Formalizing Commutative Algebra in Coq: Nakayama's Lemma*

Andrew Cousino
`acousino@ku.edu`

Emily E. Witt†
`witt@ku.edu`

Perry Alexander
`palexand@ku.edu`

Institute for Information Sciences
The University of Kansas
Lawrence, KS 66045

To do: Add to/alter author list, funding acknowledgments, title, and/or abstract as needed

Abstract

We describe our formal proof of Nakayama's Lemma, a fundamental theorem in the mathematical field of commutative algebra. The statement and proof of this result involve several commutative-algebraic structures including commutative rings, ideals of these rings, and modules over them, and we also explain our process of formalizing these structures.

Keywords: Formalization of Mathematics, Formal Proof, Commutative Algebra, Commutative Ring, Local Ring, Ideal, Module over a Ring, Finitely Generated Module.

1 Introduction

The mathematical field of *commutative algebra* stems from the study of solutions to polynomial equations. Research in the field now centers around *commutative rings*—rings in which order does not affect multiplication, i.e., $x \cdot y = y \cdot x$ for any ring elements x and y—and fundamental algebraic objects associated to them: *ideals* of these rings, and *modules* over them. Commutative algebra has deep connections with other areas of theoretical mathematics, including number theory and algebraic geometry.

Commutative algebra also has broad applications to science and technology. For instance, it has been integral to advances in robotics [7], and has helped form our current understanding of the human genome [13]. The commutative-algebraic notion of a Gröbner basis, a special type of generating set for an ideal in a ring of polynomials, has become a fundamental computational tool in coding theory and cryptography (e.g., see [14]). A implementation of Buchberger's algorithm [4] for determining Gröbner bases of ideals in polynomial rings has been proved correct within the proof assistant Coq [5, 15], and an integrated formal development of the algorithm in Coq has also been carried out [12] (see also [6]).

Our goal is to newly formalize theoretical, rather than computational, commutative algebra in Coq. We formally prove *Nakayama's Lemma* [11, 3], an essential result in the field. In doing so, we formalize algebraic structures that are fundamental to higher-level algebra, such as *local rings* and *modules over commutative rings*, and *quotient rings and modules*. Rather than build upon some of the basic objects from abstract algebra, such as groups and rings, that have been formalized in Coq, e.g., in the *Mathematical Components*

Library [1], we start from scratch. The theory, including the formalization of all algebraic structures, makes up approximately 100 kB and 3300 lines of code.

To do: Verify whether MathComp only formalized finite algebraic structures. Drew is about as certain as he can be that this is the case.

The notion of a module over a ring is an extension of the linear-algebraic notion of a vector space over a field, ubiquitous in mathematics and its applications. Less frequently referred to as the *Krull-Azumaya theorem* [1] [10], Nakayama's Lemma describes one way that a finitely generated module over an arbitrary commutative ring acts like a vector space over a field. True to the convention that "lemma" often refers to a result serving as a stepping stone toward another goal, Nakayama's Lemma is applied widely throughout the field, and the result is typically introduced in a first graduate course in commutative algebra [2, 9, 8].

2 Mathematical Basis and Motivation

2.1 The Fundamental Algebraic Structures

Here, we give a brief description of the major mathematical structures from commutative algebra that are relevant to Nakayama's Lemma.

Emily: It would be more consistent to require a ring to contain 1 in general, instead of adding this to the axioms of a commutative ring. After thinking for a while, I think it is a good idea to make this change in the code, and then here to match. Drew, does this sound OK?

Commutative rings. In abstract algebra, the quintessential example of a commutative ring is the set of integers

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

using the natural definitions of addition and multiplication.

Adding two integers produces another, and the associative and commutative laws hold for addition. The integers form an *abelian group* under addition since $0 \in \mathbb{Z}$ is the *additive identity* in the sense that adding zero has no effect on any integer, and given any integer n, the integer $-n$ is its *additive inverse* in the sense that the sum of n and $-n$ is the additive identity 0.

The set of integers also forms a *ring* due to its properties of multiplication. It is closed under this binary operation, which satisfies associativity, and the distributive law governing the compatibility of addition and multiplication holds. Even more, the integers form a *commutative ring* since $n \cdot m = m \cdot n$ for all integers n and m. We require commutative rings to contain a *multiplicative identity*, and $1 \in \mathbb{Z}$ is such an element since $n \in \mathbb{Z}$ one has $n \cdot 1 = 1 \cdot n = n$.

In general, a commutative ring is a set R with two binary operations, which we call *addition* and *mutiplication*, typically denoted $\cdot$ and $+$, respectively. As motivated by the properties of the ring of integers, addition, R must be an abelian group, multiplication must be associative, R must have a multiplicative identity, and the distributive law must hold, i.e., for all $r, s, t \in R$, $(r + s) \cdot t = r \cdot t + s \cdot t$ and $r \cdot (s + t) = r \cdot s + r \cdot t$.

Other familiar examples of commutative rings include the integers modulo a fixed integer $n > 0$, fields—commutative rings in which every nonzero element has a multiplicative inverse—such as the rings of rational numbers, real numbers, and complex numbers, and rings of polynomials in a variable x with integer coefficients, or with coefficients in a field.

*Source code for this work is available on the following site: https://github.com/ku-sldg/algebra

†Witt acknowledges support from NSF CAREER Award DMS-1945611 and the 2022-23 Ruth I. Michler Memorial Prize from the Association for Women in Mathematics.

[1] Hideyuki Matsumura explains in his text *Commutative Algebra* [9]: "This simple but important lemma is due to T. Nakayama, G. Azumaya, and W. Krull. Priority is obscure, and although it is usually called the Lemma of Nakayama, late Prof. Nakayama did not like the name."

Ideals of commutative rings. The concept of an ideal of a ring can be thought of as an extension of the notion of an integer x in the ring of integers $\mathbb{Z}$. An *ideal* of commutative ring R is a subset I of R that is itself an abelian group under addition, which also satisfies the following "absorption" property: Given any element a of I, the product $x \cdot a$ is again in I for any ring element $x \in R$.

One can verify that given any integer n, the set $n\mathbb{Z}$ of its multiples forms an ideal of $\mathbb{Z}$. For instance, $2\mathbb{Z}$ consists of all even numbers, and is an abelian group under addition: the sum of two even numbers is even, the additive identity 0 is even, and the negative of an even number is even. Moreover, the absorption property holds since the product of any integer and an even number is again even. In fact, every ideal of the ring of integers has this form $n\mathbb{Z}$ for some integer n, though ideals in general commutative rings can have more complicated properties.

Since every integer n can be written as $1 \cdot n$, the ideal $1\mathbb{Z}$ is the entire ring $\mathbb{Z}$. One can see that given a commutative ring R itself satisfies the axioms required to be an ideal of R. We call an ideal I of R *proper* if it is strictly contained in R. The *zero ideal* consisting solely of its additive identity is a proper ideal of any commutative ring.

A *maximal ideal* of a commutative ring is a proper ideal that is maximal with respect to inclusion, i.e., no other proper ideal strictly contains it. Returning to our example of the ring of integers, $6\mathbb{Z} \subsetneq 2\mathbb{Z}$ since every multiple of 6 is even, so $6\mathbb{Z}$ is not a maximal ideal of $\mathbb{Z}$. However, no proper ideal I contains $2\mathbb{Z}$: If $2\mathbb{Z} \subsetneq I \subsetneq \mathbb{Z}$, then I would necessarily contain an odd number n. Writing $n = 2k + 1$ for some integer k, we notice that since $-2k$ is in $2\mathbb{Z}$, it is also an element of the larger set I, and since I is an abelian group under addition, $(2k + 1) + (-2k) = 1$ is also in the ideal I. However, in this case, every integer $n = n \cdot 1$ is in I by absorption, so $I = \mathbb{Z}$ is not a proper ideal, a contradiction.

In fact, $3\mathbb{Z}$ is the only other maximal ideal of $\mathbb{Z}$ containing $6\mathbb{Z}$, and in general, the prime ideals in the ring of integers besides the zero ideal are those of the form $p\mathbb{Z}$, where p a prime number.

Local rings. A commutative ring is *local* if it has exactly one maximal ideal. Every field is local since the only proper ideal of a field is the zero ideal, though by our observations above, the ring of integers is not local. However, the set of all rational numbers that can be written with an odd denominator does form a subring of all rational numbers, and its unique maximal ideal consists of the elements with even numerator; in fact, this ring is the so-called *localization* of $\mathbb{Z}$ at the maximal ideal $2\mathbb{Z}$. The ring of integers modulo $n > 1$ is local if and only if n is a power of a prime number p, in which case the unique maximal ideal consists of all multiples of p.

The ring of polynomials over a field F in a variable x is not local; in fact, given any irreducible polynomial $f(x)$, the set of its multiples is a maximal ideal of the polynomial ring $F[x]$. On the other hand, the set of all formal power series in x over F is a local ring; its maximal ideal consists of the power series with no constant term.

Module over commutative rings. Let R be a commutative ring. A *module over* R, or R*-module*, is an abelian group M under a binary operation $+$, and a scalar multiplication $R \times M \to M$ denoted $\cdot$, satisfying the following compatibility properties for all $r, s \in R$ and $u, v \in M$.

1. $r \cdot (u + v) = r \cdot u + r \cdot v$
2. $(r + s) \cdot u = r \cdot u + s \cdot u$
3. $(rs) \cdot u = r \cdot (s \cdot u)$
4. $1 \cdot u = u$

From this definition, one can see that a module over a field F is precisely an F-vector space, so the notion of a module over an arbitrary commutative ring extends that of a vector space over a field. Finitely generated vector spaces form the foundation for matrix algebra, and the extension of this notion to module theory is needed to state Nakayama's Lemma. We call an R-module M *finitely generated* if there exist a fixed finite number of elements $u_1, \ldots, u_n$ of M with the following property: Given any $w \in M$, there exist $r_1, \ldots, r_n \in R$ for which

$$w = r_1 u_1 + r_1 u_2 + \cdots + r_n u_n.$$

The set $\{u_1, \ldots, u_n\}$ is called a *generating set* for the M as an R-module.

When $R = F$ is a field and $M = V$ is a finite-dimensional vector space over F, one can choose $u_1, \ldots, u_n$ to be a basis for V, i.e., $n = \dim V$. In this case, the choice of scalar coefficients in the expression above for $w \in V$ is unique. When R is not a field, however, such an expression is typically not unique.

2.2 Nakayama's Lemma, Informal Statement

In order to state Nakayama's Lemma, we first explain some notation: If I is an ideal of a commutative ring R and M is an R-module, then IM is the set of elements of the form $a_1 u_1 + a_2 u_2 + \cdots + a_k u_k$, where, for some positive integer k, $a_1, \ldots, a_k \in I$ and $u_1, \ldots, u_k \in M$. Notice that due to the absorption property of ideals, IM is an R-module contained in M.

If an R-module M consists of only one element, this element must be its additive identity 0 as an abelian group under addition. The notation $M = 0$ means that we are in this situation.

Nakayama's Lemma. *Let R be a commutative local ring, and let $\mathfrak{m}$ denote its unique maximal ideal. If M is a finitely generated R-module and $M = \mathfrak{m}M$, then $M = 0$.*

When $R = F$ is a field, its unique maximal ideal is the zero ideal, and given any vector space $M = V$ over F, the only linear combination of vectors with coefficients in the zero ideal is the zero vector. Hence in this special case, the hypothesis that $M = \mathfrak{m}M$ is equivalent to the conclusion that $M = 0$. Hence Nakayama's Lemma describes one way that finitely generated modules over commutative local rings are similar to vector spaces.

In general, the quotient $R/\mathfrak{m}$ of a local ring modulo its maximal ideal $\mathfrak{m}$ is a field, and the quotient of a module M modulo the submodule $\mathfrak{m}M$ is an $R/\mathfrak{m}$-module, i.e., $M/\mathfrak{m}M$ is a vector space over $R/\mathfrak{m}$. Nakayama's Lemma implies that if M is finitely generated, then bases for $M/\mathfrak{m}M$ corresponds, via lifting, to minimal sets of generators of M.

We point out that there are alternate statements of Nakayama's Lemma that do not require the hypothesis that R must be local. One can replace the unique maximal ideal with the Jacobson radical of the ring, which is the intersection of all maximal ideals. Alternatively, I is an arbitrary proper ideal of a commutative ring R and M is a finitely generated R-module for which $M = IM$, then this ensures the existence of a ring element r congruent to 1 modulo I such that $rM = 0$, i.e., $ru = 0$ for every $u \in M$.

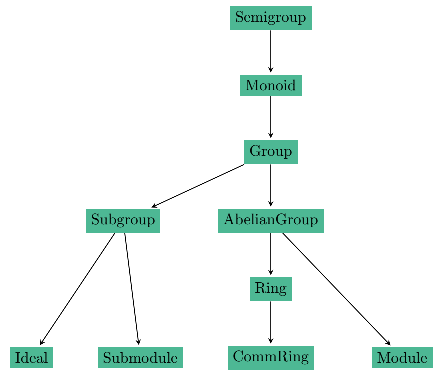
3 Formalization

We start by describing our process of formalizing the required algebraic structures detailed in the previous section. Then, with that in hand, we move on to the formal proof of Nakayama's Lemma.

3.1 Our Algebraic Hierarchy

To do: Double check source code to verify whether the hierarchy figure should be altered (subobjects, quotients, finitely generated modules, local rings, etc.) It looks good to Drew.

Figure 3.0.1: The hierarchy of our algebraic structures



Our foundation begins by defining a semigroup class, which declares a binary operation to be associative. From here, we build up through monoids, which introduce identities, to groups, which introduce inverses. Note the double equals "==" appearing in these definitions is notation for an arbitrary equivalence relation over the group's carrier set, which acts as equality.

```
Infix "==" := equiv (at level 60, no associativity).
Class Semigroup := {
  semigroup_assoc:
    forall (a b c: Carrier),
      a <o> b <o> c == a <o> (b <o> c);
}.
Class Monoid := {
  monoid_semigroup :> Semigroup equiv op;
  monoid_ident_l:
    forall (a: Carrier), ident <o> a == a;
  monoid_ident_r:
    forall (a: Carrier), a <o> ident == a;
}.
Class Group := {
  group_monoid :> Monoid equiv op ident;
  group_inv_l:
    forall (a: Carrier), inv a <o> a == ident;
  group_inv_r:
    forall (a: Carrier), a <o> inv a == ident;
}.
```

Lines such as "`monoid_semigroup :> Semigroup equiv op;`" simply coerce the monoid typeclass into a semigroup.

While in the end, our formal proof did not call upon quotients of algebraic structures, quotient rings and quotient modules are fundamental to commutative algebra, and one can use them to construct alternate proofs of Nakayama's Lemma. It is worth pointing out that we have formalized quotients of algebraic objects in Coq using typeclasses, which appear to work rather nicely.

An algebraic quotient is, roughly, the set of equivalence classes of an algebraic structure with respect to an equivalence relation on its elements, for which the set of equivalence classes inherit the same kind of algebraic structure. For example, consider the quotient of a group modulo a subgroup, i.e., a subset of elements of the group that it itself a group under the group operations. Under equivalence relation on the group, every element of the subgroup must be in the same equivalence class as the identity. With P the predicate for the subgroup, there are two ways to make an equivalence relation from this description.

```
Definition left_congru (a b: Carrier) :=
  P (inv a <o> b).
Definition right_congru (a b: Carrier) :=
  P (a <o> inv b).
```

When these two relations coincide, then we can prove that this common equivalence relation actually preserves the group structure. Subgroups which have this property are called *normal subgroups*.

```
Let normal_subgroup_congru_coincide :=
  forall (a b: Carrier),
    left_congru op inv P a b <->
    right_congru op inv P a b.

Theorem quotient_normal_subgroup_group:
  normal_subgroup_congru_coincide ->
  Group (left_congru op inv P) op ident inv.
```

The importance of quotients in commutative algebra motivates our use of equivalence relations to define the components of a group structure. If one were to instead use the regular Leibniz equality, it would be very difficult to identify a quotient group with another group. However, by defining a group in terms of an arbitrary equivalence relation, we enable our theory to state that a quotient group is simply a group under a different equivalence. Not much is lost, as Coq's setoid rewrite tactics can still be called upon; a setoid is a type equipped with an equivalence relation.

Moving onward, we formalized the structure of a ring, which has two binary operations: addition, which must be commutative, and multiplication, which need not be commutative in general. Next we defined the structure of a commutative ring, further requiring commutativity of multiplication, as well as a multiplicative identity. At this point, we formalized the notion of an ideal of a commutative ring, a subgroup of the ring under addition that satisfies the absorption property under multiplication, i.e., ra is in the ideal for every element a of the ideal, and every element r of the commutative ring. We also used this to formalize the notion of a quotient ring R/I, where I is an ideal of a commutative ring R.

It would be nice to differentiate between our structures that are typeclasses (e.g., `Ideal`), and other definitions (e.g., `maximal ideal`)

Next, we formally defined a maximal ideal, a proper ideal that are maximal with respect to inclusion, i.e., if it is strictly contained in another ideal, this larger ideal must be the entire ring. Below is the definition in Coq, which uses P as the predicate for the ideal.

```
Definition maximal_ideal :=
  exists (r: Carrier), (not (P r) /\
    forall (Q: Carrier -> Prop)
        (Q_proper: Proper (equiv ==> iff) Q)
        (Q_ideal: Ideal add zero minus mul Q),
      (forall (r: Carrier), P r -> Q r) ->
      (forall (r: Carrier), Q r) \/
        (forall (r: Carrier), Q r -> P r)).
```

Using the definition of a maximal ideal, we then were able to define a local ring, i.e., a commutative ring with a single maximal ideal.

```
Definition local_ring :=
  exists (P: Carrier -> Prop)
      (P_proper: Proper (equiv ==> iff) P)
      (P_ideal: Ideal add zero minus mul P),
    maximal_ideal P /\
    (forall (Q: Carrier -> Prop)
        (Q_proper: Proper (equiv ==> iff) Q)
        (Q_ideal: Ideal add zero minus mul Q),
      maximal_ideal Q -> forall (r: Carrier), P r <-> Q r).
```

Emily: Unfortunately, I think we need to update naming conventions since in mathematics, "vector" is reserved for an element of a vector space over a field, rather than an element of an arbitrary module. So this could cause confusion. Similar with "basis," which is especially tricking since two different generating sets of a finitely generated module can have different sizes, but all bases of a vector space have the same cardinality, and an element of a module can typically be written as a scalar combination in multiple ways, while bases are linearly independent. I've proposed a rewrite of the blue paragraph right above it. Drew, can you double check it for accuracy with respect to the code?

We'll also need to update the code. I think `vectors` should be something like `scalar-combinations`, and `basis` something like `generating-set`.

At this point we formalized the definition of a module over a commutative ring, the commutative-algebraic generalization of the notion of a vector space over a field. Nakayama's Lemma is a statement about finitely generated modules, and hence we must formalize the notion of a scalar combination of a fixed finite collection of elements $u_1, \ldots, u_n$ of an R-module M, i.e., expressions of the form $r_1 u_1 + r_1 u_2 + \cdots + r_n u_n$, where each $r_i \in R$.

In our formalization of scalar combinations, we use "list" to mean length-parameterized lists; since we don't use the simpler kind of lists, there are no name collisions. In our code, `M` is the type of module elements, `R` is the type of ring elements, act as coefficients, and `t A n` is a list whose elements are of type `A` and whose length is `n`.

Here we needed to formalize the notion of linear combinations of coefficients and module vectors. This was done by dependently typed vectors, i.e., lists parameterized by their length. Because there is an overload of the term "vector", we will use that term to refer to module vectors, and use the term "list" to mean length-parameterized lists. As we don't use the simpler kind of lists, this avoids any name collisions. A finitely generated module is like the vector space $\mathbf{R}^n$ in that there are finitely many vectors which can generate all other vectors, for $\mathbf{R}^n$ one such collection of generators are $\mathbf{e}_1 = \begin{pmatrix}1 & 0 & 0 & \cdots & 0\end{pmatrix}^T$, $\mathbf{e}_2 = \begin{pmatrix}0 & 1 & 0 & \cdots & 0\end{pmatrix}^T$, ..., $\mathbf{e}_n = \begin{pmatrix}0 & 0 & 0 & \cdots & 1\end{pmatrix}^T$. In our code, `M` is the type of module elements, `R` is the type of ring elements which act as coefficients, and `t A n` is a list whose elements are of type `A` and whose length is `n`.

```
Definition finitely_generated {n: nat}(basis: t M n) :=
  forall (vector: M),
    exists (coeffs: t R n),
      vector =M= linear_combin coeffs basis.
```

Next, given an ideal I of a commutative ring R and and an R-module M, we defined the submodule IM, the set consisting of all scalar combinations of elements of M whose coefficients are in I. We represented this in Coq as a predicate over M.

```
Context (P: R -> Prop).
Context {P_proper: Proper (Requiv ==> iff) P}.
Context {P_ideal: Ideal Radd Rzero Rminus Rmul P}.
```

```
Definition ideal_module (x: M): Prop :=
  exists (n: nat)(coeffs: t R n)(vectors: t M n),
    Forall P coeffs /\
    x =M= linear_combin Madd Mzero action coeffs vectors.
```

The use of "`Forall P coeffs`" ensures that every element of the coefficient list `coeffs` satisfies the predicate `P`.

3.2 Building the Formal Proof

Beyond formalizing the relevant structures from higher algebra, we also formally establish some basic theory. For instance, a *unit* of a commutative ring R is an element $x \in R$ with a multiplicative inverse, i.e., an element $x^{-1} \in R$ for which $x \cdot x^{-1}$ is the multiplicative identity $1 \in R$.

We formally proved that an ideal I of a commutative ring R that contains a unit x, then I must be the trivial ideal, i.e., the entire ring. The informal logic is as follows: By the absorption property, since $x \in I$, we have that $x \cdot x^{-1} = 1 \in I$. Hence for every element r of R, $r = r \cdot 1$ is also in I, i.e., $I = R$.

Every non-unit element of a commutative ring is contained in some maximal ideal. This fact relies on the Axiom of Choice. The following standard informal proof calls upon Zorn's lemma, which is equivalent to the Axiom of Choice, and says that given a partially ordered set S, if every chain in S has an upper bound, then S must have at least one maximal element.

> Set I_1 to be the principal ideal generated by an element x of a commutative ring R, i.e. the smallest ideal containing the element x, which consists of all R-multiples of x.
>
> If I_1 is not a maximal ideal, then there exists a strictly larger proper ideal I_2 of R, i.e., $x \in I_1 \subsetneq I_2 \subsetneq R$. Moreover, if I_2 is not maximal, then there exists a strictly larger proper ideal $I_3 \supsetneq I_2$.
>
> Continuing this process, if it terminates at some step, we have found a maximal ideal, and if not, one obtains an infinite chain of ideals containing x.
>
> $$x \in I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots \subsetneq R$$
>
> It is straight-forward to show that $\bigcup_{k=1}^{\infty} I_k$ satisfies the definition of an ideal of R, and this union certainly contains x. So by Zorn's lemma, since every ascending chain of ideals containing x with respect to inclusion has its union as an upper bound, there exists a maximal ideal of R containing x.

This argument has potentially infinitely many steps, and chose to avoid this issue by including an axiom that in any non-unit x is contained in some maximal ideal.

Include some relevant code

We also used classical logic to prove that $1 - x$ is a unit where x is a non-unit in any local ring. The proof used the rule $\neg\neg P \to P$ in order to do a proof by contradiction.

Include some relevant code

Finally, we turn to our formal proof of Nakayama's Lemma, our ultimate goal.

Nakayama's Lemma. *Let R be a commutative local ring, and let $\mathfrak{m}$ denote its maximal ideal. Suppose that M is a finitely generated R-module. If $M = \mathfrak{m}M$, then $M = 0$, i.e., M must be the R-module containing only one element, its identity as an additive abelian group.*

We needed a lemma before moving on to prove the main theorem which states that for a finitely generated R-module M with generating set $b_1, b_2, \ldots, b_n$, any element $x \in IM$, where I is an ideal of R, can be written as a linear combination of the generating set with coefficients coming from I. In other words, given $x \in IM$, there is by definition a linear combination between elements $u_1, \ldots, u_m \in I$, and elements $a_1, \ldots, a_m \in M$, we need a lemma that states x can be written as a linear combination between elements of I and the generating set $b_1, \ldots, b_n \in M$. This follows the informal mathematical argument going inductively through the elements needed to generate x and shows that each vector can be rewritten in terms of the generating set times coefficients from the ideal I as follows.

I'm confused: Isn't this how we defined IM? Where are the u's and a's coming from?

$$\begin{aligned} x &= \sum_{k=1}^{m} u_k a_k \\ &= \sum_{k=1}^{m} u_k (r_{k1} b_1 + \cdots + r_{kn} b_n) \\ &= \sum_{j=1}^{n} (u_1 r_{1j} + \cdots + u_m r_{mj}) b_j \end{aligned}$$

Since each u_k comes from the ideal I, the absorbing property of ideals guarantees that $u_k r_{kj}$ is also contained in I. As ideals are also closed under addition, it follows that $u_1 r_{1j} + \cdots + u_m r_{mj}$ are all elements of I. Thus, x can be written as a linear combination of the generating set with the coefficients coming from I.

I think we need to include more code here! There are a lot of pieces of formal proof that would be illustrative.

Now we move to describe the skeleton of our formal proof of Nakayama's lemma. We proceed by induction on the number of elements in a generating set for the finitely-generated module M. The base case where M is generated by 0 elements is by definition true since an empty linear combination is conventionally taken to be the zero vector. The inductive case where M is generated by the vectors $b_1, \ldots, b_m, b_{m+1}$. By assumption $M = \mathfrak{m}M$. With $b_1 \in M$, then $b_1 \in \mathfrak{m}M$ meaning that by our lemma, there exists a linear combination for b_1, say

I think we should consider using one generator for the base case.

$$b_1 = u_1 b_1 + \cdots + u_{m+1} b_{m+1}$$

for some $u_1, \ldots, u_{m+1} \in \mathfrak{m}$. Collect the b_1 terms on the left-hand side of the equation to get that

$$(1 - u_1) b_1 = u_2 b_2 + \cdots + u_{m+1} b_{m+1}.$$

As mentioned when defining maximal ideals, $\mathfrak{m}$ can only contain non-units. Namely, u_1 must be a non-unit. Then we had already proven that $1 - u_1$ is a unit as we are in a local ring. Let v_1 be the multiplicative inverse of $1 - u_1$, and multiply it on both sides of the equation.

$$\begin{aligned} v_1 (1 - u_1) b_1 &= v_1 u_2 b_2 + \cdots + v_1 u_{m+1} b_{m+1} \\ 1 b_1 &= v_1 u_2 b_2 + \cdots + v_1 u_{m+1} b_{m+1} \\ b_1 &= v_1 u_2 b_2 + \cdots + v_1 u_{m+1} b_{m+1} \end{aligned}$$

We have thus found that one of the basis vectors is not needed to generate this module. Using the induction hypothesis, we have that $M = 0$. Showing that the induction hypothesis holds in Coq takes more work than in an informal proof, but this extra work is just a lot of bookkeeping.

References

[1] Mathematical Components Library. https://math-comp.github.io/. Accessed: 2022-11-03. 2

[2] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, economy edition, 2016. For the 1969 original see [MR0242802]. 2

[3] Gorô Azumaya. On maximally central algebras. *Nagoya Math. J.*, 2:119–150, 1951. 1

[4] B. Buchberger. A theoretical basis for the reduction of polynomials to canonical forms. *ACM SIGSAM Bull.*, 10(3):19–29, 1976. 1

[5] The Coq Development Team. The Coq Proof Assistant, October 2019. 1

[6] Thierry Coquand and Henrik Persson. Gröbner bases in type theory. In *Types for proofs and programs (Irsee, 1998)*, volume 1657 of *Lecture Notes in Comput. Sci.*, pages 33–46. Springer, Berlin, 1999. 1

[7] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra. 1

[8] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry. 2

[9] Hideyuki Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series*. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980. 2

[10] Masayoshi Nagata. *Local rings*. Interscience Tracts in Pure and Applied Mathematics, No. 13. Interscience Publishers (a division of John Wiley & Sons, Inc.), New York-London, 1962. 2

[11] Tadasi Nakayama. A remark on finitely generated modules. *Nagoya Math. J.*, 3:139–140, 1951. 1

[12] Henrik Persson. *An Integrated Development of Buchberger's Algorithm in Coq*. PhD thesis, INRIA, 2001. 1

[13] Mary Lynn Reed. Algebraic structure of genetic inheritance. *Bull. Amer. Math. Soc. (N.S.)*, 34(2):107–130, 1997. 1

[14] Massimiliano Sala, Teo Mora, Ludovic Perret, Shojiro Sakata, and Carlo Traverso, editors. *Gröbner bases, coding, and cryptography*. Springer-Verlag, Berlin, 2009. 1

[15] Laurent Théery. A machine-checked implementation of Buchberger's Algorithm. *Journal of Automated Reasoning*, 20:107–137, 2001. 1