Math 145. Nakayama's Lemma

Let R be a local ring, with maximal ideal $\mathfrak{m}$, and let M be a finitely generated R-module. The quotient module $M_0 = M/\mathfrak{m}M$ is naturally a module over the residue field $k = R/\mathfrak{m}$, and so M_0 is a finite-dimensional k-vector space since any finite spanning set for M over R induces a spanning set for M_0 over k.

The aim of this handout is to prove a "residual criterion" for a finite set of elements of M to be a spanning set over R by working in the k-vector space M_0.

Theorem 0.1. *A finite subset $\{m_1, \dots, m_r\}$ of M is a spanning set over R if their residue classes $\overline{m}_i = m_i \bmod \mathfrak{m}M$ span M_0 over k. In particular, if $M_0 = 0$ then $M = 0$.*

The final part follows from the rest by taking $\{m_i\}$ to be the singleton $\{0\}$. In fact, we'll see that this special case contains all of the real content of the theorem.

Proof. Let $M' = M/(\sum Rm_i)$. This is finitely generated over R since M is, and $M'/\mathfrak{m}M' = 0$ because $M = \sum Rm_i + \mathfrak{m}M$ by hypothesis and projecting this into M' kills the m_i's and carries $\mathfrak{m}M$ into $\mathfrak{m}M'$. (That is, we have $M' = \mathfrak{m}M'$, as asserted.) Since our problem is to show that $M' = 0$, and we know that $M'/\mathfrak{m}M' = 0$, we may rename M' as M to reduce to showing that if $M_0 = 0$ then $M = 0$. This implication is what we shall now prove.

By hypothesis M has a finite generating set, say $\{v_1, \dots, v_n\}$. That is, $M = \sum Rv_i$. But $M = \mathfrak{m}M$ since $M_0 = 0$, so in fact $M = \sum \mathfrak{m}v_i$. In particular, for all j we have expressions

$$v_j = \sum a_{ij} v_i$$

with $a_{ij} \in \mathfrak{m}$. Subtracting the right side over to the left side, we get a system of n equations in the v's, taking the matrix form

$$(\mathrm{id}_n - (a_{ij})) \begin{pmatrix} v_1 \\ \dots \\ v_n \end{pmatrix} = \begin{pmatrix} 0 \\ \dots \\ 0 \end{pmatrix}.$$

The crux of the matter is to show that $n \times n$ matrix on the left side is *invertible* over R, as then we can multiply both sides by the inverse matrix and so conclude that all v_i's vanish in M, whence $M = 0$ since the v_i's were chosen to span M over R. If we call this matrix on the left side A then $\det(A) \equiv 1 \bmod \mathfrak{m}$ since $A \bmod \mathfrak{m}$ is the $n \times n$ identity matrix over $R/\mathfrak{m} = k$. Thus, $\det(A) \in R^\times$ since R is *local* ($\det(A) \in R$ is not in the unique maximal ideal $\mathfrak{m}$, so it must be a unit).

For any matrix A over any ring R whatsoever, we claim that A has a 2-sided inverse if $\det(A) \in R^\times$. (The converse is true and obvious due to multiplicativity for determinants of matrices over general commutative rings.) To prove this, consider the classical "adjugate" matrix $\mathrm{adj}(A)$ whose ij-entry is $(-1)^{i+j}$ times the $(n-1) \times (n-1)$ minor of A obtained by deleting the ith row and jth column. We claim that this satisfies the "universal identity"

$$A \cdot \mathrm{adj}(A) = \mathrm{adj}(A) \cdot A = \det(A) \cdot \mathrm{id}_n.$$

Well, this identity is reduced to the "universal" case for the matrix (X_{ij}) over the ring $\mathbf{Z}[X_{ij}]$ that is a *domain*, for which the proof is reduced to its fraction field, a case that we know via linear algebra! Hence, if $\det(A)$ is a unit then $(\det(A))^{-1}\mathrm{adj}(A)$ is a 2-sided inverse to A. ∎