WORKSHEET 6.2: EXACTNESS PT. II

Throughout this course, "ring" means *commutative* ring with unity, and all modules are assumed to be modules over the relevant ring. Let R be a ring and let M be an R-module. Recall from the previous worksheets that if $U \subset R$ is a multiplicatively closed set, the localization of M at U is a $U^{-1}R$-module, denoted $U^{-1}M$, which intuitively consists of elements of the form $\frac{m}{u}$ for $m \in M$ and $u \in U$ (up to equivalence). Further, localization is a functor, meaning given a map $\phi : M \to N$ of R-modules we get a map $U^{-1}(\phi) : U^{-1}M \to U^{-1}N$ of $U^{-1}R$-modules. On elements this map is given by $\frac{m}{u} \mapsto \frac{\phi(m)}{u}$. Further, we saw that localization is an exact functor, meaning that it preserves exact sequences.

The goal of this worksheet is to use localization in two complementary ways. First, we will prove the slogan: *exactness can be checked locally*. This means that many questions about kernels, images, injections, surjections, and isomorphisms can be answered after localizing at every prime ideal, or even every maximal ideal. Second, we will show that at least for *finitely generated* modules, many of powerful pieces of linear algebra can imported into module theory.

Recall that for a prime ideal $\mathfrak{p} \subset R$ we write $M_{\mathfrak{p}}$ for the localization of M at the multiplicatively closed set $R \setminus \mathfrak{p}$. If $f \in R$, we write $M[\frac{1}{f}]$ for the localization of M at the multiplicative set $U = \{1, f, f^2, \ldots\}$. The first local criterion is the most basic one: an R-module is zero if and only if it becomes zero after localizing at every point of $\mathrm{Spec}(R)$. The intuition behind this is simple: If $m \in M$ is nonzero, then its annihilator

$$\mathrm{Ann}(m) = \{r \in R \mid rm = 0\}$$

is a proper ideal of R. Choosing a maximal ideal containing $\mathrm{Ann}(m)$ gives a point of $\mathrm{Spec}(R)$ where m cannot disappear after localization. This is the algebraic version of saying that a nonzero object must be visible somewhere locally.

---

(1) **Local Vanishing for Modules.** Let R be a ring and M an R-module. If $\mathscr{S} \subset M$ is any subset, the *annihilator* of $\mathscr{S}$ is the ideal:

$$\mathrm{Ann}_R(\mathscr{S}) := \left\{ r \in R \;\middle|\; rs = 0 \text{ for all } s \in \mathscr{S} \right\}.$$

If $\mathscr{S} = \{m\}$ we write $\mathrm{Ann}_R(m)$ for $\mathrm{Ann}_R(\{m\})$.

(a) If $\mathscr{S} \subset M$ is any subset, prove that $\mathrm{Ann}_R(\mathscr{S})$ is an ideal of R.

(b) Let $\mathfrak{p} \subset R$ be a prime ideal. Given $m \in M$, prove that $m/1 = 0$ in $M_{\mathfrak{p}}$ if and only if there exists $s \in R \setminus \mathfrak{p}$ such that $sm = 0$ in M.

(c) Let M be the zero R-module. Explain why $U^{-1}M = 0$ for any multiplicatively closed subset $U \subset R$.

(d) Prove that $M = 0$ if and only if $M_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m} \subset R$. Hint: One direction should be easy. For the other, suppose $m \neq 0$, choose a maximal ideal containing $\mathrm{Ann}(m)$.

(e) Deduce that $M = 0$ if and only if $M_{\mathfrak{p}} = 0$ for every prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$.

(f) Let $f_1, \ldots, f_n \in R$ generate the unit ideal. Prove that $M = 0$ if and only if $M[\frac{1}{f_i}] = 0$ for every i. Hint: Again, one direction should be straightforward. For the other direction, given $m \in M$, first find powers $f_i^{t_i}$ killing m, then show that the ideal $\langle f_1^{t_1}, \ldots, f_n^{t_n} \rangle$ is the unit ideal.

(g) Let $\phi : M \to N$ be a homomorphism of R-modules. Prove that $\phi = 0$ if and only if $\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is the zero map for every maximal ideal $\mathfrak{m} \subset R$.

(2) **Homology and Localization Commute.** Let R be a ring and consider the complex of R-modules below:

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

Recall this means that $\mathrm{img}(f) \subset \ker(g)$. Define $H := \ker(g)/\mathrm{img}(f)$, which is the homology of this complex at M. Recall that the complex is exact at M if and only if $H = 0$.

(a) Explain why there is a short exact sequence of R-modules shown below. What are the maps?

$$0 \longrightarrow \mathrm{img}(f) \longrightarrow \ker(g) \longrightarrow H \longrightarrow 0$$

(b) Let $U \subset R$ be a multiplicatively closed set. Use exactness of localization and part (a) to show there is an isomorphism:

$$U^{-1}H \cong \frac{\ker(U^{-1}g)}{\mathrm{img}(U^{-1}f)}.$$

(c) Explain why the previous parts prove the slogan: *The homology of the localization is the localization of the homology.*

(d) Deduce that the complex is exact at M if and only if the complex below is exact at $M_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p} \subset R$

$$M'_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} M_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} M''_{\mathfrak{p}}.$$

(e) Prove that it is enough to check exactness after localizing at every maximal ideal.

(f) Suppose $f_1, \ldots, f_n \in R$ generate the unit ideal. Prove that the complex is exact at M if and only if the complex below is exact at $M[\frac{1}{f_i}]$ for every $i = 1, \ldots, n$:

$$M'\left[\tfrac{1}{f_i}\right] \longrightarrow M\left[\tfrac{1}{f_i}\right] \longrightarrow M''\left[\tfrac{1}{f_i}\right].$$

(g) Explain why the previous parts prove the slogan: *exactness can be checked locally.*

(3) **Checking Injectivity & Surjectivity Locally.** Let R be a ring and $\phi : M \to N$ be a homomorphism of R-modules.

(a) Prove that ϕ is injective if and only if $\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective for every maximal ideal $\mathfrak{m} \subset R$. Hint: Apply local vanishing to $\ker(\phi)$.

(b) Prove that ϕ is surjective if and only if $\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is surjective for every maximal ideal $\mathfrak{m} \subset R$. Hint: Apply local vanishing to $\operatorname{coker}(\phi)$.

(c) Deduce ϕ is an isomorphism if and only if $\phi_{\mathfrak{m}}$ is an isomorphism for every maximal ideal $\mathfrak{m} \subset R$.

(d) State and prove the analogous criterion using all prime ideals instead of all maximal ideals.

(e) State and prove the analogous criterion using a finite basic open cover $\operatorname{Spec}(R) = D(f_1) \cup \cdots \cup D(f_n)$.

(f) Let $n \geq 1$ be an integer and consider multiplication by n as a map of $\mathbb{Z}$-modules

$$\mathbb{Z} \xrightarrow{\times n} \mathbb{Z}.$$

For which prime ideals $\langle p \rangle \in \operatorname{Spec}(\mathbb{Z})$ does the localized map become an isomorphism? For which prime ideals is it injective? Surjective?

We now turn to a different technique – seemingly unrelated topic – namely attempting to port-over aspects of linear algebra to the theory of modules. The basic idea is that while a module might not have a basis – recall only free modules do – so long as a module has a finite set of generators many classical identities and facts from linear algebra remain true.

Let us first recall the relevant linear algebra. Let $\mathbb{K}$ be a field, and let A be an $n \times n$ matrix over $\mathbb{K}$. For each pair $1 \leq i, j \leq n$, let $A_{\hat{i},\hat{j}}$ denote the $(n-1) \times (n-1)$ matrix obtained from A by deleting row i and column j. The *cofactor* matrix of A is the $n \times n$ matrix whose (i,j)-th entry is $c_{i,j} \coloneqq (-1)^{i+j} \det(A_{\hat{i},\hat{j}})$. The *adjugate* of A is defined to be $\operatorname{adj}(A) \coloneqq C^{\mathsf{T}}$ where C is the cofactor matrix of A. A standard theorem from linear algebra says that the identity holds for every $n \times n$ matrix A over the field $\mathbb{K}$:

$$A \operatorname{adj}(A) = \operatorname{adj}(A) A = \det(A) \operatorname{Id}_{n \times n}.$$

This identity is often proved using Laplace expansion along rows and columns. It is also the identity behind Cramer's rule. Conceptually, it says that even if A is not invertible, multiplying by $\operatorname{adj}(A)$ turns A into the scalar matrix $\det(A) I_n$. This formula has surprisingly important consequences for the structure of endomorphisms of vector spaces.

One clean way to see this is to do the computation once in the *universal* ring

$$\mathbb{Z}[x_{i,j} \mid 1 \leq i, j \leq n],$$

where $X = (x_{i,j})$ is the generic $n \times n$ matrix whose entries are variables. Every particular matrix over every commutative ring is obtained from X by substituting $x_{i,j} \mapsto a_{i,j}$. Thus a polynomial matrix identity over this polynomial ring can be specialized to any commutative ring. The same universal idea gives a first proof of Cayley–Hamilton over arbitrary commutative rings: If $\chi_A(t) = \det(tI_n - A)$ is the characteristic polynomial of A, then $\chi_A(A) = 0$. For matrices over fields this is a theorem from linear algebra. For

matrices over arbitrary rings, one proves the identity for the generic matrix over the polynomial ring over $\mathbb{Z}$, and then specializes.

Before we prove this we need to extend our definition of an algebra slightly. Let R be a commutative ring. An R-algebra is a ring A together with a specified ring homomorphism $\phi : R \to A$. We think of this as defining a scalar multiplication on A by elements of R by defining $r \cdot a := \phi(r)a$. A morphism of R-algebras $\psi : A \to B$ is a ring homomorphism that preserves scalars, i.e. $\psi(r \cdot 1_A) = r \cdot 1_B$ for every $r \in R$.

---

(4) **Universal Adjugate Formula.** Fix a positive integer n. Let R be a ring and A be an $n \times n$ matrix with entries in R. Define the adjugate matrix of $A = (a_{ij})$ just as one does for matrices over a field. The goal of this exercise is to prove the following identity:

$$A \operatorname{adj}(A) = \operatorname{adj}(A)A = \det(A)\mathrm{Id}_{n\times n}. \tag{1}$$

In this problem let $S = \mathbb{Z}[x_{i,j} \mid 1 \le i, j \le n]$ be the polynomial ring in n^2 variables. Let $X = (x_{i,j})$ be the generic $n \times n$ matrix with entries in S.

(a) Show that an arbitrary ring has a canonical structure of a $\mathbb{Z}$-algebra.

(b) Given an $n \times n$ matrix $A = (a_{i,j})$ with entries in R show that there is a well-defined morphism of $\mathbb{Z}$-algebras:

$$\begin{array}{ccc} S & \xrightarrow{\mathrm{ev}_A} & R \\ x_{i,j} & \longmapsto & a_{i,j} \end{array}.$$

(c) Let $X = (x_{i,j})$ be the generic $n \times n$ matrix whose entries are the variables in S. Assume that (1) holds true for the matrix X. Use the homomorphism ev_A to show the identity holds true for A.

(d) Since S is a domain it embeds into its field of fractions $S \subset \mathrm{Frac}(S)$. Explain why this allows us to view X as a matrix with entries in $\mathrm{Frac}(S)$.

(e) Viola! Conclude the matrix equation (1) holds for arbitrary rings from the corresponding linear algebra fact (over fields). Be sure to check the field case too, if it's not familiar to you. It's easy, if you know about computing determinants by "expanding along a row or column".

(5) **Universal Cayley-Hamilton Theorem.** Fix a positive integer n. Let R be a ring and A be an $n \times n$ matrix with entries in R. Define the *characteristic polynomial* of A to be $\chi_A(t) = \det(tI_n - A) \in R[t]$. The goal of this is to prove the Cayley-Hamilton theorem for rings, namely: $\chi_A(A) = 0$. In this problem let $S = \mathbb{Z}[x_{i,j} \mid 1 \le i, j \le n]$ be the polynomial ring in n^2 variables. Let $X = (x_{i,j})$ be the generic $n \times n$ matrix with entries in S.

(a) Prove the Cayley-Hamilton theorem for the generic matrix X, i.e., $\chi_X(X) = 0$. Hint: Again use that you may embed S into its field of fractions.

(b) Use the specialization map ev_A from the previous problem to prove Cayley–Hamilton for every $n \times n$ matrix A over every commutative ring R.

We now use our universal adjugate formula to prove what is called the *determinant trick*, which allows us to extend the Cayley–Hamilton to endomorphisms of finitely generated modules. Recall an endomorphism of an R-module M is just an R-module homomorphism $\phi : M \to M$.

Theorem 1 (Cayley-Hamilton)**.** *Let R be a ring and $I \subset R$ an ideal. Let M be an R-module that can be generated as an R-module by n elements. Let $\phi : M \to M$ be an endomorphism of M. If $\phi(M) \subset IM$ then there exists a monic polynomial*

$$p(t) = t^n + p_1 t^{n-1} + \cdots + p_{n-1} t + p_n \in R[t]$$

with $p_k \in I^k$, such that $p(\phi) = 0$ as an endomorphism on M.

Before proving the theorem, let us spell out what the notation means. If $\phi : M \to M$ is an endomorphism, then we write $\phi^2 := \phi \circ \phi$, $\phi^3 := \phi \circ \phi \circ \phi$, and, more generally, ϕ^n means the n-fold composition of ϕ with itself. We also set $\phi^0 = \mathrm{Id}_M$. Thus, given a polynomial $p(t) = t^n + p_1 t^{n-1} + \cdots + p_{n-1} t + p_n \in R[t]$ then $p(\phi) = \phi^n + p_1 \phi^{n-1} + \cdots + p_{n-1}\phi + p_n \mathrm{Id}_M$ is in $\mathrm{End}_R(M)$. The equation $p(\phi) = 0$ means that this endomorphism is the zero map; i.e., $p(\phi)(m) = 0$ for all $m \in M$.

There is another useful way to say the same thing. Giving an R-module M together with an endomorphism $\phi : M \to M$ is the same as giving M the structure of an $R[t]$-module extending its original R-module structure. The variable t acts on M by the rule $t \cdot m := \phi(m)$ and $t^k \cdot m = \phi^k(m)$. Therefore, for a polynomial $p(t) \in R[t]$, the action of $p(t)$ on M is exactly the endomorphism $p(\phi)$. With this language, the conclusion $p(\phi) = 0$ says that the polynomial $p(t)$ annihilates M as an $R[t]$-module $p(t) \cdot M = 0$.

The determinant trick constructs such an annihilating polynomial from a finite set of generators of M. The key point is that, although M need not have a basis, the endomorphism ϕ gives us enough "linear equations" among a chosen generating set to apply the adjugate identity.

Let M be generated by $x_1, \ldots, x_n$, let $I \subset R$ be an ideal, and let $\phi : M \to M$ be an endomorphism such that $\phi(M) \subseteq IM$. Since the x_i generate M, we can write

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij} x_j \qquad \text{with} \qquad a_{ij} \in I.$$

These are n linear equations in the generators x_i, but the coefficients include the operator ϕ. The key observation is that scalar multiplication by elements of R commutes with ϕ. Thus the subring $R[\phi] \subseteq \mathrm{End}_R(M)$ generated by scalar multiplications and by ϕ is commutative; equivalently, it is the image of the evaluation map $R[t] \to \mathrm{End}_R(M)$ sending t to ϕ.

Let $A = (a_{ij})$. The equations above may be rewritten as

$$(\phi \,\mathrm{Id}_{n\times n} - A) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

Now the matrix $\phi \mathrm{Id}_{n\times n} - A$ has entries in the commutative ring $R[\phi]$, so the adjugate identity applies. Multiplying by the adjugate matrix shows that $\det(\phi I_n - A)$ kills each generator x_i, and hence kills all of M. Expanding this determinant gives a monic polynomial in ϕ whose non-leading coefficients lie in powers of I. This is the determinant trick.

---

(6) **The Determinant Trick.** Let M be an R-module generated by $x_1, \ldots, x_n$, let $I \subset R$ be an ideal, and let $\phi \in \mathrm{End}_R(M)$ satisfy $\phi(M) \subseteq IM$.

(a) Prove that there exist elements $a_{ij} \in I$ such that

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij} x_j \qquad \text{for every } i = 1, \ldots, n.$$

(b) Let $A = (a_{ij})$ and let $B = \phi I_n - A$, viewed as a matrix with entries in the commutative ring $R[\phi] \subseteq \mathrm{End}_R(M)$. Prove that

$$B \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

(c) Use the identity $\mathrm{adj}(B)B = \det(B) I_n$ to prove that $\det(\phi I_n - A) x_i = 0$ for every i.

(d) Deduce the Cayley-Hamilton theorem stated above.

(7) **Applications of the Cayley–Hamilton Theorem.** Let $A = (a_{ij})$ be an $n \times n$ matrix with entries in R, and let $\phi_A : R^n \to R^n$ be the corresponding R-linear map.

(a) Apply the determinant trick to $M = R^n$, the standard basis $e_1, \ldots, e_n$, $I = R$, and $\phi = \phi_A$. Prove that $\chi_A(\phi_A) = 0$.

(b) Translate the previous statement into the matrix identity $\chi_A(A) = 0$.

(c) Prove that if $A \in \mathrm{Mat}_{n\times n}(R)$ and $\det(A)$ is a unit, then A is invertible. Hint: Use the adjugate matrix.

(d) Prove the converse: if A is invertible, then $\det(A)$ is a unit.

(e) Combine this with the local criterion for isomorphisms to prove that $A : R^n \to R^n$ is an isomorphism if and only if $A_{\mathfrak{p}} : R^n_{\mathfrak{p}} \to R^n_{\mathfrak{p}}$ is an isomorphism for every prime ideal $\mathfrak{p} \subset R$.

(f) Show that the condition in part (e) is equivalent to $\det(A) \notin \mathfrak{p}$ for every prime ideal $\mathfrak{p} \subset R$, and hence to $\det(A)$ being a unit.

(8) **Cayley–Hamilton Computations.** Compute the characteristic polynomial in each case and verify the Cayley–Hamilton identity directly.

(a) $R = \mathbb{Z}$ and $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$.

(b) R is any ring and $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

(c) $R = \mathbb{Z}/6\mathbb{Z}$ and $A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$.

(d) R is any ring, $a, b \in R$, and $A = \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$.

(e) Let A be a 2×2 matrix over R with trace τ and determinant δ. Prove directly that

$$A^2 - \tau A + \delta I_2 = 0.$$

We now get to a series of amazingly powerful results, all of which can roughly be called some version of Nakayama's Lemma. Somewhat annoyingly each of these results will have its own hypothesis and conclusions, however, they all fit into a broad framework: The slogan is: *for finitely generated modules, if nothing remains after reducing modulo a sufficiently small ideal, then there was nothing there to begin with*. We will begin with the most used versions of this lemma before stating it in its most general form.

Lemma 2 (Nakayama's Lemma I)**.** *Let R be a ring and let M be a finitely generated R-module. If $I \subset R$ is an ideal such that $IM = M$ then there exists an element $r \in I$ that acts on M as the identity, i.e.* $(1-r)M = 0$.

Recall that a ring R is local if it has a unique maximal ideal $\mathfrak{m} \subset R$, in which case we denote it by $(R, \mathfrak{m})$. (Note Mel Hochster's notes adopt the somewhat non-standard terminology that a local ring be required to be Noetherian. We, and most commutative algebraists, do not do this.) In this setting, since $\mathfrak{m} \subset R$ is maximal the quotient $\kappa(R) := R/\mathfrak{m}$ is a field, which we call the *residue field* of R. For any ideal $I \subset R$, the quotient module $M/IM \cong M \otimes_R (R/I)$, and so has the structure of an R/I-module. This means that when we specialize to the case when $I = \mathfrak{m}$ the module $M/\mathfrak{m}M$ is isomorphic to $M \otimes_R (R/\mathfrak{m}) = M \otimes_R \kappa(R)$, meaning $M/\mathfrak{m}M$ is a $\kappa(R)$-module, i.e. it is just a vector space over the field $\kappa(R)$!

Lemma 3 ((Local) Nakayama's Lemma II)**.** *Let $(R, \mathfrak{m})$ be a local ring and let M be a finitely generated R-module. If $\mathfrak{m}M = M$ then $M = 0$.*

Lemma 4 ((Local) Nakayama's Lemma III)**.** *Let $(R, \mathfrak{m})$ be a local ring and let M be a finitely generated R-module. A finite set $\{x_1, \ldots, x_n\} \subset M$ is a generating set for M if and only if their images $\{\overline{x}_1, \ldots, \overline{x}_n\}$ span $M/\mathfrak{m}M$ as a vector space over the field $R/\mathfrak{m} = \kappa(R)$.*

While the above lemmas are the most common versions of Nakayama's Lemma one might use in commutative algebra and algebraic geometry. They all are, essentially special cases or corollaries, of a more general version. The *Jacobson radical* of R is

$$\mathrm{Jac}(R) := \bigcap_{\mathfrak{m} \in \mathrm{mSpec}(R)} \mathfrak{m},$$

the intersection of all maximal ideals of R. Note this is not the same thing in general as the nilradical $\sqrt{\langle 0\rangle}$, which is the set of nilpotent elements and is equal to the intersection of all prime ideals of R. If $a \in \mathrm{Jac}(R)$, then $1+a$ is a unit. Indeed, if $1+a$ were not a unit, it would be contained in some maximal ideal $\mathfrak{m}$; since $a \in \mathfrak{m}$ as well, this would force $1 \in \mathfrak{m}$, a contradiction. This observation will lead us to the following general version of Nakayama's Lemma.

Lemma 5 (Nakayama's Lemma IV)**.** *Let R be a ring and let M be a finitely generated R-module. If $I \subset R$ is an ideal such that I is contained in the Jacobson radical of R and $IM = M$ then $M = 0$.*

A brief historical aside: Like most results, a number of versions of Nakayama's lemma appeared before Tadashi Nakayama stated it in its now-familiar form in 1951. Krull proved the case when M was an ideal, and Goro Azumaya published a substantially generalized version (for all associative rings) in 1951. According to Matsumura, "Priority is obscure, and although it is usually called the Lemma of Nakayama, late Prof. Nakayama did not like the name."

---

(9) **Examples and Hypotheses for Nakayama's Lemma.**

(a) Let $R = \mathbb{Z}$, $I = \langle 2\rangle$, and $M = \mathbb{Z}/3\mathbb{Z}$. Verify that $IM = M$ and find $a \in I$ such that $(1-a)M = 0$.

(b) In the previous example, explain why your computation does not imply that $M = 0$. Which hypothesis from Nakayama's Lemma is missing?

(c) Let $R = \mathbb{K}[x]_{\langle x\rangle}$ and let $M = R[1/x]/R$. Prove that $M \neq 0$ but $xM = M$. Hint: Show that $1/x + R$ is nonzero and that multiplication by x is surjective on M.

(d) Explain why part (c) shows that finite generation cannot be removed from Nakayama's Lemma.

(10) **The Jacobson Radical.** Let R be a ring.

(a) Prove that if $a \in \mathrm{Jac}(R)$, then $1+a$ is a unit in R.

(b) More generally, prove that if $a \in \mathrm{Jac}(R)$ and $r \in R$, then $1+ra$ is a unit.

(c) Prove that if $(R, \mathfrak{m})$ is a local ring, then $\mathrm{Jac}(R) = \mathfrak{m}$.

(d) Compute $\mathrm{Jac}(R)$ for the following rings: $R = \mathbb{K}$ a field, $R = \mathbb{Z}$, and $R = \mathbb{Z}/12\mathbb{Z}$.

(e) Give an example of a ring R for which $\mathrm{Jac}(R)$ and $\sqrt{\langle 0\rangle}$ are not equal.

(11) **Proving Nakayama's Lemma.** Let R be a ring, $I \subset R$ an ideal, and M a finitely generated R-module.

(a) Use the determinant trick with $\phi = \mathrm{Id}_M$ to prove Nakayama's Lemma I: if $IM = M$, then there exists $r \in I$ such that $(1-r)M = 0$.

(b) Assume that $I \subset \mathrm{Jac}(R)$. Use part (a) to deduce Nakayama's Lemma IV: if $IM = M$, then $M = 0$.

(c) Explain why the local version of Nakayama's Lemma II follows from Nakayama's Lemma IV.

(12) **Applications of Nakayama's Lemma.** Let R be a ring and M a finitely generated R-module. Let $I \subset R$ be an ideal, and assume that $I \subset \mathrm{Jac}(R)$.

(a) Let $N \subseteq M$ be a submodule. Prove that if $M = N + IM$, then $M = N$. Hint: Apply Nakayama's Lemma to M/N.

(b) Let $\phi : M \to N$ be a homomorphism of finitely generated R-modules. Prove that ϕ is surjective if and only if the induced map

$$M/IM \longrightarrow N/IN$$

is surjective. Hint: Apply Nakayama's Lemma to $\mathrm{coker}(\phi)$.

(c) Let $(R, \mathfrak{m})$ be local and let M be finitely generated. Prove that $M = 0$ if and only if $M/\mathfrak{m}M = 0$.

(d) Let $(R, \mathfrak{m})$ be local and let $\phi : M \to N$ be a homomorphism of finitely generated R-modules. Prove that if the induced map

$$M/\mathfrak{m}M \longrightarrow N/\mathfrak{m}N$$

is an isomorphism, then ϕ is surjective. Give an example showing that ϕ need not be injective.

(e) Give an example showing that an injective map of finitely generated modules can become non-injective after reducing modulo $\mathfrak{m}$. Hint: Use multiplication by x on $\mathbb{K}[x]_{\langle x \rangle}$.

(13) **Surjective Endomorphisms of Finitely Generated Modules.** Let M be a finitely generated R-module and let $\phi : M \to M$ be a surjective endomorphism.

(a) Explain how we can view M as an $R[t]$-module by letting t act as ϕ. Why is M finitely generated as an $R[t]$-module?

(b) Use that ϕ is surjective to prove that $tM = M$ as an $R[t]$-module.

(c) Apply Nakayama's Lemma I over the ring $R[t]$ with the ideal $\langle t \rangle$ to prove that there exists a polynomial $q(t) \in R[t]$ such that

$$(1 - tq(t))M = 0.$$

(d) Deduce that ϕ is an automorphism of M. Hint: Translate the identity in part (c) into an identity involving ϕ and $q(\phi)$.

(e) Now suppose $(R, \mathfrak{m})$ is local and M is finitely generated. Prove that if the induced map $M/\mathfrak{m}M \to M/\mathfrak{m}M$ is an isomorphism, then ϕ is an automorphism of M.

(14) **More Applications of Nakayama's Lemma.** Let R be a nonzero ring.

(a) Prove that $R^n \cong R^m$ as R-modules if and only if $n = m$. Hint: Choose a maximal ideal $\mathfrak{m}$ and reduce modulo $\mathfrak{m}$.

(b) Let M be a free R-module such that $M \cong R^n$. Prove that any set of n elements that generate M is a basis for M as an R-module. Hint: Use the previous exercise on surjective endomorphisms.

(c) Define the *rank* of a finitely generated free R-module M to be the number of elements in a basis for M. Prove that the rank of M is well-defined.

(15) **Minimal Generating Sets over Local Rings.** Let $(R, \mathfrak{m})$ be a local ring with residue field $\kappa = R/\mathfrak{m}$. Let M be a finitely generated R-module and let $x_1, \ldots, x_r$ be elements of M.

(a) Prove that if $x_1, \ldots, x_r$ generate M as an R-module, then their images generate $M/\mathfrak{m}M$ as a κ-vector space.

(b) Prove the converse: if the images of $x_1, \ldots, x_r$ generate the κ-vector space $M/\mathfrak{m}M$, then $x_1, \ldots, x_r$ generate M as an R-module.

(c) Deduce Nakayama's Lemma III.

(d) Let $\mu_R(M)$ denote the minimal number of generators of M as an R-module. Prove that $\mu_R(M) = \dim_\kappa(M/\mathfrak{m}M)$.

(e) We say that $x_1, \ldots, x_r$ are *minimal generators* for M if they generate M and $r = \mu_R(M)$. Prove that $x_1, \ldots, x_t$ are minimal generators for M if and only if their images form a basis of $M/\mathfrak{m}M$.

(16) **Computing Minimal Numbers of Generators.** Let $R = \mathbb{K}[x, y]_{\langle x,y \rangle}$ with maximal ideal $\mathfrak{m} = \langle x, y \rangle R$ and residue field $\mathbb{K}$.

(a) Compute the minimal number of generators of $R/\langle x^2, xy, y^2 \rangle$ as an R-module.

(b) Compute the minimal number of generators of $\mathfrak{m}$ as an R-module.

(c) Compute the minimal number of generators of $\mathfrak{m}^2$ as an R-module.

(d) Let $S = \mathbb{Z}_{\langle p \rangle}$ and $M = S/\langle p^4 \rangle \oplus S/\langle p^2 \rangle$. Compute the minimal number of generators of M as an S-module.

(17) **Local Generators and Local Surjectivity.** Let R be a ring. Let M be a finitely generated R-module and let $x_1, \ldots, x_r \in M$.

(a) Prove that $x_1, \ldots, x_r$ generate M if and only if, for every maximal ideal $\mathfrak{m} \subset R$, their images generate $M_\mathfrak{m}/\mathfrak{m}M_\mathfrak{m}$ as a vector space over $\kappa(\mathfrak{m}) = R_\mathfrak{m}/\mathfrak{m}R_\mathfrak{m}$.

(b) Let $\phi : M \to N$ be a homomorphism of finitely generated R-modules. Prove that ϕ is surjective if and only if, for every maximal ideal $\mathfrak{m} \subset R$, the induced map below is surjective:

$$M_\mathfrak{m}/\mathfrak{m}M_\mathfrak{m} \longrightarrow N_\mathfrak{m}/\mathfrak{m}N_\mathfrak{m}$$

(c) Explain why the analogous statement for injectivity is false by revisiting the multiplication-by-x example over $\mathbb{K}[x]_{\langle x \rangle}$.

(d) Let $f_1, \ldots, f_n \in R$ generate the unit ideal. State and prove a version of part (b) where one first localizes at each f_i.