

## WORKSHEET 6.2: CHAIN CONDITIONS AND DECOMPOSITIONS

Let  $R$  be a ring and let  $M$  be an  $R$ -module. We say that  $M$  is *Noetherian* if every ascending chain of submodules

$$M_1 \subset M_2 \subset M_3 \subset \cdots$$

eventually stabilizes, meaning that there is an index  $n$  such that  $M_j = M_n$  for every  $j \geq n$ . This is called the *ascending chain condition*, often abbreviated ACC. Similarly,  $M$  is *Artinian* if every descending chain of submodules  $M_1 \supset M_2 \supset \cdots$  eventually stabilizes; this is the *descending chain condition*, or DCC. Notice that neither condition gives a single bound on the lengths of chains. Instead, each says that any particular process of repeatedly enlarging, or shrinking, a submodule cannot continue forever. A ring  $R$  is *left Noetherian* or *left Artinian* if its regular left module  ${}_R R$  is, and when  $R$  is commutative we simply say that  $R$  is a *Noetherian* or *Artinian ring*.

You already know examples. In Worksheet 6.1 we proved that every ascending chain of ideals in a PID stabilizes, and we used this twice: to show that factorizations into irreducibles terminate, and to show that Smith reduction terminates over a PID which is not Euclidean. In the language of this worksheet, a PID is a Noetherian ring. A finite-dimensional vector space is both Noetherian and Artinian, since a strict inclusion of subspaces changes the dimension. This familiar example can make the two conditions look more closely related than they really are:  $\mathbb{Z}$  is Noetherian, but repeatedly multiplying by 2 gives a descending chain which never stabilizes.

The goal of this worksheet is to study how a module can be built from simpler pieces over a general ring. Over a PID, a finitely generated module breaks into a free part and cyclic torsion pieces, but over a general ring there may be no comparable list of cyclic pieces. It is still natural to ask whether a module can be built from finitely many simpler modules, and whether those pieces are determined by the original module. There are two different ways to make this precise. We could look for a chain of submodules whose successive quotients are simple, or we could look for a decomposition as a direct sum of modules which cannot be split further. These need not give the same pieces, since a quotient may be simple without being a direct summand. We will develop both approaches, beginning with the finiteness conditions which make them possible, and we will compare them using the modules over  $\mathbb{K}[x]/\langle x^N \rangle$  from Worksheet 6.1.

As in the previous worksheets, all rings have a multiplicative identity but need not be commutative, and the letter  $\mathbb{K}$  will denote a field. All modules are unital, and unless we say otherwise, module means left module.

There are two other useful ways to recognize the ascending chain condition. The *maximal condition* says that every nonempty family of submodules of  $M$  has a maximal member, meaning a member which is not strictly contained in any other member of the family. Notice that a maximal member need not contain all of the other members. The third formulation says that every submodule of  $M$  is finitely generated, which

connects a condition about chains with the generators we have been using all along. In the same way, DCC is equivalent to the *minimal condition*: every nonempty family of submodules has a minimal member. We prove these statements in the following exercise.

---

1. **Noetherian and Artinian Modules.** Throughout this exercise let  $M$  be an  $R$ -module.

- (a) Suppose  $M$  satisfies ACC. If a nonempty family of submodules had no maximal member, explain how to construct an infinite strictly ascending chain of members of the family. Deduce the maximal condition.
- (b) Suppose  $M$  satisfies the maximal condition, and let  $N \subset M$  be a submodule. Choose a maximal member  $L$  of the family of finitely generated submodules of  $N$ , which includes the zero submodule. If  $n \in N \setminus L$ , what can you say about  $L + Rn$ ? Conclude that  $N = L$ .
- (c) Suppose every submodule of  $M$  is finitely generated, and let  $(M_i)$  be an ascending chain of submodules. Show that  $N := \bigcup_i M_i$  is a submodule. Choose finitely many generators of  $N$ , find a single  $M_j$  containing all of them, and prove that the chain stabilizes at  $M_j$ .
- (d) Deduce that a Noetherian module is finitely generated. Explain why the definition requires more than finite generation of  $M$  itself, using the fact that the regular module  ${}_R R$  is cyclic regardless of the left ideals of  $R$ . Use the description of ideals in a PID to show that every PID is a Noetherian ring.
- (e) Adapt part (a) to show that DCC is equivalent to the minimal condition. Prove that every finite-dimensional  $\mathbb{K}$ -vector space is both Noetherian and Artinian, and use the chain  $\mathbb{Z} \supsetneq 2\mathbb{Z} \supsetneq 4\mathbb{Z} \supsetneq \cdots$  to show that  $\mathbb{Z}$  is not Artinian.

---

Both chain conditions behave well in short exact sequences. This matters because most of our constructions produce new modules by taking submodules, quotients, or extensions. For example, if a submodule and its quotient are both Noetherian, we expect that an ascending chain in the middle module cannot continue to grow forever. To prove this, we need a way to detect a change in the chain, either inside the submodule or after passing to the quotient.

Let  $A \subset M$  be a submodule with quotient map  $q : M \rightarrow M/A$ . Each submodule  $L \subset M$  gives two pieces of information:

$$L \cap A \subset A \quad \text{and} \quad q(L) \subset M/A.$$

These two pieces do not determine  $L$  among all submodules of  $M$ . For instance, two different lines in a plane can both meet a fixed line only at zero, and have the same image in the quotient by that line. They do, however, detect whether an inclusion between two submodules is an equality, and this is exactly what we need for chains. We prove these statements in the following exercise.

---

**2. Chain Conditions and Exact Sequences.** Throughout this exercise consider an exact sequence

$$0 \longrightarrow A \longrightarrow M \xrightarrow{q} C \longrightarrow 0,$$

and identify  $A$  with its image in  $M$ .

- (a) Suppose  $X \subset Y \subset M$  are submodules with  $X \cap A = Y \cap A$  and  $q(X) = q(Y)$ . Given  $y \in Y$ , choose  $x \in X$  with  $q(x) = q(y)$ , and use  $y - x$  to prove that  $X = Y$ .
- (b) If  $M$  is Noetherian, show that  $A$  and  $C$  are Noetherian. For the quotient, use the inverse images of a chain under  $q$ . Give the same argument for Artinian modules.
- (c) Suppose  $A$  and  $C$  are Noetherian, and let  $(L_i)$  be an ascending chain of submodules of  $M$ . Show that the chains  $(L_i \cap A)$  and  $(q(L_i))$  both stabilize. Choose an index after which both have stabilized, apply part (a), and conclude that  $M$  is Noetherian.
- (d) Repeat part (c) for descending chains. Conclude that  $M$  is Noetherian if and only if  $A$  and  $C$  are Noetherian, and that  $M$  is Artinian if and only if  $A$  and  $C$  are Artinian.
- (e) Deduce that a finite direct sum of Noetherian modules is Noetherian, and similarly for Artinian modules. If  $R$  is left Noetherian, use a surjection  $R^d \rightarrow M$  to show that every finitely generated left  $R$ -module is Noetherian. Thus, over a left Noetherian ring, a module is Noetherian if and only if it is finitely generated.

---

A nonzero  $R$ -module  $S$  is *simple* if its only submodules are  $0$  and  $S$ . For example,  $\mathbb{Z}/p\mathbb{Z}$  is a simple  $\mathbb{Z}$ -module when  $p$  is prime, and a one-dimensional vector space is a simple module over its field. Notice that simplicity concerns all submodules, so it is stronger than saying that a module is not a direct sum of two nonzero submodules.

A *composition series* of an  $R$ -module  $M$  is a finite chain of submodules

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_r = M$$

such that every quotient  $M_i/M_{i-1}$  is simple. These quotients are called the *composition factors* of the series. We say that  $M$  has *finite length* if it has a composition series. The zero module has the empty composition series, with no factors.

It is natural to ask whether two composition series of the same module have the same number of factors, and whether they have the same factors. We will prove both assertions. First, however, we show that a composition series exists exactly when both chain conditions hold. The two conditions play complementary roles: the ascending chain condition supplies maximal proper submodules, and the descending chain condition guarantees that repeatedly choosing them eventually reaches zero. We prove this in the following exercise.

---

### 3. When Can We Find a Composition Series?

- (a) Show that a simple module is both Noetherian and Artinian. Use the short exact sequences

$$0 \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow M_i/M_{i-1} \longrightarrow 0$$

and Problem 2 to show that every module with a composition series satisfies both chain conditions.

- (b) Suppose  $M$  is nonzero and Noetherian. Apply the maximal condition to the family of proper submodules of  $M$  to find a maximal proper submodule  $N$ , and prove that  $M/N$  is simple.
- (c) Suppose  $M$  is both Noetherian and Artinian. Choose a maximal proper submodule  $M^{(1)} \subsetneq M$ , then a maximal proper submodule of  $M^{(1)}$  if  $M^{(1)}$  is nonzero, and so on. Explain why these choices are always possible, and why the process must reach zero after finitely many steps. Reverse the resulting chain to obtain a composition series.
- (d) Conclude that  $M$  has finite length if and only if it is both Noetherian and Artinian. Deduce that submodules and quotients of modules of finite length have finite length, and show that an extension of two modules of finite length has finite length.
- (e) Let  $B$  be a  $\mathbb{K}$ -algebra. Show that a  $B$ -module which is finite dimensional as a  $\mathbb{K}$ -vector space has finite length as a  $B$ -module. Must a simple  $B$ -module be one dimensional over  $\mathbb{K}$ ? Hint: for  $d \geq 2$ , consider  $\mathbb{K}^d$  as a module over  $\text{Mat}_d(\mathbb{K})$ , and show that matrices can send a fixed nonzero vector to any chosen vector.

---

To compare two composition series, we begin with a useful observation about a single one. Given a submodule  $N \subset M$ , intersect every term of a composition series of  $M$  with  $N$ . The resulting chain need not be strictly increasing, but we will see that its successive quotients inject into the original composition factors. Each of these quotients is therefore either zero or simple, and deleting repeated terms gives a composition series of  $N$ .

If  $N$  is a proper submodule, at least one factor must disappear. Indeed, if every successive quotient were nonzero, simplicity would force the entire first term of the series into  $N$ , then the entire second term, and so on, until  $M \subset N$ . Thus if  $M$  has a composition series with  $r$  factors, then every proper submodule has a composition series with fewer than  $r$  factors. This lets us use induction on the number of factors in a chosen series, before we know that this number does not depend on the choice.

The comparison itself rests on a small configuration of submodules. If  $A$  and  $B$  are distinct maximal proper submodules of  $M$ , then  $A + B = M$ , and with  $C := A \cap B$  the isomorphism theorems give

$$A/C \cong M/B \quad \text{and} \quad B/C \cong M/A.$$

Thus the two routes from  $C$  up to  $M$  produce the same pair of simple factors, in the opposite order. We will see that this local comparison accounts for the entire theorem.

**Theorem 1** (Jordan–Hölder). *Any two composition series of a module of finite length have the same number of factors. Moreover, after reordering, their composition factors are pairwise isomorphic.*

We prove the theorem in the following exercise.

#### 4. Comparing Two Composition Series.

- (a) Fix a composition series  $0 = M_0 \subsetneq \cdots \subsetneq M_r = M$ , and let  $N \subset M$  be a submodule. Construct an injective homomorphism

$$\frac{N \cap M_i}{N \cap M_{i-1}} \longrightarrow M_i/M_{i-1}.$$

Show that deleting repeated terms from the chain  $(N \cap M_i)$  gives a composition series of  $N$  with at most  $r$  factors.

- (b) If none of these successive quotients is zero, prove by induction on  $i$  that  $M_i \subset N$ . For the induction step, use that the map of part (a) is surjective onto the simple module  $M_i/M_{i-1}$ . Deduce that a proper submodule  $N$  has a composition series with fewer than  $r$  factors.
- (c) Prove the theorem by strong induction on the number  $r$  of factors in one chosen composition series of  $M$ . First handle the cases where  $M = 0$  or  $M$  is simple. For the induction step, let  $A$  and  $B$  be the second-to-last terms of the two series. Why does part (b) allow us to apply the induction hypothesis to every proper submodule of  $M$ ? If  $A = B$ , explain how the induction hypothesis applies to the remaining portions of the two series.
- (d) Suppose  $A \neq B$ . Prove that  $A + B = M$ . Set  $C := A \cap B$ , construct the two isomorphisms displayed above, and show that  $A/C$  and  $B/C$  are simple.
- (e) Choose a composition series of  $C$ , which exists by Problem 3. Appending  $A$  to it gives a composition series of  $A$ , and appending  $B$  gives one of  $B$ . Apply the induction hypothesis within  $A$  and within  $B$  to compare these series with the remaining portions of the original two series.
- (f) Now append the final quotients  $M/A$  and  $M/B$ . Show that each of the original two lists of factors consists, up to isomorphism and order, of the factors of  $C$  together with  $M/A$  and  $M/B$ . This completes the induction. Explain why the argument compares multiplicities, even when several of the factors are isomorphic.

We can now define the *length*  $\ell_R(M)$  of a module of finite length to be the number of factors in any composition series of  $M$ , and we write  $\ell(M)$  when the ring is clear from context. Length is a useful replacement

for dimension, although the simple factors being counted need not be isomorphic to one another. For a vector space over a field, every simple factor is one dimensional, and length is exactly dimension.

Length is additive in short exact sequences. To see why, place a composition series of the submodule underneath the inverse image of a composition series of the quotient; the resulting chain is a composition series of the middle module. Notice what additivity does not say: the short exact sequence need not split. The composition factors describe how a module is assembled from extensions, but they do not remember everything about those extensions.

For instance, both  $\mathbb{Z}/p^2\mathbb{Z}$  and  $(\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p\mathbb{Z})$  have two composition factors, each isomorphic to  $\mathbb{Z}/p\mathbb{Z}$ . Multiplication by  $p$  behaves differently on the two modules, so they are not isomorphic. Thus the Jordan–Hölder theorem gives an invariant of a module, rather than a classification of the modules with given composition factors. We check these statements in the following exercise.

## 5. Length, Exact Sequences, and What the Factors Forget.

- (a) Let  $0 \rightarrow A \rightarrow M \xrightarrow{q} C \rightarrow 0$  be an exact sequence of modules of finite length. Combine a composition series of  $A$  with the inverse images under  $q$  of the terms of a composition series of  $C$ . Verify that the successive quotients are the composition factors of  $A$  and of  $C$ , and prove that

$$\ell(M) = \ell(A) + \ell(C).$$

In particular, prove that length is additive for finite direct sums.

- (b) Show that  $\ell(M) = 0$  if and only if  $M = 0$ , and that a proper submodule has strictly smaller length. For an endomorphism  $f : M \rightarrow M$  of a module of finite length, use the exact sequences involving  $\ker(f)$  and  $\text{img}(f)$  to show that  $f$  is injective if and only if it is surjective, if and only if it is an automorphism.
- (c) In  $M = \mathbb{Z}/12\mathbb{Z}$ , check that

$$0 \subsetneq \langle \bar{6} \rangle \subsetneq \langle \bar{2} \rangle \subsetneq M \quad \text{and} \quad 0 \subsetneq \langle \bar{4} \rangle \subsetneq \langle \bar{2} \rangle \subsetneq M$$

are composition series. Compute their composition factors in order, and verify the Jordan–Hölder theorem in this example.

- (d) Construct composition series of  $\mathbb{Z}/p^2\mathbb{Z}$  and of  $(\mathbb{Z}/p\mathbb{Z})^2$ , and verify that their composition factors agree. Show that multiplication by  $p$  is nonzero on the first module and zero on the second, and deduce that the modules are not isomorphic.
- (e) Show that  $\mathbb{Z}/p^2\mathbb{Z}$  is not a direct sum of two nonzero submodules. One approach is to list its subgroups. Compare this with the direct sum  $(\mathbb{Z}/p\mathbb{Z})^2$ .

A nonzero module  $M$  is *indecomposable* if whenever  $M = A \oplus B$ , either  $A = 0$  or  $B = 0$ . Every simple module is indecomposable, but Problem 5(e) shows that the converse fails. It is worth keeping this distinction in view: a composition series is built from successive quotients, while a direct sum decomposition requires complementary submodules.

Direct sum decompositions have an equivalent description in terms of endomorphisms. The projection onto a direct summand is an *idempotent*, meaning an endomorphism  $e$  with  $e^2 = e$ . Conversely, we will see that every idempotent endomorphism  $e$  gives a decomposition

$$M = \text{img}(e) \oplus \ker(e).$$

Thus a nonzero module is indecomposable exactly when its endomorphism ring has no idempotents other than 0 and  $1 = \text{Id}_M$ . Notice that the endomorphism ring, whose multiplication is composition, may be noncommutative even when  $R$  is commutative.

For a module of finite length, it is fairly direct to decompose it into indecomposable summands. If the module is not indecomposable, split it, and then split any summand which is not indecomposable. Passing to a nonzero proper summand lowers the length, so this process cannot continue forever. Uniqueness of the decomposition is more subtle, and requires more information about the endomorphisms of an indecomposable module. We prove the existence of decompositions in the following exercise.

**6. Splittings and Idempotents.** Throughout this exercise let  $M$  be an  $R$ -module.

- (a) If  $M = A \oplus B$ , verify that the projection onto  $A$  along  $B$ , regarded as an endomorphism of  $M$ , is idempotent. Identify its image and kernel.
- (b) If  $e^2 = e$ , write  $m = e(m) + (m - e(m))$  and prove that  $M = \text{img}(e) \oplus \ker(e)$ . Deduce the criterion for indecomposability stated above.
- (c) Use induction on length to prove that every nonzero module of finite length is a finite direct sum of indecomposable modules. What is the decomposition of the zero module? Explain why the induction only uses strictly smaller positive lengths when a summand is split.
- (d) Identify the indecomposable summands of a nonzero finite-dimensional vector space, regarded as a module over its field. In this case, how is the number of summands related to length and to dimension?

Let  $f : M \rightarrow M$  be an endomorphism of a module of finite length. Iterating  $f$  gives two chains of submodules:

$$\ker(f) \subset \ker(f^2) \subset \cdots \quad \text{and} \quad \text{img}(f) \supset \text{img}(f^2) \supset \cdots.$$

Since  $M$  has finite length, both chains stabilize. The stable kernel consists of the elements which are eventually sent to zero, while the stable image consists of the elements which can still be reached after

arbitrarily many iterations. We will see that once the chains have stopped changing, these two submodules are complementary.

More precisely, for all sufficiently large  $n$  there is a decomposition, called the *Fitting decomposition*,

$$M = \ker(f^n) \oplus \operatorname{img}(f^n).$$

An endomorphism is *nilpotent* if some positive power of it is zero. We will see that  $f$  is nilpotent on the first summand and an automorphism on the second. Notice that this decomposition does not require a field, a basis, or a characteristic polynomial; it is a consequence of the two chain conditions.

If  $M$  is also indecomposable, then one of the two summands must be zero. Consequently, every endomorphism of a nonzero indecomposable module of finite length is either an automorphism or nilpotent. This is a strong restriction, and we will use it to compare different decompositions. We prove these statements in the following exercise.

**7. The Stable Kernel and Stable Image.** Throughout this exercise let  $M$  have finite length, and let  $f : M \rightarrow M$  be an endomorphism.

(a) Choose  $n \geq 1$  so large that both chains have stabilized by their  $n$ th terms. In particular, justify that

$$\ker(f^n) = \ker(f^{2n}) \quad \text{and} \quad \operatorname{img}(f^n) = \operatorname{img}(f^{2n}).$$

(b) If  $y = f^n(x)$  lies in  $\ker(f^n)$ , use the equality of kernels to prove that  $y = 0$ . Deduce that  $\ker(f^n) \cap \operatorname{img}(f^n) = 0$ .

(c) Given  $m \in M$ , use the equality of images to find  $x \in M$  with  $f^n(m) = f^{2n}(x)$ . Show that  $m - f^n(x) \in \ker(f^n)$ , and deduce the Fitting decomposition.

(d) Show that  $f$  preserves both summands, that  $f$  is nilpotent on  $\ker(f^n)$ , and that  $f$  is an automorphism of  $\operatorname{img}(f^n)$ . For the last statement, use stability of the images for surjectivity, and part (b) for injectivity. More generally, show that every endomorphism commuting with  $f$  preserves both summands.

(e) Suppose  $M$  is nonzero and indecomposable. Deduce that every  $f \in \operatorname{End}_R(M)$  is either invertible or nilpotent. Which conclusion occurs when each of the two summands is zero?

You have met commutative local rings when studying localization. For a ring which may be noncommutative, we will say that a nonzero ring is *local* if it has a unique maximal left ideal. For the endomorphism rings which appear here, we will prove a more concrete description: the nonunits form a proper two-sided ideal. This immediately makes that ideal the unique maximal left ideal, and also the unique maximal right ideal, since a proper one-sided ideal cannot contain a unit.

Why should such an ideal appear? Let  $M$  be a nonzero indecomposable module of finite length. By the Fitting decomposition, every endomorphism  $h$  of  $M$  which is not invertible is nilpotent, and then  $1 - h$  is invertible, with inverse

$$1 + h + \cdots + h^{n-1} \quad \text{if } h^n = 0.$$

This gives a way to test a proposed sum of nonunits. If  $f + g$  were invertible for nonunits  $f$  and  $g$ , multiplying on the left by its inverse would produce two nonunits summing to 1. But 1 minus a nilpotent endomorphism is invertible, which gives a contradiction.

There is a noncommutative point to settle before we can use this argument: a product involving a nonunit must again be a nonunit. In an arbitrary ring, one-sided inverses deserve care. Here, however, a one-sided inverse makes an endomorphism injective or surjective, and finite length then makes it an automorphism. These facts about modules give exactly the properties of the ring which we need. We prove these statements in the following exercise.

**8. The Endomorphism Ring of an Indecomposable Module.** Throughout this exercise let  $M$  be a nonzero indecomposable module of finite length, put  $E := \text{End}_R(M)$ , and let  $J \subset E$  be the set of nonunits of  $E$ .

- (a) Show that an endomorphism with a left inverse is injective, and that one with a right inverse is surjective. Use Problem 5(b) to conclude that an endomorphism with either kind of one-sided inverse is a unit of  $E$ .
- (b) Verify that  $0 \in J$ , that  $1 \notin J$ , and that  $-f \in J$  whenever  $f \in J$ . For  $a \in E$  and  $f \in J$ , suppose  $af$  is invertible, and use  $(af)^{-1}a$  to obtain a contradiction. Similarly, use  $a(fa)^{-1}$  to show that  $fa$  is not invertible. Thus  $af, fa \in J$ .
- (c) Suppose  $f, g \in J$ , but  $u := f + g$  is a unit. By part (b),  $h := u^{-1}f$  is a nonunit, and hence nilpotent by Problem 7. Verify directly that  $1 - h$  is invertible using the finite geometric sum. Since  $1 - h = u^{-1}g$ , obtain a contradiction, and deduce that  $J$  is closed under addition.
- (d) Conclude that  $J$  is a proper two-sided ideal. Show that every proper left ideal and every proper right ideal of  $E$  is contained in  $J$ , so that  $E$  is local in the sense above. Show also that  $E/J$  is a division ring.
- (e) If  $a_1 + \cdots + a_s = 1$  in  $E$ , prove that at least one  $a_i$  is invertible. This is the consequence of locality which we will use in the next exercise.
- (f) More generally, suppose the nonunits of a nonzero ring form an ideal. Show that the ring has no idempotents other than 0 and 1, by applying the previous part to  $e + (1 - e) = 1$  and using  $e^2 = e$ . Explain why a module with such an endomorphism ring is indecomposable.

We can now prove that decompositions into indecomposable modules are unique. The *Krull–Schmidt theorem* says that the indecomposable summands of a module of finite length are determined up to isomorphism and order. Unlike the Jordan–Hölder theorem, it concerns direct summands rather than successive quotients, and the summands need not be simple.

Suppose we have two decompositions of the same module:

$$M = A_1 \oplus \cdots \oplus A_r = B_1 \oplus \cdots \oplus B_s.$$

Start with  $A_1$ : include it into  $M$ , project onto some  $B_j$ , include  $B_j$  back into  $M$ , and project back onto  $A_1$ . Adding up these round trips over all  $j$  gives  $\text{Id}_{A_1}$ . Since  $\text{End}_R(A_1)$  is local, at least one of the round trips is invertible, and we will see that the corresponding map  $A_1 \rightarrow B_j$  is an isomorphism.

After matching these two summands, we still need to compare the remaining summands. Notice that an isomorphism between one pair of summands does not by itself give an isomorphism between their complements. Instead, we will replace  $B_j$  in the second decomposition by the submodule  $A_1 \subset M$  itself. Then the two remaining sums are complements of the same submodule, so both are isomorphic to the quotient by it. This exchange is the step which makes induction possible.

**Theorem 2** (Krull–Schmidt for Modules of Finite Length). *Every nonzero module of finite length is a finite direct sum of indecomposable modules. If two such decompositions have  $r$  and  $s$  summands, then  $r = s$ , and after reordering the summands of the two decompositions are pairwise isomorphic.*

We prove the theorem in the following exercise.

**9. Matching a Summand and Exchanging Complements.** Existence was proved in Problem 6. For uniqueness, consider the two decompositions above, with all summands indecomposable. Write  $i_a : A_a \rightarrow M$  and  $p_a : M \rightarrow A_a$  for the inclusions and projections of the first decomposition, and  $j_b : B_b \rightarrow M$  and  $q_b : M \rightarrow B_b$  for those of the second.

(a) Verify that  $\sum_{b=1}^s j_b q_b = \text{Id}_M$ , and deduce that

$$\text{Id}_{A_1} = \sum_{b=1}^s p_1 j_b q_b i_1.$$

Each term is an endomorphism of  $A_1$ . Use Problem 8(e) to choose an invertible term, and relabel so that it is the term with  $b = 1$ .

(b) Set  $u := q_1 i_1 : A_1 \rightarrow B_1$  and  $v := p_1 j_1 : B_1 \rightarrow A_1$ , so that  $vu$  is invertible. Define  $w := (vu)^{-1}v$ , and check that  $wu = \text{Id}_{A_1}$ . Prove that

$$B_1 = u(A_1) \oplus \ker(w).$$

Since  $B_1$  is indecomposable and  $A_1 \neq 0$ , deduce that  $u$  is an isomorphism.

(c) Let  $B' := B_2 \oplus \cdots \oplus B_s = \ker(q_1)$ , viewed as a submodule of  $M$ . Given  $m \in M$ , check that

$$m - i_1 u^{-1} q_1(m) \in B'.$$

Show also that  $i_1(A_1) \cap B' = 0$ . Conclude that  $M = i_1(A_1) \oplus B'$ . In other words, the first summand of the  $A$ -decomposition can replace  $B_1$  in the  $B$ -decomposition.

- (d) Put  $A' := A_2 \oplus \cdots \oplus A_r$ . Restrict the quotient map  $M \rightarrow M/i_1(A_1)$  to  $A'$  and to  $B'$ , and show that both restrictions are isomorphisms. Deduce that  $A' \cong B'$ .
- (e) Complete the proof by induction on  $\ell(M)$ , transporting the decomposition of  $B'$  along this isomorphism. Why is the length of the remaining module strictly smaller? Include the case where the remaining module is zero, and one or both of the lists of remaining summands is empty.
- (f) Does the theorem say that the summands themselves are uniquely determined as submodules of  $M$ ? Use different decompositions of  $\mathbb{K}^2$  as a direct sum of two lines to explain the difference between uniqueness of submodules and uniqueness of their isomorphism types, counted with multiplicity.

Let us bring the two decomposition theorems together in a family of modules which we can compute explicitly. Fix  $N \geq 1$  and let

$$A := \mathbb{K}[x]/\langle x^N \rangle \quad \text{and} \quad t := x + \langle x^N \rangle \in A.$$

For  $1 \leq j \leq N$ , put  $M_j := A/\langle t^j \rangle$ . In particular,  $M_N = A$ , since  $t^N = 0$ . Each  $M_j$  has  $\mathbb{K}$ -basis  $1, t, \dots, t^{j-1}$ , where we now read these elements in the quotient. By Worksheet 6.1, every finite-dimensional  $A$ -module is a direct sum of modules of this form, and we will see that this is its decomposition into indecomposable modules.

An endomorphism of  $M_j$  is determined by the image of  $1$ , and every element of  $M_j$  can occur as that image, since  $t^j$  annihilates all of  $M_j$ . Thus the endomorphism ring of  $M_j$  is again a truncated polynomial ring. In that ring, an element with nonzero constant term is invertible: factor out the constant term, and use a finite geometric series to invert the remaining factor, whose nonconstant part is nilpotent. The elements with zero constant term form the ideal generated by  $t$ . This gives a concrete example of the local endomorphism rings used to prove the Krull–Schmidt theorem.

Composition factors tell a different story. Multiplication by successive powers of  $t$  gives a composition series of  $M_j$  with  $j$  factors, all isomorphic to  $A/\langle t \rangle \cong \mathbb{K}$ . Thus the composition factors of a finite-dimensional  $A$ -module only record its dimension, while its indecomposable summands record how that dimension is grouped into modules  $M_j$ . To distinguish these groupings, we can examine how powers of  $t$  act. We compare the two theorems in the following exercise.

10. **Composition Factors and Indecomposable Pieces.** Throughout this exercise let  $A$ ,  $t$ , and  $M_j$  be as above.

- (a) Define a map  $A/\langle t^j \rangle \rightarrow \text{End}_A(M_j)$  by sending an element to multiplication by it on  $M_j$ . Prove that this map is an isomorphism of rings, using the image of 1 to prove both injectivity and surjectivity.
- (b) In  $A/\langle t^j \rangle$ , show that an element is a unit if and only if its constant term is nonzero, and write down its inverse as a finite geometric series in that case. Show that the nonunits form the ideal  $\langle t \rangle$ , and conclude that  $\text{End}_A(M_j)$  is local and  $M_j$  is indecomposable.

(c) Show that

$$0 = t^j M_j \subsetneq t^{j-1} M_j \subsetneq \cdots \subsetneq t^0 M_j = M_j$$

is a composition series, with every factor isomorphic to  $A/\langle t \rangle$ . What is this chain when  $j = 1$ ? Deduce that  $\ell_A(M_j) = j$ .

- (d) Use the classification of Worksheet 6.1 together with part (b) to describe the decomposition of every finite-dimensional  $A$ -module into indecomposable modules, and apply the Krull–Schmidt theorem to show that it is unique. Show that all of its composition factors are isomorphic to  $A/\langle t \rangle$ , and that its length equals its dimension over  $\mathbb{K}$ .

(e) Suppose  $N \geq 3$ , and compare

$$U := M_3 \oplus M_1 \quad \text{and} \quad V := M_2 \oplus M_2.$$

List their composition factors and their indecomposable summands. Compute  $\dim_{\mathbb{K}}(t^2 U)$  and  $\dim_{\mathbb{K}}(t^2 V)$  to prove directly that  $U \not\cong V$ . Explain how each of the two uniqueness theorems applies to this example.

- (f) Suppose  $N = 2$ , and compare  $A = M_2$  with  $M_1 \oplus M_1$ . Write down a short exact sequence  $0 \rightarrow M_1 \rightarrow A \rightarrow M_1 \rightarrow 0$ , and show that it does not split. Which facts about  $A$  make this consistent with its two simple composition factors?