Dimension theory and systems of parameters

Krull's principal ideal theorem

Our next objective is to study dimension theory in Noetherian rings. There was initially amazement that the results that follow hold in an arbitrary Noetherian ring.

Theorem (Krull's principal ideal theorem). *Let R be a Noetherian ring, $x \in R$, and P a minimal prime of xR. Then the height of $P \leq 1$.*

Before giving the proof, we want to state a consequence that appears much more general. The following result is also frequently referred to as *Krull's principal ideal theorem*, even though no principal ideals are present. But the heart of the proof is the case $n = 1$, which is the principal ideal theorem. This result is sometimes called *Krull's height theorem*. It follows by induction from the principal ideal theorem, although the induction is not quite straightforward, and the converse also needs a result on prime avoidance.

Theorem (Krull's principal ideal theorem, strong version, alias Krull's height theorem). *Let R be a Noetherian ring and P a minimal prime ideal of an ideal generated by n elements. Then the height of P is at most n. Conversely, if P has height n then it is a minimal prime of an ideal generated by n elements. That is, the height of a prime P is the same as the least number of generators of an ideal $I \subseteq P$ of which P is a minimal prime. In particular, the height of every prime ideal P is at most the number of generators of P, and is therefore finite. For every local ring R, the Krull dimension of R is finite.*

Proof of the first version of the principal ideal theorem. If we have a counterexample, we still have a counterexample after we localize at P. Therefore we may assume that (R, P) is local. Suppose that there is a chain of length two or more. Then there is a strict chain

$$P \supset Q \supset Q_0$$

in R. We may replace R, P, Q, Q_0 by R/Q_0, P/Q_0, Q/Q_0, (0). We may therefore assume that (R, P) is a local domain, that P is a minimal prime of xR, and that there is a prime Q with $0 \subset Q \subset P$, where the inclusions are strict. We shall get a contradiction.

Recall that $Q^{(n)} = Q^n R_Q \cap R$, the nth symbolic power of Q. It is Q-primary. Now, the ring R/xR has only one prime ideal, P/xR. Therefore it is a zero dimensional local ring, and has DCC. In consequence the chain of ideals $Q^{(n)}R/xR$ is eventually stable. Taking inverse images in R, we find that there exists N such that

$$Q^{(n)} + xR = Q^{(n+1)} + xR$$

for all $n \geq N$. For $n \geq N$ we have $Q^{(n)} \subseteq Q^{(n+1)} + xR$. Let $u \in Q^{(n)}$. Then $u = q + xr$ where $q \in Q^{(n+1)}$, and so $xr = u - q \in Q^{(n)}$. But $x \notin Q$, since P is the only minimal prime of xR in R. Since $Q^{(n)}$ is Q-primary, we have that $r \in Q^{(n)}$. This leads to the conclusion that $Q^{(n)} \subseteq Q^{(n+1)} + xQ^{(n)}$, and so

$$Q^{(n)} = Q^{(n+1)} + xQ^{(n)}.$$

But that means that with $M = Q^{(n)}/Q^{(n+1)}$, we have that $M = xM$. By Nakayama's lemma, $M = 0$, i.e., $Q^n/Q^{n+1} = 0$.

Thus, $Q^{(n)} = Q^{(N)}$ for all $n \geq N$. If $a \in Q - \{0\}$, it follows that $a^N \in Q^N \subseteq Q^{(N)}$ and is hence in the intersection of all the $Q^{(n)}$. But then, since $Q^{(n)} \subseteq Q^n R$ for all n, in the local domain R_Q, the intersection of the powers of the maximal ideal QR_Q is not 0, a contradiction. $\square$

Before proving the strong version of the principal ideal theorem, we want to record the following result on prime avoidance. In applications of part (b) of this result, W is frequently a K-algebra R, while the other subspaces are ideals of R. This shows that if there is an infinite field in the ring R, the assumptions about ideals being prime in part (a) are not needed.

Theorem (prime avoidance). *Let R be a ring. Let $V \subseteq W$ be vector spaces over an infinite field K.*

(a) *Let $\mathfrak{A}$ be an ideal of R (or a subset of R closed under addition and multiplication). Given finitely many ideals of R all but two of which are prime, if $\mathfrak{A}$ is not contained in any of these ideals, then it is not contained in their union.*

(b) *Given finitely many subspaces of W, if V is not contained in any of these subspaces, then V is not contained in their union.*

(c) *(Ed Davis) Let $x \in R$ and $I, P_1, \ldots, P_n$ be ideals of R such that the P_i are prime. If $I + Rx$ is not contained in any of the P_t, then for some $i \in I$, $i + x \notin \bigcup_t P_t$.*

Proof. (a) We may assume that no term may be omitted from the union, or work with a smaller family of ideals. Call the ideals I, J, $P_1, \ldots, P_n$ with the P_t prime. Choose elements $i \in I \cap \mathfrak{A}$, $j \in J \cap \mathfrak{A}$, and $a_t \in P_t \cap \mathfrak{A}$, $1 \leq t \leq n$, such that each belongs to only one of the ideals I, J, $P_1, \ldots, P_n$, i.e., to the one it is specified to be in. This must be possible, or not all of the ideals would be needed to cover $\mathfrak{A}$. Let $a = (i + j) + ijb$ where

$$b = \prod_{t \text{ such that } i+j \notin P_t} a_t,$$

where a product over the empty set is defined to be 1. Then $i + j$ is not in I nor in J, while ijb is in both, so that $a \notin I$ and $a \notin J$. Now choose t, $1 \leq t \leq n$. If $i + j \in P_t$, the factors of ijb are not in P_t, and so $ijb \notin P_t$, and therefore $a \notin P_t$. If $i + j \notin P_t$ there is a factor of b in P_t, and so $a \notin P_t$ again.

(b) If V is not contained in any one of the finitely many vector spaces V_t covering V, for every t choose a vector $v_t \in V - V_t$. Let V_0 be the span of the v_t. Then V_0 is a finite-dimensional counterexample. We replace V by V_0 and V_t by its intersection with V_0. Thus, we need only show that a finite-dimensional vector space K^n is not a finite union of proper subspaces V_t. (When the field is algebraically closed we have a contradiction because K^n is irreducible. Essentially the same idea works over any infinite field.) For each t we can choose a linear form $L_t \neq 0$ that vanishes on V_t. The product $f = L_1 \cdots L_t$ is a nonzero polynomial that vanishes identically on K^n. This is a contradiction, since K is infinite.

(c) We may assume that no P_t may be omitted from the union. For every t, choose an element p_t in P_t and not in any of the other P_k. Suppose, after renumbering, that $P_1, \dots, P_k$ all contain x while the other P_t do not (the values 0 and n for k are allowed). If $I \subseteq \bigcup_{j=1}^k P_j$ then it is easy to see that $I + Rx \subseteq \bigcup_{j=1}^k P_j$, and hence in one of the P_j by part (a), a contradiction. Choose $i' \in I$ not in any of $P_1, \dots, P_k$. Let q be the product of the p_t for $t > k$ (or 1, if $k = n$). Then $x + i'q$ is not in any P_t, and so we may take $i = i'q$. $\square$

Examples. Let $K = \mathbb{Z}/2\mathbb{Z}$ and let $V = K^2$. This vector space is the union of the three subspaces spanned by (1, 0), (0, 1) and (1, 1), respectively. This explains why we need an infinite field in part (b) of the preceding theorem. Now consider the K-algebra $K \oplus_K V$ where the product of any two elements of V is 0. (This ring is isomorphic with $K[x, y]/(x^2, xy, y^2)$, where x and y are indeterminates.) Then the maximal ideal is, likewise, the union of the three ideals spanned by its three nonzero elements. This shows that we cannot replace "all but two are prime" by "all but three are prime" in part (a) of the preceding theorem.

Proof of Krull's principal ideal theorem, strong version. We begin by proving by induction on n that the first statement holds. If $n = 0$ then P is a minimal prime of (0) and this does mean that P has height 0. Note that the zero ideal is the ideal generated by the empty set, and so constitutes a 0 generator ideal. The case where $n = 1$ has already been proved. Now suppose that $n \geq 2$ and that we know the result for integers $< n$. Suppose that P is a minimal prime of $(x_1, \dots, x_n)R$, and that we want to show that the height of P is at most n. Suppose not, and that there is a chain of primes

$$P = P_{n+1} \supset \cdots \supset P_0$$

with strict inclusions. If $x_1 \in P_1$ then P is evidently also a minimal prime of $P_1 + (x_2, \dots, x_n)R$, and this implies that P/P_1 is a minimal prime of the ideal generated by the images of $x_2, \dots, x_n$ in R/P_1. The chain

$$P_{n+1}/P_1 \supset \cdots \supset P_1/P_1$$

then contradicts the induction hypothesis. Therefore, it will suffice to show that the chain

$$P = P_{n+1} \supset \cdots \supset P_1 \supset 0$$

can be modified so that $x = x_1$ is in P_1. Suppose that $x \in P_k$ but not in P_{k-1} for $k \geq 2$. (To get started, note that $x \in P = P_{n+1}$.) It will suffice to show that there is a prime strictly between P_k and P_{k-2} that contains x, for then we may use this prime instead of P_{k-1}, and we have increased the number of primes in the chain that contain x. Thus, we eventually reach a chain such that $x \in P_1$.

To find such a prime, we may work in the local domain

$$D = R_{P_k}/P_{k-2}R_{P_k}.$$

The element x has nonzero image in the maximal ideal of this ring. A minimal prime P' of xR in this ring cannot be $P_k R_{P_k}$, for that ideal has height at least two, and P' has height at most one by the case of the principal ideal theorem already proved. Of course, $P' \neq 0$ since it contains $x \neq 0$. The inverse image of P' in R gives the required prime.

Thus, we can modify the chain

$$P = P_{n+1} \supset \cdots \supset P_1 \supset P_0$$

repeatedly until $x_1 \in P_1$. This completes the proof that the height of P is at most n.

We now prove the converse. Suppose that P is a prime ideal of R of height n. We want to show that we can choose $x_1, \ldots, x_n$ in P such that P is a minimal prime of $(x_1, \ldots, x_n)R$. If $n = 0$ we take the empty set of x_i. The fact that P has height 0 means precisely that it is a minimal prime of (0). It remains to consider the case where $n > 0$. We use induction on n. Let $q_1, \ldots, q_k$ be the minimal primes of R that are contained in P. Then P cannot be contained in the union of these, or else it will be contained in one of them, and hence be equal to one of them and of height 0. Choose $x_1 \in P$ not in any minimal prime contained in P. Then the height of P/x_1R in R/x_1R is at most $n-1$: the chains in R descending from P that had maximum length n must have ended with a minimal prime of R contained in P, and these are now longer available. By the induction hypothesis, P/x_1R is a minimal prime of an ideal generated by at most $n-1$ elements. Consider x_1 together with pre-images of these elements chosen in R. Then P is a minimal prime of the ideal they generate, and so P is a minimal prime of an ideal generated by at most n elements. The number cannot be smaller than n, or else by the first part, P could not have height n. $\square$

Systems of parameters for a local ring

If (R, m) is a local ring of Krull dimension n, a *system of parameters* for R is a sequence of elements $x_1, \ldots, x_n \in m$ such that, equivalently:

(1) m is a minimal prime of $(x_1, \ldots, x_n)R$.
(2) $\mathrm{Rad}\,(x_1, \ldots, x_n)R$ is m.
(3) m has a power in $(x_1, \ldots, x_n)R$.
(4) $(x_1, \ldots, x_n)R$ is m-primary.

The theorem we have just proved shows that every local ring of Krull dimension n has a system of parameters.

One cannot have fewer than n elements generating an ideal whose radical is m, for then $\dim(R)$ would be $< n$. We leave it to the reader to see that $x_1, \ldots, x_k \in m$ can be extended to a system of parameters for R if and only if

$$\dim\bigl(R/(x_1, \ldots, x_k)R\bigr) \leq n-k,$$

in which case

$$\dim\bigl(R/(x_1, \ldots, x_k)R\bigr) = n-k.$$

In particular, $x = x_1$ is part of a system of parameters iff x is not in any minimal prime P of R such that $\dim(R/P) = n$. In this situation, elements $y_1, \ldots, y_{n-k}$ extend $x_1, \ldots, x_k$ to a system of parameters for R if and only if their images in $R/(x_1, \ldots, x_k)R$ are a system of parameters for $R/(x_1, \ldots, x_k)R$.

The following statement is now immediate:

Corollary. *Let (R, m) be local and let $x_1, \ldots, x_k$ be k elements of m. Then the dimension of $R/(x_1, \ldots, x_k)R$ is at least $\dim(R) - k$.*

Proof. Suppose the quotient has dimension h. If $y_1, \ldots, y_h \in m$ are such that their images in $R/(x_1, \ldots, x_k)R$ are a system of parameters in the quotient, then m is a minimal prime of $(x_1, \ldots, x_k, y_1, \ldots, y_h)R$, which shows that $h + k \geq n$. $\square$

Polynomial and power series extensions

We next want to address the issue of how dimension behaves for Noetherian rings when one adjoins either polynomial or formal power series indeterminates.

We first note the following fact:

Lemma. *Let x be an indeterminate over R. Then x is in every maximal ideal of $R[[x]]$.*

Proof. If x is not in the maximal ideal $\mathcal{M}$ it has an inverse mod $\mathcal{M}$, so that we have $xf \equiv 1$ mod $\mathcal{M}$, i.e., $1 - xf \in \mathcal{M}$. Thus, it will suffice to show that $1 - xf$ is a unit. The idea of the proof is to show that

$$u = 1 + xf + x^2 f^2 + x^3 f^3 + \cdots$$

is an inverse: the infinite sum makes sense because only finitely many terms involve any given power of x. Note that

$$u = (1 + xf + \cdots + x^n f^n) + x^{n+1} w_n$$

with

$$w_n = f^{n+1} + x f^{n+2} + x^2 f^{n+3} + \cdots,$$

which again makes sense since any given power of x occurs in only finitely many terms. Thus:

$$u(1 - xf) - 1 = (1 + xf + \cdots + x^n f^n)(1 - xf) + x^{n+1} w_n (1 - xf) - 1.$$

The first of the summands on the right is $1 - x^{n+1} f^{n+1}$, and so this becomes

$$1 - x^{n+1} f^{n+1} + x^{n+1} w_n (1 - xf) - 1 = x^{n+1}\big(-f^{n+1} + w_n(1 - xf)\big) \in x^{n+1} R[[x]],$$

and since the intersection of the ideals $x^t R[[x]]$ is clearly 0, we have that $u(1 - xf) - 1 = 0$, as required. $\square$

Theorem. *Let R be a Noetherian ring and let $x_1, \dots, x_n$ be indeterminates. Then $S = R[x_1, \dots, x_k]$ and $T = R[[x_1, \dots, x_k]]$ both have dimension $\dim(R) + k$.*

Proof. By a straightforward induction we may assume that $k = 1$. Write $x_1 = x$. If P is a prime ideal of R then PS and PT are both prime, with quotients $(R/P)[x]$ and $(R/P)[[x]]$, and $PS + xS$, $PS + xT$ are prime as well. If $P_0 \subset \cdots \subset P_n$ is a chain of primes in R, then their expansions P_i^{e} together with $P_n^{\mathrm{e}} + (x)$ give a chain of primes of length one greater in S or T. This shows that the dimensions of S and T are at least $\dim(R) + 1$.

If R has infinite dimension, so do S and T. Therefore let $\dim(R) = n$ be finite. We want to show that S and T have dimension at most $n + 1$. We first consider the case of $S = R[x]$. Let Q be a prime ideal of this ring and let P be its contraction to R. It suffices to show that the height of Q is at most one more than the height of P. To this end we can replace R by R_P and S by $R_P[x]$: $QR_P[x]$ will be a prime ideal of this ring, and the height of Q is the same as the height of its expansion. We have therefore reduced to the local case. Let $x_1, \dots, x_n$ be a system of parameters for R (which is now local). It suffices to show that we can extend it to a system of parameters for $R[x]_Q$ using at most one more element. It therefore suffices to show that $R[x]_Q/(x_1, \dots, x_n)$ has dimension at most 1. This ring is a localization of $(R/(x_1, \dots, x_n))[x]$, and so it suffices to see that this ring has dimension at most 1. To this end, we may kill the ideal of nilpotents, which is the expansion of P, producing $K[x]$. Since this ring has dimension 1, we are done.

In the case of T we first note that, by the Lemma, every maximal ideal of T contains x. Choose Q maximal in T. Since $x \in Q$, Q corresponds to a maximal ideal m of R, and has the form $m^{\mathrm{e}} + (x)$. If m is minimal over $(x_1, \dots, x_n)$, then Q is minimal over $(x_1, \dots, x_n, x)$. This proves that the height of $Q \leq n + 1$, as required. $\square$

If R is not Noetherian but has finite Krull dimension n, it is true that $R[x]$ has finite Krull dimension, and it lies between $n + 1$ and $2n + 1$. The upper bound is proved by showing that in a chain of primes in $R[x]$, at most two (necessarily consecutive) primes lie over the same prime P of R. This result is sharp.

Finitely generated algebras over a field K

Noether normalization together with the going up and going down theorems can be used to prove strong results on the behavior of dimension for rings finitely generated over a field.

Primes $P \subset Q$ are called *consecutive* if the inclusion is strict and there is no prime strictly between P and Q. A chain of primes $P = P_0 \subset P_1 \subset \cdots \subset P_n$, where the inclusions are strict, is said to have *length* n. It is called *saturated* if for every i, $0\ leqi \leq n-1$, the primes P_i and P_{i+1} are consecutive.

Theorem. *Let R be a finitely generated algebra over a field K.*

(a) *The Krull dimension of R is the same as the maximum number of elements of R that are algebraically independent over K. If R is a domain, $\dim(R)$ is the transcendence degree of the fraction field of R over K.*

(b) *If R is a domain of Krull dimension n, all maximal ideals of R have height n, and every saturated chain from a maximal ideal to (0) has length n.*

(c) *If $P \subseteq Q$ are prime ideals of R, then any two saturated chains of primes joining P to Q have the same length. If R is a domain, for every prime ideal P, $he(P)+\dim(R/P) = \dim(R)$, and the length of any saturated chain from P to Q is* $\text{height}\,(Q) - \text{height}\,(P) = \dim(R/P) - \dim(R/Q)$.

Proof. (a) By the Noether normalization theorem, R is a module-finite extension of a polynomial ring $K[x_1, \ldots, x_n]$ over K. But then $\dim(R) = n$. It is now clear that if R is a domain, its Krull dimension is the transcendence degree of its fraction field over K.

If R has dimension n and is not necessarily a domain, we still need to see that there cannot be $n+1$ algebraically independent elements $y_1, \ldots, y_{n+1}$ in R. Let $A = K[y_1, \ldots, y_{n+1}]$. Then $W = A - \{0\}$ is a multiplicative system in R, and so there is a prime ideal P of R disjoint from $A - \{0\}$. Then A injects into the domain R/P, and we obtain $\dim(R) \geq \dim(R/P) \geq n+1$, a contradiction.

(b) We use induction on the Krull dimension n of R. If the dimension is 0, R is a field and there is nothing the statements are obvious. Assume that R has positive dimension.

As before, the domain R is module-finite over $A = K[x_1, \ldots, x_n]$, a polynomial ring. Let $(0) \subset Q_1 \subset \cdots \subset Q_h$ be a strictly ascending saturated chain in the domain R with P_h maximal. Let $A = K[x_1, \ldots, x_n] \subseteq R$ be such that R is module-finite over A. Let P_i be the contraction of Q_i to A. We first observe that P_1 is a height one prime of A. If not, there is a prime strictly between P_1 and (0). Since A is normal and R is adomain, the going down theorem applies, and there is a prime $Q \subset Q_1$ lying over P. This contradicts the fact that the (0) and Q_1 are consecutive primes in R. Thus, P_1 is a minimal nonzero prime of A, and since A is a unique factorization domain, it is generated by a nonzero, noninvertible polynomial f. As in the proof of the Noether normalization theorem, after a change of variables f can be made monic in x_n, up to multiplicaiton by a scalar. It follows that $A/(f)$ is a module-finite extension of $K[x_1, \ldots, x_{n-1}$. Hence, $A/(f) = A/P_1$ has dimension $n-1$. But R/Q_1 is a modlule-finite extension of A/P_1. Hence, R/Q_1 has dimension $n-1$. The fact that $h-1 = n-1$ now follows from the induction hypothesis applied to $0 = Q_1/Q_1 \subset Q_2/Q_1 \subset \cdots \subset Q_h/Q_1$, which is a saturated chain to the maximal ideal Q_h/Q_1 in R/Q_1.

(c) The saturated chains from P to Q correspond to the saturated chains from $P/P = (0)$ to Q/P in the domain R/P. Therefore, the first result stated follows from the domain case, and we assume from now on that R is a domain. For the second statement, consider a saturated chain of length k from (0) to P: one such chain has length iheight$\,(P)$, but we may consider any such chain. There is also a saturated chain from $(0) = P/P$ to m/P (where m is maximal in R) whose length is $\dim(R/P)$. This corresponds to a saturated chain of length $\dim(R/P)$ from P to m. By putting these two chains together (omitting the duplicated occurrence of P), we obtain a saturated chain from (0) to m, whose length is $k+\dim(R/P)$. By part (b), the length of this chain is also $\dim(R)$, as required. This shows that any saturated chain from 0 to P has length equal to $\dim(R) - \dim(R/P)$, and since the chain may be chosen so that $k = \text{height}\,(P)$, we have that $k = \dim(R) - \dim(R/P) = \text{height}\,(P)$ for all chains from 0 to P. Similarly, any saturated chain from P to Q can be combined with a saturated chain from (0) to P to produce a saturated chain from (0) to Q, from which it follows that $\text{height}\,(P) + \text{height}\,(Q/P) = \text{height}\,(Q)$. $\square$

Corollary. *Let $R \subseteq S$ be a module-finite extension of domains finitely generated over a field K. Then for every prime Q of height h in S, the height of $Q \cap R$ is h.*

Proof. The prime Q can be included in a saturated chain from (0) to a maximal ideal of S, which will have length equal to $\dim(S)$. When the primes in this chain are contracted to R, the contractions are distinct, by the lying over theorem. Hence, the chain has length $\dim(R) = \dim(S)$, and must be a saturated chain from (0) to a maximal ideal in R. It now follows that the height of any prime in either chain is equal to the number of predecessor it has in the chain, from which the result follows. $\square$