2.5 Nakayama's Lemma

We will develop a criterion for a module to be trivial!

Theorem: Let M be a finitely generated A-module, $I \lhd A$ and $\phi \in \text{Hom}_A(M, M)$ such that

$$\phi(M) \subseteq I\,M\ .$$

Then ϕ is the root of a **monic** polynomial with **nonleading** coefficients from I .

Proof: Write $M = \langle x_1 , \ldots , x_n \rangle$. Observe

$$IM = \Big\{ \sum_{j=1}^{m} b_j \, y_j \;\Big|\; m \in \mathbb{Z}^+ , \;\; b_j \in I , \qquad y_j \in M \quad (\forall j) \Big\} .$$

But each member of M is a linear combination of $x_1 , \ldots , x_n$, and I absorbs multiplication by any coefficient from A .

Hence

$$IM \;=\; \left\{ \sum_{i=1}^{n} c_i\, x_i \;\middle|\; c_i \in I \quad (\forall i) \right\} .$$

In particular, for each $i = 1, \ldots, n$, since $\phi(x_i) \in IM$,

$$\phi(x_i) \;=\; \sum_{j=1}^{n} c_{ij}\, x_j$$

for some $c_{ij} \in I \quad (j = 1, \ldots, n)$.

Thus ϕ corresponds to the matrix

$$C \;=\; [\, c_{ij} \,] \,.$$

Let $\chi(x)$ be the characteristic polynomial of C .

By the Cayley-Hamilton Theorem,

$$\chi(C) \;=\; 0$$

the **zero matrix**,

so

$$\chi(\phi) \ = \ 0$$

the **zero mapping**, when evaluated in the ring Hom $_A(M, M)$. This proves the Theorem.

Corollary: Let M be a finitely generated A-module and $I \lhd A$ such that $IM = M$. Then

$$x\,M \ = \ \{0\} \quad \text{for some} \quad x \in 1 + I \ .$$

Proof: Let $\phi : M \to M$ be the identity mapping. Then

$$\phi(M) \ = \ M \ = \ I\,M \ ,$$

so, by the previous Theorem,

for some $a_1, \ldots, a_n \in I$,

$$\phi^n \ + \ a_1\,\phi^{n-1} \ + \ \ldots \ + \ a_{n-1}\,\phi \ + \ a_n\,1 \ = \ 0$$

note monic

identity mapping

zero mapping

Hence

$$\Big(\underbrace{1}_{\text{identity element of } A} + \underbrace{a_1 + \ldots + a_n}_{\text{element of } I} \Big) \phi = \underbrace{0}_{\text{zero mapping}} .$$

Put $x = 1 + a_1 + \ldots + a_n \in 1 + I$.

Thus

$$x\, M = x\, \phi(M) = (x\phi)\, (M) = \{0\} ,$$

since $x\phi$ is the zero mapping.

Theorem (Nakayama's Lemma):

Let M be a finitely generated A-module and $I \lhd A$ such that $I \subseteq R$ (the Jacobson radical). Then

$$I\,M \;=\; M \qquad \Longrightarrow \qquad M \;=\; \{0\}\,.$$

First proof: Suppose $I\,M \;=\; M$.

By the previous Corollary, $xM \;=\; \{0\}$ for some $x \in 1 + I \;\subseteq\; 1 + R$.

But $1 + R$ consists of units

(an early observation about the Jacobson radical),

so

$$\{0\} \;=\; x^{-1}\{0\} \;=\; x^{-1}(xM) \;=\; 1\,M \;=\; M\,.$$

Second proof: Suppose $M \neq \{0\}$.

Let $\{\, u_1 \,,\, \ldots \,,\, u_n \,\}$ be a minimal set of generators of M (since M is finitely generated).

If $u_n \in IM$ then

$$u_n \;=\; a_1\,u_1 \,+\, \ldots \,+\, a_n\,u_n$$

for some $a_1 \,,\, \ldots \,,\, a_n \,\in\, I$, so

$$(1 - a_n)\,u_n \;=\; a_1\,u_1 \,+\, \ldots \,+\, a_{n-1}\,u_{n-1}$$

so

$$u_n \;=\; (1 - a_n)^{-1}\,(\,a_1\,u_1 \,+\, \ldots \,+\, a_{n-1}\,u_{n-1}\,)$$

(since $1 - a_n \,\in\, 1 + R$ is invertible)

which contradicts the minimality of the generating set.

Hence $u_n \notin I\ M$, so $I\ M \ \neq\ M$, and Nakayama's Lemma is proved.

Corollary: Let M be a finitely generated A-module, N a submodule of M and $I \ \lhd\ A$ such that $I \ \subseteq\ R$ (the Jacobson radical). Then

$$M \ = \ I\ M \ + \ N \quad \Longrightarrow \quad M \ = \ N \ .$$

Proof: Suppose $M = IM + N$. Then

$$I\,(M/N) \;=\; \Big\{ \sum_{i=1}^{n} a_i\,(m_i + N) \;\Big|\; n \in \mathbb{Z}^+ ,\; a_i \in I ,\; m_i \in M \quad \forall i \Big\}$$

$$= \Big\{ \Big(\sum_{i=1}^{n} a_i\, m_i \Big) + N \;\Big|\; n \in \mathbb{Z}^+ ,\; a_i \in I ,\; m_i \in M \quad \forall i \Big\}$$

$$= (IM + N)/N \;=\; M/N \, .$$

By Nakayama's Lemma,

$$M/N \quad = \quad \text{zero module},$$

that is, $M = N$.

Consider now a local ring A , with maximal ideal I , and put

$$F \quad = \quad A/I \, ,$$

the **residue field** of A .

Let M be a finitely generated A-module.

Then IM is a submodule of M and

$$I(M/IM) \;=\; (IM + IM)/IM \;=\; IM/IM \;,$$

the zero module, so

$$I \;\subseteq\; \text{Ann}\,(M/IM)$$

so

$$\boxed{M/IM \text{ becomes an } A/I\text{-module}}$$

so

$$\boxed{M/IM \text{ becomes a vector space over } F\ .}$$

Further, M/IM is finitely generated

(because M is),

so

$$\boxed{M/IM \text{ is finite dimensional.}}$$

Theorem: Let $x_1 , \ldots , x_n \in M$ be such that

$$\{ x_1 + IM , \ldots , x_n + IM \}$$

is a basis for the vector space M/IM .

Then

$$M = \langle x_1 , \ldots , x_n \rangle .$$

Proof: Put $N = \langle\, x_1 \,,\, \ldots \,,\, x_n \,\rangle$.

Then

$$\begin{aligned} M/IM &= \langle\, x_1 + IM \,,\, \ldots \,,\, x_n + IM \,\rangle \\ &= F(x_1 + IM) \,+\, \ldots \,+\, F(x_n + IM) \\ &= \sum_{i=1}^{n} (A/I)(x_i + IM) \\ &= \sum_{i=1}^{n} A(x_i + IM) \end{aligned}$$

Hence

$$
\begin{aligned}
M/IM &= \{ \, (\sum_{i=1}^{n} a_i x_i) + IM \mid a_1 , \ldots , a_n \in A \, \} \\
&= (N + IM)/IM \, .
\end{aligned}
$$

Hence $M = N + IM$, so $M = N$, by the previous Corollary.