CLASS 16, WEDNESDAY APRIL 4TH: NAKAYAMA'S LEMMA PROOFS

Recall the version of Nakayama we will prove is the following:

Theorem 0.1 (Nakayama's Lemma+++). *If I is an ideal of R and M is a finitely generated module such that $IM = M$, then $\exists r \equiv 1 \pmod{I}$ such that $rM = 0$.*

We will prove this using the following generalization of the Cayley-Hamilton theorem for vector spaces.

Lemma 0.2 (Atiyah-Macdonald). *Suppose M is an n-generated R-module, and $\varphi : M \to M$ is an R-linear map. If there is an ideal I with $\varphi(M) \subseteq IM$, then there is a (monic!) polynomial*

$$p(x) = x^n + a_1 x^{n-1} + \ldots + a_n \in R[x]$$

with $a_i \in I^i$ for each i and such that $p(\varphi) = 0$ as an operator on M.

Proof. Given that $M = \langle m_1, \ldots, m_n \rangle$, and $\varphi(m) \in IM$ for every $m \in M$, we have

$$\varphi(m_i) = \sum_{j=1}^{n} r_{ij} m_j$$

where $r_{ij} \in I$. Therefore, we can write $\sum_{j=1}^{n} \varphi \circ \delta_{i,j} + r_{ij}$ applied to m_i is 0, where $\delta_{i,j}$ is the Dirac delta function: $\delta_{i,j} = 1$ if $i = j$ and is 0 otherwise.

Therefore, we can form an $n \times n$ matrix M where the (i, j)-entry is exactly $\varphi \circ \delta_{i,j} - r_{ij}$. This matrix multiplies the vector $m = (m_1, \ldots, m_n)^T$ to zero by design.

Definition 0.3. The adjugate of an $n \times n$ matrix M has its (i, j)-entry as $(-1)^{ij}$ times the determinant of the matrix M with the j^{th} row and i^{th} column omitted.

If we multiply $Adj(M) \cdot M$, we get $\det(M) Id$. Therefore, this has a wonderful property that the inverse of a matrix M is given by $\frac{1}{\det(M)} Adj(M)$ (if it exists). However, in our case this shows that

$$\det(M) Id \cdot m = Adj(M) \cdot M \cdot m = Adj(M) \cdot 0 = 0$$

Therefore, since m_i are generators, either $M = 0$ (and we are done) or $m_i \neq 0$ and we get $\det(M) = 0$. But $\det(M)$ is a degree n polynomial in φ. This proves the claim. $\square$

We now apply this result to the case Nakayama's lemma:

Nakayama: The assumption of Nakayama's lemma ensures that there is $Id(M) \subseteq IM$, so we get a polynomial

$$p(1) = 1 + r_1 + \ldots + r_n$$

for which $p(1)m = 0$ for every $m \in M$. But $p(1) \equiv 1 \pmod{I}$, since each $r_i \in I$. This completes the proof. $\square$

I now continue to add a few extra corollaries:

Theorem 0.4. *If $F \cong R^n$ is a free module, any n-generators form a* **basis** *of F. That is to say, they span (generate) F and are linearly independent:*

$$a_1 f_1 + \ldots + a_n f_n = 0 \ \Leftrightarrow a_i = 0 \ \forall i = 1, \ldots, n$$

Proof. This follows from our previous claim about surjective endomorphisms. The generators $f_1, \ldots, f_n$ give a surjection $R^n \to F$. However, $F \cong R^n$, so we can form the surjection $F \to R^n \to F$. By the previous corollary, this is an isomorphism, so we have that $R^n \to F$ was also injective. Therefore, $f_1, \ldots, f_n$ form a basis. □

This combined with the final result of Homework 2 demonstrates that rank is a well defined notion:

Definition 0.5. A free module $F \cong R^n$ has **rank** n, which is equivalently the minimum number of generators of F as an R-module.

More generally, we define the rank of a module M over an integral domain R to be $\mathrm{rank}(M \otimes K(R))$, where $K(R)$ is the localization of R at the 0 ideal (thus a field).

Another application is to what are called **integral extensions**:

Definition 0.6. An inclusion of rings $R \subseteq S$ is called a **ring extension**. It is furthermore called an **integral extension** if for every $s \in S$, the module $R[s] \subseteq S$ is finite as an R-module ('s in **integral** over R'). Equivalently, s satisfies

$$s^n + r_{n-1}s^{n-1} + \ldots + r_0$$

for $r_i \in R$.

Example 0.7. Some typical examples of integral extensions are quotient rings: $R \subseteq R[x]/\langle x^2+1\rangle = S$. x naturally satisfies t^2+1, and every element of S is expressible as $r_0 + r_1 x$ due to the relation. Therefore,

$$p(t) = t^2 - 2r_0 t + r_1^2 + r_0^2$$

is a monic polynomial with $p(r_0 + r_1 x)$ given by

$$\begin{aligned} &(r_0 + r_1 x)^2 - 2r_0(r_0 + r_1 x) + r_1^2 + r_0^2 \\ = &\ r_0^2 + 2r_0 r_1 x + r_1^2 x^2 - 2r_0^2 - 2r_0 r_1 x + r_1^2 + r_0^2 \\ &= r_1^2(x^2+1) = 0 \end{aligned}$$

By Nakayama's lemma, we achieve the following (maybe unexpected) result:

Theorem 0.8 (Lying-over/Going-Up)**.** *Let $R \subseteq S$ be an integral extension of rings. If $\mathfrak{p}$ is a prime ideal of R, there exists $\mathfrak{q}$ a prime ideal of S such that $\mathfrak{q} \cap R = \mathfrak{p}$. Moreover, $\mathfrak{q}$ can be chosen to contain any given ideal $\mathfrak{q}'$ such that $\mathfrak{q}' \cap R \subseteq \mathfrak{p}$.*

Proof. Quotienting out by $\mathfrak{q}'$ and $\mathfrak{q}' \cap R$, we may assume $\mathfrak{q}' = 0$. Furthermore, localizing at the multiplicative set $R \setminus \mathfrak{p}$ in R and S, we may assume R is local.

With this setup, if $\mathfrak{q}$ is a maximal ideal of S containing $\mathfrak{p}\, S$, then $\mathfrak{q}$ satisfies the theorem. So it is enough to show that $\mathfrak{p}\, S \neq S$. Assume the contrary: $1 = s_1 p_1 + \ldots + s_n p_n \in S$ for $p \in \mathfrak{p}$. If we consider $S' = R[s_1, \ldots, s_n]$, then $\mathfrak{p}\, S' = S'$ as well. But this implies S' is a finitely generated R-module. By Nakayama's Lemma, $S' = 0$. This is a contradiction. □

By induction, this implies any chain of primes of R lifts to one for S.