NAKAYAMA LEMMAS

First, recall that the intersection of all *prime* ideals in a commutative ring is the nil-radical, the ideal of elements for which some power is 0. There is also a description of sorts of the intersection of all *maximal* ideals, which is called the *Jacobson radical*.

PROPOSITION. If A is a commutative ring, with invertible elements A^*, then

$$\bigcap_{Q\ max} Q = \{x \in A \mid 1 + rx \in A^*,\ all\ r \in A\}.$$

PROOF. If x is in all maximal ideals then $1 + rx$ is in no maximal ideal, hence is invertible. Conversely, if x is not in some maximal ideal Q, then $1 = y - rx$ for some $y \in Q,\ r \in A$. Then $1 + rx = y \in Q$ is not invertible.

We also recall that for any A-module M, the map $M \to \prod_{P\ prime} M_{(P)}$ is injective. One can even take the product of localizations at the maximal ideals. Because an element x in the kernel is annihilated by some $s_P \notin P$, for each prime ideal P. These $\{s_P\}$ generate the unit ideal of A, hence $1x = 0$. Another version of the statement here is that if all localizations $M_{(P)} = (0)$, then $M = (0)$.

Now we come to several variants of Nakayama's Lemma.

VERSION 1. If $I \subset A$ is an ideal contained in all maximal ideals of A and if M is a finitely generated A-module with $M = IM$, then $M = (0)$.

VERSION 2. If A is a local ring with maximal ideal $m \subset A$ and if $N \subset M$ are A-modules with M finitely generated and with $N + mM = M$, then $N = M$.

[Note: Since only finitely many elements of N are seen in formulas for the generators of M, one might as well assume in Version 2 that N is finitely generated.]

VERSION 3. If A is a local ring with maximal ideal $m \subset A$ and if $\{x_1, \dots, x_n\}$ are finitely many elements of a finitely generated A-module M such that the residue classes $\{\bar{x_1}, \dots, \bar{x_n}\}$ span the vector space M/mM over A/m, then $\{x_1, \dots, x_n\}$ generate M as A-module.

PROOFS. First, (2) $\Leftrightarrow$ (3) just by taking N to be the submodule generated by $\{x_1, \dots, x_n\}$, and using the note.

Next, (1) $\Rightarrow$ (2) because $\frac{N+mM}{N} = m(\frac{M}{N})$. Then apply (1) to the module M/N.

To show (2) $\Rightarrow$ (1), it suffices to show $M_{(Q)} = (0)$, for all maximal ideals $Q \subset A$. But $I \subset Q$, so if $M = IM$ then localizing gives $M_{(Q)} = QM_{(Q)} = (0) + QM_{(Q)}$. Now apply (2) with $N = (0)$.

Now we have three equivalent statements. We will see that Version (1) follows from a module form of the Cayley-Hamilton Theorem.

PROPOSITION (Cayley-Hamilton) Suppose $I \subset A$ is an ideal and $\phi : M \to IM$ is an A-module homomorphism, where M is an A-module generated by $\{x_1, \ldots, x_n\}$. Then ϕ satisfies an identity

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n \equiv 0 \in End(M),$$

with $a_j \in I^j$.

PROOF. Write $\phi x_i = \sum_j a_{ij}x_j$, and form the $n \times n$ matrix $(\phi Id_n - (a_{ij}))$ over the ring $A[\phi]$. This matrix acts on M^n, with $(\phi Id_n - (a_{ij}))(x_1, \ldots, x_n)^t = (0)^t$. There is the adjugate matrix $(\phi Id_n - (a_{ij}))^*$ with

$$(\phi Id_n - (a_{ij}))^*(\phi Id_n - (a_{ij})) = det(\phi Id_n - (a_{ij}))Id_n.$$

It follows that $det(\phi Id_n - (a_{ij}))$ annihilates all x_j, hence is the 0 endomorphism of M. Expanding the determinant shows the coefficient of ϕ^{n-j} belongs to I^j.

Of course, we recognize $P(T) = det(TId_n - (a_{ij}))$ exactly as the "charactersitic polynomial" of the endomorphism ϕ, with respect to the generating set $\{x_1, \ldots, x_n\}$ of M.

Version (1) of Nakayama's Lemma follows by taking $\phi = Id = \cdot 1 : M \to M = IM$. Cayley-Hamilton gives $(1 + a)M = (0)$, for some $a \in I$. But $1 + a \in A^*$ is invertible if I is contained in every maximal ideal of A, so $M = (0)$.

An alternate proof of Version (1) of Nakayama's Lemma is by induction on the least number of generators of M. With one generator, x, one has $(1 - a)x = 0$, with $1 - a \in A^*$, so $x = 0$. But then with n generators $\{x_1, \ldots, x_n\}$, with n least, one has $(1 - a_1)x_1 = \sum_{j=2}^{n} a_jx_j$, and again $(1 - a_1) \in A^*$, so generator x_1 is redundant. Thus $M = (0)$ is the only possibility.

We will give some applications of Nakayama's Lemma.

APPLICATION 1. If A is a Noetherian local ring with maximal ideal $m \subset A$ and if $m^{n+1} = m^n$ then $m^n = (0)$. If A is a Noetherian integral domain and $P \subset A$ is a prime ideal then the powers $\{P^n\}, n \geq 1$, are distinct.

PROOF. The first statement is immediate from Nakayama (1) with $M = m^n$. For the second statement, since A is a domain, all localization morphisms are injective. If $P^{n+1} = P^n$, localize at P and conclude from the first statement that $P^n = (0)$. But this is absurd, since A is a domain.

We can prove a stronger result by bringing in primary decomposition.

APPLICATION 2. If A is a Noetherian local ring with maximal ideal $m \subset A$, then

$$\bigcap_{n \geq 1} m^n = (0).$$

If A is a Noetherian integral domain and $P \subset A$ is a prime ideal, then $\bigcap P^n = (0)$.

PROOF. Write $J = \bigcap m^n$ and consider a primary decomposition $mJ = \bigcap Q_i$. By Nakayama (1), it suffices to prove $J \subset mJ$, that is, $J \subset Q_i$, all i. Suppose $a \in J - Q_i$. If $\sqrt{Q_i} \neq m$, choose $b \in m - \sqrt{Q_i}$. Then $ab \in mJ \subset Q_i$, but $a \notin Q_i$ and $b \notin \sqrt{Q_i}$, which contradicts Q_i primary. But if $\sqrt{Q_i} = m$, then $J \subset m^n \subset Q_i$, for some n. In all cases, we've proved $J \subset Q_i$.

The second statement concerning a prime ideal in a Noetherian domain is proved by localizing, as in Application 1.

APPLICATION 3. A finitely generated projective module E over a local ring A is free.

PROOF. We can write $E \oplus F = A^n$, for some F and n. If $m \subset A$ is the maximal ideal, then

$$\frac{E}{mE} \oplus \frac{F}{mF} = \left(\frac{A}{m}\right)^n,$$

as vector spaces over A/m. Choose bases $\{\bar{x_1}, \ldots, \bar{x_r}\}$ and $\{\bar{y_1}, \ldots, \bar{y_s}\}$ for E/mE and F/mF. Of course, $r + s = n$. Nakayama (3) says $\{x_1, \ldots, x_r\}$ and $\{y_1, \ldots, y_s\}$ generate E and F over A. We claim these generating sets are A-linearly independent, proving E and F are free A-modules.

Namely, one can express the x_i and y_j as column vectors in A^n, forming a $n \times n$ matrix. Reducing mod mA^n, these column vectors form a basis, hence the determinant is a unit in A. But this means the matrix with x's and y's is invertible over A, hence has (0) null space. This means the x's and y's are indeed linearly independent.