

# NOETHERIAN MODULES

KEITH CONRAD

## 1. INTRODUCTION

In a finite-dimensional vector space, every subspace is finite-dimensional and the dimension of a subspace is at most the dimension of the whole space. Unfortunately, the naive analogue of this for modules and submodules is wrong:

- (1) A submodule of a finitely generated module need not be finitely generated.
- (2) Even if a submodule of a finitely generated module is finitely generated, the minimal number of generators of the submodule is not bounded above by the minimal number of generators of the original module.

**Example 1.1.** Every commutative ring  $R$  is finitely generated as an  $R$ -module, namely with the generator 1, and the submodules of  $R$  are its ideals. Therefore a commutative ring that has an ideal that is not finitely generated gives us an example of a finitely generated module and non-finitely generated submodule.

Let  $R = \mathbf{R}[X_1, X_2, \dots]$  be the polynomial ring over  $\mathbf{R}$  (or another field) in countably many variables. Inside  $R$  let  $I = (X_1, X_2, \dots)$  be the ideal generated by the variables: this is the set of polynomials with constant term 0. To prove  $I$  is not finitely generated as an  $R$ -module, we will show each finitely generated ideal  $Rf_1 + Rf_2 + \dots + Rf_k$  in  $R$  doesn't contain  $X_i$  for all large  $i$ , so this ideal is not  $I$ .

Since each of the polynomials  $f_1, \dots, f_k$  involves only a finite number of variables, there's a large  $n$  such that all  $X_i$  appearing in one of  $f_1, \dots, f_k$  have  $i < n$ . The substitution homomorphism  $R \rightarrow \mathbf{R}$  that sends  $X_i$  to 0 for  $i < n$  and  $X_i$  to 1 for  $i \geq n$  sends  $f_1, \dots, f_k$  to 0 and therefore it sends every  $R$ -linear combination of  $f_1, \dots, f_k$  to 0. Since this homomorphism sends  $X_i$  to 1 for  $i \geq n$ , such  $X_i$  do not lie in  $Rf_1 + \dots + Rf_k$ .

**Example 1.2.** Here is an interesting example from complex analysis. Let  $R$  be the ring of entire functions on  $\mathbf{C}$ , *i.e.*,  $R$  consists of power series with complex coefficients and infinite radius of convergence. It turns out that every finitely generated ideal in  $R$  is a principal ideal, but that does not mean all ideals in  $R$  are principal: one example of an ideal in  $R$  that is not finitely generated is the ideal of entire functions vanishing on all but finitely many integers (the integers where the function doesn't vanish can vary with the function). Proofs of these facts about  $R$  require hard theorems in complex analysis about the existence of holomorphic functions with prescribed zeros. See [1, Remark 3.5.4, Corollary 3.5.8].

**Example 1.3.** An example of a finitely generated module and finitely generated submodule requiring more generators than the larger module is  $R = \mathbf{Z}[X]$  and  $I = (2, X)$ . As an  $R$ -module,  $R$  requires the single generator 1. The ideal  $I$  is not principal, so the fewest number of generators needed for  $I$  as an  $R$ -module is 2.

Another example is  $R = \mathbf{R}[X, Y]$  and  $I = (X, Y)$  since  $I$  is a non-principal ideal in  $R$ .

The property of being finitely generated is not well-behaved on passage to submodules (that is, a finitely generated module can have non-finitely generated submodules), so we

will give a name to the modules in which every submodule is finitely generated. Emmy Noether was the first mathematician to make a systematic study of this property, so these modules are named after her.

**Definition 1.4.** Let  $R$  be a commutative ring. An  $R$ -module is called *Noetherian* if every submodule is finitely generated.

The significance of the Noetherian condition on modules is twofold: (1) lots of modules that arise in algebra satisfy this condition and (2) this condition behaves well under many standard constructions on modules. Imposing the Noetherian condition on modules in a theorem is often regarded as a rather mild restriction.

**Example 1.5.** If  $F$  is a field, a finite-dimensional  $F$ -vector space  $V$  is a Noetherian  $F$ -module, since the submodules of  $V$  are its subspaces and they are all finite-dimensional by standard linear algebra.

**Example 1.6.** Generalizing the previous example, if  $R$  is a PID then every finitely generated  $R$ -module is a Noetherian module. This will be a consequence of Theorem 2.6.

An example of a non-Noetherian module is a module that is not finitely generated. For example, an infinite-dimensional vector space over a field  $F$  is a non-Noetherian  $F$ -module, and for a nonzero ring  $R$  the countable direct sum  $\bigoplus_{n \geq 1} R$  is a non-Noetherian  $R$ -module. If a ring  $R$  has an ideal that is not finitely generated then  $R$  is a non-Noetherian  $R$ -module.

The next theorem gives some standard equivalent conditions for being a Noetherian module. We will not use these other conditions here. Condition (2), called the ascending chain condition (ACC) can be turned around into a descending chain condition that defines the class of Artinian modules, and condition (3) leads to the idea of “Noetherian induction”, which is useful in algebraic geometry.

**Theorem 1.7.** *The following conditions on an  $R$ -module  $M$  are equivalent:*

- (1) *all submodules of  $M$  are finitely generated (i.e.,  $M$  is a Noetherian  $R$ -module).*
- (2) *each infinite increasing sequence of submodules  $N_1 \subset N_2 \subset N_3 \subset \dots$  in  $M$  eventually stabilizes:  $N_k = N_{k+1}$  for all large  $k$ .<sup>1</sup>*
- (3) *Every nonempty collection  $S$  of submodules of  $M$  contains a maximal element with respect to inclusion: there’s a submodule in  $S$  not strictly contained in another submodule in  $S$ .*

*Proof.* (1)  $\Rightarrow$  (2): If  $N_1 \subset N_2 \subset \dots$  is an increasing sequence of submodules, let  $N = \bigcup_{i \geq 1} N_i$ . This is a submodule since each pair of elements in  $N$  lies in a common  $N_i$ , by the increasing condition, so  $N$  is closed under addition and multiplication by elements of  $R$ . By (1),  $N$  is finitely generated. Using the increasing condition again, each finite subset of  $N$  lies in a common  $N_i$ , so a finite generating set of  $N$  is in some  $N_i$ . Thus  $N \subset N_i$ , and of course also  $N_i \subset N$ , so  $N = N_i$ . Then for all  $j \geq i$ ,  $N_i \subset N_j \subset N = N_i$ , so  $N_j = N_i$ .

(2)  $\Rightarrow$  (3): We will prove the negation of (3) implies the negation of (2). If (3) is false then there is a nonempty collection  $S$  of submodules of  $M$  containing no maximal member with respect to inclusion. Therefore if we start with a module  $N_1$  in  $S$ , we can recursively find modules  $N_2, N_3, \dots$  such that  $N_i$  strictly contains  $N_{i-1}$  for all  $i \geq 2$ . (If there were no submodule in  $S$  strictly containing  $N_{i-1}$  then  $N_{i-1}$  would be a maximal element of  $S$ , which doesn’t exist.)

<sup>1</sup>The notation  $\subset$  only means containment, not strict containment.

(3)  $\Rightarrow$  (1): Let  $N$  be a submodule of  $M$ . To prove  $N$  is finitely generated, let  $S$  be the set of all finitely generated submodules of  $N$ . By (3), there is an  $\tilde{N} \in S$  that's contained in no other element of  $S$ , so  $\tilde{N}$  is a finitely generated submodule of  $N$  and no other finitely generated submodule of  $N$  contains  $\tilde{N}$ . We will show  $\tilde{N} = N$  by contradiction, which would prove  $N$  is finitely generated. If  $\tilde{N} \neq N$ , pick  $n \in N - \tilde{N}$ . Since  $\tilde{N}$  is finitely generated, also  $\tilde{N} + Rn$  is finitely generated, so  $\tilde{N} + Rn \in S$ . However,  $\tilde{N} + Rn$  strictly contains  $\tilde{N}$ , which contradicts maximality of  $\tilde{N}$  as a member of  $S$ . Thus  $\tilde{N} = N$ .  $\square$

## 2. PROPERTIES OF NOETHERIAN MODULES

**Theorem 2.1.** *If  $M$  is a Noetherian  $R$ -module then every submodule of  $M$  is Noetherian.*

*Proof.* This is an immediate consequence of the definition of a Noetherian module, since a submodule of a submodule is a submodule.  $\square$

**Theorem 2.2.** *If  $M$  is a Noetherian  $R$ -module then every quotient module  $M/N$  is Noetherian.*

*Proof.* Every submodule of  $M/N$  has the form  $L/N$  where  $L$  is a submodule of  $M$  with  $N \subset L \subset M$ . Since  $M$  is Noetherian,  $L$  is finitely generated, and the reduction of those generators mod  $N$  will generate  $L/N$  as an  $R$ -module.  $\square$

**Theorem 2.3.** *Let  $M$  be an  $R$ -module and  $N$  be a submodule. Then  $M$  is Noetherian if and only if  $N$  and  $M/N$  are Noetherian.*

*Proof.* If  $M$  is Noetherian then  $N$  and  $M/N$  are Noetherian by Theorems 2.1 and 2.2. Conversely, suppose  $N$  and  $M/N$  are Noetherian. To prove  $M$  is Noetherian, let  $L$  be a submodule of  $M$ . Then the image of  $L$  in  $M/N$  is finitely generated and  $L \cap N$  is finitely generated. Let  $x_1, \dots, x_k \in L$  generate the image of  $L$  in  $M/N$  and let  $y_1, \dots, y_\ell$  generate  $L \cap N$ . For each  $x \in L$ , we have  $x \equiv r_1x_1 + \dots + r_kx_k \pmod{N}$  for some  $r_i \in R$ , so  $x - \sum r_ix_i \in L \cap N$ . Therefore  $x - \sum r_ix_i = \sum s_jy_j$  with  $s_j \in R$ , so  $x = \sum r_ix_i + \sum s_jy_j$ . Therefore  $L$  is spanned by  $x_1, \dots, x_k, y_1, \dots, y_\ell$ .  $\square$

Make sure to remember the ideas in this proof, as it's the only property of Noetherian modules we discuss here that involves a real idea (how to pass from a property of submodules of  $N$  and  $M/N$  to that property for submodules of  $M$ ).

**Theorem 2.4.** *If  $M$  and  $N$  are Noetherian  $R$ -modules then their direct sum  $M \oplus N$  is a Noetherian  $R$ -module.*

*Proof.* A fake proof would say that a submodule of  $M \oplus N$  has the form  $P \oplus Q$  for submodules  $P$  of  $M$  and  $Q$  of  $N$ , so  $P$  and  $Q$  are each finitely generated, and the union of those generating sets is a finite generating set for  $P \oplus Q$ . The reason this proof is fake is that submodules of  $M \oplus N$  need not be of the form  $P \oplus Q$ . For example, inside  $\mathbf{Z} \oplus \mathbf{Z}$  is the  $\mathbf{Z}$ -submodule  $\mathbf{Z}(1, 1) = \{(n, n) : n \in \mathbf{Z}\}$ .

For a valid proof, apply Theorem 2.3 to the module  $M \oplus N$  and submodule  $M \oplus 0 \cong M$ , where  $(M \oplus N)/(M \oplus 0) \cong N$ .  $\square$

**Corollary 2.5.** *If  $M_1, \dots, M_k$  are Noetherian  $R$ -modules then  $M_1 \oplus \dots \oplus M_k$  is a Noetherian  $R$ -module.*

*Proof.* Induct on  $k$ , with  $k = 2$  being Theorem 2.4.  $\square$

**Theorem 2.6.** *If  $R$  is a PID then every finitely generated  $R$ -module is a Noetherian  $R$ -module.*

*Proof.* Let  $M$  be a finitely generated  $R$ -module with generators  $m_1, \dots, m_k$ . Then there is a surjective  $R$ -linear map  $f: R^k \rightarrow M$  by  $f(c_1, \dots, c_k) = c_1m_1 + \dots + c_km_k$ , so  $M$  is isomorphic to a quotient module of  $R^k$ . Since  $R$  is a PID it is a Noetherian  $R$ -module, and therefore so is the  $k$ -fold direct sum  $R^k$  (Theorem 2.5) and so are quotient modules of  $R^k$  (Theorem 2.2).  $\square$

**Remark 2.7.** When  $R$  is a PID, the number of generators in a finitely generated  $R$ -module behaves like vector spaces: if  $M$  is a module over a PID with  $n$  generators then every submodule of  $M$  needs at most  $n$  generators. We don't discuss a proof here.

### 3. NOETHERIAN RINGS

**Definition 3.1.** A commutative ring  $R$  is called *Noetherian* if all ideals of  $R$  are finitely generated.

A simple (and boring) example of a Noetherian ring is a field. A more general class of examples are PIDs, since all of their ideals are singly generated. Noetherian rings can be regarded as a good generalization of PIDs: the property of all ideals being singly generated is often not preserved under common ring-theoretic constructions (*e.g.*,  $\mathbf{Z}$  is a PID but  $\mathbf{Z}[X]$  is not), but the property of all ideals being finitely generated does remain valid under many constructions of new rings from old rings. For example, we will see below that every quadratic ring  $\mathbf{Z}[\sqrt{d}]$  is Noetherian, even though many of these rings are not PIDs.

The standard example of a non-Noetherian ring is a polynomial ring  $K[X_1, X_2, \dots]$  in infinitely many variables over a field  $K$ . The ring of entire functions on  $\mathbf{C}$  is also non-Noetherian since it has an ideal that is not finitely generated (Example 1.2). So that you don't think non-Noetherian rings must always be "really huge", there is a non-Noetherian ring contained in  $\mathbf{Q}[X]$ : the ring of integral-valued polynomials

$$\text{Int}(\mathbf{Z}) = \{f \in \mathbf{Q}[X] : f(\mathbf{Z}) \subset \mathbf{Z}\}$$

is not Noetherian. This ring is bigger than  $\mathbf{Z}[X]$ , *e.g.*,  $\binom{X}{2} = \frac{X(X-1)}{2}$  is in  $\text{Int}(\mathbf{Z}) - \mathbf{Z}[X]$ , as is  $\binom{X}{n} = \frac{X(X-1)\dots(X-n+1)}{n!}$  for all  $n \geq 2$ .

The equivalent conditions for being a Noetherian module in Theorem 1.7 carry over to conditions for being a Noetherian ring: We omit the proof.

**Theorem 3.2.** *The following conditions on a commutative ring  $R$  are equivalent:*

- (1)  *$R$  is Noetherian: all ideals of  $R$  are finitely generated.*
- (2) *each infinite increasing sequence of ideals  $I_1 \subset I_2 \subset I_3 \subset \dots$  in  $R$  eventually stabilizes:  $I_k = I_{k+1}$  for all large  $k$ .*
- (3) *Every nonempty collection  $S$  of ideals of  $R$  contains a maximal element with respect to inclusion: there's an ideal in  $S$  not strictly contained in another ideal in  $S$ .*

The following two theorems put the second condition of Theorem 3.2 to use.

**Theorem 3.3.** *Let  $R$  be a Noetherian ring. Each surjective ring homomorphism  $R \rightarrow R$  is injective, and thus is an isomorphism.*

*Proof.* Let  $\varphi: R \rightarrow R$  be a surjective ring homomorphism. Each iterate  $\varphi^n$  (the  $n$ -fold composition of  $\varphi$  with itself) is surjective and the kernels  $K_n = \ker(\varphi^n)$  are ideals in  $R$  that form an increasing chain:

$$K_1 \subset K_2 \subset K_3 \subset \cdots .$$

Since  $R$  is Noetherian,  $K_n = K_{n+1}$  for some  $n$ . Pick  $y \in \ker \varphi$ , so  $\varphi(y) = 0$ . Since  $\varphi^n$  is surjective,  $y = \varphi^n(x)$ , so  $0 = \varphi(\varphi^n(x)) = \varphi^{n+1}(x)$ . Then  $x \in \ker(\varphi^{n+1}) = \ker(\varphi^n)$ , so  $y = \varphi^n(x) = 0$ . Thus  $\ker \varphi$  is 0, so  $\varphi$  is injective.  $\square$

There is no analogue of Theorem 3.3 for injective ring homomorphisms. For example,  $\mathbf{R}[X]$  is a Noetherian ring since it's a PID and the substitution homomorphism  $f(X) \mapsto f(X^2)$  on  $\mathbf{R}[X]$  is an injective ring homomorphism that is not surjective.

**Theorem 3.4.** *If  $R$  is a Noetherian integral domain that is not a field, then every nonzero nonunit in  $R$  can be factored into irreducibles.*

We assume  $R$  is not a field because irreducible factorizations don't have a meaning for units, so we want  $R$  to contain some nonzero elements that aren't units.

*Proof.* This will be a proof by contradiction.

Suppose there is an element  $a$  in  $R$  that is not 0 or a unit and has no irreducible factorization. We will find another nonzero nonunit  $b \in R$  that does not admit a factorization into irreducibles and such that there is a strict inclusion of ideals  $(a) \subset (b)$ .

Since  $a$  is not irreducible and it is not 0 or a unit, there is a factorization  $a = bc$  where  $b$  and  $c$  are nonunits (and obviously they are not 0 either). If both  $b$  and  $c$  have an irreducible factorization then so does  $a$  (just multiply together irreducible factorizations for  $b$  and  $c$ ), so at least one of  $b$  or  $c$  has no irreducible factorization. Without loss of generality, say  $b$  has no irreducible factorization. Then since  $c$  is not a unit, the inclusion  $(a) \subset (b)$  is strict.

Rewriting  $b$  as  $a_1$ , we have a strict containment of ideals

$$(a) \subset (a_1)$$

where  $a_1$  is a nonzero nonunit with no irreducible factorization. Using  $a_1$  in the role of  $a$  in the previous paragraph, there is a strict inclusion of ideals

$$(a_1) \subset (a_2)$$

for some nonzero nonunit  $a_2$  that has no irreducible factorization. This argument can be repeated and leads to an infinite increasing chain of (principal) ideals

$$(3.1) \quad (a) \subset (a_1) \subset (a_2) \subset (a_3) \subset \cdots$$

where all inclusions are strict. This is impossible in a Noetherian ring, so we have a contradiction. Therefore nonzero nonunits without an irreducible factorization do not exist: all nonzero nonunits in  $R$  have an irreducible factorization.  $\square$

This theorem is *not* saying a Noetherian integral domain has unique factorization: just because elements have irreducible factorizations doesn't mean those are unique (up to the order of multiplication and multiplication of terms by units). Many Noetherian integral domains do not have unique factorization.

We now show that some basic operations on rings preserve the property of being Noetherian.

**Theorem 3.5.** *If  $R$  is a Noetherian ring then so is  $R/I$  for each ideal  $I$  in  $R$ .*

*Proof.* Every ideal in  $R/I$  has the form  $J/I$  for an ideal  $J$  of  $R$  such that  $I \subset J \subset R$ . Since  $R$  is a Noetherian ring,  $J$  is a finitely generated ideal in  $R$ , and that finite generating set for  $J$  reduces to a generating set for  $J/I$  as an ideal of  $R/I$ .

As an alternative proof, view  $R/I$  as an  $R$ -module in the natural way:  $r(x \bmod I) = rx \bmod I$ . This equals  $(r \bmod I)(x \bmod I)$ , so ideals in  $R/I$  are the same thing as  $R$ -submodules of  $R/I$ . We know  $R/I$  is a Noetherian *module* over  $R$ : both  $R$  and  $I$  are Noetherian  $R$ -modules, so their quotient  $R/I$  is a Noetherian  $R$ -module. Therefore  $R$ -submodules of  $R/I$  are finitely generated, which means the same thing as ideals of  $R/I$  being finitely generated.  $\square$

In the second proof we used the fact that a Noetherian ring is a Noetherian module over itself. In fact a commutative ring is a Noetherian ring if and only if it is a Noetherian module over itself. *Make sure you understand this.*

To create more examples of Noetherian rings we can use the following very important theorem.

**Theorem 3.6** (Hilbert Basis Theorem). *If  $R$  is a Noetherian ring then so is  $R[X]$ .*

The reason for the name ‘‘Basis Theorem’’ is historical. It’s not about bases in the sense of linear algebra, but about generating sets for ideals: an ideal in  $R[X]$  that is initially defined with infinitely many generators has a finite set of generators.

*Proof.* Let  $I$  be an ideal in  $R[X]$ . To prove  $I$  is finitely generated we assume it is not. Then  $I \neq (0)$ , so we may define  $f_1$  to be a nonzero element of  $I$  with least degree. Since  $I \neq (f_1)$ , as  $I$  is not finitely generated, we may define  $f_2$  to be a polynomial of least degree in  $I - (f_1)$ . Note  $\deg f_1 \leq \deg f_2$  by the minimality condition on  $\deg f_1$ . For  $k \geq 2$ , if we have defined  $f_1, \dots, f_k$  in  $I$  then  $I \neq (f_1, \dots, f_k)$  since  $I$  is not finitely generated, so we may define  $f_{k+1}$  to be a polynomial of least degree in  $I - (f_1, \dots, f_k)$ . In this way we have a sequence of polynomials  $f_1, f_2, \dots$  in  $I$  and  $\deg f_k \leq \deg f_{k+1}$  for all  $k$ : we checked this when  $k = 1$  before, and for  $k \geq 2$  both  $f_k$  and  $f_{k+1}$  are in  $I - (f_1, \dots, f_{k-1})$ , so  $\deg f_k \leq \deg f_{k+1}$  by the minimality condition on  $\deg f_k$ .

For each  $k \geq 1$ , let  $c_k$  be the leading coefficient of  $f_k$ . The ideal  $(c_1, c_2, \dots)$  in  $R$  generated by all  $c_k$ ’s is finitely generated since  $R$  is Noetherian. Each element in that ideal is an  $R$ -linear combination of only finitely many  $c_k$ , so  $(c_1, c_2, \dots) = (c_1, \dots, c_m)$  for some  $m$ .

Since  $c_{m+1} \in (c_1, c_2, \dots, c_m)$ , we have

$$(3.2) \quad c_{m+1} = \sum_{k=1}^m r_k c_k$$

for some  $r_k \in R$ . From the inequalities  $\deg f_k \leq \deg f_{m+1}$  for  $k \leq m$ , we can push the leading coefficients of each of  $f_1, \dots, f_m$  into the common degree  $\deg f_{m+1}$  by using  $f_k(X)X^{\deg f_{m+1} - \deg f_k}$ , which is in  $I$  since  $f_k(X) \in I$  and  $I$  is an ideal in  $R[X]$ . By (3.2), the  $R$ -linear combination

$$\sum_{k=1}^m r_k f_k(X) X^{\deg f_{m+1} - \deg f_k}$$

is in the ideal  $(f_1, \dots, f_m)$  and its leading term is  $\sum_{k=1}^m r_k c_k X^{\deg f_{m+1}} = c_{m+1} X^{\deg f_{m+1}}$ . That is also the leading term of  $f_{m+1}(X)$ , so the difference

$$(3.3) \quad \sum_{k=1}^m r_k f_k(X) X^{\deg f_{m+1} - \deg f_k} - f_{m+1}(X)$$

is in  $I$  and its degree is less than  $\deg f_{m+1}$ . (The difference is not 0 since  $f_{m+1} \notin (f_1, \dots, f_m)$ .) We have reached a contradiction, since that difference is in  $I - (f_1, \dots, f_m)$  with degree less than that of  $f_{m+1}(X)$ . Thus  $I$  is finitely generated.  $\square$

To summarize this proof in a single phrase, “use an ideal of leading coefficients”.

**Remark 3.7.** Our proof of the Hilbert Basis Theorem was by contradiction, so it is not constructive. A constructive proof runs as follows. For a nonzero ideal  $I$  in  $R[X]$  and  $n \geq 0$ , let  $L_n$  be the set of leading coefficients of  $n$ th degree polynomials in  $I$  together with 0. Check this is an ideal in  $R$ . (While  $L_n = (0)$  if there are no polynomials of degree  $n$  in  $I$ ,  $L_n \neq (0)$  for large  $n$  since  $I$  contains a nonzero polynomial and multiplying that by powers of  $X$  gives us polynomials in  $I$  of all higher degrees.) We have  $L_n \subset L_{n+1}$  (due to the effect of multiplying by powers of  $X$  again), so the ideals  $\{L_n\}$  in  $R$  stabilize at some point, say  $L_n = L_m$  for  $n \geq m$ . Each  $L_n$  has finitely many generators, and when  $L_n \neq (0)$  we let  $P_n$  be a finite set of degree- $n$  polynomials in  $I$  whose leading coefficients generate  $L_n$ . The union of the finitely many finite sets  $P_n$  for  $n \leq m$  turns out to be a set of generators of  $I$ .

Where in the proof of Theorem 3.6 did we use the assumption that  $R$  is Noetherian? It is how we know the ideals  $(c_1, \dots, c_k)$  for  $k \geq 1$  stabilize for large  $k$ , so  $c_{m+1} \in (c_1, \dots, c_m)$  for some  $m$ . The contradiction we obtain from that really shows  $c_{m+1} \notin (c_1, \dots, c_m)$  for all  $m$ , so the proof of Theorem 3.6 could be viewed as proving the contrapositive: if  $R[X]$  is not Noetherian then  $R$  is not Noetherian.

The converse of Theorem 3.6 is also true: if the ring  $R[X]$  is Noetherian then so is the ring  $R$  by Theorem 3.5, since  $R \cong R[X]/(X)$

**Corollary 3.8.** *If  $R$  is a Noetherian ring then so is  $R[X_1, \dots, X_n]$ .*

*Proof.* We induct on  $n$ . The case  $n = 1$  is Theorem 3.6. For  $n \geq 2$ , write  $R[X_1, \dots, X_n]$  as  $R[X_1, \dots, X_{n-1}][X_n]$ , with  $R[X_1, \dots, X_{n-1}]$  being Noetherian by the inductive hypothesis, so we are reduced to the base case.  $\square$

**Remark 3.9.** Corollary 3.8 when  $R$  is a field was proved by Hilbert in 1890 [3, Theorem 1, p. 474] as a pure existence theorem in a few pages, not by an algorithmic process.<sup>2</sup> This is what first made Hilbert famous in mathematics. Earlier, Gordan [2] settled the case  $n = 2$  in 1868 by long calculations and spent 20 years unsuccessfully working on  $n = 3$ . Hilbert’s proof for all  $n$  was revolutionary, as it illustrated the power of existence proofs over laborious constructive methods, and that became characteristic of much of modern mathematics. With the rise of fast computers in the late 20th century, generating sets for polynomial ideals are now computed routinely using Gröbner bases, which are essentially a multivariable polynomial replacement for the Euclidean algorithm of polynomials in one variable.

Now we can build lots of Noetherian rings. The quadratic ring  $\mathbf{Z}[\sqrt{d}]$  for a nonsquare integer  $d$  is Noetherian, since it’s isomorphic to  $\mathbf{Z}[X]/(X^2 - d)$ , with  $\mathbf{Z}[X]$  Noetherian by Hilbert’s basis theorem and then  $\mathbf{Z}[X]/(X^2 - d)$  is Noetherian by Theorem 3.5. Similarly, the rings  $\mathbf{Z}[\sqrt{2}, \sqrt{3}]$  and  $\mathbf{Z}[i, \sqrt[3]{2}, \sqrt[7]{10}]$  are Noetherian because they are isomorphic to  $\mathbf{Z}[X, Y]/(X^2 - 2, Y^2 - 3)$  and  $\mathbf{Z}[X, Y, Z]/(X^2 + 1, Y^3 - 2, Z^7 - 10)$ . The ring  $\mathbf{Z}[X, 1/X]$  is Noetherian since it is isomorphic to  $\mathbf{Z}[X, Y]/(XY - 1)$ .

<sup>2</sup>Hilbert could not use the exact proof that we gave for his basis theorem, since he didn’t have the concept of a Noetherian ring in full generality available to him.



For a field  $K$  and ideal  $I$  in  $K[X_1, \dots, X_n]$ , the ring  $K[X_1, \dots, X_n]/I$  is Noetherian since  $K$  is Noetherian (in a trivial way). For instance,

$$\mathbf{R}[X, Y, Z]/(X^2 + Y^3 - Z^5, XYZ)$$

is Noetherian.

**Remark 3.10.** In addition to polynomials in finitely many variables, formal power series in finitely many variables are important. For a Noetherian ring  $R$  the formal power series ring  $R[[X_1, \dots, X_n]]$  is Noetherian, and as in the polynomial case writing  $R[[X_1, \dots, X_n]]$  as  $R[[X_1, \dots, X_{n-1}]][[X_n]]$  reduces the proof to the case  $n = 1$ . A formal power series usually doesn't have a leading coefficient, so the proof in the polynomial case doesn't work directly for power series. What can be used with formal power series instead of a leading term is a lowest degree term, so the proof of Theorem 3.5 can be adapted to formal power series by changing highest-degree coefficients into lowest-degree coefficients, although an infinite "limiting process" occurs in the proof since the multipliers on a generating set for the ideal will be power series. See [4, Theorem 7.11].

#### 4. FINITELY GENERATED MODULES OVER A NOETHERIAN RING

Submodules of a finitely generated module need not be finitely generated; this in fact motivated our definition of a Noetherian module. We prove in the next theorem that when the scalar ring is Noetherian, the *a priori* weaker condition of a module being finitely generated implies the stronger condition that all of its submodules are finitely generated.

**Theorem 4.1.** *If  $R$  is a Noetherian ring then an  $R$ -module is Noetherian if and only if it is finitely generated. That is, if all ideals in  $R$  are finitely generated then all submodules of an  $R$ -module  $M$  are finitely generated if and only if  $M$  is finitely generated.*

*Proof.* From the definition of a Noetherian module, an  $R$ -module that is Noetherian has to be finitely generated. Now suppose an  $R$ -module  $M$  is finitely generated, so  $M$  is a quotient module of some  $R^k$ . The module  $R^k$  is Noetherian by Corollary 2.5 and every quotient module of  $R^k$  is Noetherian by Theorem 2.2. Thus  $M$  is Noetherian, so all submodules of  $M$  are finitely generated.  $\square$

**Remark 4.2.** The part of this proof showing finitely generated modules over Noetherian rings are Noetherian is very similar to the proof in Theorem 2.6 that finitely generated modules over a PID are Noetherian. In fact, the proofs are exactly the same: the only way the proof of Theorem 2.6 used that the ring is a PID is to be sure that the ring is a Noetherian module over itself, and that property is exactly what a Noetherian ring is.

Here is a nice application of this theorem.

**Theorem 4.3.** *If  $R$  is a Noetherian ring and  $M$  and  $N$  are finitely generated  $R$ -modules, then  $\text{Hom}_R(M, N)$  is a finitely generated  $R$ -module.*

*Proof.* Since  $M$  is finitely generated, it is isomorphic to a quotient module of some  $R^k$ , say  $M \cong R^k/L$ . Then  $\text{Hom}_R(M, N) \cong \text{Hom}_R(R^k/L, N)$ . The elements of  $\text{Hom}_R(R^k/L, N)$  are the  $R$ -linear maps  $R^k/L \rightarrow N$ . Such a map is the same thing as an  $R$ -linear map  $R^k \rightarrow N$  that vanishes on  $L$ . (Make sure you understand that.) The set of all  $R$ -linear maps  $R^k \rightarrow N$  vanishing on  $L$  is a submodule of  $\text{Hom}_R(R^k, N)$ , and the module  $\text{Hom}_R(R^k/L, N)$  can be identified with it. Thus  $\text{Hom}_R(M, N)$  can be embedded into  $\text{Hom}_R(R^k, N)$ .



Writing down an  $R$ -linear map  $R^k \rightarrow N$  is the same thing as choosing a  $k$ -tuple in  $N$  and sending the standard basis of  $R^k$  there and extending by linearity, so (check!)  $\text{Hom}_R(R^k, N) \cong N^k$  by  $f \mapsto (f(e_1), \dots, f(e_k))$ . Since  $N$  is a finitely generated  $R$ -module,  $N^k$  is also a finitely generated  $R$ -module, and  $\text{Hom}_R(M, N)$  embeds as a submodule of  $N^k$  by work above. Since  $R$  is a Noetherian ring,  $N^k$  is a Noetherian  $R$ -module by Theorem 4.1, so its submodules are finitely generated. Thus  $\text{Hom}_R(M, N)$  is finitely generated.  $\square$

If we drop the condition that  $R$  is a Noetherian ring, it can be false that  $\text{Hom}_R(M, N)$  is finitely generated when  $M$  and  $N$  are.

**Example 4.4.** For an ideal  $I$  in  $R$  we have  $\text{Hom}_R(R/I, R) \cong \{r \in R : Ir = 0\}$  (an  $R$ -linear map out of  $R/I$  is determined by where  $\bar{1}$  goes), so we will give an example of an  $R$  and  $I$  where  $\{r \in R : Ir = 0\}$  is not finitely generated. Both  $R$  and  $R/I$  are finitely generated  $R$ -modules, since each is generated by 1.

Let  $K$  be a field and  $R = K[X_1, X_2, \dots]/(\dots, X_i X_j, \dots)$ . Let  $I$  be the ideal of polynomial cosets in  $R$  with constant term 0. (The constant term of a coset is well-defined  $X_i X_j$  has constant term 0.) Then  $If = 0$  if and only if  $f$  has constant term 0, so  $\{f \in R : If = 0\} = I$ . That the ideal  $I$  is not finitely generated is very similar to the proof that  $(X_1, X_2, \dots)$  in  $K[X_1, X_2, \dots]$  is not finitely generated.

**Corollary 4.5.** *If  $R$  is a Noetherian ring and  $M$  and  $N$  are Noetherian  $R$ -modules, then  $\text{Hom}_R(M, N)$  is a Noetherian  $R$ -module.*

*Proof.* Combine Theorems 4.1 and 4.3.  $\square$

**Corollary 4.6.** *If  $R$  is a Noetherian ring and  $M$  is a finitely generated  $R$ -module then its dual module  $M^\vee$  is finitely generated.*

*Proof.* Apply Theorem 4.3 with  $N = R$ .  $\square$

Without the Noetherian condition on  $R$ , Corollary 4.6 can break down. Example 4.4 uses a dual module, so a finitely generated module might not have a finitely generated dual module when  $R$  is a non-Noetherian ring.

## REFERENCES

- [1] C. A. Berenstein and R. Gay, “Complex Variables: An Introduction”, Springer-Verlag, New York, 1991.
- [2] P. Gordan, *Beweis, dass jede Covariante und Invariante einer binären Form eine ganze Function mit numerischen Coefficienten einer endlichen Anzahl solcher Formen ist*, J. Reine Angew. Mathematik **69** (1868), 323–354. Online at <https://eudml.org/doc/148066>.
- [3] D. Hilbert, *Ueber die Theorie der algebraischen Formen*, Math. Annalen **36** (1890), 473–534. Online at <https://eudml.org/doc/157506>.
- [4] N. Jacobson, “Basic Algebra II”, 2nd ed., W. H. Freeman & Co., New York, 1989.