Krull's Principal Ideal Theorem

June 17, 2020

1 Krull's Principal Ideal Theorem

We now wish to study dimension theory in Noetherian rings.

Definition 1.1. Let A be a ring and let $\mathfrak{q}$ be a prime ideal in A. The n**th symbolic power of** $\mathfrak{q}$, denoted $\mathfrak{q}^{(n)}$, is defined to be the ideal

$$\mathfrak{q}^{(n)} = \mathfrak{q}^n A_{\mathfrak{q}} \cap A = \{a \in A \mid as \in \mathfrak{q}^n \text{ for some } s \in A \backslash \mathfrak{q}\}.$$

Proposition 1.1. *Let A be a ring and let $\mathfrak{q}$ be a prime ideal in A. Then $\mathfrak{q}^{(n)}$ is the smallest $\mathfrak{q}$-primary ideal which contains $\mathfrak{q}^n$.*

Proof. It is clear that $\mathfrak{q}^n \subset \mathfrak{q}^{(n)}$. Let us show that $\mathfrak{q}^{(n)}$ is a $\mathfrak{q}$-primary ideal. Suppose $ab \in \mathfrak{q}^{(n)}$ and $a \notin \mathfrak{q}^{(n)}$. Choose $s \in A \backslash \mathfrak{q}$ such that $abs \in \mathfrak{q}^n$. Since $a \in \mathfrak{q}^{(n)}$, we must not have $bs \in A \backslash \mathfrak{q}$. In particular, this implies $b \in \mathfrak{q}$ since $A \backslash \mathfrak{q}$ is multiplicatively closed. But then $b^n \in \mathfrak{q}^n \subset \mathfrak{q}^{(n)}$. Thus $\mathfrak{q}^{(n)}$ is $\mathfrak{q}$-primary.

Now we will show that it is the smallest $\mathfrak{q}$-primary ideal which contains $\mathfrak{q}^n$. Let Q be any $\mathfrak{q}$-primary ideal which contains $\mathfrak{q}^n$ and let $a \in \mathfrak{q}^{(n)}$. Choose $s \in A \backslash \mathfrak{q}$ such that $as \in \mathfrak{q}^n \subset Q$. Since $A \backslash \mathfrak{q}$ is multiplicatively closed and since $Q \cap A \backslash \mathfrak{q} = \emptyset$, we must have $s^m \notin Q$ for all $m \in \mathbb{N}$. This implies $a \in Q$ since Q is primary. Thus $\mathfrak{q}^{(n)} \subset Q$. □

Theorem 1.1. *Let A be a Noetherian ring, $x \in A$, and $\mathfrak{p}$ a minimal prime of $\langle x \rangle$. Then height$(\mathfrak{p}) \leq 1$.*

Sketch of Proof: Proof is by contradiction. We may assume $(A, \mathfrak{p})$ is a local domain since passing to this case preserves chains. Recall that $\mathfrak{q}^{(n)}$ is the nth symbolic power of $\mathfrak{q}$. Use the fact that A/x is Artinian to deduce that $\mathfrak{q}^{(n)} + xA = \mathfrak{q}^{(n+1)} + xA$ for all $n \geq N$, for some $N \in \mathbb{N}$. Use the fact that $\mathfrak{q}^{(n)}$ is $\mathfrak{q}$-primary to conclude that $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)} + x\mathfrak{q}^{(n)}$. This implies that $\mathfrak{q}^{(n)}/\mathfrak{q}^{(n+1)} = 0$, by Nakayama's lemma. Finally, if $b \in \mathfrak{q} \backslash \{0\}$, it follows that $b^N \in \mathfrak{q}^N \subseteq \mathfrak{q}^{(N)}$ and is hence in the intersection of all the $\mathfrak{q}^{(n)}$. But then, since $\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^n A_{\mathfrak{q}}$ for all n, in the local domain $A_{\mathfrak{q}}$, the intersection of the powers of the maximal ideal $\mathfrak{q}A_{\mathfrak{q}}$ is not 0, a contradiction.

Remark. The reason we used $\mathfrak{q}^{(n)}$ and not $\mathfrak{q}^n$ is because $\mathfrak{q}^n$ is not necessarily a $\mathfrak{q}$-primary ideal. Here is counterexample: Consider the ideal $\mathfrak{p} = \langle x, y \rangle$ in $K[x, y, z]/\langle xy - z^2 \rangle$. It's easy to check that $\mathfrak{p}$ is a prime ideal in this ring, but $\mathfrak{p}^2$ is not $\mathfrak{p}$-primary. Indeed, $\mathfrak{p}^2$ contains $xy = z^2$, but it does not contain x nor y^n for any n.

Proof. Suppose there is a chain of primes of length two or more in A, say

$$\mathfrak{p} \supset \mathfrak{p}' \supset \mathfrak{p}''.$$

If we localize A at $\mathfrak{p}$, then we still have a chain of length two or more in $A_{\mathfrak{p}}$, so we may as well assume that $(A, \mathfrak{p})$ is local. Also, by passing to the quotient $A/\mathfrak{p}''$, we still get a chain of length two in $A/\mathfrak{p}''$. Thus, we may assume that $(A, \mathfrak{p})$ is a local domain, that $\mathfrak{p}$ is a minimal prime of $\langle x \rangle$, and that there is a prime $\mathfrak{q}$ with

$$\mathfrak{p} \supset \mathfrak{q} \supset \langle 0 \rangle.$$

We shall get a contradiction.

The ring A/x has only one prime ideal, namely $\mathfrak{p}/x$, since $\mathfrak{p}$ is minimal over $\langle x \rangle$ and a maximal ideal in A. Therefore it is a zero dimensional local ring, and has DCC. In consequence, the chain of ideals $\langle \mathfrak{q}^{(n)}, x \rangle / x$ is eventually stable. Taking inverse images in A, we find that there exists N such that

$$\mathfrak{q}^{(n)} + \langle x \rangle = \mathfrak{q}^{(n+1)} + \langle x \rangle$$

for all $n \geq N$. In particular, for $n \geq N$, we have $\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(n+1)} + xA$. Let $u \in \mathfrak{q}^{(n)}$. Then $u = q + xa$, where $q \in \mathfrak{q}^{(n+1)}$, and so $xa = u - q \in \mathfrak{q}^{(n)}$. But $x^k \notin \mathfrak{q}$ for any $k \in \mathbb{N}$, since $\mathfrak{p}$ is the only minimal prime of $\langle x \rangle$ in A. Since $\mathfrak{q}^{(n)}$ is $\mathfrak{q}$-primary, we have $a \in \mathfrak{q}^{(n)}$. This leads to the conclusion that $\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(n+1)} + x\mathfrak{q}^{(n)}$, and since obviously $\mathfrak{q}^{(n)} \supseteq \mathfrak{q}^{(n+1)} + x\mathfrak{q}^{(n)}$, we have

$$\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)} + x\mathfrak{q}^{(n)}.$$

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

Thus, $\mathfrak{q}^{(n)} = \mathfrak{q}^{(N)}$ for all $n \geq N$. If $b \in \mathfrak{q} \backslash \{0\}$, it follows that $b^N \in \mathfrak{q}^N \subseteq \mathfrak{q}^{(N)}$ and is hence in the intersection of all the $\mathfrak{q}^{(n)}$. But then, since $\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^n A_{\mathfrak{q}}$ for all n, in the local domain $A_{\mathfrak{q}}$, the intersection of the powers of the maximal ideal $\mathfrak{q}A_{\mathfrak{q}}$ is not 0, a contradiction. □

Theorem 1.2. *(Prime Avoidance) Let A be a ring. Let $V \subseteq W$ be vector spaces over an infinite field K.*

1. *Let $\mathfrak{U}$ be an ideal of A. Given finitely many ideals of A, all but two of which are prime, if $\mathfrak{U}$ is not contained in any of these ideals, then it is not contained in their union.*

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

3. *(Ed Davis) Let $x \in A$ and $I, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be ideals of A, such that $\mathfrak{p}_i$ are prime. If $\langle I, x \rangle$ is not contained in any of the $\mathfrak{p}_i$, then for some $b \in I$, $b + x \notin \bigcup_i \mathfrak{p}_i$.*

Proof.

1. We may assume that no term may be omitted from the union, or work with a smaller family of ideals. Call the ideals $I, J, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$ with $\mathfrak{p}_i$ prime. Choose elements $x \in I \cap \mathfrak{U}$, $y \in J \cap \mathfrak{U}$, and $z_i \in \mathfrak{p}_i \cap \mathfrak{U}$, such that each belongs to only one of the ideals $I, J, \mathfrak{p}_1, \ldots \mathfrak{p}_n$, i.e., to the one it is specified in. This must be possible, or not all of the ideals would be needed to cover $\mathfrak{U}$. For instance, if every element $x \in I \cap \mathfrak{U}$ belonged to $J \cap \mathfrak{U}$, then $I \cap \mathfrak{U} \subset J \cap \mathfrak{U}$, and thus

$$(I \cap \mathfrak{U}) \cup (J \cap \mathfrak{U}) \cup (\mathfrak{p}_1 \cap \mathfrak{U}) \cup \cdots \cup (\mathfrak{p}_n \cap \mathfrak{U}) = (J \cap \mathfrak{U}) \cup (\mathfrak{p}_1 \cap \mathfrak{U}) \cup \cdots \cup (\mathfrak{p}_n \cap \mathfrak{U}),$$

   and we would simply proceed with the ideals $J, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Let $a = (x + y) + xyb$, where

$$b = \prod_{i \text{ such that } x+y \notin \mathfrak{p}_i} z_i,$$

   where a product over the empty set is defined to be 1. Then $x + y$ is not in I nor in J, while xyb is in both, so that $a \notin I$ and $a \notin J$. Now choose i, $1 \leq i \leq n$. If $x + y \in \mathfrak{p}_i$, the factors of xyb are not in $\mathfrak{p}_i$, and so $xyb \notin \mathfrak{p}_i$, and therefore $a \notin \mathfrak{p}_i$. If $x + y \notin \mathfrak{p}_i$ there is a factor of b in $\mathfrak{p}_i$, and so $a \notin \mathfrak{p}_i$ again.

2. If V is not contained in any one of the finitely many vector spaces V_t covering V, for every t choose a vector $v_t \in V \backslash V_t$. 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.

3. We may assume that no $\mathfrak{p}_t$ may be omitted from the union. For every t, choose an element p_t in $\mathfrak{p}_t$ and not in any of the other $\mathfrak{p}_k$. Suppose, after renumbering, that $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ all contain x while the other $\mathfrak{p}_t$ do not (the values 0 and n for k are allowed). If $I \subseteq \bigcup_{j=1}^k \mathfrak{p}_j$ then it is easy to see that $\langle I, x \rangle \subseteq \bigcup_{j=1}^k \mathfrak{p}_j$, and hence in one of the $\mathfrak{p}_j$ by part (1), a contradiction. Choose $a \in I$ not in any of the $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$. Let q be the product of the p_t for $t > k$ (or 1 if $k = n$). Then $x + aq$ is not in any $\mathfrak{p}_t$, and so we may take $b = aq$.

□

Example 1.1. Consider the ring $\mathbb{F}_2[x, y]/\langle x^2, xy, y^2 \rangle$. Then $\langle x, y \rangle = \langle x \rangle \cup \langle y \rangle \cup \langle x + y \rangle$, but $\langle x, y \rangle \not\subset \langle x \rangle$, $\langle x, y \rangle \not\subset \langle y \rangle$, and $\langle x, y \rangle \not\subset \langle x + y \rangle$. This shows that we cannot replace "all but two are prime" by "all but three are prime" in part (1) of Theorem (1.2). Also note that $\mathbb{F}_2[x, y]/\langle x^2, xy, y^2 \rangle$ is a finite-dimensional $\mathbb{F}_2$-vector space which is the union of the proper subspaces $\langle 1 \rangle$ and $\langle x, y \rangle$.

Theorem 1.3. *(Krull's principal ideal theorem, strong version, alias Krulls height theorem) Let A be a Noetherian ring and $\mathfrak{p}$ a minimal prime ideal of an ideal generated by n elements. Then the height of $\mathfrak{p}$ is at most n. Conversely, if $\mathfrak{p}$ has height n, then it is a minimal prime of an ideal generated by n elements. That is, the height of a prime $\mathfrak{p}$ is the same as the least number of generators of an ideal $I \subset \mathfrak{p}$ of which $\mathfrak{p}$ is a minimal prime. In particular, the height of every prime ideal $\mathfrak{p}$ is at most the number of generators of $\mathfrak{p}$, and is therefore finite. For every local ring A, the Krull dimension of A is finite.*

Proof. We begin by proving by induction on n that the first statement holds. If $n = 0$, then $\mathfrak{p}$ is a minimal prime of $\langle 0 \rangle$ and this does mean that $\mathfrak{p}$ 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 $n = 1$ has already been proved. Now suppose that $n \geq 2$ and that we know the result for integers $< n$. Suppose that $\mathfrak{p}$ is a minimal prime of $\langle x_1, \ldots, x_n \rangle$ and that we want to show that the height of $\mathfrak{p}$ is at most n. Suppose not, and that there is a chain of primes

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_{n+1} = \mathfrak{p}$$

with strict inclusions. If $x_1 \in \mathfrak{p}_1$, then $\mathfrak{p}$ is evidently also a minimal prime of $\mathfrak{p}_1 + \langle x_2, \ldots, x_n \rangle$ and this implies that $\mathfrak{p}/\mathfrak{p}_1$ is a minimal prime of the ideal generated by the images of $x_2, \ldots, x_n$ in $A/\mathfrak{p}_1$. Then the chain

$$\mathfrak{p}_1/\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_{n+1}/\mathfrak{p}_1$$

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

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_{n+1} = \mathfrak{p}$$

can be modified so that $x = x_1$ is in $\mathfrak{p}_1$. Suppose that $x \in \mathfrak{p}_k$ but not in $\mathfrak{p}_{k-1}$ for $k \geq 2$. (To get started, note that $x \in \mathfrak{p} = \mathfrak{p}_{n+1}$.) It will suffice to show that there is a prime strictly between $\mathfrak{p}_k$ and $\mathfrak{p}_{k-2}$ that contains x, for then we use this prime instead of $\mathfrak{p}_{k-1}$, and we have increased the number of primes in the chain that contains x. Thus, we eventually reach a chain such that $x \in \mathfrak{p}_1$.

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

$$D = A_{\mathfrak{p}_k}/\mathfrak{p}_{k-2}A_{\mathfrak{p}_k}.$$

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

Thus we can modify the chain

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_{n+1} = \mathfrak{p}$$

repeatedly until $x_1 \in \mathfrak{p}_1$. This completes the proof that the height of $\mathfrak{p}$ is at most n.

We now prove the converse. Suppose that $\mathfrak{p}$ is a prime ideal of A of height n. We want to show that we can choose $x_1, \ldots, x_n$ in $\mathfrak{p}$ such that $\mathfrak{p}$ is a minimal prime of $\langle x_1, \ldots, x_n \rangle$. If $n = 0$ we take the empty set of x_i. The fact that $\mathfrak{p}$ has height 0 means precisely that it is a minimal prime of $\langle 0 \rangle$. It remains to consider the case where $n > 0$. We use induction on n. Let $\mathfrak{q}_1, \ldots \mathfrak{q}_k$ be the minimal primes of A that are contained in $\mathfrak{p}$. Then $\mathfrak{p}$ 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 $x_1 \in \mathfrak{p}$ not in any minimal prime contained in $\mathfrak{p}$. Then the height of $\mathfrak{p}/x_1$ in A/x_1 is at most $n - 1$: the chains in A descending from $\mathfrak{p}$ that had maximum length n must have ended with a minimal prime of A contained in $\mathfrak{p}$, and these are no longer available. By the induction hypothesis, $\mathfrak{p}/x_1$ 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 A. Then $\mathfrak{p}$ is a minimal prime of the ideal they generate, and so $\mathfrak{p}$ 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, $\mathfrak{p}$ could not have height n. □

2 Systems of paramaters for a local ring

Definition 2.1. Let $(A, \mathfrak{m})$ be a local Noetherian ring of Krull dimension n. A **system of parameters** for A is a sequence of elements $x_1, \ldots, x_n \in \mathfrak{m}$ such that, equivalently:

1. $\mathfrak{m}$ is a minimal prime of $\langle x_1, \ldots, x_n \rangle$.
2. $\sqrt{\langle x_1, \ldots, x_n \rangle}$ is $\mathfrak{m}$.
3. $\mathfrak{m}$ has a power in $\langle x_1, \ldots, x_n \rangle$.
4. $\langle x_1, \ldots, x_n \rangle$ is $\mathfrak{m}$-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 $\mathfrak{m}$, for then $\dim A$ would be $< n$. Note that $x_1, \ldots, x_k \in \mathfrak{m}$ can be extended to a system of paramaters for A if and only if

$$\dim(A/\langle x_1, \ldots, x_k\rangle) \leq n - k$$

in which case

$$\dim(A/\langle x_1, \ldots, x_k\rangle) = n - k.$$

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

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

3 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 3.1. *Let x be an indeterminate over A. Then x is in every maximal ideal of $A[[x]]$.*

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

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

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

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

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

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

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