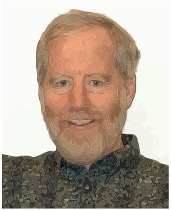
"Algebra is the metaphysics of arithmetic."

-John Ray, English Naturalist and Botanist

"If we don't make it through this proof, no one is going to lunch. Not today; maybe not even tomorrow!"

-John Wakins, American Mathematician



The Determinant Trick

or:

How I Learned to Stop Worrying and Love Matrices

Courtney Gibbons

University of Nebraska-Lincoln
(& Colorado College, '06)

April 23, 2010

The Plan:

- Linear algebra over commutative rings.
- Modules.
- The determinant trick.
- Applications in commutative algebra!

Set up

Let R be a commutative ring with $1 \neq 0$. All matrices will be square matrices with entries from R.

Warm up (#1)

Compute the determinants of the following 2×2-matrices:

1) $\det \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix} = 6 - 2 = 4$

2) $\det \begin{bmatrix} 3 & 1 \\ 0 & 1 \end{bmatrix} = 3$

3) $\det \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = 1$

4) $\det \begin{bmatrix} 1 & 3 \\ 0 & 0 \end{bmatrix} = 0$

Linear Algebra

Definition

For an $n \times n$ matrix $A = [a_{i,j}]$, let $A_{i,j}$ denote the $(n-1) \times (n-1)$ submatrix of A obtained by deleting the i-th row and j-th column of A. We call

$$(-1)^{i+j} \det(A_{i,j})$$

the i,j-**th cofactor of** A, and we denote the i,j-th cofactor by $\alpha_{i,j}$. The $n \times n$ matrix $[\alpha_{i,j}]^T = [\alpha_{j,i}]$ is the **adjoint of** A, denoted $\mathrm{adj}(A)$.

Example

Given the matrix

$$A = \begin{bmatrix} 1 & 3 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{bmatrix},$$

find $A_{2,1}$ and the $2,1$-th cofactor $\alpha_{2,1}$.

$$A = \begin{bmatrix} 1 & 3 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{bmatrix}.$$

$$A = \begin{bmatrix} 1 & 3 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{bmatrix}.$$

$$A_{2,1} = \begin{bmatrix} 3 & 1 \\ 0 & 1 \end{bmatrix}$$

$$\alpha_{2,1} = (-1)^{1+2} \det \begin{bmatrix} 3 & 1 \\ 0 & 1 \end{bmatrix} = -3$$

$$\operatorname{adj}(A) = \begin{bmatrix} 2 & \overbrace{-3}^{\alpha_{2,1}} & 4 \\ 0 & 1 & -2 \\ 0 & 0 & 2 \end{bmatrix}$$

Cramer's Rule

Theorem

Let $A = [a_{i,j}]$ *be an* $n \times n$*-matrix. Then* $\mathrm{adj}(A) \cdot A = \det(A) \cdot I_n$ *where* I_n *is the* $n \times n$ *identity matrix.*

Proof sketch.

The key ideas are

- shuffling around columns,
- cofactor expansion, and
- properties of the determinant.

$\square$

Corollary

If $\det(A)$ *is a unit in* R*, then* $A^{-1} = \frac{1}{\det(A)} \mathrm{adj}(A)$*.*

Warm up (#2)

Consider the complex numbers, $\mathbb{C}$. What is a **vector space**?

- The set of vectors over $\mathbb{C}$ should form an (additive) abelian group:
  - additive identity: $0 + v = v = v + 0$;
  - additive inverses: $v - v = 0 = -v + v$;
  - associativity: $v + (w + u) = (v + w) + u$;
  - commutativity: $v + w = w + v$.
- Scalar multiplication should distribute in the following ways:
  - over vector addition: $\alpha(v + w) = \alpha v + \alpha w$;
  - over $\mathbb{C}$ addition: $(\alpha + \beta)v = \alpha v + \beta v$.
- Compatibility of multiplication: $\alpha(\beta v) = (\alpha\beta)v$.
- The identity of $\mathbb{C}$ should act sensibly: $1v = v$.

Modules

An R-module M is an (additive) abelian group with a map $R \times M \to M$ via $(r, m) \mapsto r * m$ satisfying

(i) $(r + s) * m = r * m + s * m$,

(ii) $r * (m + n) = r * m + r * n$,

(iii) $r * (s * m)) = (r \cdot s) * m$, and

(iv) $1 * m = m$.

Example

Let $R = \mathbb{Z}$ and $M = \mathbb{Q}$. Define $r * m = rm$: $2 * 2 = 4$, $2 * \frac{9}{28} = \frac{18}{28} = \frac{9}{14}$. Then M is an R-module.

Example

Let $R = \mathbb{Z}$ and $M = \mathbb{Q} \times \mathbb{Q}$. Define $r * (q_1, q_2) = (rq_1, rq_2)$. Then M is an R-module.

A **submodule** $N \subseteq M$ is a subset of M satisfying $N \neq \varnothing$ and $m + r * n \in N$ for all $r \in R$ and $m, n \in N$.

Example

For $R = \mathbb{Z}$ and $M = \mathbb{Q}$ with the action defined earlier, $\mathbb{Z} \subseteq \mathbb{Q}$ is a submodule of $\mathbb{Q}$.

Example

If I is an ideal of R, we define a useful submodule by

$$IM := \left\{ \sum_{\text{finite}} a_i m_i \,\middle|\, a_i \in I,\ m_i \in M \right\}.$$

If M is a finitely generated R-module, we write

$$M = Rx_1 + \cdots + Rx_n.$$

We say $x_1, \ldots, x_n$ **generate** M and we call each x_i a **generator**. Given any element $m \in M$, we may write $m = r_1x_1 + \cdots + r_nx_n$.

Example

For $R = \mathbb{Z}$, the module $M = \mathbb{Z} \times \mathbb{Z}$ is generated by $(1, 0)$ and $(0, 1)$. The module $N = \mathbb{Q}$ is not finitely generated as a $\mathbb{Z}$-module.

Example

Is $\mathbb{Q}$ a finitely generated $\mathbb{Q}$-module? Prove or disprove (email solutions to s-cgibbon5@math.unl.edu).

Let M and N be R-modules. An R-**module homomorphism** is a map $f : M \to N$ such that $f(0) = 0$, $f(m+n) = f(m) + f(n)$ and $f(r *_M m) = r *_N f(m)$ for all $m, n \in M$ and $r \in R$.

Example

Let $R = \mathbb{Z}$ and let $M = \mathbb{Q} \times \mathbb{Q}$ and $N = \mathbb{Q}$. Define $f : M \to N$ by $f((q_1, q_2)) = q_1$. This defines a module homomorphism.

Finitely Generated Modules and Homomorphisms

Theorem

For a finitely generated R-module $M = Rx_1 + \cdots + Rx_n$, any homomorphism is uniquely determined by its action on the generators of M.

Proof.

Suppose $\phi : M \to M$ is an R-module homomorphism. Identify $\{a_{i,j}\}_{i,j=1}^{n}$ so that $\phi(x_i) = a_{i,1}x_1 + \cdots + a_{i,n}x_n$. Then for $m = r_1x_1 + \cdots r_nx_n$, we have

$$\begin{aligned}
\phi(m) &= \phi(r_1x_1 + \cdots + r_nx_n) = r_1\phi(x_1) + \cdots + r_n\phi(x_n) \\
&= r_1\left(\sum_{j=1}^{n} a_{1,j}x_j\right) + \cdots + r_n\left(\sum_{j=1}^{n} a_{n,j}x_j\right) = s_1x_1 + \cdots s_nx_n.
\end{aligned}$$

$\square$

We call $[a_{i,j}]$ the **matrix of** ϕ.

The Determinant Trick: Set Up

The key players will be

1. a finitely generated R-module $M := Rx_1 + \cdots + Rx_n$,
2. a module homomorphism $\phi : M \to M$,
3. an ideal $I \subseteq R$ satisfying $\phi(M) \subseteq IM$,
4. the related matrix of ϕ given by

$$[a_{i,j}]_{n\times n}$$

   where $\phi(x_i) = a_{i,1}x_1 + \cdots + a_{i,n}x_n$ and the $a_{i,j} \in I$ for all $0 \leq i, j \leq n$, and
5. the matrix $A = I_n - [a_{i,j}]_{n\times n}$ where I_n is the $n \times n$ identity matrix:

$$A = \begin{bmatrix} 1 - a_{1,1} & -a_{1,2} & \cdots & -a_{1,n} \\ -a_{2,1} & 1 - a_{2,2} & \cdots & -a_{2,n} \\ \vdots & & & \vdots \\ -a_{n,1} & -a_{n,2} & \cdots & 1 - a_{n,n} \end{bmatrix}.$$

The Determinant Trick!

Exploit Cramer's Rule applied to A. (Simple, huh?)

Nakayama's Lemma

"The Guiding Principle of the Universe"

Theorem

Let M be a finitely generated R-module and I an ideal of R. If $M = IM$, then there exists $\omega \in I$ such that $(1 + \omega)m = 0$ for all $m \in M$.

Proof.

- Write $M = Rx_1 + \cdots + Rx_n$. Construct $[a_{i,j}]$ with entries in I so that $x_i = a_{i,1}x_1 + \cdots + a_{i,n}x_n$ for $1 \leq i \leq n$. Define $A = I_n - [a_{i,j}]$.
- For $m = r_1x_1 + \cdots + r_nx_n$, the homomorphism defined by A gives

$$m \mapsto \sum_{i=1}^{n} \left(r_i x_i - r_i(a_{i,1}x_1 + \cdots + a_{i,n}x_n) \right).$$

$$m \mapsto r_1x_1 - r_1x_1 + \cdots + r_nx_n - r_nx_n = 0.$$

- Make a vector $\underline{x_i} = [0, \ldots, x_i, 0, \ldots, 0]$. Note $A\underline{x_i} = \underline{0}$. So $\operatorname{adj}(A)A\underline{x_i} = \underline{0}$.
- Cramer's rule says

$$\begin{bmatrix} \det(A) & 0 & 0 & \cdots & 0 \\ 0 & \det(A) & 0 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & \cdots & 0 & 0 & \det(A) \end{bmatrix} \begin{bmatrix} 0 \\ \vdots \\ x_i \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \det(A) I_n \underline{x_i} = \underline{0},$$

  so $\det(A)x_i = 0$ for $1 \leq i \leq n$.
- So, $\det(A)m = 0$ for all $m \in M$. Expanding $\det(A)$, we get $\det A = 1 + \sum(\text{stuff in } I)$.

Wait a minute! That's not the NAK I know!

Theorem (Ex 14.11, *Topics in Commutative Ring Theory*)

Let R be a commutative ring with $1 \neq 0$ and let J be the Jacobson radical of R. Let M be a finitely generated R-module. If $JM = M$, then $M = 0$.

Proof Sketch.

- Write $M = Rx_1 + \cdots + Rx_n$.
- Use the determinant trick to find $\omega \in J$ so that $(1 + \omega)M = 0$.
- Do Ex 14.10: If $\omega \in J$, then $1 + \omega$ is a unit in R.
- Notice that $(1 + \omega)x_i = 0$ implies that $x_i = 0$ for all generators of M.
- Conclude that $M = 0$.

□

Quick application of NAK

Theorem

Suppose M is a finitely generated R-module, and suppose $f : M \to M$ is a surjective module homomorphism. Then f is an isomorphism.

Proof.

- Let x be an indeterminate and define an action of $R[x]$ on M by $r * m = r * m$ for all $r \in R$ and $x * m = f(m)$. (I like to think of this as the *indeterminate trick*.)
- Show injectivity: $f(m) = 0$ implies $m = 0$.
- Let $I = (x)$; notice $M = IM$.
- NAK: there exists $\omega = hx \in I$ such that $(1 + hx)M = 0$.
- If $f(m) = 0$, then

$$0 = (1 + hx)m = 1m + hxm = m + hf(m) = m.$$

□

Integral Closure

Let $R \subseteq S$ be commutative rings with 1. We say $t \in S$ is **integral over** R if there is a monic polynomial

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \in R[x]$$

such that $f(t) = 0$.

Theorem

If $R \subseteq S$ are rings and S is a finitely generated R-module, then every element of S is integral over R.

Proof.

Write $S = Rs_1 + \cdots + Rs_n$ and let $t \in S$. Then $ts_i = \sum a_{i,j} s_j$ where $a_{i,j} \in R$. We can apply the determinant trick to obtain

$$\underbrace{t^n + r_1 t^{n-1} + \cdots + r_{n-1} t + r_n}_{\det(tI_n - [a_{i,j}])} = 0,$$

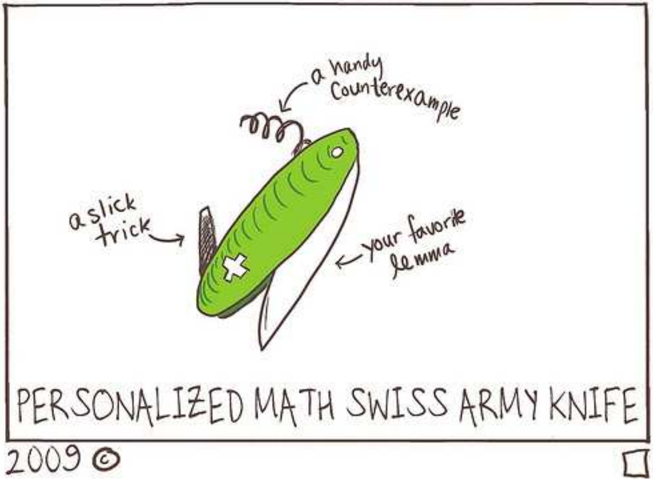
where $r_i \in R$. $\square$

The End - For Now...

References

- Huneke & Swanson, *Integral Closure of Ideals, Rings, and Modules*
- Matsumura, *Commutative Ring Theory*
- Watkins, *Topics in Commutative Ring Theory*

Thanks, CC!


a handy counterexample
a slick trick
your favorite lemma
PERSONALIZED MATH SWISS ARMY KNIFE
2009 ©