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 $x, y \in A \setminus P$; 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 **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 $m_0 = p_0m_0 + \ldots, p_nm_n$ 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 $b \in I$. $\square$

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. $\square$

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 $a_1, \ldots, a_r \in A$ are called *algebraically dependent* if there exists a nonzero polynomial $f \in k[x_1, \ldots, x_r]$ such that $f(a_1, \ldots, a_r) = 0$; 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 $\bar{a}_1, \ldots, \bar{a}_r$ 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 $a_0, a_1 \ldots, a_r$ are algebraically independent over k. Assume not, and let $f \in k[x_0, x_1, \ldots, x_r]$ be a nonzero polynomial with $f(a_0, a_1, \ldots, a_r) = 0$. As A is a domain,we may assume that f is irreductible, and in particular not divisible by x_0. But then $f(0, x_1, \ldots, x_r) \in k[x_1, \ldots, x_r]$ is a nonzero polynomial with $f(0, \bar{a}_1, \ldots, \bar{a}_r) = 0$, contradiction. $\square$

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 $x_1, \ldots, x_d$ such that A is a finitely generated module over the subring $k[x_1, \ldots, x_d] \subset A$.*

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

Proof. We only do the case where k is infinite; it is a bit easier. Let $x_1, \ldots, x_n$ 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 $f(x_1, \ldots, x_n) = 0$. Denote by m the degree of f and by f_m its homogeneous part of degree m. Since k is infinite, we find $a_1, \ldots, a_{n-1} \in k$ such that $f_m(a_1, \ldots, a_{n-1}, 1) \neq 0$. Setting $x_i' := x_i - a_i x_n$ for $i = 1, \ldots, n-1$ we compute

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

with some $g_i \in k[x_1', \ldots, x_{n-1}']$. Dividing by $f_m(a_1, \ldots, a_{n-1}, 1)$ we see that x_n satisfies a monic polynomial relation with coefficients in $k[x_1', \ldots, x_{n-1}']$, so that $A = k[x_1', \ldots, x_{n-1}'][x_n]$ is a finitely generated module over its subalgebra $k[x_1', \ldots, x_{n-1}']$. By induction we know that $k[x_1', \ldots, x_{n-1}']$ is a finitely generated module over the polynomial ring $k[x_1, \ldots, x_d]$, 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 $i = 1, \ldots, r$.*

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 $R := k[x_1, \ldots, x_d]$ 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 $(0) \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \ldots x_d)$ 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. □