Chapter 5

A miscellaneous collection of algorithms

5.1 Testing if a ring is a field

One basic question we may ask ourselves when presented with a finite ring is if it is not in fact a field.

Lemma 5.1.1. *Let p be a prime and R a finite commutative $\mathbb{F}_p$-algebra. Then the following are equivalent:*

(i) *The map $F : R \to R$ given by $x \mapsto x^p$ is injective.*
(ii) *R has no nonzero nilpotent elements.*
(iii) *R is a field.*

Proof. Note that F is an $\mathbb{F}_p$-linear map.

(i)⇒(ii): Suppose there exists $0 \neq x \in R$ and $n \in \mathbb{Z}_{>1}$ such that $x^{n-1} \neq 0$ and $x^n = 0$. Choose $d \in \mathbb{Z}_{\geq 0}$ maximal such that $dp < n$. Then $(d+1)p \geq n$ and $d+1 < n$, so $0 \neq x^{d+1} \in \ker(F)$.

(ii)⇒(iii): If R has no nonzero nilpotent elements, then R is semisimple (see Theorem 1.4.9, part (iii)). Since R is commutative, it must be a field.

(iii)⇒(i) is clear. □

Theorem 5.1.2. *There exists a deterministic polynomial-time algorithm that, given a finite ring R, determines whether or not R is a field.*

Proof. If $\mathrm{char}(R)$ is not a prime or R is not commutative, then R is not a field. This can be tested using Theorem 1.1.3 and Theorem 3.3.1. Otherwise R is a commutative $\mathbb{F}$-algebra and we use Lemma 5.1.1, part (i) to test whether it is a field. □

Note 5.1.3. Another deterministic polynomial-time algorithm for testing if a finite ring is a field is given in [4], Section 5, Theorem 4.

Note 5.1.4. A deterministic polynomial-time algorithm for the case where $R^+ = (\mathbb{Z}/p\mathbb{Z})^n$, for some prime p and some $n \in \mathbb{Z}_{>0}$ is given in [23], Section 4.

5.2 Testing if a ring is simple

We have seen in Theorem 1.1.3 that primality testing is in P. It is therefore natural to ask whether we can construct a deterministic polynomial-time algorithm which decides whether a finite ring is simple.

Lemma 5.2.1. *Let R be a semisimple ring. Then the centre of R is a field if and only if R is simple.*

Proof. Since R is semisimple, it is a finite product of simple rings. Hence the centre of R is the product of the centres of these simple rings, and so, is a finite product of fields. This product is then a field itself if and only if R was simple to begin with. □

Theorem 5.2.2. *There exists a deterministic polynomial-time algorithm that, given a finite ring R, determines whether R is simple, and if it is, outputs a prime p and two positive integers m and n such that $R \cong \mathcal{M}_n(\mathbb{F}_{p^m})$.*

Proof. Compute $k := \mathrm{Z}(R)$ and test if it is a field using Theorem 5.1.2. If k is not a field, then R cannot be simple. If it is a field, then R is a finite-dimensional algebra over k, and we can compute its Jacobson radical using Theorem 3.4.1. If $\mathrm{J}(R) \neq 0$, then R cannot be simple. If $\mathrm{J}(R) = 0$, then R is a semisimple algebra whose centre is a field, which by Lemma 5.2.1 implies R is simple. Proceed by computing $m \in \mathbb{Z}_{>0}$, the dimension of k over $\mathbb{F}_p$, and $n \in \mathbb{Z}_{>0}$, the size of the matrix ring, both of which can be done in polynomial time.

□

Note 5.2.3. Given two finite rings R and R', we can now decide if they are simple and isomorphic: simply compare the size of the matrices which will be produced by Theorem 5.2.2 and test if the centres of R and R' are isomorphic fields, using Theorem 3.5.2.

The algorithm above does not explicitly exhibit an isomorphism between R and $\mathcal{M}_n(\mathrm{Z}(R))$. We can use Theorem 3.5.2 to get an isomorphism of fields $\mathrm{Z}(R) \cong \mathbb{F}_{p^m}$, for some $m \in \mathbb{Z}_{>0}$, but we can say no more than that.

The problem of exhibiting an isomorphism $R \cong \mathcal{M}_n(\mathrm{Z}(R))$ is often referred to as the *explicit isomorphism problem*, and has received recent attention in [45, 46]. In the case that $\mathrm{Z}(R)$ is a finite field and n is a power of 2, this problem has a deterministic polynomial-time solution. In general, the problem of finding an isomorphism between finite algebras over finite fields is not believed to be NP-hard, but is at least as hard as the graph isomorphism problem ([41, 52]).

5.3 Testing if a module is simple

Testing simplicity of a module can also be done in polynomial time.

Theorem 5.3.1. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and a finite R-module M, determines whether M is simple or not.*

Proof. By Schur's Lemma (Theorem 1.6.1), if M is simple, then $\mathrm{End}_R(M)$ is a division ring, so we start by computing $n := \mathrm{char}(\mathrm{End}_R(M)) = \exp(M^+)$ using Theorem 3.3.1. If n is not a prime, then we conclude that M is not simple. Otherwise, if n is a prime, then nR is a two-sided ideal in R, and $R' := R/nR$ is an algebra over a finite field, so we may compute its Jacobson radical using Theorem 3.4.1. Now M is an R'-module, since nR annihilates M.

If $\mathrm{J}(R')$ does not annihilate M, then M is not simple over R', and hence M is not simple over R. Otherwise, M is an $R'/\mathrm{J}(R')$-module and by Theorem 1.6.4, it is now enough to test whether $\mathrm{End}_{R'/\mathrm{J}(R')}(M)$ is a field, which can be done by Theorem 5.1.2. □

Second proof. Alternatively, compute

$$I := \mathrm{ann}(M) = \ker(R \to \mathrm{End}_{\mathbb{Z}}(M^+), r \mapsto r \cdot m),$$

where "$\cdot$" denotes the action of R on M. Then M is a faithful R/I-module and so if M is simple, we claim that R/I is simple as a ring. To see this, suppose M is simple. Then the Jacobson radical of R/I annihilates M, but since M is faithful, $\mathrm{J}(R/I) = 0$, hence R/I is semisimple. Now M is a faithful simple module over a semisimple ring, so R/I must in fact be simple.

We thus begin by testing simplicity of R/I as a ring, using Theorem 5.2.2. If R/I is not simple, then M cannot be simple and we are done. Otherwise, the algorithm in Theorem 5.2.2 will output a prime p, and two integers m, n such that $R/I \cong \mathcal{M}_n(\mathbb{F}_{p^m})$ as rings. Now, by Theorem 1.4.2, the only simple $\mathcal{M}_n(\mathbb{F}_{p^m})$-module, up to isomorphism, is $(\mathbb{F}_{p^m})^n$, and the other modules over $\mathcal{M}_n(\mathbb{F}_{p^m})$ are direct sums of $(\mathbb{F}_{p^m})^n$. Moreover, R/I-modules are exactly the R-modules annihilated by I. Hence M is simple over R if and only if $|M| = p^{nm}$. □

5.4 Testing if a module is projective

For many future algorithms it will be very useful to be able to test if a module is projective.

Theorem 5.4.1. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and a R-module M, together with a generating set of cardinality d, for some $d \in \mathbb{Z}_{\geq 0}$, determines if M is R-projective or not, and if it is, produces a splitting of the natural surjection $R^d \twoheadrightarrow M$.*

Proof. Recall that M is projective if and only if the natural surjection $f : R^d \twoheadrightarrow M$ has a left inverse. The latter can be tested using Proposition 2.5.1, which will also produce a left inverse. □

Second proof. Another way to determine whether M is projective comes as a consequence of Theorem 4.1.1, since M is projective if and only if M is a direct summand of R^d. We compute the largest isomorphic common direct summand of R^d and M, say S. If $M \cong S$, then M is projective and the isomorphism $M \to S$, which is also produced by the algorithm, induces a splitting of $R^d \to M$. Otherwise the algorithms concludes that M is not projective. □

5.5 Constructing projective covers

Recall the definition of a projective cover given in Definition 1.6.24 and the fact that over left-artinian rings, all modules have a projective cover, unique up to isomorphism (Theorem 1.6.25).

Theorem 5.5.1. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and a finite R-module M, outputs a projective cover of M.*

Proof. Use the algorithm in the proof of Theorem 4.1.3 to construct a sequence of R-modules $(S_i)_{i=1}^t$, two sequences of integers $(a_i)_{i=1}^t$ and $(c_i)_{i=1}^t$, and a two-sided nilpotent ideal $\mathfrak{a}$ such that

$$R/\mathfrak{a} \cong \bigoplus_{i=1}^{t} S_i^{a_i} \quad \text{and} \quad M/\mathfrak{a}M \cong \bigoplus_{i=1}^{t} S_i^{c_i},$$

where for all $1 \leq i \leq t$, we have that $a_i > 0$ and $c_i \geq 0$. Relabel, to write $R/\mathfrak{a} \cong \bigoplus_{i\in I} S_i$ and $M/\mathfrak{a}M \cong \bigoplus_{j\in J} S_j$. Then for each $j \in J$ we have a surjective map $g_j : M \twoheadrightarrow S_j$, such that $\mathfrak{a}M = \bigcap_{j\in J} \ker(g_j)$.

For each $j \in J$, pick $j' \in I$ such that $S_j \cong S_{j'}$. Since $S_{j'}$ is a direct summand of $R/\mathfrak{a}$, there exists an idempotent $\overline{e}_j \in R/\mathfrak{a}$ such that $S_{j'} \cong (R/\mathfrak{a})\overline{e}_j$ (see Theorem 1.5.4). To find $\overline{e}_j$, look at the image of 1 under the isomorphism $R/\mathfrak{a} \cong \bigoplus_{i\in I} S_i$ and identify the entry corresponding to j'. Replace all other entries by zeros and let $\overline{e}_j$ be the preimage of this element under the same isomorphism.

Thus, the decomposition $R/\mathfrak{a} \cong \bigoplus_{i\in I} S_i$ gives rise to a sequence of idempotent elements $\overline{e}_1, \ldots, \overline{e}_{|J|}$ in $R/\mathfrak{a}$ such that for all $j \in J$ we have $S_{j'} \cong (R/\mathfrak{a})\overline{e}_j$.

By Proposition 1.5.8, these idempotents can then be lifted deterministically in polynomial time to idempotents $e_1, \ldots, e_{|J|}$ in R. For all $j \in J$, let $P_j = Re_j$. Since e_j is an idempotent in R, we can write $R = Re_j \oplus R(1 - e_j)$, so P_j is projective. Hence we can construct a sequence of maps f_j such that for each $j \in J$ the following diagram commutes:

$$\begin{array}{ccc} & & P_j \\ & {\scriptstyle f_j}\swarrow & \downarrow{\scriptstyle \pi_j} \\ M & \xrightarrow[g_j]{} & S_j, \end{array}$$

where $\pi_j : P_j \to S_j$ is the natural projection map. This can be done by solving a system of linear equations over R. Let $P = \bigoplus_{j\in J} P_j$ and let $f : P \to M$ be the direct sum of the f_j.

We claim that for each $j \in J$, the pair (P_j, π_j) is a projective cover of S_j. Clearly π_j is surjective and P_j is projective. We need to show that $\ker(\pi_j) \subseteq_s P_j$. Let $N \leq P_j$ be a submodule such that $\ker(\pi_j) + N = P_j$. By construction, $\ker(\pi_j) = \mathfrak{a}P_j$. Since $\mathfrak{a} \subseteq \mathrm{J}(R)$, by Nakayama's Lemma we must have $N = P_j$. Since taking projective covers commutes with direct sums, $(P, \bigoplus_{j\in J} \pi_j)$ is a projective cover for $M/\mathfrak{a}M$. Since $\mathfrak{a}$ is nilpotent, f is surjective and (P, f) is a projective cover of M. □

5.6 Constructing injective hulls

Recall the definition of injective hulls given in Definition 1.6.28 and the fact that injective hulls exist for modules over any ring. Moreover, two injective hulls of a module M are isomorphic (Theorems 1.6.29).

To construct injective hulls, we will make use of the *character module* (see Definition 1.9.1). Recall that for a finite ring R, the character functor defines a duality between ${}^{\mathrm{fg}}_{R}\mathfrak{M}$ and $\mathfrak{M}^{\mathrm{fg}}_{R}$. (see Theorem 1.9.2). Moreover, the following holds.

Proposition 5.6.1. *Let R be a left-noetherian ring and M a finitely generated R-module. Then*

(i) *M is projective in ${}_{R}\mathfrak{M}$ if and only if M is projective in ${}^{\mathrm{fg}}_{R}\mathfrak{M}$.*
(ii) *M is injective in ${}_{R}\mathfrak{M}$ if and only if M is injective in ${}^{\mathrm{fg}}_{R}\mathfrak{M}$.*

Proof. The "only if" directions of both (i) and (ii) are clear. We prove the converse statements below.

Suppose M is projective in ${}_{R}\mathfrak{M}$. Then M is a direct summand of a finitely generated free R-module, so it is projective in ${}^{\mathrm{fg}}_{R}\mathfrak{M}$.

Suppose M is injective in ${}_{R}\mathfrak{M}$. Since R is left-noetherian, all its left ideals are finitely generated. Hence by Theorem 1.6.12, part (iii) (Baer's test), M is injective in ${}^{\mathrm{fg}}_{R}\mathfrak{M}$. □

Note 5.6.2. The left-noetherian condition on R is not needed for part (i).

Corollary 5.6.3. *Let R be a finite ring and M an R-module. Then M is injective over R if and only if $\widehat{M}$ is projective over R^{o}, the opposite ring of R.*

Note 5.6.4. If R is a finite ring and M is a finite R-module, then we may take

$$\widehat{M} = \mathrm{Hom}_{\mathbb{Z}}(M, \frac{1}{e}\mathbb{Z}/\mathbb{Z}), \tag{5.1}$$

where e is a multiple of $\exp(M^+)$.

Theorem 5.6.5. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and a finite R-module M, computes an injective hull of M.*

Proof. Compute $\widehat{M} = \mathrm{Hom}_{\mathbb{Z}}(M, \frac{1}{e}\mathbb{Z}/\mathbb{Z})$, where e is a multiple of $\exp(M^+)$. Using Theorem 5.5.1, compute a projective cover (P, f) of $\widehat{M}$ over R^{o}. Now set $I := \widehat{P} = \mathrm{Hom}_{\mathbb{Z}}(P, \frac{1}{e'}\mathbb{Z}/\mathbb{Z})$, where e' is a multiple of $\exp(P^+)$. Then (I, g) is an injective hull of M by Theorem 1.9.2. The algorithm also produces a map $g : \widehat{\widehat{M}} \hookrightarrow I$, given by precomposition with f, such that $\mathrm{im}(g) \supseteq_e I$. □

5.7 Testing if a module is injective

Recall that a module is injective if and only if it is isomorphic to its injective hull (Theorem 1.6.30).

Theorem 5.7.1. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and a finite R-module M, determines if M is injective.*

Proof. Construct an injective hull I of M using Theorem 5.6.5. Now check if the map $g : M \hookrightarrow I$ produced by Theorem 5.6.5 is bijective. □

5.8 Testing if a ring is quasi-Frobenius

Recall that a finite ring R is quasi-Frobenius if R is left self-injective (Theorem 1.7.1, Definition 1.7.2).

Theorem 5.8.1. *There exists a deterministic polynomial-time algorithm that, given a finite ring R, determines whether R is quasi-Frobenius.*

Proof. Use Theorem 5.7.1 to determine if the left-regular R-module ${}_RR$ is injective. □

5.9 Constructive tests for existence of injective and surjective module homomorphisms

In this section we discuss the algorithmic problem of testing for existence and of finding injective and surjective homomorphisms between two finite length modules over a ring R. If R is a finite-dimensional algebra over a field, this problem can be cast in the context of matrix completion, and has been shown to be NP-hard in [42]. In view of the results of [10, 15] and of Theorem 4.1.2, this result is striking. It is not however an isolated type of result: the subgraph isomorphism problem is an NP-hard problem, while the graph isomorphism problem is believed to be NP-intermediate.

While in the general case, testing constructively for existence of injective and surjective module homomorphisms is NP-hard, with certain restrictions on the modules considered, the problem turns out to be tractable. We are interested in the case where R is a finite ring and one of the modules is either projective or injective over R, for which the problem simplifies somewhat.

Theorem 5.9.1. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and two finite R-modules M and N, one of which is projective, determines whether there exists a surjection $M \twoheadrightarrow N$. If one exists, the algorithm exhibits one such.*

Proof. If N is projective, then it suffices to test whether N is a direct summand of M, which can be done by Theorem 4.1.3. This will also produce a surjection $M \twoheadrightarrow N$.

If M is projective, then we proceed by constructing a projective cover (P, f) of N. Note that existence of a surjection $M \twoheadrightarrow N$ is equivalent to existence of a surjection $M \twoheadrightarrow P$. If there exists a surjection $M \twoheadrightarrow P$, simply compose it with f to get a surjection $M \twoheadrightarrow N$. Conversely, if there exists a surjection $M \twoheadrightarrow N$, then, since P is a projective cover of N, there exists a surjective map $g : M \twoheadrightarrow P$ making the following diagram commute

$$\begin{array}{ccc} & & P \\ & \overset{g}{\nearrow} & \downarrow f \\ M & \longrightarrow\!\!\!\!\!\rightarrow & N. \end{array}$$

This reduces the problem to the previous case. □

Second proof for the case where M is projective. If M is projective, we can also decide existence of a surjection $M \to N$ in a more direct manner. Use the algorithm in the proof of Theorem 4.1.3 to construct a two-sided nilpotent ideal $\mathfrak{a} \subset R$ and a sequence of R-modules $(S_i)_{i=1}^t$ that is "compatible" both with M and with N, i.e. such that

$$M/\mathfrak{a}M \cong \bigoplus_{i=1}^{t} S_i^{a_i} \quad \text{and} \quad N/\mathfrak{a}N \cong \bigoplus_{i=1}^{t} S_i^{b_i},$$

for some $a_i, b_i \in \mathbb{Z}_{\geq 0}$. This is done by running the algorithm in the proof of Theorem 4.1.3 on the ring R and the module M, and including N as one of the candidates for the isomorphism classes of simple R-modules in the UPDATE subroutine. Note that, by construction, the algorithm ensures that for all $i \neq j$, we have $\mathrm{Hom}_R(S_i, S_j) = 0$.

We claim that existence of a surjection $M/\mathfrak{a}M \twoheadrightarrow N/\mathfrak{a}N$, which can be easily tested by comparing a_i and b_i for each $1 \leq i \leq t$, is equivalent to existence of a surjection $M \to N$. If there exists a surjection $M \to N$, then clearly it induces a surjection $M/\mathfrak{a}M \twoheadrightarrow N/\mathfrak{a}N$. Conversely, if there exists a surjection $\overline{f} : M/\mathfrak{a}M \twoheadrightarrow N/\mathfrak{a}N$, then, since M is projective, there exists a map $f : M \to N$ making the following diagram commute:

$$\begin{array}{ccc} M & \overset{f}{\dashrightarrow} & N \\ \downarrow & & \downarrow \\ M/\mathfrak{a}M & \underset{\overline{f}}{\longrightarrow\!\!\!\!\!\rightarrow} & N/\mathfrak{a}N, \end{array}$$

and f is surjective since $\mathfrak{a}$ is nilpotent. □

Note 5.9.2. The case where $M \cong R^n$, for some $n \in \mathbb{Z}_{>0}$ can be settled using the algorithm for computing the minimum number of generators of a module, given in Theorem 4.1.3.

Dually to Theorem 5.9.1, we have the following result:

Theorem 5.9.3. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and two finite R-modules M and N, one of which is injective, determines whether or not there exists an injection $M \hookrightarrow N$. If one exists, the algorithm exhibits one such.*

Proof. Let $k := \frac{1}{e}\mathbb{Z}/\mathbb{Z}$, where $e \in \mathbb{Z}_{>0}$ is a multiple of $\exp(M^+)$ and $\exp(N^+)$, and apply Theorem 5.9.1 to modules $\mathrm{Hom}_k(N, k)$ and $\mathrm{Hom}_k(M, k)$.

□

The remaining cases, not treated by Theorems 5.9.1 and 5.9.3, are constructive tests for existence of the following R-module homomorphisms:

- $P \hookrightarrow M$, for P a projective module,
- $M \hookrightarrow P$, for P a projective module,

and their respective duals,

- $N \twoheadrightarrow I$, for I an injective module,
- $I \twoheadrightarrow N$, for I an injective module.

Mimicking the construction given in the proof of Theorem 1.2 of [42], we settle these as being NP-hard, even when R is a finite local commutative ring and $P = R$. This is done by a reduction from an instance of the *nonsingular matrix completion problem*, which is known to be NP-hard.

The nonsingular matrix completion problem is an algorithmic question that can be formulated as follows: given a square matrix A, whose entries are homogeneous linear polynomials in $\mathbb{F}[x_1, \ldots, x_n]$, for some field $\mathbb{F}$, decide if there exist values from $\mathbb{F}$ that can be assigned to the variables $x_1, \ldots, x_n$, so as to make A nonsingular. The constructive version of this problem asks for values of $x_1, \ldots, x_n$ making A nonsingular to be exhibited.

Nonsingular matrix completion problems arise naturally in spaces of linear transformations. Let $n \in \mathbb{Z}_{>0}$ and $\mathbb{F}$ be a field. Let $A \subset \mathcal{M}_n(\mathbb{F})$ be a linear subspace and let $\{A_1, \ldots, A_m\}$ be a basis of A over $\mathbb{F}$. Deciding existence of (resp. finding) a nonsingular matrix in A is equivalent to deciding existence of (resp. finding) a sequence $c_1, \ldots, c_m \in \mathbb{F}$ such that $\sum_{i=1}^{m} c_i A_i$ is nonsingular.

The complexity of the nonsingular matrix completion problem is very much dependent on the size of the field $\mathbb{F}$ (see [40, 42]). If $\mathbb{F}$ is "large enough", then the Schwartz-Zippel lemma (see [81, 89]) provides an efficient randomized solution. However, over finite fields, nonsingular matrix completion is NP-complete ([14, 40]).

Theorem 5.9.4. *There exists a deterministic polynomial-time reduction from the decision (resp. constructive) version of nonsingular matrix completion to the problem of deciding existence of (resp. finding) an injective module homomorphism from a finite commutative local ring R containing a field, to an R-module M.*

Proof. Let $\mathbb{F}$ be a finite field and let U, V be two finite-dimensional $\mathbb{F}$-vector spaces of the same dimension. Let $0 \neq L \leq \mathrm{Hom}_{\mathbb{F}}(U, V)$ be a linear subspace. Consider the ring

$$R = \mathbb{F} \oplus U,$$

with componentwise addition and multiplication given by

$$(a, x)(b, y) = (ab, ay + bx).$$

Then R is a commutative local ring, with maximal ideal U, and $U^2 = 0$.

Put

$$M = L \oplus V.$$

We make M into an R-module by defining an action:

$$(a, u) \cdot (l, v) := (al, av + l(u)),$$

for all $a \in \mathbb{F}$, $u \in U$, $l \in L$ and $v \in V$.

Note that any homomorphism $R \to M$ is determined by the image of 1_R. Let $\psi : R \to M$ be an R-module homomorphism, and suppose $1 \mapsto (l, v)$, for some $(l, v) \in M$. Then

$$\mathrm{im}(\psi) = \mathbb{F}(l, v) + (0, lU)$$

and $\psi \in \mathrm{Hom}_R(R, M)$ is injective if and only if $l \in L$ is an isomorphism.

□

Theorem 5.9.5. *There exists a deterministic polynomial-time reduction from the decision (resp. constructive) version of nonsingular matrix completion to the problem of deciding existence of (resp. finding) an injective module homomorphism from an R-module M to R, where R is a finite commutative local ring containing a field.*

Proof. Let $\mathbb{F}$ be a finite field and let U, V be two finite-dimensional $\mathbb{F}$-vector spaces of the same dimension. Let $0 \neq L \subseteq \mathrm{Hom}_{\mathbb{F}}(U, V)$ be a linear subspace. Consider the ring

$$R = \mathbb{F} \oplus L \oplus U \oplus V,$$

with componentwise addition and multiplication given by

$$(f, l, u, v) \cdot (f', l', u', v') = (ff', fl' + f'l, fu' + f'u, fv' + fv + l(u') + l'(u)).$$

Then R is a commutative ring with unique maximal ideal $L \oplus U \oplus V$. Note that $L \oplus V$ is a two-sided ideal in R. Put

$$M := R/(L \oplus V) \cong \mathbb{F} \oplus U.$$

Note that $U^2 = 0$, so M also has the structure of a local commutative ring, with maximal ideal U.

Note that

$$\mathrm{Hom}_R(M, R) \cong \mathrm{ann}_R(L \oplus V) = L \oplus U_0 \oplus V, \tag{5.2}$$

where $U_0 = \bigcap_{f \in L} \ker(f)$ and the isomorphism in (5.2) is given by mapping $f \mapsto f(\overline{1})$. Let ϕ be an R-module homomorphism. Then ϕ corresponds uniquely to an element $(0, l_0, u_0, v_0) \in L \oplus U_0 \oplus V$ and

$$\mathrm{im}(\phi) \cong \mathbb{F}(0, l_0, u_0, v_0) + (0, 0, 0, l_0 U).$$

Hence $\phi \in \mathrm{Hom}_R(M, R)$ is injective if and only if $l_0 \in L$ is an isomorphism.

□

We consider now another weaker variant of the problem of testing constructively for injective and surjective module homomorphisms. Suppose we are given a finite ring R and two modules M and N. Instead of looking for a surjection $M \twoheadrightarrow N$, we may ask if there is an integer k such that there exists a surjective homomorphism $f : M^k \twoheadrightarrow N$. If such a pair (k, f) exists, we would like to exhibit it. Note that we do not ask for k to be minimal with this property. This problem turns out to have an easy solution.

Theorem 5.9.6. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and two finite R-modules M, N, decides if there exists a pair (k, f), where $k \in \mathbb{Z}_{\geq 0}$ and $f : M^k \to N$ is a surjective R-module homomorphism. If it exists, the algorithm exhibits such a pair.*

Proof. Compute a set S of $\mathbb{Z}$-generators of $\mathrm{Hom}_R(M, N)$. If $N = \sum_{f \in S} f(M)$, then output $(|S|, \sum_{f \in S} f)$. Otherwise conclude that there does not exist a pair as required.

□

Dually, we have the following result:

Theorem 5.9.7. *There exists a deterministic polynomial-time algorithm that, given a finite ring R and two finite R-modules M, N, decides if there exists a pair (k, f), where $k \in \mathbb{Z}_{\geq 0}$ and $f : M \to N^k$ is an injective R-module homomorphism. If it exists, the algorithm exhibits such a pair.*

Proof. Compute a set S of $\mathbb{Z}$-generators of $\mathrm{Hom}_R(M, N)$. If $\bigcap_{f \in S} \ker(f) = \{0\}$, then output $(|S|, \prod_{f \in S} f)$. Otherwise conclude that there does not exist a pair as required.

□