



HAL
open science

Nakayama's lemma and applications

Rodney Coleman, Laurent Zwald

► **To cite this version:**

| Rodney Coleman, Laurent Zwald. Nakayama's lemma and applications. 2020. hal-03040587

HAL Id: hal-03040587

<https://hal.science/hal-03040587v1>

Preprint submitted on 4 Dec 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Nakayama's lemma and applications

Rodney Coleman, Laurent Zwald

December 4, 2020

Abstract

We give two versions of Nakayama's lemma in the context of commutative rings and some applications, in particular, we prove two versions of Krull's intersection theorem. To do so, we will use the Artin-Rees lemma, for which we will give a detailed proof. We will suppose that all rings are commutative with identity.

There are various closely related results all of which bear the name Nakayama's lemma. Here we will prove two such results.

Nakathml

Theorem 1 (*Nakayama's lemma version 1*) *Let R be a ring, M a finitely generated module over R and I an ideal in R , with $IM = M$. Then there exists $a \in I$ such that $(1 - a)M = 0$.*

PROOF Let x_1, \dots, x_m be generators of M over R . Since $M = IM$, each x_i may be written $x_i = \sum_{j=1}^m z_{ij}x_j$, with $z_{ij} \in I$. In other words, $\sum_{j=1}^m (\delta_{ij} - z_{ij})x_j = 0$, where δ_{ij} is the Kronecker symbol. Let d be the determinant of the $m \times m$ matrix $A = (\delta_{ij} - z_{ij})$. We have $d = 1 - a$, where $a \in I$, because all the terms of the matrix A have this form or are elements of I . There exists a matrix $B = (b_{ij})$, the complementary matrix of A , such that $BA = AB = dI_m$. Writing out the terms in the product BA , we have $\sum_{i=1}^m b_{hi}a_{ij} = d\delta_{hj}$, for all h and j . Hence

$$\sum_{j=1}^m \sum_{i=1}^m b_{hi}a_{ij}x_j = \sum_{j=1}^m d\delta_{hj}x_j = dx_h,$$

for every h . However, we may change the order of summation to obtain

$$\sum_{i=1}^m \sum_{j=1}^m a_{ij}x_j b_{hi} = dx_h.$$

Given that $\sum_{j=1}^m a_{ij}x_j = 0$, because $a_{ij} = \delta_{ij} - z_{ij}$, we obtain that $dx_h = 0$, for all h ; this implies that $dM = 0$, as required. \square

In a commutative ring R the Jacobson radical $J(R)$ is the intersection of all maximal ideals of R . An element $a \in R$ is quasi-regular if $1 - a$ is a unit.

Proposition 1 *The Jacobson radical $J(R)$ is the largest ideal in R consisting entirely of quasi-regular elements.*

PROOF Let $a \in J(R)$. If $1 - a$ is not a unit, then $(1 - a)$ is a proper ideal contained in a maximal ideal M . But then a and $1 - a$ are both contained in M , which implies that 1 belongs to M , which is impossible. Thus $J(R)$ is composed entirely of quasi-regular elements.

Now let I be an ideal composed entirely of quasi-regular elements. If $a \in I \setminus J(R)$, then for some maximal ideal M , a does not belong to M . Since M is maximal, we have $I + M = R$, so $1 = b + c$, with $b \in I$ and $c \in M$. As b is quasi-regular, $c = 1 - b$ is a unit and it follows that 1 belongs to M , which is impossible. Hence $I \subset J(R)$. This concludes the proof. \square

Nakathm2

Theorem 2 (Nakayama's lemma version 2) *Let R be a ring, M a finitely generated R -module and I an ideal of R . If $I \subset J(R)$ and $IM = M$, then $M = \{0\}$.*

PROOF From Theorem [Nakathm1](#), there is an element $a \in I$ such that $(1 - a)M = 0$. As $a \in J(R)$, $(1 - a)$ is invertible, hence $M = 0$. \square

We give a second proof of Theorem [Nakathm2](#):

PROOF Assume that $M \neq \{0\}$ and let x_1, \dots, x_n be generators of M , with n minimal. Then $n > 0$ and $x_i \neq 0$, for all i . Since $x_n \in M = IM$, we may write $x_n = \sum_{i=1}^m b_i y_i$, with $b_i \in I$ and $y_i \in M$. Each y_i can be expressed in terms of the generators x_1, \dots, x_n : $y_i = \sum_{j=1}^n a_{ij} x_j$, with $a_{ij} \in R$. Hence

$$x_n = \sum_{i=1}^m b_i \left(\sum_{j=1}^n a_{ij} x_j \right) = \sum_{j=1}^n \left(\sum_{i=1}^m a_{ij} b_i \right) x_j = \sum_{j=1}^n c_j x_j,$$

where $c_j \in I$. From this we obtain

$$(1 - c_n)x_n = \sum_{j=1}^{n-1} c_j x_j,$$

where $1 - c_n$ is a unit, because I is included in the Jacobson radical. If $n > 1$, then x_n is a linear combination of the other x_i , contradicting the minimality of n . Hence $n = 1$. But then $(1 - c_n)x_1 = 0$, which implies that $x_1 = 0$, which is again a contradiction. Therefore $M = \{0\}$. \square

Here is a first application of Nakayama's lemma. A surjective endomorphism of a finite-dimensional vector space is always injective. We have an analogous result for a finitely generated module over a ring.

Theorem 3 *Let R be a ring and M a finitely generated R -module. If f is a surjective endomorphism of M , then f is injective.*

PROOF Let R be a ring, M a finitely generated R -module and $f : M \rightarrow M$ a surjective endomorphism. We make M into an $R[X]$ -module by setting $P(X) \cdot m = P(f)(m)$. M is finitely generated over R , hence over $R[X]$: If m_1, \dots, m_k are generators of M over R and $m \in M$, then there exist $r_1, \dots, r_k \in R$ such that $m = r_1 m_1 + \dots + r_k m_k$. If $P_i(X)$ is the constant polynomial of value r_i , then

$$P_1(X) \cdot m_1 + \dots + P_k(X) \cdot m_k = r_1 m_1 + \dots + r_k m_k = m,$$

so the m_i form a set of generators of M over $R[X]$.

Let $I = (X) \subset R[X]$. Then

$$I \cdot M = R[X]X \cdot M = R[f]f(M) \subset M.$$

However, if $m \in M$, then there exists $m' \in M$ such that $f(m') = m$, because f is surjective. Also, $1 \in R[X]$, so $m \in R[f]f(M)$ and it follows that $R[f]f(M) = M$. From Theorem [Nakathm1](#), there exists $Q(X)X \in I$ such that $(1 - Q(X)X) \cdot M = 0$, i.e., $m = Q(f)f(m)$, for all $m \in M$. If $f(m) = 0$, then

$$m = Q(f)f(m) = 0,$$

so f is injective. □

We now turn to Krull's intersection theorem, where once again we will use Nakayama's lemma. We need a preliminary result.

Nakalem1

Lemma 1 (Artin-Rees) *Let I be an ideal in a noetherian ring R , M a finitely generated R -module and N a submodule of M . Then there exists a positive integer c such that, for $n \geq c$,*

$$I^n M \cap N = I^{n-c}(I^c M \cap N).$$

PROOF Consider the set

$$S = R \oplus I \oplus I^2 \oplus \cdots = \bigoplus_{n \geq 0} I^n,$$

where $I^0 = R$. We recall that in a direct sum S , if $(a_0, a_1, \dots) \in S$, then all but a finite number of the a_i are nonzero. We define an addition and a multiplication on S as for polynomials, using the fact that $I^m I^n \subset I^{m+n}$. With these operation S is a ring. As R is noetherian, I is finitely generated, so we may write $I = (r_1, \dots, r_t) \subset R$. We define a mapping $\phi : R[X_1, \dots, X_t] \rightarrow S$ by

$$\phi(X_1^{e_1} \cdots X_t^{e_t}) = r_1^{e_1} \cdots r_t^{e_t} \in I^{e'_t},$$

where $e'_t = \max\{e_1, \dots, e_t\}$. The mapping ϕ is clearly a ring homomorphism. However, ϕ is also surjective: An element $a \in I^n$ is a sum of products of the form $a_1 \cdots a_n$, with $a_i \in I$. We may write $a_i = \sum_{j=1}^t a_{ij} r_j$, with $a_{ij} \in R$, so $a_1 \cdots a_n$ is a sum of monomials of the form $br_1^{e_1} \cdots r_t^{e_t}$, with $b \in R$ and $e_1 + \cdots + e_t = n$. As $\phi(br_1^{e_1} \cdots r_t^{e_t}) = br_1^{e_1} \cdots r_t^{e_t}$, there exists $f \in R[X_1, \dots, X_t]$ such that $\phi(f) = a$. It now follows easily that ϕ is surjective, so there is an isomorphism of $R[X_1, \dots, X_t]/\ker(\phi)$ onto S . Hence S is noetherian.

We now consider the set A defined by

$$A = M \oplus IM \oplus I^2 M \oplus \cdots = \bigoplus_{n \geq 0} I^n M.$$

We define an addition on A in a natural way and a scalar multiplication by elements of S in a way analogous to that used to define the multiplication defined on S , once again using the fact that $I^m I^n \subset I^{m+n}$. With these operations A is an S -module. We claim that A is finitely generated: Let m_1, \dots, m_s be a generating set of M . If $u \in I^n M$, then u is a sum of terms of the form am , where $a \in I^n$ and $m \in M$.

As we saw above, the element a is a sum of monomials of the form $br_1^{e_1} \cdots r_t^{e_t}$, with $b \in R$ and $e_1 + \cdots + e_t = n$; also, $m = v_1 m_1 + \cdots + v_s m_s$, with $v_i \in R$. Therefore am is a sum of elements of the form $(br_1^{e_1} \cdots r_t^{e_t})v_j m_j$. Collecting terms, we find that am can be written in the form $c_1 m_1 + \cdots + c_s m_s$, where $c_i \in I^n$ and it follows that a term $u \in I^n M$ has this form. Any element of A is a finite sum of elements of this form with different values of n , so the set m_1, \dots, m_s generates A over S , thus A is finitely generated as claimed.

Our next step is to consider the subset $B = \bigoplus_{n \geq 0} (I^n M \cap N)$ of A . We claim that B is an S -submodule of A . It is sufficient to consider the scalar product of a set I^n with a set $I^m M \cap N$. We must show that this product is included in B . An element of I^n is a sum of monomials of the form $br_1^{e_1} \cdots r_t^{e_t}$, with $b \in R$ and $e_1 + \cdots + e_t = n$. As such monomials belong to R and N is an R -submodule, the scalar product of $br_1^{e_1} \cdots r_t^{e_t}$ with an element of $I^m M \cap N$ must belong to B . It follows that B is an S -submodule of A .

Since S is a noetherian ring and A finitely generated, B must be finitely generated. Let ξ_j , $j = 1, \dots, k$, be a set of generators. By decomposing each ξ_j into its homogeneous parts, we may assume that each ξ_j belongs to $I^{d_j} M \cap N$, for some d_j . We set $c = \max\{d_j\}$. Suppose now that $x \in I^n M \cap N$. There exist $u_1, \dots, u_k \in S$ such that $x = u_1 \xi_1 + \cdots + u_k \xi_k$. The term $u_j \xi_j$ belongs to $I^n M \cap N = I^{n-d_j} (I^{d_j} M \cap N)$, so there exists $u'_j \in I^{n-d_j}$ and $m_j \in I^{d_j} M \cap N$ such that $u_j \xi_j = u'_j m_j$. Now $m_j = v_{j,1} \xi_1 + \cdots + v_{j,k} \xi_k$, with the $v_{j,i} \in S$. Since $m_j \in I^{d_j} M \cap N$, we must have $m_j = a \xi_j$, with $a \in R$, and it follows that $u_j \xi_j = \tilde{u}_j \xi_j$, with $\tilde{u}_j \in I^{n-d_j}$. From this we deduce that $x = \sum_{j=1}^k \tilde{u}_j \xi_j$, with $\tilde{u}_j \in I^{n-d_j}$ and $\xi_j \in I^{d_j} M \cap N$. However,

$$n - d_j = n - c + c - d_j \implies I^{n-d_j} (I^{d_j} M \cap N) = I^{n-c} (I^{c-d_j} I^{d_j} M \cap N) = I^{n-c} (I^c M \cap N)$$

and it follows that $x \in I^{n-c} (I^c M \cap N)$.

We have established that $I^n M \cap N \subset I^{n-c} (I^c M \cap N)$. The inclusion $I^{n-c} (I^c M \cap N) \subset I^n M \cap N$ is trivial, therefore we have the desired equality. \square

Nakacor1

Corollary 1 *Let R be a noetherian ring and I, J ideals in R . Then there exists $c \in \mathbf{N}^*$ such that*

$$I^n \cap J = I^{n-c} (I^c \cap J),$$

for $n \geq c$.

PROOF It is sufficient to set $M = R$ in the Artin-Rees lemma \square **Nakalemi**

We now aim to prove two versions of Krull's intersection theorem. We will use the corollary to the Artin-Rees lemma and both versions of Nakayama's lemma.

Theorem 4 *Let R be a noetherian integral domain and I a proper ideal in R . Then $\bigcap_{n=1}^{\infty} I^n = (0)$.*

PROOF Let $J = \bigcap_{n=1}^{\infty} I^n$. From Corollary \square **Nakacor1** there exists $c \in \mathbf{N}^*$ such that

$$I^n \cap J = I^{n-c} (I^c \cap J),$$

for $n \geq c$. Setting $n = c + 1$ we obtain

$$I^{c+1} \cap (\bigcap_{n=1}^{\infty} I^n) = I (I^c \cap (\bigcap_{n=1}^{\infty} I^n)),$$

i.e.,

$$\bigcap_{n=1}^{\infty} I^n = I (\bigcap_{n=1}^{\infty} I^n).$$

As R is noetherian, the ideal $J = \bigcap_{n=1}^{\infty} I^n$ is finitely generated. From Nakayama's lemma version 1 (Theorem \square **Nakathmi**), there exists $a \in I$ such that $(1 - a)J = (0)$. As I is a proper ideal, we have $a \neq 1$, so $1 - a \neq 0$. If $x \in J$, then $(1 - a)x = 0$; as R is an integral domain, we must have $x = 0$. \square

We now suppose that the ring R is not necessarily an integral domain but impose another condition.

Theorem 5 *Let R be a noetherian ring and I an ideal included in the Jacobson radical $J(R)$. Then $\bigcap_{n=1}^{\infty} I^n = (0)$.*

PROOF We proceed as in the proof of the previous theorem to show that

$$\bigcap_{n=1}^{\infty} I^n = I(\bigcap_{n=1}^{\infty} I^n).$$

We now apply Nakayama's lemma version 2 (Theorem ^{Nakathm2}2) to obtain $J = (0)$. □

Corollary 2 *Let (R, M) be a noetherian local ring. Then $\bigcap_{n=1}^{\infty} M^n = (0)$.*

PROOF It is sufficient to notice that in this case the Jacobson radical is M . □