Nakayama's Lemma

math center

This note tries to cover some basic commutative algebra. So *all rings are commutative.*

Indeed, Nakayama's lemma is used to reduce finite modules to linear algebra. Let's start with the linear algebra.

Theorem 0.1 (Hamilton-Cayley)**.** Let R be a ring and let $A \in \mathrm{Mat}_n(R)$. Then $\chi_A(A) = 0$.

Proof. There are of course a ton of ways to prove this. The most standard proof is

$$\chi_A(t) := \det(t - A) \implies \chi_A(A) = \det(0) = 0.$$

In more details, let $Y = R[t]$ be a formal polynomial ring, and $V := R^{\oplus n}$ has a Y-module structure given by $t \rightsquigarrow A$. Consider the base change $V_Y = Y^{\oplus n}$ of V and $t - A \in \mathrm{End}(V_Y)$. Observe that the composition

$$V \hookrightarrow V_Y \longrightarrow \mathrm{coker}\,(t - A)$$

is an isomorphism of Y-modules. Thus $\chi_A(t) = (t - A)^\vee (t - A)$ annihilates V. $\square$

Remark 0.2. Alternatively, observe that this is a purely formal proposition and it suffices to give a proof over the field $\mathbb{Q}(X_{11}, X_{12}, \cdots, X_{nn})$. Since a matrix A is non-diagonalizable if and only if the discriminant of the determinant of $t - A$ vanishes, the set these matrices is a Zariski closed set. Indeed, an infinite field, every nonempty Zariski open set is dense. Hence we may reduce to the case where A is diagonal, which is trivial.

1 Nakayama

Theorem 1.1 (Nakayama's lemma, 1st version)**.** Let R be a ring and I be an ideal. If M is a finitely generated R-module, we have

(a) If $\varphi \in \mathrm{End}(M)$ and $\varphi(M) \subset IM$, then φ satisfies a polynomial equation $X^n + \sum_{d=0}^{n-1} a_d X^d = 0$, where $a_d \in I^{n-d}$.

(b) If $IM = M$, then there exists $\alpha \in 1 + I$ which annihilates M.

Proof. (b) follows from (a) by taking $\varphi = \mathrm{id}_M$. Pick a set $\{e_i\}_{i=1}^n$ of generators of M. Using condition of (a) we have elements $a_{ij} \in I$ satisfying

$$\varphi(e_i) = \sum_j a_{ij} e_j, \quad \forall i.$$

In other words, the matrix $A = (a_{ij})$ makes the following diagram commute:

$$\begin{tikzcd} R^{\oplus n} \arrow[rr, "A"] \arrow[dr, two heads] & & M^{\oplus n} \arrow[dl, two heads] \\ & M & \end{tikzcd}$$

where the two surjections are both given by $(x_i)_i \mapsto \sum x_i e_i \in M$. The polynomial $\chi_A(t)$ has the required form, and by Hamilton-Cayley, $\chi_A(\varphi) = 0 \in \mathrm{End}_R(M)$. $\square$

Proposition 1.2. Let M be a finitely generated R-module. If $\varphi : M \to M$ is surjective, then it is an isomorphism.

Proof. M has a finitely generated $R[t]$-module structure given by $t \rightsquigarrow \varphi$. In Theorem 1.1 (b), take $I = (t)$. The condition $IM = M$ follows from surjectivity of φ. We conclude that $1 + tf(t)$ annihilates M for some $f(t) \in R[t]$, and the result follows. $\square$

Definition 1.3. The Jacobson radical in a ring R is the intersection of all maximal ideals, denoted by $\mathrm{rad}(R)$.

Lemma 1.4. If I is an ideal of R, then $I \subset \mathrm{rad}(R)$ if and only if every element of $1 + I$ is a unit.

Proof. If $\beta \in \mathrm{rad}(R)$, then $1+\beta$ does not lie in any maximal ideal, so it must be a unit. Conversely, if $I \not\subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subset R$, then the quotient map $R \to R/\mathfrak{m}$ is surjective on I. In particular, there exists $\beta \in I$ such that $1 + \beta \in \mathfrak{m}$. $\square$

Corollary 1.5. Let M be a finitely generated R-module. If $I \subset \mathrm{rad}(R)$ and $IM = M$, then $M = 0$.

Proof. By Theorem 1.1 (b). $\square$

Put $k := R/I$ and denote the base change as $(-)_k := (-) \otimes k$, even when k if not a field.

Corollary 1.6 (Nakayama's lemma, 2nd version)**.** Let M, N be R-modules, $I \subset \mathrm{rad}(R)$. Suppose that M is finitely generated. We have

(a) If $M_k = 0$, then $M = 0$.

(b) If $\varphi \in \mathrm{Hom}_R(N, M)$ and φ_k is surjective, then so is φ.

(c) A subset $\{x_i\}_{i=1}^n \subset M$ generates M if and only if $\{\bar{x}_i\}_i$ generates M_k.

Proof. If $M_k = M \otimes (R/I) = M/IM = 0$, then $M = 0$ by the last corollary. This proves (a). Now tensor the following SES with k,

$$0 \longrightarrow N \longrightarrow M \longrightarrow \mathrm{coker} \longrightarrow 0$$

And we see that $\mathrm{coker} \otimes k = 0$. Clause (b) then follows from (a). Finally, we show (c) by applying (b) to the map $R^{\oplus n} \longrightarrow M$. $\square$

2 An application

Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring, and M be a finitely generated flat R-module. Then M is in fact free.

To see this, and consider the kernel

$$0 \longrightarrow \ker \longrightarrow R^{\oplus n} \longrightarrow M \longrightarrow 0$$

On tensoring with k, since $\mathrm{Tor}_1^R(M, k) = 0$, we obtain an exact sequence of k-vector spaces

$$0 \longrightarrow \ker \otimes k \longrightarrow k^{\oplus n} \longrightarrow M_k \longrightarrow 0$$

The End

Compiled on 2025/10/28.
Home page