# Cayley-Hamilton

Recall that the classical Cayley-Hamilton Theorem says a matrix $A$ on a finite-dim vector space satisfies its characteristic polynomial, $p(x) = \det(x\mathbb{I} - A)$. ($\mathbb{I}$: identity matrix) We prove a more general version for finitely generated modules:

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

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

s.t. $p_j \in I^j$ for each $j$ w/ $p(\varphi) = 0$, as a map $M \to M$.

**Pf:** Let $m_1, \dots, m_n$ be generators for $M$. Then we can write

$$\varphi(m_i) = \sum a_{ij} m_j, \quad a_{ij} \in I, \text{ and let } A = (a_{ij}).$$

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

Set $m = \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$. Then we can rewrite the above as

$(x\mathbb{1})m = Am \Rightarrow (x\mathbb{1} - A)m = 0$

Recall from linear algebra that if $B$ is the matrix of cofactors for $(x\mathbb{1} - A)$, then $B(x\mathbb{1} - A) = \det(x\mathbb{1} - A)\mathbb{1}$.

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

i.e. $\det(x\mathbb{1} - A)\, m_i = 0 \quad \forall\ i$. 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 $a_{ij} \in I$, it's straightforward to check that the coefficients are in the correct powers of $I$. □

Cayley-Hamilton is usually stated for vector spaces, and in fact, gives us some results that show certain modules behave kind of like vector spaces.

**Def:** Let $R$ be a ring, $F$ an $R$-module. $F$ is <u>free</u> with <u>free basis</u> $\mathcal{B} \subseteq F$ if every element of $F$ is uniquely an $R$-linear combination of elements of $\mathcal{B}$. Equivalently, if $b_1, \dots, b_n \in \mathcal{B}$ are distinct, then $a_1 b_1 + \dots + a_n b = 0 \Rightarrow$ all $a_i = 0$.

Of course if $R$ is a field, this is the same as a vector space

basis.

Freeness is equivalent to $F \cong \bigoplus_{b \in B} Rb$, which is isomorphic to $R^n$, in which $(1,0,\dots), (0,1,0,\dots)\dots$ gives a free basis.

C-H has some surprising corollaries for modules:

**Cor:** $R$ a ring, $M$ f.g. $R$-module.

a.) If $\alpha : M \to M$ is surjective, 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.) Again $M$ is an $R[t]$-module where $tm := \alpha(m)$.

If $I = (t)$, then since $\alpha$ is surjective, $IM = M$.

So we can apply C-H w/ $\varphi = id$.

So there's a polynomial $p(x) = x^n + p_1 x^{n-1} + \dots + p_n$

s.t. $p(id)M = 0$, and $p_i \in (t)^i \Rightarrow p_i = a_i t^i$, some $a_i \in R$.

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

$$\Rightarrow (1 + t(\underbrace{a_1 + a_2 t + \dots}_{q(t)})) M = 0$$

$\Rightarrow 1 + q(t)t = 0 \rightarrow \left(-q(\alpha)\right)\alpha = 1,$

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

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

$\beta : R^n \to M$ sending each basis elt to an $m_i$.

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. □

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

For instance when we localize at $\{1, a, a^2, \ldots\}$, this is the same as $R[x]/(ax-1)$.

Cayley-Hamilton gives us a result dealing w/ the case when $p(x)$ is a monic polynomial of arbitrary degree:

**Prop:** Let $R$ be a ring and $J \subseteq R[x]$ an ideal. Let $S = R[x]/J$, and $s$ = the 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's generated by $1, s, \ldots, s^{n-1}$.

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

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

$s^{d-n} p(s) = s^d + r_1 s^{d-1} + \text{lower deg terms} = 0$, so $s^d$ is generated by smaller powers.

$\Rightarrow 1, s, \ldots, s^{n-1}$ generate $S$.

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

Let $I = R$. Then C-H says $\exists \quad p(x) = x^n + p_1 x^{n-1} + \ldots p_n$

s.t. $p_i \in R$ and $p(s) = 0$. Thus $p(x) \in J$.

b.) Suppose $J$ is generated by a monic polynomial $p$ of degree $n$. Then by a.), the first $n$ powers of $s$ generate $S$.

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

Then $q(x) = a_0 + a_1 x + \dots a_{n-1} s^{n-1} \in J = (p)$.

But $p$ has degree $n$, so $q = 0 \Rightarrow 1, s, \dots, s^{n-1}$ form a free basis.

Conversely, assume $S$ is a free module of rank $n$.

By a.), there is a monic polynomial $p$ 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 basis for $S$.

We claim $J = (p)$. 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 degree terms.

Then $f - a_d x^{d-n} p \in J$ has lower degree. Repeating this process, we get $f - qp \in J$, which has deg $< n$

$\Rightarrow f - qp = 0 \Rightarrow f \in (p)$. $\square$

## R-algebras and integrality

**Def:** An R-algebra $S$ is a ring along with a map $\varphi: R \to S$.

In this way it's also an $R$-module, so we can just write $rs$ rather than $\varphi(r)s$. Usually we care about the case where $R \subseteq S$. $S$ is finitely-generated if $\exists\ v_1, \dots, v_n \in S$ s.t. $S$ is the ring generated by $\varphi(R)$ and $v_1, \dots, v_n$.

**Def:** $s \in S$ is integral over $R$ if it is the zero of some monic polynomial in $R[x]$. If every element of $S$ is integral over $R$, then $S$ is integral over $R$.

We'll soon prove that the set of elements integral over $R$ is a subalgebra of $S$, called the integral closure of $R$ in $S$ (or the normalization of $R$ in $S$). If $R$ is an integral domain, the integral closure (or normalization) of $R$ (without reference to a bigger ring) is the integral closure in its field of fractions.

Geometrically, normalizing a ring corresponds to improving the singularities of a variety or scheme. e.g. the normalization of a curve is always smooth!

**Def:** An $R$-algebra $S$ is <u>finite over $R$</u> if it is finitely generated as an $R$-module. (finiteness $\Rightarrow$ f.g. as an algebra)

**Ex:** 1.) $R[x]$ is a finitely generated $R$-algebra, but it's not finite or integral over $R$.

2.) $R[x]/(x^2)$ is finite and integral over $R$.

3.) $\mathbb{Q}[\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots]$ is integral over $\mathbb{Q}$ but not finite.

In fact, finiteness is a stronger condition than integrality:

**Prop:** An $R$-algebra $S$ is finite over $R$ iff $S$ is generated as an $R$-algebra by finitely many integral elements.
(i.e. $S = R[\alpha_1, \ldots, \alpha_n]$, $\alpha_n \in S$.)

($R$: image of $R$ in $S$; $\alpha_1, \ldots, \alpha_n$: generators integral/$R$)

**Pf:** Suppose $S$ is finite over $R$. If $s \in S$, then mult. by $S$ is a map $S \to S$ and the Cayley-Hamilton thm shows that $s$ satisfies a monic polynomial.

Conversely, if $S$ is generated as an $R$-algebra by $t$ elements, let $S' \subseteq S$ be the algebra generated by $t-1$ of them. By induction, $S'$ is finite over $R$.

Assume $S'$ is generated by $\{s_i\}$ (finite) as an $R$-module. The last (algebra) generator of $S$, call it $s$, is integral over $R$ and is thus integral over $S'$, so $\frac{S'[x]}{(p)} \twoheadrightarrow S \cong \frac{S'[x]}{I}$

$x \longmapsto s$

where $p$ is monic and $p(s) = 0$. Thus $p \in I$, so by the above prop, there is a finite set of generators for $S$ as an $S'$-module, say $\{t_i\}$

Thus, $S$ is generated as an $R$-module by $\{s_i t_j\}$. $\square$

Another application of C-H gives us a criterion for when an element is integral over a ring.

**Prop:** If $S$ is an $R$-algebra and $s \in S$ then $s$ is integral over $R$ iff $\exists$ an $S$-module $N$ and a f.g. $R$-submodule $M \subseteq N$ not annihilated by any nonzero element of $S$, s.t. $sM \subseteq M$.
In particular, $s$ is integral $\iff R[s]$ is a f.g. $R$-module.

**Pf:** First of all, we show why the last sentence follows.
If $s$ is integral, then the previous prop implies $R[s]$ is finite over $R$.

If $R[s]$ is finite over $R$, then set $N = R[s]$, $M = R[s]$. $1 \in R[s]$ is not annihilated by any elt of $S$. $\Rightarrow$ $s$ is integral.

For the first sentence, first assume $s$ is integral over $R$. Take $N=S$. Then $M = R[s] \subset S$. But then $M \cong R[x]/I$, where $I$ contains some monic polynomial that $s$ satisfies. Thus, $M$ is finite over $R$.

For the converse, Let $\varphi : M \to M$ be multiplication by $s$. Then we can apply C-H with $I = R$, and we get a monic poly. $p(x)$ w/ coefficients in $R$ s.t. $p(s)M = 0$. But $M$ is not annihilated by nonzero elements of $S$, so $p(s) = 0 \Rightarrow s$ is integral over $R$. □

As previously mentioned, integral elements over $R$ form a subalgebra. So in particular, if $s_1, \dots, s_n$ are integral over $R$, so is $R[s_1, \dots, s_n]$.

**Thm:** Let $S$ be an $R$-algebra. The set of all elements of $S$ integral over $R$ is a subalgebra of $S$.

**Pf:** $a, b$ integral over $R$. WTS $a+b$ and $ab$ are as well.

$R[a,b]$ is finite over $R$. If $s = ab$ or $a+b$, set $N = S$, $M = R[a,b]$. Then $M$ is not annihilated by any elt of $S$, and $sM \subseteq M$. Thus, $s$ is integral over $R$. □

We now give one more corollary of C-H that will help us prove Nakayama's Lemma:

**Cor:** $M$ a f.g. $R$-module, $I$ an ideal of $R$ s.t. $IM = M$. Then $\exists$

an element $r \in I$ that acts as the identity on $M$. i.e. $(1-r)M = 0$.

**Pf:** Let $\varphi = id$. 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 $r = -(p_1 + \dots + p_n)$. $\square$

**Def:** The <u>Jacobson radical</u> of a ring $R$ is the intersection of all the maximal ideals.

**Note:** The Jacobson radical contains the Nilradical, but in general they don't coincide: e.g. $k[x,y]_{(x,y)}$ has Jacobson radical $(x,y)$, but nilradical $0$.

**<u>Nakayama's Lemma</u>:** Let $I$ be an ideal contained in the Jacobson radical of a ring $R$, 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 corollary $\Rightarrow \exists$ $r \in I$ s.t. $(1-r)M = 0$.

$r$ is in every max'l ideal, so $1-r$ is in no max'l ideal, so $1-r$ is a unit $\Rightarrow M = 0$.

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

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

$\Rightarrow N = IN$, so $N = 0 \Rightarrow M = \Sigma Rm_i$. $\square$

**Note:** We assumed $M$ is f.g., so we can't use part b.) to prove some 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 $P$ is the max'l ideal, Nakayama $\Rightarrow M/PM \neq 0$. This is an $R/P$-vector space, so there's a surjection $M/PM \longrightarrow R/P$.

Thus, $M \otimes N = 0$ surjects onto $R/P \otimes N = N/PN$. $\Rightarrow N = PN \Rightarrow N = 0$.

Now if $R$ is not local, assume $\operatorname{ann} M + \operatorname{ann} N \neq R$.
Find some prime $P$ containing $\operatorname{ann} M$ and $\operatorname{ann} N$.

Then $M_P \otimes_{R_P} N_P = 0 \Rightarrow$ either $M_P$ or $N_P$ is 0.
$M_P = 0 \Rightarrow$ there's an elt not in $P$ that annihilates each generator so the product annihilates $M$, a contradiction. $\square$