A determinant-free proof in basic commutative algebra

Andrei Sipoş

Abstract

In this short note, we give an alternative, determinant-free proof of a theorem usually proven by way of the Cayley-Hamilton theorem for finitely generated modules over a commutative ring.

This note has a slightly convoluted history. I first figured out the argument below in May 2013, during my master's degree, but I gave the handwritten notes to a professor of mine, so they were promptly lost. I then reconstructed the ideas from memory in October 2015 and wrote them up in LaTeX, in the form of this note. Occasionally, over the next few years, I tried to get it published in journals which accepted short expository notes, but it got rejected every time. In June 2020, I cleaned it up a bit when I presented the proof to an online seminar. I have now (July 2026) decided to make the note public on my website.

There is a basic result in commutative algebra which associates to any endomorphism φ of a finitely generated module M over a ring A such that $\varphi(M) \subseteq IM$, where I is an ideal of A (it can be A itself), a polynomial in $A[X]$ that φ satisfies in the ring $A'[\varphi] \subseteq End_A(M)$. Since its usual proof uses a generalized Cayley-Hamilton theorem for modules, the theorem is named either the "determinant trick" (see e.g. [3, p. 43]) or even "Cayley–Hamilton" (see [2, Theorem 4.3]). Applications of it include Nakayama's lemma (in its local and generalized form) and a crucial lemma in the basic theory of integral extensions. Given that the Nakayama lemmas are frequently proven using more elementary arguments, it is reasonable to ask whether that proof method can be extended to the general result. Below, we give an affirmative answer to the question, from which we hope the exposition of integral extensions will primarily benefit – in that context, as far as we know, this kind of argument has not yet appeared anywhere else in the literature.

If A is a commutative ring and M an A-module, we denote by A' the image of the morphism of rings $A \to End_A(M)$, which takes an element $a \in A$ to multiplication by a. Then for any $\varphi \in End_A(M)$, the ring $A'[\varphi]$ is commutative; from now on, all identities involving a $\varphi \in End_A(M)$ will be considered in $A'[\varphi]$.

The usual proof of the statement requires the generalized Cayley-Hamilton theorem, which we now state and prove.

Theorem 1 (Generalized Cayley-Hamilton Theorem)**.** *Let A be a commutative ring, M be a finitely generated A-module and $\varphi : M \to M$ an endomorphism of M. Let $\{m_1, \ldots, m_n\}$ be a set of generators for M. Let $\{a_{ij}\}_{1 \leq i,j \leq n} \subseteq A$ be such that for each $i \in \{1, \ldots, n\}$,*

$$\varphi(m_i) = \sum_{j=1}^{n} a_{ij} m_j.$$

Set $F := (\delta_{ij}\varphi - a_{ij})_{1 \leq i,j \leq n}$. Then $\det F = 0$.

Proof. We have that for each $i \in \{1, \ldots, n\}$,

$$\sum_{j=1}^{n} (\delta_{ij}\varphi - a_{ij}) m_j = 0. \tag{1}$$

Let $B := (b_{ki})_{1 \leq k,i \leq n}$ be the adjugate matrix of F, such that for any k, $j \in \{1, \ldots, n\}$ we have that

$$\sum_{i=1}^{n} b_{ki}(\delta_{ij}\varphi - a_{ij}) = (\det F)\delta_{kj},$$

so, for any k, $j \in \{1, \ldots, n\}$,

$$\sum_{i=1}^{n} b_{ki}(\delta_{ij}\varphi - a_{ij})m_j = (\det F)\delta_{kj}m_j.$$

Summing out over j, we obtain, for any $k \in \{1, \ldots, n\}$, that

$$\sum_{i=1}^{n} b_{ki} \sum_{j=1}^{n} (\delta_{ij}\varphi - a_{ij})m_j = (\det F) \sum_{j=1}^{n} \delta_{kj}m_j.$$

The left hand side of the above is 0, from (1), so, for any $k \in \{1, \ldots, n\}$,

$$0 = (\det F)m_k,$$

therefore $\det F \in A'[\varphi]$ is the zero endomorphism. □

We may now state the main theorem and give its usual proof.

Theorem 2 ("the determinant trick")**.** *Let A be a commutative ring, I an ideal of A, M be a finitely generated A-module and $\varphi : M \to M$ an endomorphism of M. Suppose that $\varphi(M) \subseteq IM$.*

Then there exist an $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in A$ such that for any $i \in \{1, \ldots, n\}$, $a_i \in I$ and $\varphi^n + a_1\varphi^{n-1} + \ldots + a_{n-1}\varphi + a_n = 0$.

Proof. Let $\{m_1, \ldots, m_n\}$ be a set of generators for M. Since $\varphi(M) \subseteq IM$, there are $\{a_{ij}\}_{1 \leq i,j \leq n} \subseteq I$ such that for each $i \in \{1, \ldots, n\}$,

$$\varphi(m_i) = \sum_{j=1}^{n} a_{ij}m_j.$$

Set $F := (\delta_{ij}\varphi - a_{ij})_{1 \leq i,j \leq n}$. Applying Theorem 1, "$\det F = 0$" provides the required identity. □

An immediate corollary is the following one.

Corollary 3. *Let A be a commutative ring, I an ideal of A and M a finitely generated A-module. Suppose that $IM = M$.*

Then there is an $x \in A$ such that $x - 1 \in I$ and $xM = 0$.

Proof. We apply Theorem 2 for $\varphi := id_M$. We get that $(1 + b)id_M = 0$, where $b := \sum_{i=1}^{n} a_i \in I$. Take $x := 1 + b$. □

From here, the usual Nakayama lemma follows.

Lemma 4 (Nakayama)**.** *Let A be a local ring with maximal ideal $\mathfrak{m}$ and M a finitely generated A-module. Suppose that $\mathfrak{m}M = M$.*

Then $M = 0$.

Proof. We apply Corollary 3 for $I := \mathfrak{m}$. Then there is an $x \in A$ with $x - 1 \in \mathfrak{m}$ and $xM = 0$. Since $1 \notin \mathfrak{m}$, we get that $x \notin \mathfrak{m}$, so x is invertible. Then $M = x^{-1}xM = x^{-1}0 = 0$. □

The Nakayama lemma also has the following generalized form.

Lemma 5 (Generalized Nakayama Lemma)**.** *Let A be a commutative ring, I an ideal of A and M a finitely generated A-module. Suppose that $IM = M$.*

Then $I + Ann_A(M) = A$.

Proof. This statement can be easily seen as an equivalent formulation of Corollary 3.

Assume first Corollary 3. We get that there is an $x \in A$ such that $x - 1 \in I$ and $xM = 0$, so $x \in Ann_A(M)$. Then $1 = -(x - 1) + x \in I + Ann_A(M)$.

Assume now the Generalized Nakayama Lemma. Then there are elements $x \in Ann_A(M)$ and $y \in I$ such that $x + y = 1$. So $xM = 0$ and $x - 1 = -y \in I$. □

A separate application is the following basic property of integral extensions.

Lemma 6. *Let $A \subseteq B$ be commutative rings and $y \in B$. Suppose that there is a ring C such that $A[y] \subseteq C \subseteq B$ and C is a finitely generated A-module.*

Then y is integral over A.

Proof. Apply Theorem 2 for $A := A$, $I := A$, $M := C$ and $\varphi : C \to C$ defined for any $x \in C$, by $\varphi(x) := yx$.

We get that there is an $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in A$ such that and the relation

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

holds in $A'[\varphi] \subseteq End_A(C)$. Evaluating the map above in $1 \in C$, we obtain that

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

which was what we sought to show. □

To our knowledge, there is no proof in the literature, direct or indirect, of Lemma 6 that avoids the use of determinants. However, the usual Nakayama lemma is given in some textbooks the following alternative, determinant-free proof.

Proof of Lemma 4. Let $\{m_1, \ldots, m_n\}$ be a set of generators for M.

Since $m_1 \in M = \mathfrak{m}M$, there are $\{b_k\}_{k=1}^n \subseteq \mathfrak{m}$ such that

$$m_1 = \sum_{k=1}^{n} b_k m_k,$$

so

$$(1 - b_1)m_1 = \sum_{k=2}^{n} b_k m_k.$$

Since $b_1 \in \mathfrak{m}$, $1 - b_1$ is invertible, so

$$m_1 = \sum_{k=2}^{n} (1 - b_1)^{-1} b_k m_k.$$

Therefore $\{m_2, \ldots, m_n\}$ is also a set of generators for M. By induction, we get that $\emptyset$ is a set of generators for M, so $M = 0$. □

A more general form of the argument above has been used – see [1, Lemma 1.7] – to prove the Generalized Nakayama Lemma (Lemma 5). We reproduce it below.

Proof of Lemma 5. Let $\{m_1, \ldots, m_n\}$ be a set of generators for M.

We set for any $i \in \{1, \ldots, n+1\}$, $M_i := \langle (m_j)_{j=i}^n \rangle$. Then

$$M = M_1 \supseteq \ldots \supseteq M_n \supseteq M_{n+1} = 0.$$

We construct, for any $i \in \{1, \ldots, n+1\}$, an $a_i \in I$ such that $(1 - a_i)M \subseteq M_i$.

For $i = 1$, take $a_i = a_1 := 0$. Then $(1 - a_i)M = M \subseteq M = M_1$. Suppose now that we have constructed $a_1, \ldots, a_i$. Then

$$(1 - a_i)M = (1 - a_i)IM = I(1 - a_i)M \subseteq IM_i.$$

In particular, $(1 - a_i)m_i \in IM_i$, so there are $\{b_k\}_{k=i}^n \subseteq I$ such that

$$(1 - a_i)m_i = \sum_{k=i}^{n} b_k m_k,$$

so

$$(1 - a_i - b_i)m_i = \sum_{k=i+1}^{n} b_k m_k \in M_{i+1}.$$

In particular, we get that $(1-a_i-b_i)M_i \subseteq M_{i+1}$. Take now

$$a_{i+1} := 2a_i + b_i - a_i^2 - a_i b_i \in I.$$

We have that $1-a_{i+1} = (1-a_i-b_i)(1-a_i)$, so

$$(1-a_{i+1})M = (1-a_i-b_i)(1-a_i)M \subseteq (1-a_i-b_i)M_i \subseteq M_{i+1}.$$

Now that we have finished the construction, we get that $(1-a_{n+1})M \subseteq M_{n+1} = 0$, so $1-a_{n+1} \in Ann(M)$, so

$$1 = a_{n+1} + (1-a_{n+1}) \in I + Ann(M),$$

which was what we sought to show. □

We are now ready to give our determinant-free proof for Theorem 2, adapting the argument from [1] reproduced above.

Proof of Theorem 2. Let $\{m_1, \ldots, m_n\}$ be a set of generators for M.

We set for any $i \in \{1, \ldots, n+1\}$, $M_i := \langle (m_j)_{j=i}^n \rangle$. Then

$$M = M_1 \supseteq \ldots \supseteq M_n \supseteq M_{n+1} = 0.$$

We construct, for any $i \in \{1, \ldots, n+1\}$, a $P_i \in A[X]$ such that $P_i(\varphi)M \subseteq M_i$.

For $i = 1$, take $P_i = P_1 := 1$. Then $P_1(\varphi)M = M \subseteq M = M_1$. Suppose now that we have constructed $P_1, \ldots, P_i$. Then

$$P_i(\varphi)\varphi M \subseteq P_i(\varphi)IM = IP_i(\varphi)M \subseteq IM_i.$$

In particular, $(P_i(\varphi)(\varphi(m_i)) \in IM_i$, so there are $\{b_k\}_{k=i}^n \subseteq I$ such that

$$(P_i(\varphi)(\varphi(m_i)) = \sum_{k=i}^{n} b_k m_k,$$

so

$$(P_i(\varphi)\varphi - b_i)m_i = \sum_{k=i+1}^{n} b_k m_k \in M_{i+1}.$$

In particular, we get that $(P_i(\varphi)\varphi - b_i)M_i \subseteq M_{i+1}$. Take now

$$P_{i+1} := (P_i X - b_i)P_i.$$

We obtain that

$$P_{i+1}(\varphi)M = (P_i(\varphi)\varphi - b_i)P_i(\varphi)M \subseteq (P_i(\varphi)\varphi - b_i)M_i \subseteq M_{i+1}.$$

Now that we have finished the construction, we get that $P_{n+1}(\varphi)M \subseteq M_{n+1} = 0$, so $P_{n+1}(\varphi) = 0$ in $A'[\varphi]$. We want to take this P_{n+1} as the polynomial in the statement. To do that, we have to check that the leading coefficient is 1 and the remaining ones are in I. The first fact is directly seen from the recursive formula above. To prove the last fact, write, for an arbitrary i, P_i as $X^m + \sum_{i=0}^{m-1} a_i X^i$ and suppose by induction that all a_i's are in I. (For P_1 there is nothing to check.) Thus $P_{i+1} = (X^{m+1} + \sum_{i=1}^{m} a_{i-1}X^i - b_i)(X^m + \sum_{i=0}^{n-1} a_i X^i)$ and we get that its non-leading coefficients are in I. □

We finally comment that the procedure above gives a polynomial of degree significantly much larger than the proof using determinants. If n is the cardinality of a set of generators for M, then the determinant proof gives us a polynomial of degree n. To compute the degree of the polynomial obtained by the algorithm in our proof, note that $\deg P_1 = 0$ and for any i, $\deg P_{i+1} = (\deg P_i + 1) + \deg P_i = 2\deg P_i + 1$. Solving this recurrence, we get that $\deg P_i = 2^{i-1} - 1$. The final polynomial is P_{n+1}, which has degree $2^n - 1$.

References

[1] F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings*. Lecture Notes in Mathematics, Vol. 181. Springer-Verlag, Berlin-New York, 1971.

[2] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*. Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.

[3] M. Reid, *Undergraduate commutative algebra*. London Mathematical Society Student Texts, 29. Cambridge University Press, Cambridge, 1995.