Cayley-Hamilton

Recall that the Cayley-Hamilton Theorem in linear algebra says that an $n \times n$ matrix A satisfies its own characteristic equation. The characteristic polynomial for A is $p_A(x) = \det(x \underbrace{\mathbb{1}_n}_{n \times n \text{ identity matrix}} - A)$. That is, C-H says that $p_A(A) = 0$.

We will prove a version of this for f.g. modules that has useful/surprising applications.

Theorem: (Cayley-Hamilton) Let R be a ring, I an ideal, and M an R-module generated by n elements. Let $\varphi: M \longrightarrow M$ be a homomorphism. If $\varphi(M) \subseteq IM$, then there is a monic polynomial (i.e. leading coefficient 1)

$$p(x) = x^n + p_1 x^{n-1} + \dots + p_n$$

with $p_j \in I^j$ for each j such that $p(\varphi) = 0$ as a homomorphism. i.e. $p(\varphi)(M) = 0$.

Pf: Let $m_1, \dots, m_n$ be generators for M. Then we can write $\varphi(m_i) = \sum a_{ij} m_j$ such that each $a_{ij} \in I$.

We can treat M as an $R[x]$-module by setting $xa = \varphi(a)$ for $a \in M$. i.e. x acts as φ.

Let $A = (a_{ij})$ and $\vec{m} = \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$.

Then we can rewrite the above equation as

$$(x\mathbb{1})\vec{m} = A\vec{m} \implies (x\mathbb{1} - A)\vec{m} = 0.$$

Recall from linear algebra that if $\operatorname{adj} A$ is the adjugate matrix of A, then $(\operatorname{adj} A)A = (\det A)\mathbb{1}$.
On the HW, we'll see this holds for arbitrary rings!

Let B be the adjugate of $x\mathbb{1} - A$. Then

$$B(x\mathbb{1} - A) = \det(x\mathbb{1} - A)\mathbb{1}.$$

Multiplying both sides by $\vec{m}$, we get

$$\det(x\mathbb{1} - A)\mathbb{1}\vec{m} = 0.$$

i.e. $\det(x\mathbb{1} - A)m_i = 0 \;\; \forall i$. Thus, $\det(x\mathbb{1} - A)$ annihilates M, so if $p(x) = \det(x\mathbb{1} - A)$, then $p(\varphi)$ is the zero map.

Since $a_{ij} \in I$, the coefficients are in the correct powers of I. $\square$

Cayley-Hamilton shows us that free modules behave a lot like vector spaces. We first give another definition for free modules.

Def: Let R be a ring, F an R module. F is free w/ free basis $\mathcal{B} \subseteq F$ if every element of F is uniquely an R-linear combination of elements of $\mathcal{B}$.
Equivalently, if $b_1, \ldots, b_n \in \mathcal{B}$ are distinct, then
$\sum a_i b_i = 0 \Rightarrow$ all $a_i = 0$.

(Of course if R is a field, this is the same as a vector space basis.)

As mentioned at the beginning of the semester, freeness is equivalent to $F \cong \bigoplus_{b \in \mathcal{B}} Rb$. In the f.g. case, this is isomorphic to R^n, and $(1,0,0,\ldots)$, $(0,1,0,\ldots), \ldots$ gives a free basis.

CH has some surprising corollaries for modules:

Cor: R a ring, M a finitely generated R-module.

a.) If $\alpha: M \to M$ is a surjective homomorphism, it's an isomorphism.

b.) If $M \cong R^n$, then any set of n elements that generate M is a free basis. In particular, the rank, n, of M is well-defined.

Pf: a.) We can give M the structure of an $R[t]$-module where $tm := \alpha(m)$.

Let $I = (t)$. Since α is surjective, we have $IM = M$. Thus, we can apply C-H w/ $\varphi = id$.

So there is a polynomial $p(x) = x^n + p_1 x^{n-1} + \dots + p_n$ s.t. $p(id) M = 0$, and $p_i \in (t)^i$. i.e. $p_i = a_i t^i$ for $a_i \in R$. (if $a_i \in R[t]$, can redistribute higher powers of t to other coeffs.)

Thus, $(1 + a_1 t + a_2 t^2 + \dots + a_n t^n) M = 0$

$$\Rightarrow \left(1 + t\underbrace{(a_1 + a_2 t + \dots + a_n t^{n-1})}_{q(t)}\right) M = 0$$

$$\Rightarrow 1 + q(t)t = 0, \text{ i.e. } (-q(\alpha))\alpha = id_M$$

so $-q(\alpha)$ is an inverse for α, so α is an isomorphism.

b.) Choose generators $m_1, \dots, m_n$ for M. We can define a surjection

$$\beta : R^n \longrightarrow M$$

which sends the i^{th} basis element to m_i.

Choose an isomorphism $\gamma: M \to R^n$. Then $\beta\gamma: M \to M$ is a surjection, so it's an isomorphism. Thus, $(\beta\gamma)\gamma^{-1} = \beta$ is an isomorphism, so $m_1, \ldots, m_n$ must be linearly independent and thus form a basis.

To see that rank is well-defined, suppose $R^m \cong R^n$ and $m < n$. Let $a_1, \ldots, a_m$ be a free basis for R^m. If we add $n-m$ 0s, we get n generators that don't form a free basis. $\square$

Remark: If $p \in R[x]$, we can think of $R[x]/(p)$ as adjoining a root of p to R.

e.g. $R[x]/(ax-1) \cong R[1/a] = R$ localized at $\{1, a, a^2, \ldots\}$

C-H gives us a result dealing w/ the case when $p(x)$ is a monic polynomial:

Prop: Let R be a ring and $J \subseteq R[x]$ an ideal. Let $S = R[x]/J$ and s = image of x in S.

a.) S is generated by $\leq n$ elements as an R-module iff it contains a monic polynomial of degree $\leq n$, in which case it is generated by $1, s, \dots, s^{n-1}$.

b.) S is a f.g. free module iff J is generated by a monic polynomial. In this case, $1, s, \dots, s^{n-1}$ is a free basis.

Pf: a.) $1, s, s^2, \dots$ certainly generate S. If J contains a monic polynomial p of deg n, then

$$s^n = a_1 s^{n-1} + \text{lower deg terms},$$

so for $d > n$,

$$s^d = a_1 s^{d-1} + \text{lower deg terms},$$

so by induction S is generated by $1, s, \dots, s^{n-1}$.

Conversely, suppose S is generated by n elements. Let $\varphi : S \to S$ be defined $\varphi(a) = sa$.

Let $I = R$. Then $\varphi(S) \subseteq RS = S$, so C-H says there is some $p(t) = t^n + p_1^{\,n-1} + \dots + p_n$ s.t. $p_i \in R$ and $p(\varphi) = 0$. i.e. $p(x) \in \operatorname{Ann} S = J$.

b.) Suppose $J = (p)$, p a monic polynomial of deg n. Then by a.), $1, s, \dots, s^{n-1}$ generate S.

Suppose $a_0 + a_1 s + \dots + a_{n-1} s^{n-1} = 0$, some $a_i \in R$.

Then $a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \in J = (p)$, but p is monic of deg n, so all $a_i = 0 \Rightarrow 1, s, s^2, \dots, s^{n-1}$ form a free basis.

Conversely, assume S is a free module of rank n. By a.), there is a monic polynomial of deg n in J, so S is generated by $1, \dots, s^{n-1}$.

But S is free of rank n, so this is a free basis for S. WTS: $J = (p)$.

If $f \in J$ and $\deg f < n$, this gives a linear relation among $1, \dots, s^{n-1}$, so $f = 0$.

If $\deg f = d \geq n$, write $f = a_d x^d +$ lower deg terms. Then

$$f - a_d x^{d-n} p \in J \text{ has lower degree.}$$

Repeating this, we get $f - qp \in J$ w/ degree $< n$
$\Rightarrow f - qp = 0 \Rightarrow f \in (p)$. Thus $(p) = J$. $\square$

Nakayama's Lemma

As a corollary of C-H, we get Nakayama's Lemma, a surprisingly useful result about finitely generated modules. First we need the following lemma:

Lemma: If M is a finitely generated R-module and $I \subseteq R$ an ideal such that $IM = M$, then there is some $r \in I$ that acts as the identity on M, i.e. $(1-r)M = 0$.

Pf: Let $\varphi = id$ on M. By C-H, $\exists$ $p_1, \dots, p_n$ s.t. $p_j \in I^j \subseteq I$ s.t. $(1 + p_1 + \dots + p_n)M = 0$.
Set $r = -(p_1 + \dots + p_n)$. $\square$

Recall that the Jacobson radical of R, $J(R)$, is the intersection of the maximal ideals.

Nakayama's Lemma: Let $I \subseteq R$ be an ideal contained in $J(R)$, and let M be a finitely generated R-module.

a.) If $IM = M$, then $M = 0$.

b.) If $m_1, \dots, m_n \in M$ have images in M/IM that generate it as an R-module, then $m_1, \dots, m_n$ generate M as an R-module.

Pf: a.) The previous lemma says there is some $r \in I$ s.t. $(1-r)M = 0$. r is in every max'l ideal, so $1-r$ is in no maximal ideal, so $1-r$ is a unit, so $M = (1-r)M = 0$.

b.) Let $N = M/(\Sigma R m_i)$.

Then $N/IN = M/(IM + (\Sigma R m_i)) = 0$.

Thus, $N = IN$, so $N = 0 \Rightarrow M = \Sigma R m_i$. $\square$

Note: We assumed M is f.g., so we can't use b.) to prove a module is finitely generated.

Cor: If M and N are f.g. R-modules and $M \otimes_R N = 0$, then $\operatorname{Ann} M + \operatorname{Ann} N = R$. If R is local, M or N is 0.

Pf: First assume R is local and $M \neq 0$. If $P \subseteq R$ is the maximal ideal, then $J(R) = P$, so Nakayama says $M \neq PM$. Thus $M/PM \neq 0$. This is an R/P-vector space, so there's a surjection

$$M/PM \longrightarrow R/P.$$

Thus, $M \otimes_R N = 0$ surjects onto $R/P \otimes_R N = N/PN$

$\Rightarrow N = PN \Rightarrow N = 0$.

If R is not local, assume $I = \operatorname{Ann} M + \operatorname{Ann} N \neq R$. Then we can find a prime ideal P containing I.

Then $M_P \otimes_{R_P} N_P = 0$ (by assumption), so by the local case M_p or $N_p = 0$. Assume WLOG that $M_p = 0$. Then $P \notin \operatorname{Supp}(M) \underset{\substack{\uparrow \\ \text{since } M \\ \text{is f.g.}}}{=} V(\operatorname{Ann} M)$, so

$\operatorname{Ann} M \not\subset P$, a contradiction. $\square$