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 $Rf_1 + Rf_2 + \cdots + Rf_k$ 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 $R \to \mathbf{R}$ 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 $Rf_1 + \cdots + Rf_k$.

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, in her major paper [6] on ring theory in 1921, so these modules are named after her.[1]

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[2] on modules is twofold: (1) many 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 standard equivalent conditions for being a Noetherian module. We will use the second condition at the end of Section 2 and will not use the third one.

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 $N_1 \subset N_2 \subset N_3 \subset \cdots$ in M eventually stabilizes: $N_k = N_{k+1}$ for all large k.*[3]
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 $N_1 \subset N_2 \subset \cdots$ 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) $\Rightarrow$ (1): We prove the contrapositive. Suppose (1) is false, so M has a submodule N that is not finitely generated. Pick $n_1 \in N$. Since N is not finitely generated, $N \neq Rn_1$, so there is an $n_2 \in N - Rn_1$. Since $N \neq Rn_1 + Rn_2$, there is an $n_3 \in N - (Rn_1 + Rn_2)$. Proceed in a similar way to pick n_k in N for all $k \geq 1$ by making $n_k \notin N - (Rn_1 + \ldots + Rn_{k-1})$ for $k \geq 2$. Then we have an increasing sequence of submodules $Rn_1 \subset Rn_1 + Rn_2 \subset \cdots \subset$

[1] Strictly speaking, in [6] Noether focused mostly on rings whose ideals are all finitely generated. This is a special type of Noetherian module, namely a ring that is a Noetherian module over itself (its submodules are its ideals).

[2] Noether did not use the label "Noetherian", but referred in her paper [6] to "the finiteness condition" (die Endlichkeitsbedingung).

[3] The notation $\subset$ only means containment, not strict containment.

$Rn_1 + \ldots + Rn_k \subset \cdots$ in M where each submodule is *strictly* contained in the next one, so (2) is false.

(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 $N_2, N_3, \ldots$ such that N_k strictly contains N_{k-1} for all $k \geq 2$. (If there were no submodule in S strictly containing N_{k-1} then N_{k-1} would be a maximal element of S, which doesn't exist.)

(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 $\widetilde{N} \in S$ that's contained in no other element of S, so $\widetilde{N}$ is a finitely generated submodule of N and no other finitely generated submodule of N contains $\widetilde{N}$. We will show $\widetilde{N} = N$ by contradiction, which would prove N is finitely generated. If $\widetilde{N} \neq N$, pick $n \in N - \widetilde{N}$. Since $\widetilde{N}$ is finitely generated, also $\widetilde{N} + Rn$ is finitely generated, so $\widetilde{N} + Rn \in S$. However, $\widetilde{N} + Rn$ strictly contains $\widetilde{N}$, which contradicts maximality of $\widetilde{N}$ as a member of S. Thus $\widetilde{N} = N$. □

Condition (2) is called the ascending chain condition (ACC)[4] and there is an analogous descending chain condition that defines the class of Artinian modules. Condition (3) leads to the idea of "Noetherian induction", which is useful in algebraic geometry.

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. □

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. □

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 $x_1, \ldots, x_k \in L$ generate the image of L in M/N and let $y_1, \ldots, y_\ell$ generate $L \cap N$. For each $x \in L$, we have $x \equiv r_1 x_1 + \cdots + r_k x_k \bmod N$ for some $r_i \in R$, so $x - \sum r_i x_i \in L \cap N$. Therefore $x - \sum r_i x_i = \sum s_j y_j$ with $s_j \in R$, so $x = \sum r_i x_i + \sum s_j y_j$. Therefore L is spanned by $x_1, \ldots, x_k, y_1, \ldots, y_\ell$. □

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.*

[4]Noether called the result (1) $\Rightarrow$ (2) the "theorem of the finite chain" (Satz von der endlichen Kette).

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 $(M \oplus N)/(M \oplus 0) \cong N$. □

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

Proof. Induct on k, with $k = 2$ being Theorem 2.4. □

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 $m_1, \ldots, m_k$. Then there is a surjective R-linear map $f\colon R^k \to M$ by $f(c_1, \ldots, c_k) = c_1 m_1 + \cdots + c_k m_k$, 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). □

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.

The next theorem applies the second condition of Theorem 1.7 (ascending chain condition).

Theorem 2.8. *For a Noetherian R-module M, each surjective R-linear map $M \to M$ is injective and thus is an isomorphism.*

Proof. Let $\varphi\colon M \to M$ be a surjective R-linear map. For the nth iterate φ^n (the n-fold composition of φ with itself), let $K_n = \ker(\varphi^n)$. This is a submodule of M and these submodules form an increasing chain:

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

since $m \in K_n \Rightarrow \varphi^n(m) = 0 \Rightarrow \varphi^{n+1}(m) = \varphi(\varphi^n(m)) = \varphi(0) = 0$, so $m \in K_{n+1}$. Since M is a Noetherian R-module, $K_n = K_{n+1}$ for some n. Pick $m \in \ker \varphi$, so $\varphi(m) = 0$. The map φ^n is surjective since φ is surjective, so $m = \varphi^n(m')$ for some $m' \in M$. Thus $0 = \varphi(m) = \varphi(\varphi^n(m')) = \varphi^{n+1}(m')$. Therefore $m' \in \ker(\varphi^{n+1}) = \ker(\varphi^n)$, so $m = \varphi^n(m') = 0$. That shows $\ker \varphi = \{0\}$, so φ is injective. □

Theorem 2.8 does not have an analogue for injective R-linear maps. For example, $\mathbf{Z}$ is a Noetherian $\mathbf{Z}$-modules (its submodules are all principal, and thus finitely generated), and the mapping $\varphi\colon \mathbf{Z} \to \mathbf{Z}$ where $\varphi(m) = 2m$ is $\mathbf{Z}$-linear and injective but not surjective.

3. Noetherian rings

Definition 3.1. A commutative ring R is called *Noetherian*[5] if all ideals of R are finitely generated.

[5]The label "Noetherian ring" is due to Chevalley [2] in 1943.

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; 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). Non-Noetherian rings need not be "really huge", there is a non-Noetherian ring contained in $\mathbf{Q}[X]$: the ring of integral-valued polynomials

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

is not Noetherian. This ring is bigger than $\mathbf{Z}[X]$, *e.g.*, $\binom{X}{2} = \frac{X(X-1)}{2}$ is in $\mathrm{Int}(\mathbf{Z}) - \mathbf{Z}[X]$, as is $\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!}$ 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, as in the next theorem. 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 $I_1 \subset I_2 \subset I_3 \subset \cdots$ 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 (ascending chain condition) to use.

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

Proof. An analogue of this theorem was proved for a linear self-map on a Noetherian module in Theorem 2.8. We'll check that the proof carries over to Noetherian rings.

Let $\varphi\colon R \to R$ be a surjective ring homomorphism. Each iterate φ^n 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 φ^n is surjective, $y = \varphi^n(x)$, so $0 = \varphi(y) = \varphi(\varphi^n(x)) = \varphi^{n+1}(x)$. Then $x \in \ker(\varphi^{n+1}) = \ker(\varphi^n)$, so $y = \varphi^n(x) = 0$. Thus $\ker\varphi$ is 0, so φ is injective. □

As with the module analogue in Theorem 2.8, Theorem 3.3 does not have a variant for injective ring homomorphisms. For instance, $\mathbf{R}[X]$ 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 a as a_1 and b as a_2, we have a strict containment of ideals

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

where a_2 is a nonzero nonunit with no irreducible factorization. Using a_2 in the role of a_1 in the previous paragraph, there is a strict inclusion of ideals

$$(a_2) \subset (a_3)$$

for some nonzero nonunit a_3 that has no irreducible factorization. This argument can be repeated and leads to an infinite increasing chain of (principal) ideals

$$(a_1) \subset (a_2) \subset (a_3) \subset \cdots \tag{3.1}$$

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 in R: all nonzero nonunits in R have an irreducible factorization. □

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. □

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 that a generating set for an ideal may be called a "basis" even if it's not linearly independent (*cf.* the modern term "Gröbner basis"). The theorem says if each ideal in R has a "finite basis" then this is true of ideals in $R[X]$.

Proof. The theorem is clear if $R = 0$, so assume $R \neq \{0\}$. To prove each ideal I in $R[X]$ is finitely generated, we assume I is not finitely generated and will get a contradiction.

We have $I \neq (0)$. Define a sequence of polynomials $f_1, f_2, \dots$ in I as follows.

(1) Pick f_1 to be an element of $I - (0)$ with minimal degree. (It is not unique.)
(2) Since $I \neq (f_1)$, as I is not finitely generated, pick f_2 in $I - (f_1)$ with minimal degree. Note $\deg f_1 \leq \deg f_2$ by the minimality condition on $\deg f_1$.
(3) 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 pick f_{k+1} in $I - (f_1, \dots, f_k)$ with minimal degree.

We have $\deg f_k \leq \deg f_{k+1}$ for all k: the case $k = 1$ was checked before, and for $k \geq 2$, 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 $k \geq 1$, let $d_k = \deg f_k$ and c_k be the leading coefficient of f_k, so $d_k \leq d_{k+1}$ and $f_k(X) = c_k X^{d_k} +$ lower-degree terms.

The ideal $(c_1, c_2, \dots)$ in R (an ideal of leading coefficients) is finitely generated since R is Noetherian. Each element in this ideal is an R-linear combination of 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

$$c_{m+1} = \sum_{k=1}^{m} r_k c_k \tag{3.2}$$

for some $r_k \in R$. From the inequalities $d_k \leq d_{m+1}$ for $k \leq m$, the leading term in $f_k(X) = c_k X^{d_k} + \cdots$ can be moved into degree d_{m+1} by using $f_k(X)X^{d_{m+1}-d_k} = c_k X^{d_{m+1}} + \cdots$, and this is in I since $f_k(X) \in I$ and I is an ideal in $R[X]$. By (3.2), the R-linear combination

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

is in the ideal $(f_1, \dots, f_m)$ and its coefficient of $X^{d_{m+1}}$ is $\sum_{k=1}^{m} r_k c_k$, which equals the leading coefficient c_{m+1} of $f_{m+1}(X)$ in degree d_{m+1}. The difference

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

is in I, it is *not* 0 since $f_{m+1} \in I - (f_1, \dots, f_m)$, and it has degree *less than* d_{m+1} since the terms $c_{m+1}X^{d_{m+1}}$ cancel out. But $f_{m+1}(X)$ has minimal degree among polynomials in $I - (f_1, \dots, f_m)$, and (3.3) is in $I - (f_1, \dots, f_m)$ with lower degree than d_{m+1}. That's a contradiction. Thus I is finitely generated. □

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

In the proof, the Noetherian property of R is used where we said $(c_1, c_2, \dots) = (c_1, \dots, c_m)$ for some m. All we need to get the contradiction in the proof is $c_{m+1} \in (c_1, \dots, c_m)$ for some m. Since $(c_1) \subset (c_1, c_2) \subset (c_1, c_2, c_3) \subset \cdots$, what we need is the following property: for each infinite increasing sequence of ideals $I_1 \subset I_2 \subset I_3 \subset \cdots$ in R, $I_m = I_{m+1}$ for some

m. Of course this is implied by the Noetherian property, but it also implies the Noetherian property since a non-Noetherian ring has an infinite increasing sequence of ideals with strict containments at each step: see the proof of (2) $\Rightarrow$ (1) in Theorem 1.7 with $M = R$.

Remark 3.7. Our proof of the Hilbert Basis Theorem, which is due to Sarges [7], is by contradiction and thus is not constructive. A constructive proof runs as follows. For $R \neq 0$, I a nonzero ideal in $R[X]$, and $n \geq 0$, let L_n be the set of leading coefficients of polynomials in I of degree at most n together with 0. This is an ideal in R by the way polynomials add and get scaled by R. (While L_n might be (0) for small n, $L_n \neq (0)$ 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.) Since $L_n \subset L_{n+1}$, the ideals $\{L_n\}$ in R stabilize at some point, say $L_n = L_m$ for $n \geq m$. (Thus L_m is generated by the leading coefficients of *all* nonzero polynomials in I, so we could have defined L_m that way.) Each L_n has finitely many generators. When $L_n \neq (0)$, let P_n be a finite set of polynomials of degree at most n in I whose leading coefficients generate L_n. The union of the finite sets P_n for $n \leq m$ where $L_n \neq (0)$ is a generating set for I [5, Sect. 7.10]. This way of proving Hilbert's basis theorem is essentially due to Artin, according to van der Waerden [8].

Where in the proof of Theorem 3.6 did we use the assumption that R is Noetherian? It is how we know the ideals $(c_1, \ldots, c_k)$ for $k \geq 1$ stabilize for large k, so $c_{m+1} \in (c_1, \ldots, c_m)$ for some m. The contradiction we obtain from that really shows $c_{m+1} \notin (c_1, \ldots, c_m)$ 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 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 $R[X_1, \ldots, X_n]$.*

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

Remark 3.9. Corollary 3.8 when R is a field was proved by Hilbert in 1890 [4, Theorem 1, p. 474] as a pure existence theorem in a few pages, not by an algorithmic process.[6] This is what first made Hilbert famous in mathematics. Earlier, Gordan [3] 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 this became characteristic of much of modern mathematics. With the rise of fast computers in the late 20th century, generating sets for polynomial ideals can be computed routinely with Gröbner bases, which are 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: it's isomorphic to $\mathbf{Z}[X]/(X^2 - d)$, $\mathbf{Z}[X]$ is Noetherian by Hilbert's basis theorem, and $\mathbf{Z}[X]/(X^2 - d)$ is Noetherian by Theorem 3.5. Similarly, $\mathbf{Z}[\sqrt{2}, \sqrt{3}]$ 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 $\mathbf{Z}[X, Y]/(XY - 1)$.

[6] 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 $K[X_1, \ldots, X_n]$, the ring $K[X_1, \ldots, X_n]/I$ is Noetherian since K is trivially Noetherian. 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 $R[[X_1, \ldots, X_n]]$ is Noetherian, and as in the polynomial case writing $R[[X_1, \ldots, X_n]]$ as $R[[X_1, \ldots, X_{n-1}]][[X_n]]$ 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 [5, 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. □

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

Writing down an R-linear map $R^k \to N$ 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!) $\mathrm{Hom}_R(R^k, N) \cong N^k$ by $f \mapsto (f(e_1), \ldots, f(e_n))$. Since N is a finitely generated R-module, N^k is also a finitely generated R-module, and $\mathrm{Hom}_R(M, N)$ 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 $\mathrm{Hom}_R(M, N)$ is finitely generated. □

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

Example 4.4. For an ideal I in R we have $\mathrm{Hom}_R(R/I, R) \cong \{r \in R : Ir = 0\}$ (an R-linear map out of R/I is determined by where $\overline{1}$ 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 $R = K[X_1, X_2, \dots]/(\dots, X_iX_j, \dots)$. Let I be the ideal of polynomial cosets in R with constant term 0. (The constant term of a coset is well-defined since all X_iX_j have 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 $\mathrm{Hom}_R(M, N)$ is a Noetherian R-module.*

Proof. Combine Theorems 4.1 and 4.3. □

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 $N = R$. □

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] C. Chevalley, *On the Theory of Local Rings*, Ann. of Math. **44** (1943), 690–708. URL https://www.jstor.org/stable/1969105.

[3] 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. URL https://eudml.org/doc/148066.

[4] D. Hilbert, *Ueber die Theorie der algebraischen Formen*, Math. Annalen **36** (1890), 473–534. URL https://eudml.org/doc/157506.

[5] N. Jacobson, "Basic Algebra II", 2nd ed., W. H. Freeman & Co., New York, 1989.

[6] E. Noether, *Idealtheorie in Ringbereichen*, Math. Annalen **83** (1921), 24–66. URL https://eudml.org/doc/158855. English translation by D. Berlyne https://arxiv.org/abs/1401.2577.

[7] H. Sarges, *Ein Beweis des Hilbertschen Basissatzes*, J. Reine Angew. Math. **283** (1976), 436–437. URL https:// eudml.org/doc/151744.

[8] B. L. van der Waerden, *On the sources of my book Moderne Algebra*, Historia. Math. **2** (1975), 31–40. URL https://core.ac.uk/download/pdf/82253306.pdf.