Commutative Algebra: Two Module Theorems

Dr. Zvi Rosen

Department of Mathematical Sciences,
Florida Atlantic University

FLORIDA ATLANTIC UNIVERSITY

The Two Theorems

Cayley-Hamilton Theorem

Nakayama's Lemma

Applications

Definition: Free Module

Let A be a ring.

A free module is a direct sum $\bigoplus_{i \in I} M_i$ where $M_i \simeq A$ for all i.

Finitely-Generated A-module = Quotient of A^n

Recall: A finitely generated module $M = \sum_{i=1}^{n} A x_i$, for $\{x_1, \dots, x_n\} \subseteq M$.

A finitely generated free module will be $A \oplus \cdots \oplus A =: A^n$.

Let $\varphi : A^n \longrightarrow M$ map generators of A^n to the x_i's. $A^n / \ker(\varphi) \cong M$.

Cayley-Hamilton Theorem

Let M be a finitely generated A-module, let $\mathfrak{a}$ be an ideal of A, and let ϕ be an A-module endomorphism of M such that $\phi(M) \subseteq \mathfrak{a}M$.

Then ϕ satisfies an equation of the form

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$$

where the a_i are in $\mathfrak{a}$.

(Version in Atiyah-MacDonald)

Familiar Form from Linear Algebra

k-vector space

Let M be a ~~finitely generated A-module~~, ~~let $\mathfrak{a}$ be an ideal of A~~, and let ϕ be ~~an A-module endomorphism of M such that $\phi(M) \subseteq \mathfrak{a}M$~~.

a k-linear map $M \to M$

Then ϕ satisfies an equation of the form

$$p_A(\phi) = \phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$$

given by $p_A(\lambda) = \det(\lambda I - A)$ where A is a matrix representing ϕ ~~where the a_i are in $\mathfrak{a}$~~.

William Rowan Hamilton

Proved a version of the theorem for quaternions (which he invented) in 1853.

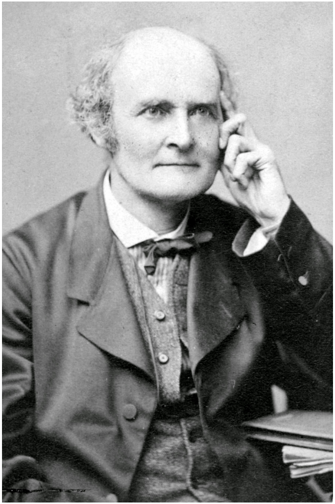
[Photo from Wikipedia]

Arthur Cayley

Verified the theorem for 3×3 matrices in 1858.

"I have not thought it necessary to undertake the labor of a formal proof of the theorem in the general case of a matrix of any degree"

[Photo & Quotation from Wikipedia]



Proof of Cayley-Hamilton

$\phi(M) \subseteq \mathfrak{a}M$. generators of M: $x_1, \dots, x_n$.

$$\phi(x_j) = \sum_{i=1}^{n} a_{ij} x_i, \quad a_{ij} \in \mathfrak{a}. \quad \text{for all } j.$$

$$\phi(x_j) - \sum_{i=1}^{n} a_{ij} x_i = 0$$

δ_{ij}

$$\Rightarrow \sum_{i=1}^{n} (\delta_{ij}\phi - a_{ij}) x_i = 0$$

Proof of Cayley-Hamilton

For any matrix B, $\exists \tilde{B}$ also $\mathrm{adj}(B)$

s.t. $\mathrm{adj}(B)B = \det(B)I$

$$\det(\delta_{ij}\phi - a_{ij})_{ij} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\underbrace{\det(\phi I_n - a_{ij})}_{\text{polynomial as demanded by the theorem.}}{}_{ij} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Nakayama's Lemma

Let M be a finitely generated A-module and $\mathfrak{a}$ an ideal of A contained in the Jacobson radical $\mathfrak{R}$ of A. Then $\mathfrak{a}M = M$ implies $M = 0$.

intersection of all maximal ideals of A.

$\mathfrak{R} = \{x : \forall y \in A,\ 1 - xy \text{ unit}\}$

Tadashi Nakayama

Published the general form of Nakayama's Lemma in 1951.

Earlier (less general) versions were proved by Krull, Azumaya, and Jacobson.

[Photo from MacTutor]

Proof 1

Lemma

Let M be a finitely generated A-module, $\mathfrak{a} \subseteq A$ an ideal such that $\mathfrak{a}M = M$. Then there exists $x \equiv 1 \mod \mathfrak{a}$ such that $xM = 0$.

Proof of Lemma:

Let ϕ be identity. $\phi(M) = M = \mathfrak{a}M$.

$\Rightarrow$ ϕ satisfies $\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$

Cayley Hamilton

$\Rightarrow$ $1 + a_1 + \cdots + a_n = 0 \Rightarrow x = 1 + a_1 + \cdots + a_n$ satisfies Lemma.

Proof 1, cont'd

Take x from the Lemma, $x \equiv 1 \mod \mathfrak{a}$ and $xM = 0$.

$\mathfrak{a} \subset R$. $x - 1 \in \mathfrak{a}$. Take $y = 1$.

$1 - (x-1) \cdot 1 = x$ is a unit of A.

$\Rightarrow \exists x^{-1}$. $x^{-1}(xM) = (x^{-1}x)M = M = 0$.

$\square$

Proof 2

Suppose $M \neq 0$.

M f.g. and $\mathfrak{a}M = M$.

Take a minimal set of generators

$x_1, \ldots, x_n$. $\mathfrak{a}M = M \Rightarrow x_n = a_1 x_1 + \cdots + a_n x_n$

$(1-a_n)x_n = a_1 x_1 + \cdots + a_{n-1} x_{n-1}$

$\mathfrak{a} \subseteq \mathfrak{R} \Rightarrow (1-a_n)$ unit in $A \Rightarrow b = (1-a_n)^{-1}$

$x_n = b a_1 x_1 + \cdots + b a_{n-1} x_{n-1}$. $\Rightarrow\!\Leftarrow$.

Surjective endomorphisms of f.g. module

Corollary 4.4(a), Eisenbud

Let A be a ring, M a finitely-generated A-module. If $\alpha : M \to M$ is a surjective homomorphism, then it is an isomorphism.

Consider M as an $A[t]$-module, with $tv = \alpha(v)$, let $I = (t)$. Surjectivity implies $IM = M$. Let $\phi = 1$.

C-H $\Rightarrow 1 + t q(t) = 0 \Rightarrow t(-q(t)) = 1$

$\Rightarrow (\alpha)(-q(\alpha)) = 1 \Rightarrow$ α isomorphism.

Rank of a free module is well-defined

Corollary 4.4(b), Eisenbud

Let A be a ring, M a finitely-generated A-module. If $M \cong A^n$, then any n-element set of generators forms a free basis.

Free basis: a set of generators $x_1, \dots, x_n$

s.t. $\sum_{i=1}^{n} A x_i = A^n$.

$\beta : A^n \to M$, $\beta(a_1, \dots, a_n) = a_1 x_1 + \cdots + a_n x_n$

surjective homomorphism.

$M \cong A^n \Rightarrow \exists \gamma : M \to A^n$ isomorphism.

Rank of a free module is well-defined

Corollary 4.4(b), Eisenbud

Let A be a ring, M a finitely-generated A-module. If $M \cong A^n$, then any n-element set of generators forms a free basis.

Then $\beta\gamma : M \to M$ surjective endomorphism $\Rightarrow$ $\beta\gamma$ isomorphism.

$\Rightarrow$ β isomorphism $\Rightarrow$ $x_1, \dots, x_n$ free basis.

Pulling back generators of quotient module

Corollary 4.8(b), Eisenbud

Let $I \subseteq \mathfrak{R} \subseteq A$, and M a finitely-generated A-module as in Nakayama's Lemma.

If $m_1, \ldots, m_n \in M$ have images generating M/IM as an A-module, then $m_1, \ldots, m_n$ generate M as an A-module.

Proof: Let $N = M / \sum_{i=1}^{n} Am_i$.

$$N/IN = M / \underbrace{\left(IM + \sum_{i=1}^{n} Am_i\right)}_{=M} = 0.$$

$\Rightarrow N = IN.$

N f.g. module, $IN = N \Rightarrow N = 0.$

$\Rightarrow M / \sum A m_i = 0 \Rightarrow M = \sum_{i=1}^{n} A m_i$

$\blacksquare$