The many faces of Nakayama's Lemma

rapha • 24 Feb 2025

In this article, I want to discuss four versions of Nakayama's Lemma, ranging from quite algebraic to quite geometric. I'll prove that the first version is true, and then show that all versions are logically equivalent.

As usual, all rings are commutative with unit.

> **Nakayama's Lemma (I).** Let M be an A-module of finite type and let $\mathfrak{i}$ be an ideal of A such that $M = \mathfrak{i}M$. Then there exists an element $x \in A$ such that $xM = 0$ and $x \equiv 1 \pmod{\mathfrak{i}}$. (Equivalently, there exists an element $y \in \mathfrak{i}$ that acts on M as the identity, i.e. $ym = m$ for all $m \in M$.)

Proof. Write $g_1, g_2, \ldots, g_n$ for the generators for M. The equation $M = \mathfrak{i}M$ implies that for each of those, there's an equation

$$g_i = \sum_{j=1}^{n} c_{ij} g_j,$$

where the c_{ij} are elements of $\mathfrak{i}$. By writing C for the square matrix (c_{ij}) and g for the vector consisting of the generators, we can conveniently rewrite all of these equations at once in a single matrix equation:

$$(I - C)g = 0.$$

Here I is the identity matrix of the appropriate size. Recall that for any square matrix X has an *adjugate matrix* $\mathrm{adj}(X)$ whose entry at (j, i) is the determinant of the submatrix obtained by removing the i-th row and the j-th column, times $(-1)^{i+j}$. In other words, the adjugate matrix is the transpose of the cofactor matrix. Laplace expansion says that we always have the relation

$$\mathrm{adj}(X)X = \det(X)I.$$

In our case, therefore, we have

$$\mathrm{adj}(I - C)(I - C)g = \det(I - C)g = 0.$$

From this we see the element $x = \det(I - C) \in A$ anihilates all of the generators g_i. Hence x anihilates the whole of M, that is, $xM = 0$. Notice that the expansion of the determinant gives a polynomial with constant term 1, and all other monomials products of elements in $\mathfrak{i}$. Therefore, when passing to the quotient $A/\mathfrak{i}$, all that's left of x is 1.

Given such an x, one can choose $y = 1 - x$ which is an element of $\mathfrak{i}$ and which verifies $ym = (1 - x)m = m - xm = m$ for all $m \in M$. On the other hand, given such an y, one can choose $x = 1 - y$, so that $x \equiv 1 \bmod \mathfrak{i}$ and $xm = (1 - y)m = m - m = 0$ for all $m \in M$. ■

Notice this proof is constructive: not only does it assert the existence of the element x, but it gives us a receipe to actually construct it. Let's see a concrete example. Take $M = (\mathbb{Z}/4\mathbb{Z})[i]$ the gaussian integers mod 4, seen as a $\mathbb{Z}$-module. This is finitely generated by the elements $\{1, i\}$. For the ideal, choose $3\mathbb{Z}$. For any element $a + bi$ of M, we can write it as $9a + 9bi$ since $9 \equiv 1 \bmod 4$. Therefore, $M = (3\mathbb{Z})M$. In fact, $1 = 9 \cdot 1$ and $i = 9 \cdot i$, so our matrix C above looks like $9I$, which is nine times the identity matrix. Therefore the element x we're after is $\det(-8I)$, which is 64. And indeed, $64M = 0$ while $64 \equiv 1 \bmod 3$.

> **Nakayama's Lemma (II).** Let M be an A-module of finite type and let $\mathfrak{i}$ be an ideal of A such that $M = \mathfrak{i}M$. If $\mathfrak{i}$ is contained in the Jacobson radical $J(A)$ of A, then $M = 0$.

Proof that (I) ⇒ (II). Recall that the Jacobson radical $J(A)$ is the intersection of all maximal ideals in the ring. In this context, notice that any element $x \equiv 1 \bmod \mathfrak{i}$ is invertible in A. To see this, suppose it is not. Then the principal ideal (x) is contained in some maximal ideal $\mathfrak{m}$, and so $\mathfrak{i} \subseteq \mathfrak{m}$. Therefore $x \equiv 1 \bmod \mathfrak{m}$, which is a contradiction with $x \in \mathfrak{m}$. Now Nakayama's Lemma (I) guarantees the existence of an element $x \equiv 1 \pmod{\mathfrak{i}}$ such that $xM = 0$. We've just shown that x must be invertible, whence $M = 0$.

> **Nakayama's Lemma (III).** Let M be an A-module of finite type, let N be a submodule, and let $\mathfrak{i}$ be an ideal of A which is contained in the Jacobson radical $J(A)$ of A. If $N/\mathfrak{i}N \to M/\mathfrak{i}M$ is surjective, then $M = N$.

Proof that (II) ⇒ (III). Notice that $M = N$ if and only if $M/N = 0$. The reason I'm pointing this out is because that looks like the conclusion of (II); the quotient of a module of finite type by any submodule is also of finite type (hint: being of finite type means there's a surjection $A^n \to M$ for some integer n), so

we reduced to problem to showing the equality of A-modules $M/N = \mathfrak{i}(M/N)$. Let m be any element of M. From the surjectivity hypothesis, there exists an element $n \in N$ such that $n + \mathfrak{i}M = m + \mathfrak{i}M$. In particular, we have $m \in n + \mathfrak{i}M$ so there exists an integer $k \geq 0$ and elements $i_1, \ldots, i_k \in \mathfrak{i}$ and $m_1, \ldots, m_k \in M$ such that

$$m = n + i_1 m_1 + \cdots + i_k m_k.$$

Passing m to the quotient M/N, we find $m + N \in \mathfrak{i}(M/N)$. Since m was arbitrary, this shows *any* element of M/N is in $\mathfrak{i}(M/N)$. ■

> **Nakayama's Lemma (IV).** Let M be an A-module of finite type, with $(A, \mathfrak{m})$ being a local ring, so $M/\mathfrak{m}M$ is a finite-dimensional vector space over $A/\mathfrak{m}$. Let $f_1, f_2, \ldots, f_n$ be elements of M such that their images in $M/\mathfrak{m}M$ form a basis. Then these elements form a minimal set of generators for M.

Proof that (III) $\Rightarrow$ (IV). Let N be the submodule of M generated by the f_i's. From (III), we simply have to show that $N/\mathfrak{m}N \to M/\mathfrak{m}M$ is a surjective morphism. But this is obvious! ■

I'll come back later and add more explanations and examples.