \in A$. Since A is a domain, we must have $p = yb$ and hence $p \in (y)$ as claimed. □

Remark 1.21. Let K be a field of characteristic 0. It contains $\mathbf{Q}$ as its prime subfield; let A be the integral closure of $\mathbf{Z}$ in K. Then A has Krull dimension 1. Indeed, if $P \subset A$ is a nonzero prime ideal and $x \in P$ a nonzero element, then x satisfies an irreducible monic polynomial equation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ over $\mathbf{Z}$. Here $a_0 \in P \cap \mathbf{Z}$ is a nonzero element by irreducibility of the polynomial, so $P \cap \mathbf{Z} \neq (0)$ and therefore $P \cap \mathbf{Z} = (p)$ for some prime number p. But then $\mathbf{Z}/p\mathbf{Z} \subset A/P$ is an integral extension of integral domains, so A/P is a field by Lemma 1.17. This shows that P is maximal.

Assume moreover K is a finite extension of $\mathbf{Q}$; in this case K is called an *algebraic number field* and A the *ring of integers* of K. Then it can be proven using arguments from field theory that A is a finitely generated $\mathbf{Z}$-module; in particular, it is Noetherian. Thus the localization A_P by a maximal P as above is a discrete valuation ring by Proposition 1.19 (one checks easily that localizations of integrally closed domains are again integrally closed). We conclude that the ring of integers in a number field is a Dedekind domain (in fact, this was the first example studied historically).

We conclude this section with a structure theorem for ideals in Dedekind domains, generalizing unique factorization in $\mathbf{Z}$.

Theorem 1.22. *In a Dedekind domain every ideal $I \neq 0$ can be written uniquely as a product $I = P_1^{n_1} \cdots P_r^{n_r}$, where the P_i are prime ideals.*

Recall the following basic property of Noetherian rings:

Lemma 1.23. *If A is a Noetherian ring and $I \subset A$ is an ideal, there are finitely many prime ideals $P \supset I$ that are minimal with this property.*

Proof. We first show that the radical $\sqrt{I}$ is the intersection of finitely many prime ideals. Indeed, assume this is not the case. Since A is Noetherian, we may assume I is maximal with this property. Plainly $\sqrt{I}$ cannot be a prime ideal, so we find $a_1, a_2 \notin \sqrt{I}$ with $a_1 a_2 \in \sqrt{I}$. For $i = 1, 2$ let I_i be the intersection of the prime ideals containing I and a_i. Then $I_1 \cap I_2 = \sqrt{I}$ by Lemma 1.4 applied to $A/\sqrt{I}$, but each I_i is the intersection of finitely many prime ideals by maximality of I, contradiction.

Now if $\sqrt{I} = P_1 \cap \cdots \cap P_r$ with some prime ideals P_i and $P \supset I$ is a prime ideal different from the P_i, then $P \supset P_1 \cdots P_r$ and therefore $P \supset P_i$ for some i, so P is not minimal above I. □

We shall need another easy lemma:

Lemma 1.24. *Let A be an arbitrary ring, I, J ideals of A. We have $I = J$ if and only if $IA_P = JA_P$ for all maximal ideals $P \subset A$.*

Proof. For the nontrivial implication assume $a \in J$ is not contained in I. Then $\{x \in A : xa \in I\} \subset A$ is an ideal different from A, hence contained in a maximal ideal P. By definition, the image of a in JA_P lies in IA_P if and only if $sa \in I$ for some $s \in A \setminus P$ but that's not possible by choice of P, so $IA_P \neq JA_P$. □

Proof of Theorem 1.22. Since $\dim(A) = 1$, there are only finitely many prime ideals $P_1, \ldots, P_r$ containing I by Lemma 1.23. Since A_{P_i} is a discrete valuation ring for all i, we have $IA_{P_i} = (t_i^{n_i})$ for some $n_i > 0$, where t_i generates $P_i A_{P_i}$. So $IA_{P_i} = P_i^{n_i} A_{P_i}$ for all i. Now consider $J = P_1^{n_1} \cdots P_r^{n_r}$. If P is a prime ideal different from the P_i, it does not contain I by assumption and therefore cannot contain any of the P_i. Since it is a prime ideal, it cannot contain J either, so for $P \neq P_i$ we have $IA_P = JA_P = A_P$. A similar reasoning shows that for $i \neq j$ we have $P_i \not\supset P_j^{n_j}$, so $P_j^{n_j} A_{P_i} = A_{P_i}$ and therefore $IA_{P_i} = P_i^{n_i} A_{P_i} = JA_{P_i}$. Now the lemma above shows $I = J$. □

2. Dimension of finitely generated algebras

In this section we compute the Krull dimension of fintely generated algebras by means of another invariant.

Definition 2.1. Let A be an integral domain containing a field k. Elements $a_1, \dots, a_r \in A$ are called *algebraically dependent* if there exists a nonzero polynomial $f \in k[x_1, \dots, x_r]$ such that $f(a_1, \dots, a_r) = 0$; otherwise they are *algebraically independent.*

The *transcendence degree* of A over k is the maximal number of elements in A that are algebraically independent over k; it may be infinite.

From now on we assume that A is a *finitely generated* k-algebra that is moreover an integral domain. Under this assumption the transcendence degree is finite; we denote it by $\mathrm{tr.deg}_k(A)$.

Theorem 2.2. *Under the above assumptions* $\mathrm{tr.deg}_k(A) = \dim A$.

The inequality $\mathrm{tr.deg}_k(A) \geq \dim A$ is easy to prove; indeed, it results from the following lemma by induction along a chain of prime ideals.

Lemma 2.3. *Let A be as above and $P \subset A$ a nonzero prime ideal. Then* $\mathrm{tr.deg}_k(A/P) < \mathrm{tr.deg}_k(A)$.

Proof. Let $\bar{a}_1, \dots, \bar{a}_r$ be a system of algebraically independent elements in A/P, with $r = \mathrm{tr.deg}_k(A/P)$. Lift the $\bar{a}_i$ to elements $a_i \in A$ and let $a_0 \in P$ be a nonzero element. It suffices to show that $a_0, a_1 \dots, a_r$ are algebraically independent over k. Assume not, and let $f \in k[x_0, x_1, \dots, x_r]$ be a nonzero polynomial with $f(a_0, a_1, \dots, a_r) = 0$. As A is a domain,we may assume that f is irreductible, and in particular not divisible by x_0. But then $f(0, x_1, \dots, x_r) \in k[x_1, \dots, x_r]$ is a nonzero polynomial with $f(0, \bar{a}_1, \dots, \bar{a}_r) = 0$, contradiction. □

The proof of the reverse inequality is based on two ingredients. The first is:

Lemma 2.4 (Noether's normalization lemma)**.** *Assume A has transcendence degree d over k. Then there exist algebraically independent elements $x_1, \dots, x_d$ such that A is a finitely generated module over the subring $k[x_1, \dots, x_d] \subset A$.*

Here we mean the k-subalgebra of A generated by $x_1, \dots, x_d$; by algebraic independence it is isomorphic to the polynomial ring $k[x_1, \dots, x_d]$.

Proof. We only do the case where k is infinite; it is a bit easier. Let $x_1, \dots, x_n$ be a system of k-algebra generators for A; we may assume that the first d are algebraically independent. We do induction on n starting from the case $n = d$ which is obvious. Assume the case $n - 1$ has been settled. Since $n > d$, there is a nonzero polynomial f in n variables over k such that $f(x_1, \dots, x_n) = 0$. Denote by m the degree of f and by f_m its homogeneous part of degree m. Since k is infinite, we find $a_1, \dots, a_{n-1} \in k$ such that $f_m(a_1, \dots, a_{n-1}, 1) \neq 0$. Setting $x_i' := x_i - a_i x_n$ for $i = 1, \dots, n-1$ we

compute

$$0 = f(x_1, \dots, x_n) = f(x'_1 + a_1 x_n, \dots, x'_{n-1} + a_{n-1} x_n, x_n) = \\ = f_m(a_1, \dots, a_{n-1}, 1) x_n^m + g_{m-1} x_n^{m-1} + \cdots + g_0$$

with some $g_i \in k[x'_1, \dots, x'_{n-1}]$. Dividing by $f_m(a_1, \dots, a_{n-1}, 1)$ we see that x_n satisfies a monic polynomial relation with coefficients in $k[x'_1, \dots, x'_{n-1}]$, so that $A = k[x'_1, \dots, x'_{n-1}][x_n]$ is a finitely generated module over its subalgebra $k[x'_1, \dots, x'_{n-1}]$. By induction we know that $k[x'_1, \dots, x'_{n-1}]$ is a finitely generated module over the polynomial ring $k[x_1, \dots, x_d]$, and we are done. □

Now we turn to the second ingredient.

Lemma 2.5. *Suppose $A \subset B$ is an integral extension of rings. Given a prime ideal $P \subset A$, there exists a prime ideal $Q \subset B$ such that $Q \cap A = P$.*

Proof. Localizing both A and B by the multiplicatively closed subset $A \setminus P$ we obtain a ring extension $A_P \subset B_P$ where A_P is local with maximal ideal P. We contend that $PB_P \neq B_P$. Indeed, otherwise we have an equation $1 = p_1 b_1 + \cdots + p_r b_r$ with $p_i \in P$ and $b_i \in B_P$. If $C \subset B_P$ is the A_P-subalgebra generated by the b_i, then C satisfies $PC = C$ and moreover is finitely generated as an A_P-module because the b_i are integral over A_P. Thus $C = 0$ by Nakayama's lemma which is impossible since $1 \in C$. Therefore indeed $PB_P \neq B_P$ and we find a maximal ideal $Q_P \subset B_P$ containing PB_P. By construction $Q_P \cap A_P \supset P$, hence $Q_P \cap A_P = P$ by maximality of P. Thus $Q := Q_P \cap B$ will do. □

Corollary 2.6 (Going up theorem of Cohen–Seidenberg)**.** *Under the assumptions of the lemma given a chain $P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_r$ of prime ideals in A, there exists a chain $Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq Q_r$ of prime ideals in B such that $Q_i \cap A = P_i$ for $i = 1, \dots, r$.*

Proof. We use induction on r. By the lemma we find $Q_1 \subset B$ with $Q_1 \cap A = P_1$. Assume $Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq Q_{r-1}$ have been constructed, and denote by $\bar{P}_r$ the image of P_r in A/P_{r-1}. Since B/Q_{r-1} is integral over A/P_{r-1}, the lemma gives a prime ideal $\bar{Q}_r$ in B/Q_{r-1} such that $\bar{Q}_r \cap (A/P_{r-1}) = \bar{P}_r$. Now take Q_r to be the preimage of $\bar{Q}_r$ in B. □

Proof of Theorem 2.2. By Noether's normalization lemma we find a polynomial ring $R := k[x_1, \dots, x_d]$ contained as a k-subalgebra in A such that A is a finitely generated R-module, so in particular $d = \mathrm{tr.deg}_k(A)$. Since A is integral over R, by the going up theorem we may extend the maximal chain $(0) \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \dots x_d)$ of prime ideals in R to a chain $(0) \subsetneq Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq Q_d$ of prime ideals in A, whence $\dim A \geq d$. As already noted, the reverse inequality follows from Lemma 2.3. □

Remark 2.7. The theorem contains as a special case the weak form of Hilbert's Nullstellensatz: if A as in the theorem is a field, it has Krull dimension 0, hence has transcendence degree 0 over k by the theorem, i.e. it is a finite extension. In particular, if moreover k is algebrically closed, it must be k itself. Consequently, if P is a maximal ideal in the polynomial ring $k[x_1, \dots, x_n]$ with k algebraically closed, we have $A := k[x_1, \dots, x_n]/P \cong k$, so denoting by a_i the image of x_i mod P we get $P \supseteq (x_1 - a_1, \dots, x_n - a_n)$. Since $(x_1 - a_1, \dots, x_n - a_n)$ is a maximal ideal, this inclusion is an equality. We have proven that every maximal ideal of $k[x_1, \dots, x_n]$ is of the form $(x_1 - a_1, \dots, x_n - a_n)$ with some $a_i \in k$.

We now prove a stronger form of Theorem 2.2.

Theorem 2.8. *Let A be an integral domain that is a finitely generated algebra of transcendence degree d over a field k. Every maximal chain of prime ideals of A has length d.*

As consequences we have:

Corollary 2.9. *Let A be as in the theorem.*

(1) *Every prime ideal $P \subset A$ satisfies the equality* $\mathrm{ht}(P) = \mathrm{tr.deg}_k(A) - \mathrm{tr.deg}_k(A/P)$.
(2) *Given two prime ideals $P \subset Q$ of A, every maximal chain of prime ideals between P and Q has length* $\mathrm{ht}(P) - \mathrm{ht}(Q)$.

Proof. For statement (1) choose a maximal chain of prime ideals $P_1 \subsetneq P_2 \cdots \subsetneq P_r \subsetneq P$ and extend it to a maximal chain $P_1 \subsetneq P_2 \cdots \subsetneq P_r \subsetneq P \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_s$ of prime ideals in A. By construction $\mathrm{ht}(P) = r$ and by the theorem $\dim(A) = r + s$, $\dim(A/P) = s$. Statement (2) follows from (1). □

Rings having the property in (2) above are called *catenary* rings.

The following proof of the theorem is based on:

Proposition 2.10 (Going down theorem of Cohen–Seidenberg)**.** *Let $A \subset B$ be an integral extension of integral domains such that A is integrally closed in its fraction field K and the fraction field L of B is a finite extension of K.*

Given prime ideals $P_1 \subsetneq P_2$ of A and a prime ideal $Q_2 \subset B$ with $Q_2 \cap A = P_2$, there exists a prime ideal $Q_1 \subsetneq Q_2$ of B with $Q_1 \cap A = P_1$.

Remarks 2.11.

1. Of course, as in Corollary 2.6 one concludes by induction that for every finite descending chain of prime ideals of A we can find a finite descending chain of prime ideals of B lying above it.
2. The proposition also holds without the assumption $L|K$ finite but we'll only use the finite case. The proof in the general case uses infinite Galois theory.

We begin the proof of the going down theorem with some preliminary observations.

Remarks 2.12.

1. If $A \subset B$ is an integral extension of rings and $Q_1 \subsetneq Q_2$ are prime ideals in B, then the intersections $P_i := Q_i \cap A$ satisfy $P_1 \subsetneq P_2$. Indeed, if $Q_1 \cap A = Q_2 \cap A = P$, then after localizing by $A \setminus P$ we obtain an integral extension $A_P \subset B_P$ with two prime ideals $Q_1 B_P \subsetneq Q_2 B_P$ whose intersection with A is the maximal ideal P. Passing to the integral extensions $A_P/PA_P \subset B_P/Q_i B_P$ we see from Lemma 1.17 that both $Q_1 B_P$ and $Q_2 B_P$ must be maximal ideals, which is impossible.

2. Let $A \subset B$ be an extension of integral domains and assume that the extension $K \subset L$ of their fraction fields is finite and purely inseparable. This means that both have characteristic $p > 0$ and $L = K(\sqrt[p^{r_1}]{a_1}, \ldots, \sqrt[p^{r_m}]{a_m})$ for some $a_i \in K$ and $r_i > 0$. In particular, for r large enough $L^{p^r} \subset K$. Assume moreover that $B \cap K = A$ (this is the case e.g. in the situation of the proposition). Then it is straightforward to check that if $P \subset A$ is a prime ideal, then $P^B := \{b \in B : b^{p^r} \in P\}$ is a prime ideal of B. Moreover $P^B \cap A = P$ and for a prime ideal $Q \subset B$ we have $(Q \cap A)^B = Q$. Thus the assignment $P \to P^B$ gives an inclusion-preserving bijection between the prime ideals of A and B.

Recall the following basic lemma that will serve many times.

Lemma 2.13. (Prime avoidance) *Let A be any ring, and $I_1, \ldots, I_n, J \subset A$ ideals such that all I_j are prime ideals except perhaps for I_{n-1} and I_n. If $J \not\subseteq I_j$ for all j, then there exists $x \in J$ such that $x \notin I_j$ for all $j \leq n$.*

Equivalently, $J \subseteq \cup I_j$ implies $J \subseteq I_j$ for some $j \leq n$.

Proof. Induction on n: the case $n = 1$ is clear. For $n > 1$, assume that $J \not\subseteq I_j$ for all j. By induction, for $i = 1, \ldots, n$ there exist $x_i \in J$ such that $x_i \notin I_j$ for all $j \neq i$. If for some i we also have $x_i \notin I_i$, we are done, so assume $x_i \in I_i$ for all i. Then for $n = 2$ we also get $x_1 + x_2 \notin I_1$ and $x_1 + x_2 \notin I_2$, so $x_1 + x_2$ works. If $n > 2$, then I_1 is necessarily a prime ideal, so $x_2 \cdots x_n \notin I_1$ and therefore $x_1 + x_2 \cdots x_n$ works. □

We also need the following lemma generalizing a well-known fact from algebraic number theory.

Lemma 2.14. *In the situation of the proposition assume moreover that B is the integral closure of A in L and the extension $L|K$ is Galois with group G. If $P \subset A$ is a prime ideal, then G acts transitively on the set of prime ideals $Q \subset B$ with $Q \cap A = P$.*

Note that if $\sigma \in G$ and $b \in B$, then $\sigma(b) \in B$ because it is integral over A (in fact it satisfies the same monic polynomial) and B is the integral closure of A in L. Furthermore, if $Q \subset B$ is a prime ideal, then $\sigma(Q) := \{\sigma(b) \in B : b \in Q\}$ is a prime ideal in B with $\sigma(Q) \cap A = Q \cap A = P$, which defines the G-action in the lemma.

Proof. Let $Q, Q' \subset B$ be prime ideals with $Q \cap A = Q' \cap A = P$ and assume that $\sigma(Q) \neq Q'$ for any $\sigma \in G$. Here $Q' \nsubseteq \sigma(Q)$ for any $\sigma \in G$ by Remark 2.12 (1), so by prime avoidance (Lemma 2.13) we find $b \in Q'$ such that $b \notin \sigma(Q)$ for any $\sigma \in G$. Then $N_{L|K}(b) := \Pi_{\sigma \in G}\sigma(b) \in B \cap K = A$ because b is fixed by G and A is integrally closed. But since G contains the identity map of L, we have $N_{L|K}(b) \in Q' \cap A = P$. But then $N_{L|K}(b) \in Q$, so since Q is a prime ideal, we have $\sigma(b) \in Q$ for some $\sigma \in G$, whence $b \in \sigma^{-1}(Q)$, a contradiction. □

Proof of Proposition 2.10. Assume first the extension $L|K$ is separable. Embed L in a finite Galois extension L' of K with group G, and let B' be the integral closure of A in L'. By the going up theorem we find prime ideals $Q_1' \subsetneq Q_2'$ in B' such that $Q_i' \cap A = P_i$ for $i = 1, 2$. Furthermore, by Lemma 2.5 we find a prime ideal $Q' \subset B'$ with $Q' \cap B = Q_2$. Since $Q' \cap A = Q_2' \cap A = P_2$, by Lemma 2.14 we find $\sigma \in G$ with $\sigma(Q_2') = Q'$. It follows that $\sigma(Q_1') \subset Q'$ is a prime ideal satisfying $\sigma(Q_1') \cap A = P_1$, and therefore $Q_1 := \sigma(Q_1') \cap B$ has the required properties.

In the general case let $K \subset L^s \subset L$ be the maximal separable subextension and set $B^s := B \cap L^s$. The proposition holds for the extension $A \subset B^s$ by the previous paragraph. Since $L|L^s$ is a purely inseparable extension, we conclude by applying Remark 2.12 (2) to the extension $B^s \subset B$. □

Now that the going down theorem is proven, we can turn to:

Proof of Theorem 2.8. We use induction on $d = \dim(A) = \mathrm{tr.deg}_k(A)$. The case $d = 0$ is clear because then A is a field. Assume $d > 0$ and use the Noether normalization lemma to find a polynomial ring $R := k[x_1, \ldots, x_d]$ over which A is finitely generated as a module. Consider a maximal chain $(0) \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_m$ of prime ideals of A, and set $P_i := Q_i \cap R$ for all i. Since $P_1 \neq (0)$ by Remark 2.12 (1), we find a nonzero irreducible polynomial $f \in P_1$. The principal ideal $(f) \subset P_1$ is a prime ideal as f is a prime element in the unique factorization domain $R = k[x_1, \ldots, x_d]$. If $(f) \neq P_1$, then applying the going down theorem to $(f) \subset P_1$ and Q_1 we find a prime ideal $Q_0 \subset Q_1$ in A with $Q_0 \cap R = (f)$. But then $(0) \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_m$ cannot be a maximal chain, so we have $(f) = P_1$. In this case $\bar{A} := A/Q_1$ is a finitely generated $R/(f)$-module, hence of transcendence degree $d - 1$. By induction every maximal chain of prime ideals in $\bar{A}$ has length $d - 1$, so every maximal chain in A starting with $(0) \subset Q_1$ has length d. As Q_1 was arbitrary, the theorem is proven. □

3. KRULL'S HAUPTIDEALSATZ

Our next topic is a fundamental theorem that gives a relation between the height of a prime ideal and the number of its generators.

Theorem 3.1. (Krull's Hauptidealsatz) *Let A be a Noetherian ring and $x \in A$. If P is a minimal prime ideal such that $x \in P$, then $\mathrm{ht}(P) \leq 1$.*

Note that the statement of the theorem is non-vacuous only if x is not a unit, so this is implicitly assumed. The following is Krull's original proof.

Proof. We show that if $Q \subsetneq P$ is a prime ideal, then $\mathrm{ht}(Q) = 0$. Replacing A by A_P we may assume that A is local with maximal ideal P. Define the *n-th symbolic power* of Q by

$$Q^{(n)} := \{q \in A \mid \exists s \notin Q \text{ such that } sq \in Q^n\}.$$

This is in fact the preimage of $(QA_Q)^n$ by the localization map $A \to A_Q$.

Since P is minimal over (x), the ring $A/(x)$ is local of Krull dimension 0, hence Artinian by Proposition 1.3. Therefore the chain

$$(x, Q) \supseteq (x, Q^{(2)}) \supseteq (x, Q^{(3)}) \supseteq \cdots$$

stabilizes at some level n. So if $f \in Q^{(n)} \subseteq (x, Q^{(n)}) = (x, Q^{(n+1)})$ then $f = ax + q$ for some $a \in A$ and $q \in Q^{(n+1)}$. Then $ax = f - q \in Q^{(n)}$ but $x \notin Q$ because $Q \subsetneq P$ and P is minimal over x. By definition, there exists $s \notin Q$ such that $sax \in Q^n$ but then $a \in Q^{(n)}$ since $sx \notin Q$ because Q is a prime ideal.

In summary, we got that $Q^{(n)} \subseteq (x)Q^{(n)} + Q^{(n+1)}$ and the reverse inclusion is automatic. Therefore, $Q^{(n)}/Q^{(n+1)} = P(Q^{(n)}/Q^{(n+1)})$ because $x \in P$ and we just proved that every element of $Q^{(n)}/Q^{(n+1)}$ can be expressed as an element of $(x)Q^{(n)}/Q^{(n+1)}$. So by Nakayama's lemma we get $Q^{(n)}/Q^{(n+1)} = 0$. In other words, $(QA_Q)^n = (QA_Q)^{n+1}$ as ideals in A_Q. Now we can apply Nakayama's lemma in A_Q where the maximal ideal is QA_Q, and obtain $(QA_Q)^n = 0$. Now we are left with a local ring with a nilpotent maximal ideal. By Lemma 1.4 this implies that QA_Q is the only prime ideal in A_Q, whence $\mathrm{ht}(Q) = 0$ as required. □

Remark 3.2. Equality does not always hold in the theorem. For instance, in the 0-dimensional ring $k[x]/(x^2)$ the image of x generates a prime ideal, and so does the image of 2 in the 0-dimensional ring $\mathbf{Z}/6\mathbf{Z}$.

In these examples, the generators of the principal ideal are zero-divisors. However, if x is not a zero-divisor and P is a minimal prime ideal above (x), then $\mathrm{ht}(P) = 1$. This is because the minimal prime ideals in A consist of zero-divisors. Indeed, if P is a minimal prime ideal, then A_P is local of dimension 0, so PA_P is a nilpotent

ideal. But then for every $y \in P$ we have $y^n = 0$ in A_P, i.e. $sy^n = 0$ for some $s \notin P$, and therefore y is a zero-divisor.

Theorem 3.3. (Generalization of Krull's Hauptidealsatz) *Let A be a Noetherian ring and $x_1, \dots, x_r \in A$. If P is a prime ideal which is minimal among the prime ideals with $x_i \in P$ for all i then $\mathrm{ht}(P) \leq r$.*

Proof. We proceed by induction on r. The case $r = 1$ is exactly the Hauptidealsatz. For $r > 1$ pick any prime ideal $P_1 \subsetneq P$ such that there does not exist P': $P_1 \subsetneq P' \subsetneq P$. We show that there exist $y_1, \dots, y_{r-1} \in A$ such that P_1 is minimal over $(y_1, \dots, y_{r-1})$, and then we can use induction.

We may assume that P is maximal by replacing A by A_P. Since $P_1 \subsetneq P$ and P is minimal above $(x_1, \dots, x_r)$, there exists an i such that $x_i \notin P_1$, say $i = r$. Then P is a minimal prime ideal such that $(x_r, P_1) \subseteq P$, hence $A/(x_r, P_1)$ has Krull dimension 0 with nilradical the image of P. Therefore for all $i \leq r-1$ we have $x_i^m = a_i x_r + y_i$ for some $y_i \in P_1$, $a_i \in A$ and big enough m. Thus the image of $(x_1, \dots, x_r)$ in $A/(y_1, \dots, y_{r-1}, x_r)$ is nilpotent; on the other hand the image of P in $A/(x_1, \dots, x_r)$ is the nilradical. We conclude that the image of P in $A/(y_1, \dots, y_{r-1}, x_r)$ is nilpotent, hence the image of P in $A/(y_1, \dots, y_{r-1})$ is minimal over (x_r). As such it has height ≤ 1 by the Hauptidealsatz, so the image of P_1 in $A/(y_1, \dots, y_{r-1})$ has height 0 as required. □

Remark 3.4. The previous theorem has the following geometric interpretation. Take $I = (f_1, \dots, f_r) \subset k[x_1, \dots, x_n]$ and consider $X = V(I) \subset \mathbb{A}^n$. The irreducible components of X correspond to the minimal prime ideals above I. The theorem then says that *each* of these components has dimension $\geq n - r$ (it would be much easier to prove that *some* component has dimension $\geq n - r$).

More generally, we may consider an affine variety $Y \subset \mathbb{A}^n$. The ideal I induces an ideal $\bar{I} = (\bar{f_1}, \dots, \bar{f_r}) \subset \mathcal{A}_Y$. The irreducible components of $X \cap Y$ correspond to the minimal prime ideals above $\bar{I}$. The theorem applied to $\bar{I}$ then says that each of these components has dimension $\geq \dim Y - r$.

Corollary 3.5. *In a Noetherian ring every prime ideal has finite height, hence the prime ideals satisfy the descending chain condition. Also, a Noetherian* local *ring has finite Krull dimension.*

Remark 3.6. The corollary does *not* imply that a Noetherian ring has finite Krull dimension; there are counterexamples to this statement.

The Hauptidealsatz has the following converse.

Theorem 3.7. *If A is Noetherian and $P \subset A$ is a prime ideal with $\mathrm{ht}(P) = r > 0$, there exist $x_1, \dots, x_r \in P$ such that P is minimal above $(x_1, \dots, x_r)$.*

Proof. We construct inductively a sequence $x_1, \ldots, x_r$ of elements of P with the property that for all $1 \leq i \leq r$ all minimal prime ideals above $(x_1, \ldots, x_i)$ will have height $\geq i$ (hence exactly i by the generalized Hauptidealsatz). For $i = r$ it will follow that P is minimal above $(x_1, \ldots, x_r)$, for otherwise its height would be $> r$.

For $1 < i \leq r$ assume we have already constructed $x_1, \ldots, x_{i-1}$. Consider the ideal

$$I_{i-1} := \begin{cases} (x_1, \ldots, x_{i-1}) & i > 1 \\ (0) & i = 1. \end{cases}$$

Choose an $x_i \in P$ not contained in the minimal primes above I_{i-1}. By Lemma 2.13 such an x_i exists; otherwise the lemma would give that one of the minimal primes above I_{i-1} contains P, but then Theorem 3.3 would give $\mathrm{ht}(P) \leq i - 1 < r$ which is impossible. Now a minimal prime ideal Q_i above $(x_1, \ldots, x_i)$ is not minimal above I_{i-1} by our choice of x_i, so it contains a prime ideal Q_{i-1} minimal above I_{i-1} which has height at least $i - 1$ by induction. Therefore $\mathrm{ht}(Q_i) \geq i$ as required. □

Corollary 3.8. *The height of a nonzero prime ideal P is the smallest integer r such that P is minimal above an ideal generated by r elements.*

As a first application of the above results we can compute the dimensions of some concrete rings. We begin by studying the behaviour of heights of prime ideals under homomorphisms.

Proposition 3.9. *Let $\varphi : A \to B$ be a homomorphism of Noetherian rings, $Q \subseteq B$ be a prime ideal, and $P := \varphi^{-1}(Q)$. Then $\mathrm{ht}(Q) \leq \mathrm{ht}(P) + \dim B_Q/PB_Q$.*

Here, as usual, the notation PB_Q stands for $\varphi(P)B_Q$.

Proof. Without loss of generality we may replace A by A_P, P by PA_P, B by B_Q and Q by QB_Q since the heights of P and Q do not change under these localizations. (Note also that the composite $A \xrightarrow{\varphi} B \to B_Q$ induces a map $A_P \to B_Q$ by the universal property of localization.) So we may assume that A and B are local and then we have to prove that $\dim B \leq \dim A + \dim B/PB$. Set $r := \mathrm{ht}(P)$ and $s := \mathrm{ht}(Q \bmod PB)$. By Proposition 3.7 we find $x_1, \ldots, x_r \in A$ such that P is minimal above them and similarly, we find $y_1, \ldots, y_s \in B$ such that Q modulo PB is minimal above $y_1 \ldots, y_s$ modulo PB. As in the proof of the Hauptidealsatz we obtain that for N and M sufficiently large $Q^N \subseteq PB + (y_1, \ldots, y_s)$ and $P^M \subseteq (x_1, \ldots, x_r)$. Therefore $Q^{NM} \subseteq (\varphi(x_1), \ldots \varphi(x_r), y_1, \ldots, y_s)$ and therefore Q is a minimal prime ideal above $(\varphi(x_1), \ldots \varphi(x_r), y_1, \ldots, y_s)$.

To sum up, we have $\dim(B) = \mathrm{ht}(Q) \leq r + s = \mathrm{ht}(P) + \dim(B/PB)$, where the inequality is a consequence of the Generalized Hauptidealsatz (Theorem 3.3). □

Remark 3.10. The proposition has an important geometric interpretation. We discuss an easy special case first. Suppose k is an algebraically closed field and $A = k[x]$, $B = k[x, y]$ with φ the natural inclusion. From the Nullstellensatz we know that maximal ideals of $k[x, y]$ are of the form $Q = (x - a, y - b)$ for $a, b \in K$. Here $P = \phi^{-1}(Q) = (x-a)$, so geometrically ϕ corresponds to the projection $\pi : \mathbf{A}^2_k \to \mathbf{A}^1_k$ given by $(a, b) \mapsto a$. We have $B/PB = k[x, y]/(x - a) \cong k[y]$ which is a ring of dimension 1, and so is the localization B_Q/PB_Q. The maximal ideals of B/PB correspond to points with first coordinate a, i.e. the points in the fibre of π above the point $x = a$ of $\mathbf{A}^1_k$. The Proposition says that this fibre has dimension at least $\mathrm{ht}(Q) - \mathrm{ht}(P) = 2 - 1 = 1$ which is indeed true.

In general, a homomorphism $\phi : A \to B$ of finitely generated k-algebras corresponds to a map of affine varieties $X \to Y$ and the proposition translates as the fact that every fibre of such a morphism has dimension at least $\dim(X) - \dim(Y)$. In the above example equality holds for all fibres but not in general; for instance, there are morphisms of surfaces that contract whole curves.

As a consequences of the proposition we can determine the Krull dimension of polynomial and power series rings.

Corollary 3.11. *If A is a Noetherian ring, then $\dim A[x] = \dim A + 1$. Consequently, $\dim A[x_1, \ldots, x_n] = \dim A + n$.*

Here by convention "$\infty + 1 = \infty$".

Proof. The inequality $\dim A[x] \geq \dim A+1$ is easy: a chain of prime ideals $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ in A can be considered as a chain of prime ideals in $A[x]$ using the natural embedding $A \hookrightarrow A[x]$ since the quotients $A[x]/P_iA[x] \cong (A/P_i)[x]$ are again integral domains. However, a maximal ideal $P_n \subset A$ will not be maximal in $A[x]$ because the quotient $(A/P_n)[x]$ is not a field, so the Krull dimension of $A[x]$ is strictly larger.

Conversely, it is enough to show that for a maximal ideal $Q \subset A[x]$ we have $\mathrm{ht}(Q) \leq \mathrm{ht}(A \cap Q) + 1$. For this, set $P := A \cap Q$ which is a prime ideal in A. By the previous proposition we know that

$$\mathrm{ht}(Q) \leq \mathrm{ht}(P) + \dim(A[x]_Q/P \cdot A[x]_Q)$$

So we need to prove that the second term on the right is ≤ 1 (in fact it equals 1). We compute

$$A[x]_Q/PA[x]_Q \cong (A[x]/PA[x])_{\bar{Q}} \cong ((A/P)[x])_{\bar{Q}} \cong ((A/P)_P[x])_{\bar{Q}} \cong (\kappa(P)[x])_{\bar{Q}}$$

using the notation $\bar{Q} := Q \bmod PA[x]$ and $\kappa(P) := A_P/PA_P$ for the residue field at P. Since $\kappa(P)[x]$ is a one-variable polynomial ring over a field, it has dimension

1 (every irreducible polynomial generates a maximal ideal) and localizing at Q can only lower the dimension.

This proves the first statement. The second statement follows by induction from the first, noting that polynomial rings over a Noetherian ring are Noetherian by the Hilbert Basis Theorem. □

Remark 3.12. Without the Noetherian property the statement is not true: For a ring A, the polynomial ring $A[x]$ can have arbitrary dimension between $\dim A + 1$ and $2\dim A + 1$. The point where we rely on the Noetherian property is in Proposition 3.9 and its proof.

Similarly, we obtain:

Corollary 3.13. *If A is a Noetherian ring, then $\dim A[[x]] = \dim A + 1$.*

Proof. As in the previous proof, an increasing chain of prime ideals in A gives an increasing chain of prime ideals in $A[[x]]$ as well, whence $\dim A[[x]] \geq \dim A + 1$. Conversely, for a maximal ideal $Q \subset A$ and $P = A \cap Q$ we again have

$$\mathrm{ht}(Q) \leq \mathrm{ht}(P) + \dim\left(A[[x]]_Q / P \cdot A[[x]]_Q\right)$$

by Proposition 3.9. As before, we compute

$$A[[x]]_Q/P \cdot A[[x]]_Q \cong ((A/P)[[x]])_{\bar{Q}} \cong ((A/P)_P[[x]])_{\bar{Q}} \cong (\kappa(P)[[x]])_{\bar{Q}}$$

It remains to recall that $\kappa(P)[[x]]$ has dimension 1 because it is a discrete valuation ring. □

Corollary 3.14. *For A Noetherian we have $\dim A[[x_1, \ldots, x_n]] = \dim A + n$.*

This follows by induction from the preceding corollary, combined with the following proposition:

Proposition 3.15. *If A is a Noetherian ring, 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 $a_r x^r + a_{r+1}x^{r+1} + \ldots$ contained in I. Then $I_0 \subset I_1 \subset I_2 \subset \ldots$ is an ascending chain, so there is n for which $I_n = I_{n+1} = I_{n+2} = \ldots$ 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 $s = a_r x + a_{r+1}x^{r+1} + \ldots$ 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 $A[[x]]$. □

4. Regular local rings and regular sequences

Observe that if A is a local ring with maximal ideal P, then $\kappa(P) := A/P$ is a field (the *residue field* of A) and P/P^2 inherits a $\kappa(P)$-vector space structure from the A-module structure on P.

Definition 4.1. *A Noetherian local ring A with maximal ideal P is a* regular *local ring if* $\dim_{\kappa(P)} P/P^2 = \dim A$.

If $x_1, \ldots, x_r \in P$ are such that their mod P^2 images form a basis in P/P^2, we call them a regular system of parameters.

Remarks 4.2.

1. The algebraic meaning of regularity is the following. If $x_1, \ldots, x_r \in P$ are such that their images modulo P^2 generate P/P^2, then they also generate P as an ideal by Corollary 1.9. In fact, they form a *minimal* system of generators if and only if their mod P^2 images form a $\kappa(P)$-basis of P/P^2. By the Hauptidealsatz $r \geq \dim A$, so a Noetherian local ring is regular if and only if P is generated by the smallest possible number of elements.

2. If A is the local ring of an (affine) variety X at some point P, it is a theorem of Zariski that P/P^2 is the dual space of the tangent space of X at P. Points where the dimension of the tangent space equals the dimension of the variety are called smooth (or nonsingular) points in algebraic geometry. Thus regular local rings are the local rings of smooth points. We'll come back to this fact later.

Examples 4.3.

1. Basic examples of regular local rings of dimension n are power series rings $k[[x_1, \ldots, x_n]]$ over a field k. (We know that they are Noetherian and local of dimension n, and $x_1, \ldots, x_n$ form a regular system of parameters.)

2. The regular local rings of dimension 1 are exactly the discrete valuation rings. This follows from Proposition 1.7 and Theorem 4.6 below.

Proposition 4.4. *If A is a regular local ring and $x_1, \ldots, x_r$ a regular system of parameters in A, then $A/(x_1, \ldots, x_i)$ is a regular local ring of dimension $r - i$ for all $1 \leq i \leq r$.*

In fact, we prove more:

Proposition 4.5. *If A is a Noetherian ring, P is a minimal prime ideal above $x_1, \dots, x_r$ and $\mathrm{ht}(P) = r$, then $\mathrm{ht}(P/(x_1, \dots, x_i)) = r - i$ in $A/(x_1, \dots, x_i)$ for all $1 \leq i \leq r$.*

Proof. Set $s := \mathrm{ht}(P/(x_1, \dots, x_i))$. By the generalized Hauptidealsatz we have $s \leq r-i$ since $P/(x_1, \dots, x_i)$ is minimal above the images of $x_{i+1}, \dots, x_r$ in $A/(x_1, \dots, x_i)$. On the other hand, by the converse of Hauptidealsatz (Proposition 3.7) we get elements $\bar{y_1}, \dots, \bar{y_s}$ such that $P/(x_1, \dots, x_i)$ is minimal above $\bar{y_1}, \dots, \bar{y_s}$. Lifting these elements to $y_1, \dots, y_s \in P$ we get that it is minimal above $x_1, \dots, x_i, y_1, \dots, y_s$, whence $i + s \geq r$, again by the Hauptidealsatz. This proves $s = r - i$ as required. □

Theorem 4.6. *A regular local ring is an integral domain.*

Proof. We proceed by induction on $d := \dim A$. If $d = 0$, then the maximal ideal P satisfies $P = P^2$, hence equals (0) by Nakayama's lemma and the statement is clear. Now assume the proposition holds for $d - 1$. Let $P_1, \dots, P_m$ be the minimal prime ideals of A. We apply prime avoidance (Lemma 2.13) to $P_1, \dots, P_m, P^2$ and P. We know that $P \not\subseteq P_i$ and $P \not\subseteq P^2$, so there exists an $x \in P \backslash P^2$ such that $x \notin P_i$ for all i. Since $x \notin P^2$, it is part of a regular system of parameters of A (as x mod P^2 is part of a basis of P/P^2). By Proposition 4.4 the quotient $A/(x)$ is then regular and local of dimension $d - 1$. Hence by induction we know that $A/(x)$ is an integral domain, so (x) is a prime ideal. Since $x \notin P_i$ for all i, the prime ideal (x) cannot be minimal, so it properly contains one of the minimal prime ideals P_i. In particular, $x \notin P_i$ but for all $y \in P_i$ we have $y = ax$ for some $a \in A$. So $a \in P_i$ and we conclude that $P_i = (x)P_i$. This implies $P_i = PP_i$, so by Nakayama's lemma $P_i = (0)$, i.e. (0) is a prime ideal. □

Now comes a key definition.

Definition 4.7. *Let A be a ring. Elements $x_1, \dots, x_r \in A$ form a* regular sequence *if*

(1) *x_i is not a zero-divisor modulo $(x_1, \dots, x_{i-1})$ for all $1 \leq i \leq r$.*
(2) *$(x_1, \dots, x_r) \neq A$.*

Note that when A is local, the second condition implies that all x_i are contained in the maximal ideal.

Remarks 4.8.
1. If A is Noetherian and local with maximal ideal P, every permutation of a regular sequence is again a regular sequence. (The condition that A is local is necessary: one can check that in the polynomial ring $k[x_1, x_2, x_3]$ the sequence $x_1(x_1 - 1), x_1x_2 - 1$, x_1x_3 is regular but $x_1(x_1 - 1), x_1x_3, x_1x_2 - 1$ is not.)

To see this, it is enough to show that for all i interchanging x_i and x_{i+1} in a regular sequence gives a regular sequence. Replacing A by $A/(x_1, \dots, x_{i-1})$ if necessary we reduce to $i = 1$ and then to $r = 2$. Let (x_1, x_2) be a regular sequence in A and K the kernel of the map given by multiplication by x_2. If $x \in K$, we have $x = x_1 x'$ for some x' as x_2 is not a zero divisor modulo (x_1). Here $x' \in K$ because $x_2 x_1 x' = 0$ and x_1 is not a zero divisor. It follows that $x_1 K = K$, hence $PK = K$ and $K = 0$ by Nakayama's lemma. This shows x_2 is not a zero divisor in A. To see that x_1 is not a zero divisor mod (x_2), assume $x_1 y = x_2 z$ for some $y, z \in A$. Since x_2 is not a zero divisor mod (x_1), we get $z = x_1 z'$ for some z', whence (using that x_1 is not a zero divisor) $y = x_2 z'$, as required.

2. For $A = k[x_1, \dots, x_n]$ the geometric meaning of the definition is the following: a sequence of nonconstant elements $f_1, \dots, f_r$ forms a regular sequence if and only if for all i the hypersurface $V(f_i)$ intersects each irreducible component of $V(f_1, \dots, f_{i-1})$ properly.

Theorem 4.9. *Let A be a Noetherian local ring with maximal ideal P and $x_1, \dots, x_d$ a minimal system of generators for P. Then A is a regular local ring if and only if $x_1, \dots, x_d$ is a regular sequence.*

Proof. By Remark 4.2 (1) the x_i form a minimal system of generators for P if and only if modulo P^2 their images form a basis of P/P^2. So if A is regular, then the x_i form a regular system of parameters, hence a regular sequence by Proposition 4.4 and Theorem 4.6. The converse results from the following lemma. □

Lemma 4.10. *If A is a Noetherian local ring and $x_1, \dots, x_r$ is a regular sequence in A, then $\dim A/(x_1, \dots, x_r) = \dim A - r$.*

The lemma looks similar to Proposition 4.5 but does not follow from it: there we assumed $\mathrm{ht}(P) = r$ whereas here we want to prove it using the fact that the sequence is regular.

Proof. As in the proof of Proposition 4.5, setting $s = \dim A/(x_1, \dots, x_r)$ and applying Proposition 3.7 to $A/(x_1, \dots, x_r)$ we find $y_1, \dots, y_s \in P$ such that P is a minimal prime ideal containing $x_1, \dots, x_r, y_1, \dots, y_s$. The generalized Hauptidealsatz then gives $\dim A = \mathrm{ht} P \leq r + s$. For the reverse inequality, observe that x_1 is not a zero divisor in A, so for all minimal prime ideals $P' \supseteq (x_1)$ we have $\mathrm{ht}(P') = 1$ by Remark 3.2. In other words, $\dim A/(x_1) \leq \dim A - 1$, so we can use induction along the regular sequence $x_1, \dots, x_r$ to obtain $s = \dim A/(x_1, \dots, x_r) \leq \dim A - r$. □

Remark 4.11. If A is regular local of dimension d, it is not necessarily true that a regular sequence of length d generates the maximal ideal. One counterexample among many: $x_1, x_2, \dots, x_{d-1}, x_d^2$ in $k[[x_1, \dots, x_d]]$.

To close this section we globalize the definition of regular local rings.

Definition 4.12. A Noetherian ring A is *regular* if all localizations A_P by prime ideals $P \subseteq A$ are regular local rings.

Remark 4.13. We shall prove later that every localization of a regular local ring by a prime ideal is again regular. It will follow that a Noetherian ring is regular if and only if all localizations by *maximal* ideals are regular local rings.

Examples 4.14.

(1) By Proposition 1.19 Dedekind domains are regular.
(2) If X is a smooth affine variety over an algebraically closed field, then the coordinate ring $\mathcal{A}_X$ is regular. We'll prove this in a more general form later.

We give an algebraic proof for the latter example in the case of affine space:

Proposition 4.15. *If A is a regular ring, then $A[t]$ is regular as well. Consequently, if k is a field, then $k[t_1, \ldots, t_n]$ is regular.*

Proof. Let $Q \subseteq A[t]$ be a prime ideal and take $P := Q \cap A$. Then $A[t]_Q$ is a localization of $A_P[t]$ where A_P is regular, so we can assume that A is regular local with maximal ideal P. The prime ideal Q maps to a principal ideal $(\overline{f}) \subseteq k[t]$ modulo P. If $\overline{f} = 0$, then $Q = PA[t]$ and so $\dim A[t]_Q = \dim A$ using Corollary 3.11 (and its proof), whereas a regular system of parameters for P is also one for Q. So we may assume $\overline{f} \neq 0$ and lift $\overline{f}$ to $f \in A[t]$. We obtain $Q = (P, f)$ where f is not a zero-divisor modulo P. Therefore choosing a regular system of parameters for P and adding f we get a regular sequence generating Q; by construction it is a minimal system of generators. By Theorem 4.9 this proves that $A[t]_Q$ is regular. □

5. COMPLETIONS

Completion is an algebraization of the notion of power series expansion for analytic functions. Here is the precise definition.

Definition 5.1. Let A be a ring, and $I \subset A$ an ideal. The *completion* of A with respect to I is

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

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 basic example is:

Example 5.2. Consider the polynomial ring $A = k[x_1, \dots, x_n]$, k a field, and $I = (x_1, \dots, x_n)$. Then $\widehat{A}$ is the formal power series ring $k[[x_1, \dots, x_n]]$.

Observe that we get the same power series ring if instead of A we start with the localization $A_I = k[x_1, \dots, x_n]_{(x_1,\dots,x_n)}$. We shall soon see that the completion with respect to the maximal ideal of any regular local ring containing a field is a power series ring.

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 descending chains of submodules $M = M^0 \supset M^1 \supset M^2 \supset \dots$ of a fixed A-module M; such chains are called *filtrations*. 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 is a natural map $M \to \widehat{M}$ given by sending $m \in M$ to the sequence $(m \bmod M^n)$. In general it is neither injective nor surjective. However, in the case when it is an isomorphism, we say that M is *complete* (with respect to the filtration (M^n)).

There are natural surjective projections $p_n : \widehat{M} \to M/M^n$ for each n; set $\bar{M}^n := \ker(p_n)$. The p_n induce isomorphisms $\widehat{M}/\bar{M}^n \cong M/M^n$, so that $\widehat{M}$ is complete with respect to the chain $(\bar{M}^n)$. Note also that by definition $\cap_n \bar{M}^n = (0)$ but $\cap_n M^n$ can be nontrivial.

Remark 5.3. 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. The topology is Hausdorff if and only if the intersection of the M^n is 0.

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

Proposition 5.4. *Given an A-module M, consider two filtrations $M^0 \supset M^1 \supset M^2 \supset \dots$ and $N^0 \supset N^1 \supset N^2 \supset \dots$ by submodules. If 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*

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

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.

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. □

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

Proposition 5.5. *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.

Before proving the proposition we derive a series of corollaries.

Corollary 5.6. *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 $n > 0$.*

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

Note that this corollary implies in particular that the ideals $\widehat{I^n}$ of $\widehat{A}$ considered in the previous corollary are the n-th powers of $\widehat{I}$.

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 5.8. *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-algebra 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 5.5 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 5.7 we have $\widehat{J} \cong J\widehat{B}$, so it remains to observe that $\widehat{B} \cong A[[x_1, \dots, x_n]]$. □

Combining Proposition 3.15 with Corollary 5.8 we get:

Corollary 5.9. *If A is a Noetherian ring, any completion $\widehat{A}$ of A by an ideal is Noetherian.*

The *proof of Proposition 5.5* 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 establish an isomorphism $\varprojlim M_1/(I^n M_2 \cap M_1) \cong \varprojlim M_1/I^n M_1$.

Step 1 follows by applying part $a)$ of 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 5.10. *Let $(A_n), (B_n)$ and (C_n) be inverse systems of abelian groups such that there are commutative diagrams with exact rows*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_{n+1} & \longrightarrow & B_{n+1} & \longrightarrow & C_{n+1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi_n^A} & & \downarrow{\scriptstyle \phi_n^B} & & \downarrow{\scriptstyle \phi_n^C} & & \\ 0 & \longrightarrow & A_n & \longrightarrow & B_n & \longrightarrow & C_n & \longrightarrow & 0 \end{array}$$

for each $n > 0$.

The induced sequence

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to 0$$

of inverse limits is exact in each of the following cases:

$a)$ The maps ϕ_n^A are surjective for all n.

$b)$ For each n there exists $m \geq n$ such that the map $\phi_{mn}^A := \phi_n^A \circ \phi_{n+1}^A \circ \cdots \circ \phi_m^A : A_{m+1} \to A_n$ is 0.

Proof. Left exactness of the sequence (without any of the additional conditions) is immediate from the definition of the inverse limit. For surjectivity on the right we have to show that every sequence $(c_n) \in \varprojlim C_n$ is the image of a sequence $(b_n) \in \varprojlim B_n$. Choose arbitrary liftings b_n of the c_n. We modify them by adding suitable elements $a_n \in A_n$ so that $\phi_n(b_{n+1}) = b_n$ will hold for all n.

Assuming condition $a)$ we use induction on n. Assume that b_i have been constructed for $i \leq n$ such that $\phi_i(b_{i+1}) = b_i$ for $i \leq n-1$. Now consider b_{n+1}. The element $\phi_n^B(b_{n+1}) - b_n$ maps to 0 in C_n, hence it comes from some $a_n \in A_n$. As ϕ_n^A is surjective, we find $a_{n+1} \in A_{n+1}$ with $\phi_n^A(a_{n+1}) = a_n$. Then $b_{n+1} - a_{n+1}$ still maps to c_{n+1} in C_{n+1} but moreover it maps to b_n in B_n.

Assuming condition $b)$, consider $a_n = \phi_n^B(b_{n+1}) - b_n$ for all n and set

$$a'_n := a_n + \sum_{m=n}^{\infty} \phi_{mn}^A(a_{m+1}).$$

By condition b) all sums here are finite. Moreover, $\phi^A_{n+1}(a'_{n+1}) = a'_n - a_n$, so replacing b_n by $b_n + a'_n$ we have $\phi^B_{n+1}(b_{n+1} + a'_{n+1}) = b_n + a'_n$ as required. □

Remarks 5.11.
1. In case b) the assumption actually implies $\varprojlim A_n = 0$, so $\varprojlim B_n \xrightarrow{\sim} \varprojlim C_n$.

2. A more general sufficient (but not necessary) condition for right exactness of the inverse limit is the *Mittag–Leffler condition:* the images $\phi_{mn}(A_{m+1}) \subset A_n$ for all $m \geq n$ satisfy the descending chain condition. In these notes we'll only need the easier special cases a) and b) above.

We shall prove **Step 2** in a stronger form. Assume given an ideal $I \subset A$ and a filtration (M^n) of an A-module M satisfying $I^m M^n \subset M^{m+n}$ for all m, n. We say that (M^n) is *stably I-adic* if $M^{n+1} = IM^n$ for all n large enough. Obviously the I-adic filtration $(I^n M)$ of M is stably I-adic.

Lemma 5.12. *If (M^n) is a stably I-adic filtration on M, there is an isomorphism*

$$\varprojlim M/M^n \cong \varprojlim M/I^n M.$$

Proof. We check the condition of Proposition 5.4. On the one hand, for all n we have $I^n M = I^n M^0 \subset M^n$ by assumption. On the other hand, if $M^{n+1} = IM^n$ for $n \geq n_0$, then $M^{n_0+m} = I^m M^{n_0} \subset I^m M$ for all $m > 0$. □

Now consider the graded ring[1]

$$I^{\oplus} := \bigoplus_{n=0}^{\infty} I^n$$

and the direct sum of A-modules

$$M^{\oplus} := \bigoplus_{n=0}^{\infty} M^n.$$

Here $M^{\oplus}$ is a graded $I^{\oplus}$-module, which means that there is an $I^{\oplus}$-module structure $I^{\oplus} \times M^{\oplus} \to M^{\oplus}$ on $M^{\oplus}$ which in all degrees m, n restricts to $I^m \times M^n \to M^{m+n}$ (this uses our condition on (M^n) above).

Lemma 5.13 (Cartier)**.** *Assume A is Noetherian and M is finitely generated over A. The filtration (M^n) is stably I-adic if and only if $M^{\oplus}$ is a finitely generated $I^{\oplus}$-module.*

[1]Recall that a graded ring is a ring R together with a family of additive subgroups R_d for each $d \geq 0$ such that $R_d R_e \subset R_{d+e}$ and $R = \bigoplus_d R_d$.

Proof. Suppose first $M^{n+1} = IM^n$ for all $n \geq n_0$. For $n \leq n_0$ each M_n is finitely generated over A; choose a finite system S of generators for their direct sum. Since for all $m > 0$ we have $M^{n_0+m} = I^m M^{n_0}$, we conclude that S generates $M^\oplus$ over $I^\oplus$. Conversely, if $M^\oplus$ is finitely generated over $I^\oplus$, we may assume all generators lie in some homogeneous component M^n and let n_0 be the largest n involved. Now for $m > 0$ each element of M^{n_0+m} is a sum of elements of the form $i_{n_0+m-n}x_n$ with $x_n \in M^n$ a generator and $i_{n_0+m-n} \in I^{n_0+m-n}$. Since $I^{n_0+m-n} = I^m I^{n_0-n}$ and $I^{n_0-n}M^n \subset M^{n_0}$, we obtain $M^{n_0+m} = I^m M^{n_0}$. □

Corollary 5.14 (Artin–Rees lemma)**.** *Assume moreover $M_1 \subset M$ is a submodule. The filtration $(I^n M \cap M_1)$ of M_1 is stably I-adic.*

Proof. First note that the filtration $(I^n M \cap M_1)$ satisfies $I^m(I^n M \cap M_1) \subset (I^{n+m}M \cap M_1)$ for all n, m. Next, observe that a finite system of generators of I generates $I^\oplus$ as an *A-algebra*, so $I^\oplus$ is Noetherian by the Hilbert basis theorem. By the lemma $I^\oplus M = \oplus I^n M$ is a finitely generated $I^\oplus$-module, so its submodule $\oplus(I^n M \cap M_1)$ is also finitely generated. Now apply the other implication of the lemma. □

Proof of Proposition 5.5. As noted above, Lemma 5.10 $a)$ implies exactness of the sequence

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

Now $\varprojlim M_1/(I^n M_2 \cap M_1) \cong \varprojlim M_1/I^n M_1$ follows from the Artin–Rees lemma (Corollary 5.14) applied with $M = M_2$ and Lemma 5.12. □

The Artin–Rees lemma has another important consequence:

Corollary 5.15. (Krull intersection theorem) *If A is a Noetherian local ring and $I \subsetneq A$ is an ideal, then*

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

Proof. We may assume $I = P$, the maximal ideal of A, since $I \subset P$. Write N for the intersection of the P^n. As N is an ideal, we have $PN \subset N$. On the other hand, applying the Artin–Rees lemma to $N \subset A$ gives an n_0 for which

$$N = P^{n_0+1} \cap N = P(P^{n_0} \cap N) \subset PN.$$

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

Corollary 5.16. *If A is a Noetherian local ring and $\widehat{A}$ its completion with respect to some ideal $I \subsetneq A$, the natural map $A \to \widehat{A}$ is injective.*

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

Remark 5.17. The Krull intersection theorem also holds for A Noetherian but not necessarily local if the ideal I is such that there is a prime ideal $P \supset I$ for which the localization map $A \to A_P$ is injective; this is always the case when A is an integral domain. However, it does not hold for every ideal in a Noetherian ring. For instance, in $A = \mathbf{Z}/6\mathbf{Z}$ the principal ideal I generated by 2 mod 6 satisfies $I^2 = I$.

While we are at local rings, let us also record the following fact.

Proposition 5.18. *If A is a Noetherian local ring with maximal ideal P, its completion $\widehat{A}$ with respect to an ideal $I \subset A$ is a local ring with maximal ideal $\widehat{P} = P\widehat{A}$.*

The proof uses a general lemma whose technique will serve many times.

Lemma 5.19. *Let A be a ring complete with respect to an ideal I. An element $a \in A$ is a unit in A if and only if a mod I is a unit in A/I.*

Proof. Assume a mod I is a unit in A/I, the other implication being trivial. We first treat the case $I^2 = 0$ (note that under this assumption A is indeed I-adically complete). There is $b \in A$ and $h \in I$ with $ab = 1 + h$. Then $ab(1 - h) = 1 - h^2 = 1$, so $b(1 - h)$ is an inverse for a.

Since $I^n/I^{n+1} \subset A/I^{n+1}$ is an ideal of square zero, we get using induction on n that the lemma holds if $I^{n+1} = 0$. In the general case we know from the above that a mod I^n has a multiplicative inverse $b_n \in A/I^n$ for each $n > 0$. Since the multiplicative inverse of a ring element is unique, we must have $b_n = b_{n+1}$ mod I^n/I^{n+1} for all n, so (b_n) defines an element of A which is an inverse of a. □

Proof of Proposition 5.18. Given $t \in \widehat{P}$, the element $1 + t$ is a unit in $\widehat{A}$. Indeed, t mod I lifts to an element $t_0 \in P$ and $1 + t_0$ is a unit in A. Now apply the lemma above.

By Corollary 5.6 the quotient $\widehat{A}/\widehat{P} \cong A/P$ is a field, so $\widehat{P}$ is a maximal ideal. Now given $t \in \widehat{P}$ and a maximal ideal $P' \subset \widehat{A}$, we have $t \in P'$. Indeed, otherwise $(t, P') = \widehat{A}$ so there exist $a \in \widehat{A}$ and $b \in P'$ with $at + b = 1$, but this contradicts the fact proven above that $1 - at$ is a unit. So $\widehat{P} \subset P'$, whence $\widehat{P} = P'$. □

Remark 5.20. The above argument also shows that if A is any ring and $\widehat{A}$ its completion with respect to an ideal $I \subset A$, then $\widehat{I}$ is contained in all maximal ideals of $\widehat{A}$, i.e. in its *Jacobson radical*.

To proceed further we need the notion of a *flat* A-module: An A-module N is flat if for every exact sequence

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

of A-modules the tensored sequence

$$0 \to M_1 \otimes_A N \to M_2 \otimes_A N \to M_3 \otimes_A N \to 0$$

remains exact.

Remarks 5.21.
1. Since the sequence is always right exact by a basic property of the tensor product, flatness is equivalent to injectivity of $M_1 \otimes_A N \to M_2 \otimes_A N$ for all injective maps $M_1 \to M_2$. In fact, here we may restrict to *finitely generated* M_i. Indeed, assume $\alpha = \sum m_i \otimes a_i$ is an element of $M_1 \otimes_A N$ that maps to 0 in $M_2 \otimes_A N$. To prove that $\alpha = 0$ we may replace M_1 by the finitely generated submodule generated by the m_i. Also, by construction of the tensor product the image of α in $M_2 \otimes_A N$ is 0 if the corresponding element of the free A-module $A[M_2 \times N]$ is a sum of finitely many relations occurring in the definition of $M_2 \otimes_A N$, so we find a finitely generated submodule $M_1 \subset M^f \subset M_2$ such that α maps to 0 already in $M^f \otimes_A N$.

2. If N is flat over A and B is an A-algebra, then $N \otimes_A B$ is flat over B. Indeed, if $M_1 \to M_2$ is an injection of B-modules, it can also be viewed as an injection of A-modules via the map $A \to B$, and $M_i \otimes_B (N \otimes_A B) \cong M_i \otimes_A N$ for $i = 1, 2$.

Proposition 5.22. *If A is Noetherian and $\widehat{A}$ is the completion of A with respect to some ideal $I \subset A$, then $\widehat{A}$ is flat over A.*

Proof. We check that for all finitely generated A-modules M we have isomorphisms $\widehat{M} \cong M \otimes_A \widehat{A}$. In view of Remark 5.21 (1) the flatness of $\widehat{A}$ will then follow from Proposition 5.5.

When $M = A^n$ the isomorphism $A^n \otimes_A \widehat{A} \cong \widehat{A}^n$ is easily checked using the definition of completions. In the general case we can find m and n such that there is an exact sequence

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

It gives rise to a commutative diagram with exact rows

$$\begin{array}{ccccccc} A^m \otimes_A \widehat{A} & \longrightarrow & A^n \otimes_A \widehat{A} & \longrightarrow & M \otimes_A \widehat{A} & \longrightarrow & 0 \\ \downarrow \cong & & \downarrow \cong & & & & \\ \widehat{A}^m & \longrightarrow & \widehat{A}^n & \longrightarrow & \widehat{M} & \longrightarrow & 0 \end{array}$$

where the top row comes from tensoring with $\widehat{A}$ and using right exactness of the tensor product, and the lower row comes from right exactness of completion (part

of Proposition 5.5). The two vertical isomorphisms are those established above and give rise to the required isomorphism $M \otimes_A \widehat{A} \xrightarrow{\sim} \widehat{M}$ by the diagram. □

Proposition 5.23. *If A is a Noetherian local ring and $\widehat{A}$ its completion with respect to some ideal $I \subset A$, then $\dim A = \dim \widehat{A}$.*

Proof. Applying Proposition 3.9 to the inclusion map $A \to \widehat{A}$ and the maximal ideal $P\widehat{A} \subset \widehat{A}$ we obtain $\dim \widehat{A} \leq \dim A$. To prove the reverse inequality, choose a chain $P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_d \subsetneq P$ of maximal length in A. Applying the lemma below with $B = \widehat{A}$ and the ideals $P_d \subsetneq P$ and $P\widehat{A}$ we obtain a prime ideal $Q_d \subsetneq P\widehat{A}$ with $Q_d \cap A = P_d$. Now the process may be repeated with $P_{d-1} \subsetneq P_d$ and so on, until we obtain a chain of prime ideals $Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq Q_d \subsetneq P\widehat{A}$. Note that the lemma applies in view of Proposition 5.22 (and Corollary 5.16). □

Lemma 5.24 (Going down theorem for flat extensions)**.** *Let $A \subset B$ be a ring extension making B a flat A-module. If $P_1 \subsetneq P_2$ are prime ideals in A such that there exists a prime ideal $Q_2 \subset B$ with $Q_2 \cap A = P_2$, then there exists a prime ideal $Q_1 \subsetneq Q_2$ with $Q_1 \cap A = P_1$.*

Proof. By Remark 5.21 (2) the ring extension $A/P_1 \subset B/P_1B \cong B \otimes_A (A/P_1)$ is still flat, so we may replace A by A/P_1 and assume $P_1 = (0)$ (in particular, A is an integral domain). Choose a minimal prime ideal $Q_1 \subset Q_2$ in B (it exists by Zorn's lemma as the intersection of a descending chain of prime ideals is a prime ideal[2]). If $x \in A$ is a nonzero element, the map $A \to A$ given by $a \mapsto xa$ is injective on A, hence so is the similar map $B \to B$ by flatness of B over A. So x is not a zero-divisor in B and as such cannot be contained in the minimal prime ideal Q_1 by Remark 3.2. This shows $Q_1 \cap A = (0)$ as required; in particular, $Q_1 \subsetneq Q_2$. □

Remark 5.25. In the above proof we did not really use that A was a subring of B. So the statement holds more generally for any flat A-algebra B if we understand $Q_i \cap A$ as $\varphi^{-1}(Q_i)$, where $\varphi : A \to B$ is the natural homomorphism giving the A-algebra structure on B. Of course, at the end we have to work with $\varphi(x)$ as an element of B.

The above arguments may also be used to prove that in the inequality of Proposition 3.9 equality holds when the ring B is a flat A-algebra via the map $\varphi : A \to B$.

Finally, we obtain:

Corollary 5.26. *If A is a Noetherian local ring, A is regular if and only if its completion $\widehat{A}$ with respect to some ideal I is regular.*

[2]For B Noetherian the existence of Q_1 is obvious by Corollary 3.5.

Proof. By Corollary 5.9 and Proposition 5.18 the completion $\widehat{A}$ is again Noetherian and local; moreover, they have the same dimension by Proposition 5.23. To finish the proof, note that the maximal ideal $P \subset A$ satisfies $\widehat{P}/\widehat{P}^2 \cong \widehat{P/P^2} \cong P/P^2$, the first isomorphism resulting from Proposition 5.5 and the second from $I^2 \subset P^2$. □

Example 5.27. 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*. Since $\mathbf{Z}_p$ is also the completion of the localization $\mathbf{Z}_{(p)}$ by its maximal ideal, it is a discrete valuation ring by the corollary above. In particular, it is an integral domain; its fraction field $\mathbf{Q}_p$ is the *field of p-adic numbers*. Every nonzero $a \in \mathbf{Q}_p$ can be written uniquely as $a = up^{v_p(a)}$ with $u \in \mathbf{Z}_p$ a unit and $v_p(a) \in \mathbf{Z}$. The function $a \mapsto v_p(a)$ gives the discrete valuation of $\mathbf{Q}_p$.

By Corollary 5.8 we have an isomorphism $\mathbf{Z}_p \cong \mathbf{Z}[[x]]/(x - p)$. This may actually be taken as a quick, albeit unorthodox, definition of p-adic integers.

6. The Cohen structure theorem

From now on, when speaking about complete local rings we always understand completion with respect to the maximal ideal. The Cohen structure theorem describes the structure of complete regular local rings. The easiest case is:

Theorem 6.1. *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 $k[[x_1, \dots, x_d]]$.*

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

Note that all the assumptions of the theorem are satisfied by the completion of the local ring of a smooth point on an algebraic variety over an algebraically closed field.

For the proof we need the *associated graded ring* of a ring complete with respect to the I-adic filtration. It is defined by

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

Lemma 6.2. *Let $\phi : A \to B$ be a homomorphism of complete local rings such that $\phi(P_A^n) \subset P_B^n$ for all $n \geq 1$, where P_A (resp. P_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

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

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 $(b_n) \subset B = \widehat{B}$ with $b_n \in B/P_B^n$, we have to find a sequence of elements $a_n \in A/P_A^n$ with $\phi_n(a_n) = b_n$ and a_{n+1} mod $P_A^n = a_n$. We do this by induction on n: assuming a_n has been constructed, we lift it to $a_{n+1} \in A/P_A^{n+1}$ arbitrarily. This a_{n+1} may not map to b_{n+1} in A/P_A^{n+1} but $\phi_{n+1}(a_{n+1}) - b_{n+1}$ comes from P_B^n/P_B^{n+1}. By surjectivity of $\mathrm{gr}_n(\phi)$ we may therefore modify a_{n+1} by an element of P_A^n/P_A^{n+1} so that its image becomes b_{n+1}. □

Proof of Theorem 6.1. Let $t_1, \ldots, t_d$ be a system of generators for the maximal ideal P 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 $\lambda : k[[x_1, \ldots, x_d]]/(x_1, \ldots, x_d)^n \cong k[x_1, \ldots, x_d]/(x_1, \ldots, x_d)^n \to A/P^n$ sending the image of x_i to that of t_i; as A is complete, these assemble to a homomorphism λ as required. As $A/P \cong k$ and the t_i generate P, 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, resulting from Corollary 5.26, that A is regular if and only if $\widehat{A}$ is. By Corollary 5.16 the natural map embeds A in $\widehat{A}$, so the theorem implies:

Corollary 6.3. *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 6.4. 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 P is principal. Fix a generator t of P and pick $a \in A$. Set $a_0 := a$ mod P and $b_0 = a - a_0$. Then $b_0 = b_1 t$ with a unique $b_1 \in A$ and we set $a_1 := b_1$ mod P. Continuing the process we get $a = a_0 + a_1 t + \ldots a_n t^n + b_n$ with $b_n \in P^n$ 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.

We now prove that the assumption in Theorem 6.1 is always satisfied if the characteristic of A equals that of its residue field. The key property used in the proof is the following.

Definition 6.5 (Grothendieck)**.** An R-algebra S is *formally smooth* if it satisfies the following property: given a commutative diagram

$$\begin{array}{ccc} S & \xrightarrow{\bar{\lambda}} & B/I \\ \uparrow & & \uparrow \\ R & \xrightarrow{\mu} & B \end{array} \tag{1}$$

with a ring B and an ideal $I \subset B$ satisfying $I^2 = 0$, the map $\bar{\lambda}$ lifts to a map $\lambda : S \to B$ making the diagram commute. If moreover the lifting λ is unique, then S is *formally étale* over R.

An obvious example of a formally smooth R-algebra is a free R-algebra. The following proposition gives another example.

Proposition 6.6. *If $S = R[T]/(f)$ with some $f \in R[T]$ such that the derivative f' maps to a unit in S, then S is formally étale over R.*

Proof. Write t for the image of T in S and lift $\bar{\lambda}(t)$ to $b \in B$ arbitrarily; since $f'(b)$ maps to $\bar{\lambda}(f'(t))$ mod I, it is a unit in B by Lemma 5.19 (here we evaluate f' at b via applying μ to its coefficients). To define λ, we have to find $h \in I$ such that $f(b+h) = 0$ (with the same convention of evaluating f via μ), 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. □

Remark 6.7. Note that the proof above only used the somewhat weaker condition that $\bar{\lambda}(f'(t))$ is a unit in B.

A classical application is the following. Let A be a complete local ring with maximal ideal P and residue field k, and let $f \in A[T]$ be a polynomial with image $\bar{f}$ in $k[T]$. Assume that $\bar{a} \in k$ satisfies $\bar{f}(\bar{a}) = 0$ but $\bar{f}'(\bar{a}) \neq 0$. A form of *Hensel's lemma* says that there is a unique $a \in A$ reducing to $\bar{a}$ modulo P with $f(a) = 0$. To find a we have to construct a coherent sequence of elements $a_n \in A/P^n$ starting with $a_1 = \bar{a}$ so that $f(a_n) = 0$ in A/P^n for all n. Assuming a_{n-1} has been constructed, apply the proposition inductively with $R = B = A/P^n$, $I = P^{n-1}/P^n$, μ the identity map and

$\bar{\lambda}$ induced by sending t to a_{n-1}. The proposition gives a map $\lambda : (A/P^n)[t] \to A/P^n$ lifting $\bar{\lambda}$, and we set $a_n := \lambda(t)$. (Note that $f'(a_{n-1}) \in A/P^{n-1}$ is a unit since it reduces to $\bar{f}'(\bar{a}) \in k$ which is nonzero by assumption, so the proposition works with the weaker condition noted above.)

We shall use Proposition 6.6 through the following consequence.

Corollary 6.8. *Let $L|K$ be a separable algebraic field extension. Then L is formally étale over K.*

Proof. Assume first that $L|K$ is a finite extension. By the theorem of the primitive element we may then write $L \cong K[T]/(f)$ with f a polynomial having only simple roots, so we may apply the proposition with $R = K$ and $S = L$ to conclude. If $L|K$ is an infinite separable algebraic extension, we may write it as a union of finite separable extensions, and then conclude from the finite case using uniqueness of the lifting in Proposition 6.6. □

Another useful case of formal smoothness is given by fields of positive characteristic.

Proposition 6.9. *A field L of characteristic $p > 0$ is formally smooth over $\mathbf{F}_p$.*

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 B is an $\mathbf{F}_p$-algebra, $p \geq 2$ and $I^2 = 0$. The map λ_p is well defined because the map $x \mapsto x^p$ is injective on L, and it is a homomorphism. Moreover, it 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.[3] By Zorn's lemma there exists a maximal subfield $L' \subset L$ containing L^p 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, a 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'. □

We now return to the assumption in Theorem 6.1.

Definition 6.10. Let A be a local ring with maximal ideal P 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 $A \to k$.

We can now state:

[3] For L perfect the proof stops here.

Theorem 6.11 (Cohen)**.** *If A is a complete local ring containing a field, then A has a coefficient field.*

Proof. If the residue field k has characteristic $p > 0$, it is formally smooth over $\mathbf{F}_p$ by Proposition 6.9, so we may lift the identity map of k inductively to maps $k \to A/P^n$ for all n and then pass to the inverse limit.

If k has characteristic 0, let $k' \subset k$ be a maximal subfield such that the identity map of k' lifts to a map $k' \to A$. By a simple application of 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 P trivially (otherwise we would have $k'[x] \cap P = (f)$ 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 applying Corollary 6.8 inductively with $L = k$, $K = k'$ and $B = A/P^n$ and passing to the inverse limit again contradicts the maximality of k'. □

Assume moreover that A is an integral domain. We say that A is *of equal 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 P trivially (otherwise the intersection would contain a prime number p which would force k to have characteristic p), and therefore all of its elements are units in A, i.e. A contains $\mathbf{Q}$. Thus combining the previous theorem with Theorem 6.1 we obtain:

Corollary 6.12. *Let A be a complete Noetherian local domain of equal characteristic 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 $A \cong k[[x_1, \ldots, x_d]]$.

We now turn to the Cohen structure theorem in *mixed characteristic*, i.e. for complete local domains of characteristic 0 whose residue field is of characteristic $p > 0$.

For a start, define a *Cohen ring* as a complete discrete valuation ring of characteristic 0 with maximal ideal generated by a prime number p. Cohen rings will play the role of coefficient fields in mixed characteristic.

Proposition 6.13. *Given a field k of characteristic $p > 0$, there exists a Cohen ring A_0 with residue field $A_0/pA_0 \cong k$.*

Proof. First let $\langle x_\lambda : \lambda \in \Lambda \rangle \subset k$ be a maximal algebraically independent system over $\mathbf{F}_p$. Let $\mathbf{Z}_p\langle x_\lambda \rangle$ be the free $\mathbf{Z}_p$-algebra generated by the x_λ, and let R_0 be its

localization by the prime ideal $p\mathbf{Z}_p\langle x_\lambda\rangle$. By construction R_0 is a local integral domain with maximal ideal (p) and moreover $\cap_i(p^i) = 0$ in R_0. Hence R_0 is a discrete valuation ring by Proposition 1.7 (3) (and its proof).

We now construct a discrete valuation ring $R \supset R_0$ with maximal ideal pR and residue field k. This will finish the proof, as we may then take A_0 to be the p-adic completion of R. By construction k is algebraic over the residue field k_0 of R. Let $\overline{K}$ be an algebraic closure of the fraction field of R_0, and consider the system $\mathcal{S}$ of pairs (S, ρ), where $R_0 \subset S \subset \overline{K}$ is a subring that is a discrete valuation ring with maximal ideal pS, and $\rho : S \to k$ is a homomorphism with kernel pS. These pairs are naturally partially ordered by inclusion, and satisfy the condition of Zorn's lemma. Indeed, if $(S_1, \rho_1) \leq (S_2, \rho_2) \leq (S_3, \rho_3) \leq \dots$ is an ascending chain, then the union $\widetilde{S}$ of the S_i inside $\overline{K}$ has a homomorphism $\widetilde{\rho} : \widetilde{S} \to k$ with kernel $p\widetilde{S}$ induced by the ρ_i. Moreover, here $\cap_j p^j \widetilde{S} = 0$ because the S_i are discrete valuation rings. Hence $\widetilde{S}$ also satisfies the condition of Proposition 1.7 (3), which means that $\widetilde{S}$ is a discrete valuation ring and therefore $(\widetilde{S}, \widetilde{\rho}) \in \mathcal{S}$. So let (S, ρ) be a maximal element in $\mathcal{S}$ furnished by Zorn's lemma. We contend that its residue field k_S equals k. If not, there is some $\alpha \in k \setminus k_S$ algebraic over k_S. Let $f \in S[x]$ be a monic irreducible polynomial mapping modulo pS to the minimal polynomial of α over k_S. Since S is a unique factorization domain, f is also irreducible over the fraction field of S, so since $\overline{K}$ is algebraically closed, we find an injective homomorphism $S' := S[x]/(f) \to \overline{K}$ where moreover $pS' \subset S'$ is a maximal ideal with $S'/pS' \cong k_S(\alpha)$. Now if $P' \subset S'$ is any maximal ideal, then $P' \cap S$ is maximal in S by Lemma 1.14 applied to the integral extension $S'/P' \supset S/(P' \cap S)$, so $P' = pS'$ and S' is local with maximal ideal pS'. Moreover, S' is Noetherian since it is a finitely generated S-algebra, so by Proposition 1.7 S' is a discrete valuation ring, which contradicts the maximality of S. □

Next we prove the following analogue of Theorem 6.11.

Theorem 6.14 (Cohen)**.** *Let A be a complete local domain of mixed characteristic with maximal ideal P. There exists a subring $A_0 \subset A$ which is a Cohen ring and moreover the inclusion map $A_0 \to A$ induces an isomorphism $A_0/pA_0 \xrightarrow{\sim} A/P$.*

The key ingredient in the proof is the following proposition.

Proposition 6.15. *Let $\phi : R \to S$ be a homomorphism of rings and $I \subset R$ a nilpotent ideal. If S is free as an R-module and S/IS is formally smooth over R/I, then S is formally smooth over R.*

Proof. Recall the following criterion from homological algebra (that uses the freeness of S over R): S is formally smooth over R if and only if the symmetric Hochschild

cohomology group $HH^2_s(S, M)$ is 0 for every S-module M. By assumption we have $HH^2_s(S/IS, M/IM) = 0$, so given a symmetric Hochschild 2-cocycle $f : S \times S \to M$, there is a 1-cochain $g_0 : S/IS \to M/IM$ with $f \bmod I = \partial^1(g_0)$. We may lift g_0 to an R-linear map $S \to M/IM$ and finally to an R-linear map $g_1 : S \to M$ by projectivity of S over R. Then $f - \partial^1(g_1)$ is a 2-cocyle with values in IM. Repeating the argument for $f - \partial^1(g_1)$ with IM in place of M we obtain a 2-cocyle with values in I^2M, so after finitely many repeats we get $g_2, \ldots, g_n : S \to M$ such that $f - \partial^1(g_1 + \cdots g_n)$ has values in I^nM which is 0 for n large enough. This proves that the class of f in $HH^2_s(S, M)$ is 0. □

In order to ensure that the freeness assumption in the proposition holds when we shall apply it, we shall need:

Lemma 6.16. *Let A be a ring, and $I \subset A$ a nilpotent ideal. If M is a flat A-module such that M/IM is a free A/I-module, then M is a free A-module.*

Before starting the proof, recall the following simple observation about flat modules: if M is a flat module over a ring A and $I \subset A$ is an ideal, then the multiplication map $I \otimes_A M \to IM$ is an isomorphism. Indeed, it is certainly surjective, and for injectivity we tensor the injection $I \to A$ by M. The resulting map $I \otimes_A M \to M$ is injective by flatness, and its image identifies with IM.

Proof. Choose a free A-module F so that F/IF (which is a free A/I-module) is isomorphic to M/IM. By freeness of F we may lift the composite map $F \to F/IF \xrightarrow{\sim} M/IM$ to a map $\phi : F \to M$; we contend that it is an isomorphism.

First note that the induced maps $\phi_n : I^nF/I^{n+1}F \to I^nM/I^{n+1}M$ are isomorphisms for all n. Indeed, tensoring the exact sequence

$$0 \to I^{n+1} \to I^n \to I^n/I^{n+1} \to 0$$

by F we obtain isomorphisms

$$(I^n/I^{n+1}) \otimes_A F \cong (I^n \otimes_A F)/(I^{n+1} \otimes_A F) \cong I^nF/I^{n+1}F,$$

where the second isomorphism holds by flatness of F over A in view of the remark above. But

$$(I^n/I^{n+1}) \otimes_A F \cong (I^n/I^{n+1}) \otimes_{A/I} (A/I \otimes_A F) \cong (I^n/I^{n+1}) \otimes_{A/I} F/IF,$$

so finally

$$I^nF/I^{n+1}F \cong (I^n/I^{n+1}) \otimes_{A/I} F/IF.$$

By the same argument, we have an isomorphism

$$I^nM/I^{n+1}M \cong (I^n/I^{n+1}) \otimes_{A/I} M/IM$$

using flatness of M, so the required isomorphism follows by tensoring the isomorphism $F/IF \cong M/IM$ by I^n/I^{n+1} over A/I.

Now consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I^nF/I^{n+1}F & \longrightarrow & F/I^{n+1}F & \longrightarrow & F/I^{n+1}F & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi_n} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I^nM/I^{n+1}M & \longrightarrow & M/I^{n+1}M & \longrightarrow & M/I^{n+1}M & \longrightarrow & 0 \end{array}$$

Here the left vertical arrow is an isomorphism, so it follows by induction on n (starting from the obvious case $n = 0$) that the map $F/I^{n+1}F \to M/I^{n+1}M$ is an isomorphism. We conclude by taking n large enough. □

Proof of Theorem 6.14. First note that since $p \in P$, the natural map $\mathbf{Z} \to A$ sending 1 to 1 induces homomorphisms $\mathbf{Z}/p^n\mathbf{Z} \to A/p^nA$ for all $n > 0$, whence a map $\mathbf{Z}_p \to A$ after passing to the inverse limit. We may thus consider A as a $\mathbf{Z}_p$-algebra. Now take a Cohen ring A_0 with residue field k; it is also a $\mathbf{Z}_p$-algebra by the same argument. It will suffice to show that the identity map of k lifts to a homomorphism $A_0 \to A$; indeed, as A is a domain of characteristic 0 and the only nonzero prime ideal of A_0 is (p), the map $A_0 \to A$ must be injective.

As A_0 is an integral domain, it is torsion free over $\mathbf{Z}_p$ and hence a flat $\mathbf{Z}_p$-algebra as $\mathbf{Z}_p$ is a principal ideal domain. Since A_0/p^nA_0 is then flat over $\mathbf{Z}/p^n\mathbf{Z}$ as well, it follows from Proposition 6.16 that A_0/p^nA_0 is a free module over $\mathbf{Z}/p^n\mathbf{Z}$ for all n. Given that k is formally smooth over $\mathbf{F}_p$ by Proposition 6.9, Proposition 6.15 implies that A_0/p^nA_0 is also formally smooth over $\mathbf{Z}/p^n\mathbf{Z}$. We now prove that the identity map of k lifts to maps $\phi_n : A_0/p^nA_0 \to A/P^n$ for all n with $\phi_n = \phi_{n+1} \bmod p^n$, from which the theorem will follow by passing to the inverse limit. We proceed by induction on n, the case $n = 0$ being trivial. If ϕ_n has been constructed, consider the exact sequence $0 \to P^n/P^{n+1} \to A/P^{n+1} \to A/P^n \to 0$ of $\mathbf{Z}/p^{n+1}\mathbf{Z}$-algebras. Since P^n/P^{n+1} is an ideal of square 0, the composite map $A_0/p^{n+1}A_0 \to A_0/p^nA_0 \xrightarrow{\phi_n} A/P^n$ lifts to $\phi_{n+1} : A_0/p^{n+1}A_0 \to A/P^{n+1}$ by formal smoothness of $A_0/p^{n+1}A_0$ over $\mathbf{Z}/p^{n+1}\mathbf{Z}$. □

We can now prove the mixed characteristic case of the Cohen structure theorem.

Theorem 6.17. *Let A be a Noetherian complete local domain of mixed characteristic, and let $A_0 \subset A$ be a Cohen ring given by the previous theorem.*

(1) *There is a surjective homomorphism $A_0[[x_1, \dots, x_n]] \twoheadrightarrow A$ for some $n > 0$.*
(2) *If moreover A is regular of dimension $d + 1$ and $p \in P \setminus P^2$, there is such a map with $n = d$, inducing an isomorphism $A \cong A_0[[x_1, \dots, x_d]]$.*

Here, as usual, P denotes the maximal ideal of A.

Proof. For (1) choose elements $t_1, \ldots, t_n \in P$ so that $P = (p, t_1, \ldots, t_n)$. For every $i > 0$ we have an isomorphism

$$A_0[[x_1, \ldots, x_n]]/(p, x_1, \ldots, x_n)^i \cong A_0[x_1, \ldots, x_n]/(p, x_1, \ldots, x_n)^i,$$

whence a unique map of A_0-algebras $A_0[[x_1, \ldots, x_n]]/(p, x_1, \ldots, x_n)^i \to A/P^i$ which sends x_j to t_j for all j. By passing to the inverse limit over i we obtain a map $A_0[[x_1, \ldots, x_n]] \to A$ whose surjectivity follows from Lemma 6.2 as in the proof of Theorem 6.1.

Under the assumptions of (2) we may moreover take $n = d$ and find t_i so that $p, t_1, \ldots, t_d$ is a regular system of parameters for P. As in the proof of Theorem 6.1, the surjection $A_0[[x_1, \ldots, x_d]] \to A$ must then be an isomorphism for dimension reasons. □

If A is regular but $p \in P^2$, then p cannot be part of a regular system of parameters as in the above proof, because then A/pA cannot be an integral domain, contradicting Proposition 4.4 and Theorem 4.6. So in this case there is no isomorphism with a power series ring as in the theorem. The best we can get is:

Proposition 6.18. *Let A be a Noetherian complete local domain of mixed characteristic and dimension $d+1$, and let $A_0 \subset A$ be a Cohen ring. There exists an injective homomorphism $A_0[[x_1, \ldots, x_d]] \hookrightarrow A$ such that A is finitely generated as a module over its image.*

We shall need an easy lemma.

Lemma 6.19. *Let R be a ring complete with respect to an ideal $I \subset R$, and M an R-module satisfying $\cap_j I^j M = (0)$. If M/IM is finitely generated over R/I, then M is finitely generated over R.*

Proof. Choose elements $m_1, \ldots, m_r \in M$ whose images modulo IM generate M/IM over R/I. The equality

$$M = Rm_1 \oplus \cdots \oplus Rm_r + IM \tag{2}$$

then implies

$$I^j M = I^j m_1 \oplus \cdots \oplus I^j m_r + I^{j+1} M \tag{3}$$

for all j. So if $m \in M$, we may write

$$m = \sum_i r_{i0} m_i + n_1$$

with $r_{i0} \in R$ and $n_1 \in IM$ using (2), and then construct inductively elements $r_{ij} \in I^j$ and $n_j \in I^j M$ satisfying

$$n_j = \sum_i r_{ij} m_i + n_{j+1}$$

using (3). Here the sums $r_{i0} + r_{i1} + r_{i2} + \dots$ converge to $r_i \in R$, but then the element $m - \sum_i r_i m_i$ lies in $\cap_j I^j M$, so it equals 0 by assumption. □

Proof of Proposition 6.18. The quotient ring A/pA is Noetherian local of dimension d by Lemma 4.10, so by the converse of the Hauptidealsatz we find $t_1, \dots, t_d \in P$ such that P is minimal above $J = (p, t_1, \dots, t_d)$. Since then some power of P lies in J, it follows from Proposition 5.4 that A is also J-adically complete. As in the previous proof we then obtain a map $\rho : A_0[[x_1, \dots, x_d]] \to A$ induced by sending x_i to t_i and passing to the inverse limit over the quotients A/J^i. Hence A is a module over $R := A_0[[x_1, \dots, x_d]]$ via ρ, and if we put $I = (p, x_1, \dots, x_d) \subset R$, then $J = IA$. Since A/J is Noetherian of dimension 0, it is Artinian, hence finite dimensional over $R/I \cong A_0/pA_0 \cong A/P$. So applying the lemma above with $M = A$ we see that A is a finitely generated R-module. On the other hand, applying Proposition 3.9 to the map $\rho(R) \to A$ we see that $\dim(A/IA) = 0$ implies that $\rho(R)$ has Krull dimension $\geq d + 1$, which is only possible if ρ is injective. □

7. Witt vectors

In this section we study Cohen rings with perfect residue field. Under this assumption, the Cohen ring with residue field k is unique up to unique isomorphism and Theorem 6.14 is very easy to prove.

We prove a more general existence statement involving not necessarily local or Noetherian rings.

Definition 7.1. Let p be a prime number. A *strict p-ring* is a ring A complete with respect to the ideal (p) such that p is not a zero-divisor in A.

Proposition 7.2. *Assume A is a strict p-ring such that the ideal (p) is maximal. Then A is a complete discrete valuation ring with maximal ideal (p).*

Proof. Since every $x \in A \setminus (p)$ is a unit modulo the maximal ideal (p), it is a unit by Lemma 5.19. This shows that A is local with maximal ideal (p). We have $\cap_j (p^j) = (0)$ by completeness, so for every nonzero $a \in A$ we find a unique $r \geq 0$ such that $a \in (p^r) \setminus (p^{r+1})$. Then $a = up^r$ where $u \notin (p)$, hence u is a unit. Moreover, if $a = up^r$ were a zero-divisor, so would be p which is not the case. We conclude that A satisfies the condition of Proposition 1.7 (3) and therefore is a discrete valuation ring. □

Now recall that an integral domain R of characteristic $p > 0$ is *perfect* if the map $x \mapsto x^p$ is an automorphism of R.

Theorem 7.3. *Given a perfect ring R of characteristic p, there exists a strict p-ring $W(R)$ with $W(R)/pW(R) \cong R$. Such a $W(R)$ is unique up to unique isomorphism and functorial in R, i.e. any homomorphism $R \to S$ induces a homomorphism $W(R) \to W(S)$.*

When R is a perfect field, then $W(R)$ is a discrete valuation ring.

In the case when R is a perfect field the ring $W(R)$ was constructed by Ernst Witt in 1937, whence the name 'Witt vectors'. Later several other constructions have been given. Recently a particularly simple one was found by Cuntz and Deninger[4]. We explain their arguments, following the original paper closely.

Construction 7.4. View R as a monoid under multiplication and let $\mathbf{Z}[R]$ be the associated free monoid algebra. Its elements are formal sums of the form $\Sigma_{r\in R} n_r[r]$ with almost all $n_r = 0$. Addition and multiplication are the obvious ones. Note that $[1] = 1$ but $[0] \neq 0$. Multiplicative maps $R \to B$ into commutative rings mapping 1 to 1 correspond to ring homomorphisms $\mathbf{Z}[R] \to B$. The identity map $R = R$ induces the surjective ring homomorphism $\pi : \mathbf{Z}[R] \to R$ which sends $\Sigma n_r[r]$ to $\Sigma n_r r$. Let I be its kernel, so that we have an exact sequence

$$0 \longrightarrow I \longrightarrow \mathbf{Z}[R] \xrightarrow{\pi} R \longrightarrow 0 \ .$$

The multiplicative isomorphism $r \mapsto r^p$ of R induces a ring isomorphism $F : \mathbf{Z}[R] \to \mathbf{Z}[R]$ mapping $\Sigma n_r[r]$ to $\Sigma n_r[r^p]$. It satisfies $F(I) = I$.

Let $W(R) := \varprojlim \mathbf{Z}[R]/I^i$ be the I-adic completion of $\mathbf{Z}[R]$. By construction $W(R)$ is complete with respect to the filtration given by the ideals

$$\widehat{I^i} := \varprojlim I^i/I^{i+n} \subset W(R)$$

where the inverse limit is taken over n. (Note that we do not know a priori that $\widehat{I^i}$ is the i-th power of $\widehat{I}$; this will follow from the proof of Proposition 7.5 below.)

Plainly, the above construction of $W(R)$ is functorial in R.

Proposition 7.5. *If R is a perfect ring of characteristic p, then $W(R)$ is a strict p-ring with $W(R)/pW(R) = R$.*

The proof will require some lemmas. Consider first the map $\delta : \mathbf{Z}[R] \to \mathbf{Z}[R]$ defined by the formula

$$\delta(x) = \frac{1}{p}(F(x) - x^p) \ .$$

[4]J.Cuntz, C. Deninger, An alternative to Witt vectors, Münster J. Math. 7 (2014), no. 1, 105-114.

It is well defined since $F(x) \equiv x^p \mod p\mathbf{Z}[R]$ and because $\mathbf{Z}[R]$, being a free $\mathbf{Z}$-module, has no p-torsion, and therefore for every $x \in p\mathbf{Z}[R]$ we find a unique y with $py = x$.

Lemma 7.6. *For $x, y \in \mathbf{Z}[R]$ the following equalities hold.*

$$\delta(x+y) = \delta(x) + \delta(y) - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} x^i y^{p-i} \tag{4}$$

$$\delta(xy) = \delta(x)F(y) + x^p\delta(y)\ . \tag{5}$$

Proof. Equality (4) follows from the additivity of F and the binomial formula; equality (5) is a straightforward calculation using the multiplicativity of F. □

Corollary 7.7. *We have $\delta(I^n) \subset I^{n-1}$ for all $n \geq 1$.*

Proof. Applying (5) inductively gives the relation

$$\delta(x_1 \cdots x_n) = \sum_{i=1}^{n} x_1^p \cdots x_{i-1}^p \delta(x_i) F(x_{i+1}) \cdots F(x_n) \quad \text{for } x_i \in \mathbf{Z}[R]\ .$$

Equation (4) shows that we have

$$\delta(x+y) \equiv \delta(x) + \delta(y) \mod I^n \quad \text{if } x \text{ or } y \text{ is in } I^n\ .$$

Since elements of I^n are sums of n-fold products of elements of I, the corollary follows from the above formulas. □

Lemma 7.8. *Let R be a perfect ring of characteristic p and $n \geq 1$ an integer.*
a) If $pa \in I^n$ for some $a \in \mathbf{Z}[R]$ then $a \in I^{n-1}$.
b) $I^n = I^i + p^n\mathbf{Z}[R]$ for any $i \geq n$.

Proof. a) According to the previous corollary we have $\delta(pa) \in I^{n-1}$. On the other hand, by definition:

$$\delta(pa) = F(a) - p^{p-1}a^p\ ,$$

and therefore since $pa \in I^n$

$$\delta(pa) \equiv F(a) \mod I^n\ .$$

It follows that $F(a) \in I^{n-1}$ and hence $a \in I^{n-1}$ since F is an automorphism with $F(I) = I$.
b) We prove the inclusion $I^n \subset I^i + p^n\mathbf{Z}[R]$ for $i \geq n$ by induction with respect to $n \geq 1$. The other inclusion is clear. For $y \in \mathbf{Z}[R]$ and $i \geq 1$ we have

$$F^i(y) \equiv y^{p^i} \mod p\mathbf{Z}[R]\ .$$

Applying this to $y = F^{-i}(x)$, we get for all $x \in \mathbf{Z}[R]$

$$x \equiv F^{-i}(x)^{p^i} \mod p\mathbf{Z}[R] .$$

For $x \in I$ this shows that $x \in I^i + p\mathbf{Z}[R]$ settling the case $n = 1$ of the assertion. Now assume that $I^n \subset I^i + p^n\mathbf{Z}[R]$ has been shown for a given $n \geq 1$ and all $i \geq n$. Fix some $i \geq n+1$ and consider an element $x \in I^{n+1}$. By the inductive assumption $x = y + p^n z$ with $y \in I^i$ and $z \in \mathbf{Z}[R]$. Hence $p^n z = x - y \in I^{n+1}$. Using assertion a) of the lemma repeatedly shows that $z \in I$. Hence $z \in I^i + p\mathbf{Z}[R]$ by the case $n = 1$. Writing $z = a + pb$ with $a \in I^i$ and $b \in \mathbf{Z}[R]$ we find

$$x = (y + p^n a) + p^{n+1}b \in I^i + p^{n+1}\mathbf{Z}[R] .$$

Thus we have shown the inductive step $I^{n+1} \subset I^i + p^{n+1}\mathbf{Z}[R]$. □

Proof of Proposition 7.5. We show that there is an equality of ideals $(p^n) = \widehat{I^n}$ for all $n \geq 1$ in $W(R)$ and that p is not a zero-divisor in $W(R)$; since by construction $W(R)$ is complete with respect to the filtration given by the ideals $\widehat{I^n}$, this will show that it is a strict p-ring. We'll then also have $W(R)/pW(R) = W(R)/\widehat{I} \cong R$. Let $p^{-n}(I^i)$ be the inverse image of I^i under p^n-multiplication on $\mathbf{Z}[R]$. Then for any $i \geq n \geq 1$ we have an exact sequence

$$0 \longrightarrow p^{-n}(I^i)/I^i \longrightarrow \mathbf{Z}[R]/I^i \xrightarrow{p^n} I^n/I^i \longrightarrow 0$$

where the surjectivity on the right is due to part b) of Lemma 7.8. From this we get an exact sequence of inverse systems whose transition maps for $i \geq n$ are the reduction maps. In the limit we have an exact sequence

$$0 \longrightarrow \lim_{\leftarrow} p^{-n}(I^i)/I^i \longrightarrow W(R) \xrightarrow{p^n} \widehat{I^n} .$$

The transition map $p^{-n}(I^{i+n})/I^{i+n} \to p^{-n}(I^i)/I^i$ is the zero map since $a \in p^{-n}(I^{i+n})$ implies $p^n a \in I^{i+n}$ and hence $a \in I^i$ by part a) of Lemma 7.8. So condition $b)$ of Lemma 5.10 is satisfied, and therefore the map $p^n : W(R) \to \widehat{I^n}$ is surjective. By Remark 5.11 (1) it also follows that $\lim_{\leftarrow} p^{-n}(I^i)/I^i = 0$, so that $p^n : W(R) \to W(R)$ is injective with image $\widehat{I^n}$, as claimed. □

Remark 7.9. There is an isomorphism

$$R \xrightarrow{\sim} I^n/I^{n+1} \quad \text{given by } r \longmapsto p^n[r] .$$

This holds because

$$I^n/I^{n+1} = \widehat{I^n}/\widehat{I^{n+1}} = p^n W(R)/p^{n+1}W(R) \overset{p^{-n}}{=} W(R)/pW(R) = R .$$

It remains to show the uniqueness property of $W(R)$. We do this via a method that at the same time will yield Theorem 6.14 for complete local rings of mixed characteristic with perfect residue field. We first prove:

Lemma 7.10. *Let A be a ring complete with respect to an ideal $P \subset A$ such that A/P is a perfect ring of characteristic $p > 0$. The natural map $\pi : A \to A/P$ has a unique multiplicative retraction, i.e. a map $\rho : A/P \to A$ satisfying $\pi \circ \rho = \mathrm{id}$ and $\rho(\bar{a}\bar{b}) = \rho(\bar{a})\rho(\bar{b})$ for $\bar{a}, \bar{b} \in A/P$.*

Given $\bar{a} \in A/P$, the element $\rho(\bar{a}) \in A$ is often called the *Teichmüller representative* of $\bar{a}$ and ρ the Teichmüller retraction. A basic example is $A = \mathbf{Z}_p$: each nonzero element $\bar{a}$ of the residue field $\mathbf{F}_p$ satisfies the polynomial $x^{p-1} - 1$ and hence lifts to an element of $\mathbf{Z}_p$ by Hensel's lemma. In other words, $\mathbf{Z}_p$ contains the group μ_{p-1} of $p-1$-st roots of unity whose elements, together with 0, are the Teichmüller representatives of the elements of $\mathbf{F}_p$.

Proof. Given $\bar{a} \in A/P$, we show that there is a unique $\rho(\bar{a}) \in A$ satisfying the properties

$$\bar{a} = \rho(\bar{a}) \bmod P, \quad \rho(\bar{a}) \in \bigcap_{n=0}^{\infty} A^{p^n}. \tag{6}$$

This will define the required multiplicative retraction, since for $\bar{b} \in A/P$ the product $\rho(\bar{a})\rho(\bar{b})$ lifts $\bar{a} \cdot \bar{b}$ and is contained in A^{p^n} for all $n > 0$. Note that since A/P is perfect, any multiplicative retraction ρ must satisfy the conditions in (6), so uniqueness will also follow.

First we show that for all $i \geq 1$ there is a unique element $a_i \in A/P^{i+1}$ mapping to $\bar{a}$ mod P that is in the image of A^{p^i} mod P^{i+1}. Indeed, since A/P is perfect, we find a unique $\bar{x} \in A/P$ with $\bar{a} = \bar{x}^{p^i}$. Lifting $\bar{x}$ to $x \in A$ we have $(x+y)^{p^i} = x^{p^i}$ mod P^{i+1} for $y \in P$ since $p \in P$ and therefore $p^i \in P^i$ by assumption. Hence the class

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

does not depend on x and is the unique class we were looking for. Moreover, since obviously $x^{p^i} \in A^{p^{i-1}}$, by uniqueness we must have

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

Therefore, since A is complete with respect to P, the sequence (a_i) defines an element of $\varprojlim A/P^{i+1} = A$ mapping to $\bar{a}$ modulo P. Denote it by $\rho(\bar{a})$.

Now fix $n > 0$ and let $\bar{b}_n \in A/P$ be the unique element with $\bar{b}_n^{p^n} = \bar{a}$. Then $\rho(\bar{b}_n)^{p^n}$ mod P^{i+1} also comes from A^{p^i} for all i and maps to $\bar{a}$ mod P. By uniqueness of the a_i we must have $\rho(\bar{a}) = \rho(\bar{b}_n)^{p^n}$. It follows that $\rho(\bar{a}) \in A^{p^n}$ for all n, as required. □

Example 7.11. For $A = W(R)$ the composite map $R \to \mathbf{Z}[R] \to W(R)$ is multiplicative, so by uniqueness it must be the Teichmüller retraction.

Corollary 7.12. *If A is as in Lemma 7.10 and R is a perfect ring of characteristic p, every homomorphism $\bar{\varphi} : R \to A/P$ lifts to a unique homomorphism $\varphi : W(R) \to A$ such that the induced map $W(R)/pW(R) \to A/P$ coincides with $\bar{\varphi}$.*

Note that if ϕ exists, it must map $(p) \subset W(R)$ to $P \subset A$ by assumption and hence (p^i) to P^i; in other words, it must be continuous for the topologies of the complete local rings $W(R)$ and A.

Proof. The composite map $\rho \circ \bar{\varphi} : R \to A/P \to A$ preserves multiplication, hence extends uniquely to a ring homomorphism $\tilde{\varphi} : \mathbf{Z}[R] \to A$. By construction $\tilde{\varphi}(I) \subset P$, hence $\tilde{\varphi}(I^i) \subset P^i$. Thus there is a canonical induced map φ from the I-adic completion $W(R)$ of $\mathbf{Z}[R]$ to the P-adically complete A. For uniqueness of the lifting φ denote by ρ_W the Teichmüller retraction of $W(R)$ and by ρ that of A. Given $r \in R$, any lifting of $\bar{\varphi}$ must send $\rho_W(r)$ to $(\rho \circ \bar{\varphi})(r)$ by uniqueness of the Teichmüller retractions; in the remaining steps of the construction uniqueness holds. □

Proof of Theorem 7.3. Existence was proven in proposition 7.5 and uniqueness follows from the previous corollary. The last statement follows from Proposition 7.2. □

The following corollary gives an easy proof of Theorem 6.14 in the case when k is perfect.

Corollary 7.13. *Let A be a complete local integral domain of characteristic 0 with maximal ideal P and perfect residue field k of characteristic $p > 0$. The identity map of k induces an injective map $\varphi : W(k) \to A$ where $\varphi^{-1}(P) = pW(k)$.*

Proof. Apply the previous corollary with $R = k$. Since A is an integral domain of characteristic 0, the kernel of φ is a prime ideal that must be different from (p), and hence equals (0). □

Remark 7.14. Classically, elements of $W(R)$ are represented by infinite sequences ('vectors')

$$(r_0, r_1, r_2, \dots) \tag{7}$$

with $r_i \in R$. The vector (7) corresponds to the convergent sum

$$\sum_{i=0}^{\infty} \rho(r_i)^{p^{-i}} p^i \in W(R)$$

where ρ is the Teichmüller retraction. Note, therefore, that the ring operations in $W(R)$ do *not* correspond to componentwise addition and multiplication on the sequences (7)!

There are two important operations on Witt vectors. The first is the *Frobenius*

$$F : (r_0, r_1, r_2, \dots) \mapsto (r_0^p, r_1^p, r_2^p, \dots).$$

It corresponds to the unique automorphism of $W(R)$ induced by F on $\mathbf{Z}[R]$; it exists because of $F(I) = I$.

The second is the *Verschiebung* ('shift') given by

$$V : (r_0, r_1, r_2, \dots) \mapsto (0, r_0, r_1, r_2, \dots).$$

On $W(R)$ it corresponds to the additive homomorphism defined by $V(x) = pF^{-1}(x)$. By definition $\operatorname{Im} V^i = p^i W(R)$ and $V \circ F = F \circ V = p$.

8. Derivations and differentials

In differential geometry, the tangent space at a point P on some variety is defined to consist of so-called *linear derivations*, i.e. linear maps that associate a scalar to each function germ at P and satisfy the Leibniz rule. Here is an algebraic version of this notion.

Definition 8.1. Let B be a ring and M a B-module. A *derivation* of B into M is a map $d : B \to M$ subject to the two conditions:

(1) (Additivity) $d(x + y) = dx + dy$;
(2) (Leibniz rule) $d(xy) = xdy + ydx$.

Here we have written dx for $d(x)$ to emphasise the analogy with the classical derivation rules. If moreover B is an A-algebra for some ring A (for example $A = \mathbf{Z}$), an A-linear derivation is called an *A-derivation*. The set of A-derivations of B to M is equipped with a natural B-module structure via the rules $(d_1 + d_2)x = d_1x + d_2x$ and $(bd)x = b(dx)$. This B-module is denoted by $\operatorname{Der}_A(B, M)$.

Note that applying the Leibniz rule to the equality $1 \cdot 1 = 1$ gives $d(1) = 0$ for all derivations; hence all A-derivations are trivial on the image of A in B.

In the example one encounters in (say) real differential geometry we have $A = M = \mathbf{R}$, and B is the ring of germs of differentiable functions at some point; $\mathbf{R}$ is a B-module via evaluation of functions. Now comes a purely algebraic example.

Example 8.2. Assume given an A-algebra B which decomposes *as an A-module* into a direct sum $B \cong A \oplus I$, where I is an ideal of B with $I^2 = 0$. Then the natural projection $d : B \to I$ is an A-derivation of B into I. Indeed, A-linearity is immediate;

for the Leibniz rule we take elements $x_1, x_2 \in B$ and write $x_i = a_i + dx_i$ with $a_i \in k$ for $i = 1, 2$. Now we have

$$d(x_1x_2) = d[(a_1 + dx_1)(a_2 + dx_2)] = d(a_1a_2 + a_2dx_1 + a_1dx_2) = x_2dx_1 + x_1dx_2$$

where we used several times the facts that $I^2 = 0$ and $d(A) = 0$.

In fact, given any ring A and A-module I, we can define an A-algebra B as above by defining a product structure on the A-module $A \oplus I$ by the rule $(a_1, i_1)(a_2, i_2) = (a_1a_2, a_1i_2 + a_2i_1)$. So the above method yields plenty of examples of derivations.

Now notice that for fixed A and B the rule $M \to \mathrm{Der}_A(B, M)$ defines a functor on the category of B-modules; indeed, given a homomorphism $\phi : M_1 \to M_2$ of B-modules, we get a natural homomorphism $\mathrm{Der}_A(B, M_1) \to \mathrm{Der}_A(B, M_2)$ by composing derivations with ϕ.

Proposition 8.3. *There exists a B-module $\Omega^1_{B/A}$ together with an A-derivation $d : B \to \Omega^1_{B/A}$ such that for every B-module M and derivation $\delta \in \mathrm{Der}_A(B, M)$ we have a factorization $\delta = \phi \circ d$ with a B-homomorphism $\Omega^1_{B/A} \to M$.*

Proof. Define $\Omega^1_{B/A}$ to be the quotient of the free B-module generated by symbols dx for each $x \in B$ modulo the relations given by the additivity and Leibniz rules as in Definition 8.1 as well as the relations $d(\lambda(a)) = 0$ for all $a \in A$, where $\lambda : A \to B$ is the map defining the A-module structure on B. The map $x \to dx$ is an A-derivation of B into $\Omega^1_{B/A}$. Moreover, given any B-module M and A-derivation $\delta \in \mathrm{Der}_A(B, M)$, the map $dx \to \delta(x)$ induces a B-module homomorphism $\Omega^1_{B/A} \to M$ whose composition with d is just δ. □

We call $\Omega^1_{B/A}$ the module of *relative differentials* of B with respect to A. We shall often refer to the elements of $\Omega^1_{B/A}$ as *differential forms*.

Next we describe how to compute relative differentials of a finitely presented A-algebra.

Proposition 8.4. *Let B be the quotient of the polynomial ring $A[x_1, \ldots, x_n]$ by an ideal generated by finitely many polynomials $f_1, \ldots, f_m$. Then $\Omega^1_{B/A}$ is the quotient of the free B-module on generators $dx_1, \ldots, dx_n$ modulo the B-submodule generated by the elements $\sum_j (\partial_j f_i) dx_j$ $(i = 1, \ldots, m)$, where $\partial_j f_i$ denotes the j-th (formal) partial derivative of f_i.*

Proof. First consider the case $B = A[x_1, \ldots, x_n]$. As B is the free A-algebra generated by the x_i, one sees that for any B-module M there is a bijection between $\mathrm{Der}_A(B, M)$ and maps of the set $\{x_1, \ldots, x_n\}$ into B. This implies that $\Omega^1_{B/A}$ is the free A-module generated by the dx_i.

The general case follows from this in view of the easy observation that given any M, composition by the projection $A[x_1, \dots, x_n] \to B$ induces an isomorphism of $\mathrm{Der}_A(B, M)$ onto the submodule of $\mathrm{Der}_A(A[x_1, \dots, x_n], M)$ consisting of derivations mapping the f_i to 0. □

Next some basic properties of modules of differentials.

Lemma 8.5. *Let A be a ring and B an A-algebra.*

(1) *(Direct sums) For any A-algebra B'*

$$\Omega^1_{(B\oplus B')/A} \cong \Omega^1_{B/A} \oplus \Omega^1_{B'/A}.$$

(2) *(Base change) Given a ring homomorphism $A \to A'$, denote by B' the A'-algebra $B \otimes_A A'$. There is a natural isomorphism*

$$\Omega^1_{B/A} \otimes_B B' \cong \Omega^1_{B'/A'}.$$

(3) *(Localization) For any multiplicatively closed subset $S \subset B$ there is a natural isomorphism*

$$\Omega^1_{B_S/A} \cong \Omega^1_{B/A} \otimes_B B_S.$$

Proof. The first property follows from the definitions. For base change, note first that the universal derivation $d : B \to \Omega^1_{B/A}$ is an A-module homomorphism and so tensoring it by A' we get a map

$$d' : B' \to \Omega^1_{B/A} \otimes_A A' \cong \Omega^1_{B/A} \otimes_B B \otimes_A A' \cong \Omega^1_{B/A} \otimes_B B'$$

which is easily seen to be an A'-derivation. Now any A'-derivation $\delta' : B' \to M'$ induces an A-derivation $\delta : B \to M'$ by composition with the natural map $B \to B'$. But δ factors as $\delta = \phi \circ d$, with a B-module homomorphism $\phi : \Omega^1_{B/A} \to M'$, whence a map $\phi' : \Omega^1_{B/A} \otimes_B B' \to M'$ constructed as above. Now one checks that $\delta' = \phi' \circ d'$ which means that $\Omega^1_{B/A} \otimes_B B'$ satisfies the universal property for $\mathrm{Der}_{A'}(B', M')$.

For the localization property, given an A-derivation $\delta : B \to M$, we may extend it uniquely to an A-derivation $\delta_S : B_S \to M \otimes_B B_S$ by setting $\delta_S(b/s) = (\delta(b)s - b\delta(s)) \otimes (1/s^2)$. (We leave it to the reader to check that for $b'/s' = b/s$ we get the same result.) This applies in particular to the universal derivation $d : B \to \Omega^1_{B/A}$, and one argues as in the previous case to show that any A-derivation $B_S \to M_S$ factors uniquely through d_S. □

There are two fundamental exact sequences that are instrumental in computing modules of differentials.

Proposition 8.6. *Let $\phi : B \to C$ be a homomorphism of A-algebras.*

(1) *There is an exact sequence of C-modules*

$$\Omega^1_{B/A} \otimes_B C \to \Omega^1_{C/A} \to \Omega^1_{C/B} \to 0. \tag{8}$$

(2) *If moreover ϕ is surjective with kernel I, we have an exact sequence of C-modules*

$$I/I^2 \to \Omega^1_{B/A} \otimes_B C \to \Omega^1_{C/A} \to 0.$$

Note that I/I^2 is indeed a module over $B/I \cong C$.

For the proof recall the following easy lemma.

Lemma 8.7. *Let M_1, M_2, M_3 be A-modules and*

$$M_1 \xrightarrow{i} M_2 \xrightarrow{p} M_3 \to 0 \tag{9}$$

a sequence of A-homomorphisms. This is an exact sequence if and only if for any A-module N the sequence induced by composition of R-homomorphisms

$$0 \to \mathrm{Hom}_A(M_3, N) \to \mathrm{Hom}_A(M_2, N) \to \mathrm{Hom}_A(M_1, N) \tag{10}$$

is an exact sequence of A-modules.

Proof. The proof that exactness of (9) implies that of (10) is easy and is left to the readers. The converse is not much harder: taking $N = M_3/M_2$ shows that injectivity of the second map in (10) implies the surjectivity on the right in (9), and taking $N = M_2/im(i)$ shows that if moreover (10) is exact in the middle, then the surjection $M_2/im(i) \to M_3$ has a section $M_3 \to M_2/im(i)$ and thus $im(i) = ker(p)$. □

Proof of Proposition 8.6. For the first statement note that for any C-module M we have a natural exact sequence

$$0 \to \mathrm{Der}_B(C, M) \to \mathrm{Der}_A(C, M) \to \mathrm{Der}_A(B, M)$$

of C-modules isomorphic to

$$0 \to \mathrm{Hom}_C(\Omega^1_{C/B}, M) \to \mathrm{Hom}_C(\Omega^1_{C/A}, M) \to \mathrm{Hom}_B(\Omega^1_{B/A}, M).$$

Now observe that there is an isomorphism $\mathrm{Hom}_B(\Omega^1_{B/A}, M) \cong \mathrm{Hom}_C(\Omega^1_{B/A} \otimes_B C, M)$ induced by mapping a homomorphism $\Omega^1_{B/A} \to M$ to the composite $\Omega^1_{B/A} \otimes_B C \to M \otimes_B C \to M$ where the second map is multiplication. An inverse is given by composition with the natural map $\Omega^1_{B/A} \to \Omega^1_{B/A} \otimes_B C$. Thus we may rewrite the previous exact sequence as

$$0 \to \mathrm{Hom}_C(\Omega^1_{C/B}, M) \to \mathrm{Hom}_C(\Omega^1_{C/A}, M) \to \mathrm{Hom}_C(\Omega^1_{B/A} \otimes_B C, M). \tag{11}$$

Set $M = \Omega^1_{C/B}$. The image of $\mathrm{id}_{\Omega^1_{C/B}} \in \mathrm{Hom}_C(\Omega^1_{C/B}, \Omega^1_{C/B})$ by the first map of the above exact sequence gives a map in $\mathrm{Hom}_C(\Omega^1_{C/A}, \Omega^1_{C/B})$ which is the second map in (8). Similarly, setting $M = \Omega^1_{C/A}$ and taking the image of $\mathrm{id}_{\Omega^1_{C/A}} \in \mathrm{Hom}_C(\Omega^1_{C/A}, \Omega^1_{C/A})$

in (11) defines the first map in (8). Finally, since the sequence (11) is exact for all C-modules M, the sequence in (8) is exact by the lemma above.

If the map $B \to C$ is surjective, then any B-derivation $C \to M$ is trivial, so $\Omega^1_{B/C} = 0$ and the first map in the first exact sequence is surjective, giving the surjectivity of the second map in the second sequence. Now define a map $\delta : I \to \Omega^1_{B/A} \otimes_B C$ by $\delta(x) := dx \otimes 1$. This is a B-module map because the Leibniz rule for d implies $\delta(bx) = bdx \otimes 1$ for $b \in B$, $x \in I$; indeed, we have $xdb \otimes 1 = db \otimes x$ which is 0 in $\Omega^1_{B/A} \otimes_B C$. If $x \in I^2$, the same argument shows that $\delta(x) = 0$, whence the C-module map $\bar{\delta} : I/I^2 \to \Omega^1_{B/A} \otimes_B C$ in the second exact sequence. To conclude, it will again suffice to verify the exactness of the dual sequence

$$0 \to \mathrm{Der}_A(C, M) \to \mathrm{Der}_A(B, M) \to \mathrm{Hom}_C(I/I^2, M)$$

for all C-modules M, where injectivity on the left is already proven. The second map is induced by composition with the inclusion map $I \to B$: indeed, if we restrict a derivation $\delta : B \to M$ to I, then the Leibniz rule for δ gives $\delta(I^2) = 0$ as well as $\delta(bx) = b\delta(x) + x\delta(b) = b\delta(x)$ for all $b \in B$, $x \in I$. This implies exactness in the middle. □

Here is a first application.

Proposition 8.8. *A finite extension $K|k$ of fields is separable if and only if $\Omega^1_{K/k} = 0$.*

Proof. If $K|k$ is separable, then $K \cong k[x]/(f)$ with a polynomial f satisfying $f' \neq 0$, so Proposition 8.4 gives $\Omega^1_{K/k} = 0$. For the converse we may assume k has characteristic $p > 0$. Recall from field theory[5] that there exists an intermediate field $k \subset K_0 \subset K$ such that $K_0|k$ is separable and $K = K_0(\sqrt[p^{r_1}]{a_1}, \ldots, \sqrt[p^{r_m}]{a_m})$ for some $a_i \in K_0$ and $r_i > 0$. Applying Proposition 8.6 (1) with $A = k$, $B = K_0$, $C = K$ gives $\Omega^1_{K/k} \cong \Omega^1_{K/K_0}$ by the first part of the proof, and then Proposition 8.4 gives $\Omega^1_{K/K_0} \cong K_0^m$, which can be 0 only for $K = K_0$. □

9. Differentials, regularity and smoothness

By means of differentials we obtain a new characterization of regular local rings coming from geometry.

Proposition 9.1. *Let k be a perfect field, and let A be an integral domain of dimension d which is a finitely generated k-algebra. Given a prime ideal P, the localization A_P is a regular local ring if and only if $\Omega^1_{A_P/k}$ is a free A_P-module of rank d.*

For the proof we need a lemma from field theory:[6]

[5] See e.g. Lang, Algebra, Chapter V, §6.

[6] For a proof, see e.g. Lang, Algebra, Chapter VIII, Corollary 4.4.

Lemma 9.2. *Let k be a perfect field and let $K|k$ be a finitely generated field extension of transcendence degree n. Then there exist algebraically independent elements $x_1, \ldots, x_n \in K$ such that the finite extension $K|k(x_1, \ldots, x_n)$ is separable.*

Corollary 9.3. *In the situation of the lemma, the K-vector space $\Omega^1_{K/k}$ is of dimension n, a basis being given by the dx_i.*

Proof. We may write the field K as the fraction field of the quotient A of the polynomial ring $k[x_1, \ldots, x_n, x]$ by a single polynomial relation f. Here f is the minimal polynomial of a generator of the extension $K|k(x_1, \ldots, x_n)$ multiplied with a common denominator of its coefficients. Now according to Proposition 8.4 the A-module $\Omega^1_{A/k}$ has a presentation with generators $dx_1, \ldots, dx_n, dx$ and a relation in which dx has a nontrivial coefficient because $f' \neq 0$ by the lemma. The corollary now follows using Lemma 8.5 (3). □

Proof of Proposition 9.1. We denote the maximal ideal of A_P again by P and by κ its residue field. Applying the second exact sequence of Proposition 8.6 to the surjection $A_P \twoheadrightarrow \kappa$ we obtain an exact sequence of κ-vector spaces

$$P/P^2 \to \Omega^1_{A_P/k} \otimes_{A_P} \kappa \to \Omega^1_{\kappa/k} \to 0.$$

We contend that here the first map is injective. To prove this we may replace A_P by A_P/P^2. Indeed, applying Proposition 8.6 (2) to the surjection $A_P \twoheadrightarrow A_P/P^2$ we obtain an exact sequence

$$P^2/P^4 \to \Omega^1_{A_P/k} \otimes_{A_P} (A_P/P^2) \to \Omega^1_{(A_P/P^2)/k} \to 0$$

which gives an isomorphism $\Omega^1_{A_P/k} \otimes_{A_P} \kappa \to \Omega^1_{(A_P/P^2)/k} \otimes_{A_P/P^2} \kappa$ upon tensoring with κ. Thus we may assume $P^2 = 0$, in which case A_P is *complete*. Applying Theorem 6.11 we obtain a subfield in A_P isomorphic to κ and an isomorphism of κ-vector spaces $A_P \cong \kappa \oplus P$. Now recall that for every κ-vector space M the map

$$\mathrm{Hom}_\kappa(\Omega^1_{A_P/k} \otimes_{A_P} \kappa, M) \to \mathrm{Hom}_\kappa(P, M) \tag{12}$$

identifies with the map $\mathrm{Der}_k(A_P, M) \to \mathrm{Hom}_\kappa(P, M)$ obtained by composing with the inclusion $P \to A_P$. But this map has a retraction: composing a κ-homomorphism $P \to M$ by the quotient map $A_P \to A_P/\kappa \cong P$ of k-vector spaces gives a k-derivation $A_P \to M$ as in Example 8.2. So the map (12) is surjective for all M, whence the required injectivity.

Now return to the general case. By the injectivity proven above, reading off dimensions in the above exact sequence gives

$$\dim{}_\kappa(\Omega^1_{A_P/k} \otimes_{A_P} \kappa) = \dim{}_\kappa P/P^2 + \dim{}_\kappa \Omega^1_{\kappa/k}.$$

Here $\dim {}_\kappa\Omega^1_{\kappa/k} = \mathrm{tr.deg}_k(\kappa) = d - \dim A_P$ by Corollary 9.3 and Corollary 2.9 (1). Thus A_P is regular if and only if $\dim {}_\kappa(\Omega^1_{A_P/k} \otimes_{A_P} \kappa) = d$. If $\Omega^1_{A_P/k}$ is free of rank d, this certainly holds. Conversely, choose elements $dt_1, \dots, dt_d \in \Omega^1_{A_P/k}$ such that their images in $\Omega^1_{A_P/k} \otimes_{A_P} \kappa = \Omega^1_{A_P/k}/P\Omega^1_{A_P/k}$ form a basis over κ. By Nakayama's lemma they then generate $\Omega^1_{A_P/k}$ as an A_P-module, so by sending the standard generators of the free module A_P^d to the dt_i we obtain an exact sequence of the form

$$0 \to N \to A_P^d \to \Omega^1_{A_P/k} \to 0.$$

The fraction field K of A_P is a flat A_P-module, so the induced sequence

$$0 \to N \otimes_{A_P} K \to K^d \to \Omega^1_{A_P/k} \otimes_{A_P} K \to 0$$

is exact. But by Lemma 8.5 (3) and Corollary 9.3 the K-vector space $\Omega^1_{A_P/k} \otimes_{A_P} K \cong \Omega^1_{K/k}$ has dimension d, so the last exact sequence gives $N \otimes_{A_P} K = 0$. Since A_P is an integral domain and N is a submodule of A_P^d, this is only possible for $N = 0$, i.e. when $\Omega^1_{A_P/k}$ is free of rank d. □

The proposition can be made explicit as follows. Consider a presentation

$$A = k[x_1, \dots, x_n]/(f_1, \dots, f_r),$$

and introduce the $n \times r$ *Jacobian matrix* $J := [\partial_i f_j]$. Given a preimage Q of P in $k[x_1, \dots, x_n]$, we consider J as a matrix with entries in $k[x_1, \dots, x_n]_Q$. In this way it makes sense to view J mod Q as a matrix with entries in κ.

Corollary 9.4 (Jacobian criterion)**.** *With notations and assumptions as above, the ring A_P is regular if and only if the matrix J* mod *Q has rank $n - d$.*

Proof. For ease of notation set $R := k[x_1, \dots, x_n]$ and write I for the ideal $(f_1, \dots, f_r)R_Q$. We then have an exact sequence $0 \to I \to R_Q \to A_P \to 0$, whence by Proposition 8.6 (2) an exact sequence of A_P-modules

$$I/I^2 \to \Omega^1_{R_Q/k} \otimes_{R_Q} A_P \to \Omega^1_{A_P/k} \to 0.$$

Tensoring by κ gives an exact sequence of κ-vector spaces

$$I/I^2 \otimes_{A_P} \kappa \xrightarrow{\bar\delta} \Omega^1_{R_Q/k} \otimes_{R_Q} \kappa \to \Omega^1_{A_P/k} \otimes_{A_P} \kappa \to 0.$$

Here $\Omega^1_{R_Q/k} \otimes_{R_Q} \kappa \cong \Omega^1_{R/k} \otimes_R \kappa \cong \kappa^n$ by Lemma 8.5 (3) and Proposition 8.4, and from the previous proposition we know that $\Omega^1_{A_P/k} \otimes_{A_P} \kappa \cong \kappa^d$ if and only if A_P is regular. So A_P is regular if and only if $\mathrm{Im}(\bar\delta)$ has dimension $n - d$. Now if we identify $\Omega^1_{R_Q/k} \otimes_{R_Q} \kappa$ with κ^n via the κ-basis given by $dx_1, \dots, dx_n$, we obtain that the map $\bar\delta$ is induced by the map $\lambda : I \to \kappa^n$ given by $f \mapsto (\partial_1 f, \dots, \partial_n f)$ mod Q. It remains to note that $\dim \mathrm{Im}(\lambda)$ equals the rank of the matrix J mod Q. □

We now relate the above to the property of formal smoothness encountered during the discussion of the Cohen structure theorem. Recall that an R-algebra S of rings is *formally smooth* if it satisfies the following property: given a commutative diagram

$$\begin{array}{ccc} S & \xrightarrow{\bar{\lambda}} & B/I \\ \uparrow & & \uparrow \\ R & \xrightarrow{\mu} & B \end{array} \tag{13}$$

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

Here are some basic properties of formal smoothness.

Lemma 9.5. *Let S be a formally smooth R-algebra.*

1. *(Base change) If R' is any R-algebra, then $S \otimes_R R'$ is formally smooth over R'.*
2. *(Transitivity) If S' is a formally smooth S-algebra, then it is also formally smooth over R.*
3. *(Tensor product) If S_1 and S_2 are formally smooth R-algebras, then so is $S_1 \otimes_R S_2$.*
4. *(Localization) If $T \subset S$ is a multiplicatively closed subset, then the localization S_T is also formally smooth over R.*

Proof. For (1), note first that any R'-algebra B' is also an R-algebra. Given an R'-algebra map $\bar{\lambda}' : S \otimes_R R' \to B'/I'$ with $I'^2 = 0$, it induces an R-algebra map $S \to B'/I'$ by composition with the map $s \mapsto s \otimes 1$, whence a lifting $S \to B'$ by formal smoothness of S. Since B' is an R'-algebra, there is an induced map $S \otimes_R R' \to B'$ lifting $\bar{\lambda}'$. For statement (2), assume given $\bar{\lambda} : S' \to B/I$ with an R-algebra B and $I^2 = 0$. By formal smoothness of S over R the composite map $S \to S' \to B/I$ lifts to an R-algebra map $S \to B$, so that B is also an S-algebra. Then by formal smoothness of S' over S $\bar{\lambda}$ lifts to a map $S' \to B$ as required. Statement (3) follows from (1) and (2): by (1) the tensor product $S_1 \otimes_R S_2$ is formally smooth over S_2, hence over R by (2).

For (4) assume given $\bar{\lambda}_T : S_T \to B/I$ with an R-algebra B and $I^2 = 0$. The composite map $S \to S_T \to B/I$ lifts to a map $\lambda : S \to B$ by formal smoothness of S over R. By Lemma 5.19 the elements of $\lambda(T)$ are units in B, so λ induces a map $S_T \to B$ lifting $\bar{\lambda}_T$, as required. □

Now we come to a key example, already studied above.

Proposition 9.6. *Let k be a field, $A = k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$, and $P \subset A$ a prime ideal with preimage $Q \subset k[x_1, \ldots, x_n]$. If the Jacobian matrix $J = [\partial_i f_j]$ has rank r modulo Q, then A_P is formally smooth over k.*

Proof. We proceed like in the proof of Proposition 6.6. As before, write $R := k[x_1, \dots, x_n]$. Assume given $\bar{\lambda} : A_P \to B/I$ with a k-algebra B and $I^2 = 0$. It will be enough to lift the composite map $\bar{\mu} : R/(f_1, \dots, f_r) \to A_P \to B/I$ to a map $R/(f_1, \dots, f_r) \to A_P \to B/I$, for then the lifting will factor through A_P as in the proof of Lemma 9.5 (4). Choose preimages $b_i \in B$ of $\mu(x_i) \in B/I$ for all i. In order to construct the required lifting, it suffices to find $h_i \in I$ such that $f_j(b_1 + h_1, \dots b_n + h_n) = 0$ for all j. Now the multivariable Taylor formula of degree 2 gives a matrix equation

$$\begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} f_1(b_1 + h_1, \dots, b_n + h_n) \\ \vdots \\ f_r(b_1 + h_1, \dots, b_n + h_n) \end{bmatrix} = \begin{bmatrix} f_1(b_1, \dots, b_n) \\ \vdots \\ f_r(b_1, \dots, b_n) \end{bmatrix} + J(b_1, \dots, b_n) \begin{bmatrix} h_1 \\ \vdots \\ h_n \end{bmatrix} \tag{14}$$

in view of $I^2 = 0$. Note that by assumption some $r \times r$ minor of J maps to a unit in R_Q, hence in A_P, and therefore $J(b_1, \dots, b_n)$ mod I is a unit. Hence it is a unit in B as well, i.e. the matrix $J(b_1, \dots, b_n)$ has rank r and the matrix equation is solvable.[7] □

Remark 9.7. The same argument shows that if A is a ring, $B = A[x_1, \dots, x_n]/(f_1, \dots, f_r)$ and the Jacobian matrix $J = [\partial_i f_j]$ has an $r \times r$ minor which is a unit in B, then B is formally smooth over A.

In the presence of formal smoothness we have a strengthening of Proposition 8.6.

Proposition 9.8. *Let $\phi : B \to C$ be a formally smooth homomorphism of A-algebras.*

(1) *There is a split exact sequence of C-modules*

$$0 \to \Omega^1_{B/A} \otimes_B C \to \Omega^1_{C/A} \to \Omega^1_{C/B} \to 0.$$

(2) *If moreover ϕ is surjective with kernel I, we have a split exact sequence of C-modules*

$$0 \to I/I^2 \to \Omega^1_{B/A} \otimes_B C \to \Omega^1_{C/A} \to 0.$$

Proof. For (1), note that from the proof of Proposition 8.6 we already have an exact sequence

$$0 \to \mathrm{Der}_B(C, M) \to \mathrm{Der}_A(C, M) \to \mathrm{Der}_A(B, M).$$

for all C-modules M. It will be enough to extend it to a split exact sequence

$$0 \to \mathrm{Der}_B(C, M) \to \mathrm{Der}_A(C, M) \to \mathrm{Der}_A(B, M) \to 0.$$

[7] Indeed, we may assume the first $r \times r$ minor of $J(b_1, \dots, b_n)$ is a unit. Denoting the corresponding $r \times r$ matrix by A the inverse A^{-1} exists by Cramer's formula. Now the equation (14) is solvable if and only if it is solvable after multiplying by A^{-1} on the left. But $A^{-1}J(b_1, \dots, b_n)$ is the unit matrix with $n - r$ extra columns added, so solvability is immediate.

Fix a derivation $D \in \mathrm{Der}_A(B, M)$ and consider the commutative diagram

$$\begin{array}{ccc} C & \xrightarrow{\mathrm{id}} & C \\ \uparrow & & \uparrow \\ B & \xrightarrow{(\phi, D)} & C \oplus M \end{array}$$

where $C \oplus M$ is given a ring structure with $M^2 = 0$ as in Example 8.2. By formal smoothness there is a map $C \to C \oplus M$ making the diagram commute which, composed with the projection $C \oplus M \to M$, gives an element in $\mathrm{Der}_A(C, M)$ whose restriction to B is D by construction. This defines the required retraction $\mathrm{Der}_A(B, M) \to \mathrm{Der}_A(C, M)$. Statement (2) is proven by the same argument as in the first half of the proof of Proposition 9.1, using formal smoothness instead of the application of Theorem 6.11. □

We may now complete Proposition 9.1 as follows.

Theorem 9.9. *Let k be a perfect field, $A = k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$ an integral domain of dimension d, and $P \subset A$ a prime ideal with preimage $Q \subset k[x_1, \ldots, x_n]$. The following are equivalent.*

(1) *The Jacobian matrix $J = [\partial_i f_j]$ has rank $n - d$ modulo Q.*
(2) *The localization A_P is formally smooth over k.*
(3) *The A_P-module $\Omega^1_{A_P/k}$ is free of rank d.*
(4) *A_P is a regular local ring.*

Proof. The equivalence of (1), (3) and (4) is Proposition 9.1 together with Corollary 9.4, and the implication $(1) \Rightarrow (2)$ will follow from Proposition 9.6 once we show that we may assume $r = n - d$. Write $R := k[x_1, \ldots, x_n]$ as before. We may number the variables x_i and the polynomials f_j so that the $(n - d) \times (n - d)$ minor $\det[(\partial_i f_j)_{1 \le i,j \le n-d}]$ is nonzero mod Q. If we set $\kappa := R_Q/QR_Q$, this means that the map $\rho : QR_Q \to \kappa^n$ given by $\rho(f) := (\partial_1 f, \ldots \partial_n f)$ mod Q maps $f_1, \ldots, f_{n-d}$ to linearly independent elements in κ^n. But ρ factors through $QR_Q/(QR_Q)^2$, so we conclude that $f_1, \ldots, f_{n-d}$ give linearly independent elements in the κ-vector space $QR_Q/(QR_Q)^2$. Here R_Q is a regular local ring, so the f_i form a regular sequence in R_Q by Theorem 4.9. On the other hand, using Lemma 4.10 we then obtain that $\mathrm{ht}((f_1, \ldots, f_{n-d})R_Q) = \mathrm{ht}(f_1, \ldots, f_{n-d}) = n - d$, which is also the height of $(f_1, \ldots, f_r)$ by Remark 2.9 (1). This shows $(f_1, \ldots, f_{n-d}) = (f_1, \ldots, f_r)$ as required.

Finally, for $(2) \Rightarrow (3)$, set $I = (f_1, \ldots, f_r)R_Q$ and apply Proposition 9.8 (2) to obtain a split exact sequence

$$0 \to I/I^2 \to \Omega^1_{R_Q/k} \otimes_{R_Q} A_P \to \Omega^1_{A_P/k} \to 0.$$

Here $\Omega^1_{R_P/k}$ is free of rank n by Proposition 8.4, so the finitely generated A_P-module $\Omega^1_{A_P/k}$ is a direct summand of a free module. It is thus projective over A_P, hence free. Its rank is calculated as in the proof of Proposition 9.1: for the fraction field K of A_P we have $\Omega^1_{K/k} \cong \Omega^1_{A_P/k} \otimes_{A_P} K$ by Lemma 8.5 (3) and this K-vector space has dimension d by Corollary 9.3. □

Remark 9.10. By Lemma 9.5 (4) formal smoothness of A_P over k implies that of K. It can be shown that this implies that K is separably generated over k, whence the proof of $(2) \Rightarrow (3)$ goes through without assuming k perfect. In fact, inspection of the proof of Corollary 9.4 then shows that the equivalence of conditions $(1) - (3)$ in the above theorem holds over arbitrary k.

On the other hand, it is not hard to show using the arguments seen so far that if A is a Noetherian local ring containing a field k and A is formally smooth over k, then A is regular. The converse does not hold in general.