8. Finite generation and ACC

I continued the discussion of finitely generated modules by talking about Noetherian modules and rings. One example lead to a discussion of the "restriction of scalars" functor and the basis theorem for finite dimensional vector spaces over a field. This is a precursor to the fundamental theorem for f.g. modules over a PID and applications to matrices.

8.1. **Noetherian rings and modules.**

8.1.1. *definitions.*

Definition 8.1. If M is an R-module, an An *ascending chain* of submodules of M is an increasing sequence of submodules:

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq M$$

We say that M satisfies the *ascending chain condition* (ACC) for submodules if every such sequence stops, i.e., if there is a k so that $N_n = N_k$ for all $n \geq k$.

Definition 8.2. A module M is *Noetherian* if it satisfies the ACC for submodules. A commutative ring R is called *Noetherian* if it satisfies the ACC for ideals. This is equivalent to saying that R is a Noetherian when considered as an R-module. (A noncommutative ring is called *left-Noetherian* if it satisfies the ACC for left ideals.)

8.1.2. *examples.* The first example I gave was $\mathbb{Z}$.

Theorem 8.3. *$\mathbb{Z}$ is Noetherian (as a ring and as a module over $\mathbb{Z}$).*

I proved this twice. The first time, I used the properties of the integers. The second time I used only the fact that $\mathbb{Z}$ is a PID.

Proof. To show that $\mathbb{Z}$ is Noetherian we took an ascending chain:

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq \mathbb{Z}$$

Each submodule N_i is an ideal (or $\mathbb{Z}$) generated by one element $n_i \geq 0$ and the condition $N_i \subseteq N_{i+1}$ is equivalent to saying that n_{i+1} divides n_i. In particular, $n_{i+1} \leq n_i$. So,

$$n_1 \geq n_2 \geq n_3 \geq \cdots .$$

Since these numbers are bounded below (by 0), the sequence stops (becomes constant) at some point. Thus $n_k = n_{k+1} = \cdots$. This is equivalent to saying that

$$N_k = N_{k+1} = \cdots .$$

So, the ACC holds and $\mathbb{Z}$ is Noetherian. □

Second proof. In the second proof, I took the union of the N_i and called it N_∞

$$N_\infty = \bigcup_{i=1}^{\infty} N_i.$$

This is a submodule of $\mathbb{Z}$ since it is closed under addition and scalar multiplication: If $a \in N_i$ and $b \in N_j$ where $i \le j$ then $a + b \in N_j$. The submodule N_∞ is generated by one element n_∞ which is contained in some N_k. But then:

$$(n_\infty) \subseteq N_k \subseteq N_{k+1} \le N_{k+2} \le \cdots \subseteq N_\infty = (n_\infty).$$

So,

$$N_k = N_{k+1} = N_{k+2} = \cdots$$

as before. □

The second proof works for any PID. This is Corollary 8.6 below.

Some other easy examples of Noetherian rings and modules are the following.

(1) Any finite ring or module is Noetherian.
(2) Any quotient of a Noetherian ring or module is Noetherian.
(3) A finite product of Noetherian rings is Noetherian. (Proof: Every ideal in $R \times S$ has the form $I \times J$ where I is an ideal in R and J is an ideal in S. In any ascending chain $(I_n \times J_n)$, both sequences I_n and J_n have to stop.)

8.1.3. *theorem.* Here is the general theorem about Noetherian modules.

Theorem 8.4. *An R-module is Noetherian M if and only if every submodule is finitely generated.*

Corollary 8.5. *A commutative ring is Noetherian if and only if every ideal is finitely generated.*

Corollary 8.6. *Every PID is Noetherian.*

Proof. Suppose first that M has a submodule N which is not finitely generated. Then, any finite subset of N will generate a proper submodule.

Let $x_1 \in N$. Then $Rx_1 \subsetneq N$. So, there is an $x_2 \in N$, $x_2 \notin Rx_1$. Then $Rx_1 + Rx_2 \subsetneq N$. So, there is an $x_3 \in N \backslash Rx_1 + Rx_2$. Continuing in this way, we get a strictly increasing sequence of submodules

$$Rx_1 \subsetneq Rx_1 + Rx_2 \subsetneq Rx_1 + Rx_2 + Rx_3 \subsetneq \cdots$$

So, the ACC fails and M is not Noetherian.

Conversely, suppose that every submodule of M is finitely generated. Then we have to show that any ascending chain:

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq M$$

stops. To show this take the union

$$N_\infty = \bigcup N_i$$

This is a submodule of M and is therefore finitely generated. Let $x_1, \cdots, x_n$ be the generators. Then each x_i is contained in some N_j. If k is the maximum of the indices j then all the x_i will be contained in N_k. But then N_k must equal N_∞. So,

$$N_k = N_{k+1} = N_{k+2} = \cdots$$

and the ACC holds. So, M is Noetherian. □

8.2. **restriction of scalars.** I explained one example of a Noetherian module which used restriction of scalars and the basis theorem for f.g. vector spaces. I explained these tools after the example. So, I will do the same thing here.

Example 8.7. Let R be the polynomial ring $R = F[T]$ over a field F. Then a module M can be constructed as follows. Suppose that A is an $n \times n$ matrix with coefficients in the field F. Then $M = F^n$ is a module if we define the action of a polynomial $p(T) = \sum r_i T^i \in R = F[T]$ by

$$p(T)x = \sum r_i A^i x$$

then M is a Noetherian R-module. To see this take any ascending chain of submodules:

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq M$$

Since R contains the ground field F, every R-module is also a vector space over F. Thus every N_i is a vector space over F. So, it has a dimension d_i. Since $M \cong F^n$, its dimension is n. So,

$$d_1 \leq d_2 \leq d_3 \leq \cdots \leq n$$

This implies that the sequence stops, i.e., there is a $k \geq 1$ so that

$$d_k = d_{k+1} = \cdots$$

But, every proper subspace of a vector space has smaller dimension, so

$$N_k = N_{k+1} = \cdots$$

I.e., the ACC holds and M is Noetherian.

The key point is the realization that an R-module is also a vector space over F. This is called "restriction of scalars." The definition is as follows.

Definition 8.8. Suppose that either

(1) S is a subring of R or
(2) $\phi : S \to R$ is a ring homomorphism. (We can let $\phi : S \to R$ be the inclusion map to make (1) a special case of (2).)

Then, in either case, we get a *restriction of scalars* functor

$$\phi^* : R\text{-}\mathrm{Mod} \to S\text{-}\mathrm{Mod}$$

given on objects by $\phi^*(M) = M$ considered as an S-module in the following way:

(1) When $S \subseteq R$ we just restrict the action of R. So, for any $a \in S$ and $x \in M$ we let $ax = ax$. This makes sense since $a \in R$.
(2) In the general case we let $sx = \phi(s)x$. In other words, the action of S on M is given by the composition

$$S \xrightarrow{\phi} R \xrightarrow{\alpha} \mathrm{End}_{\mathbb{Z}}(M)$$

where α is the action of R on M.

Just as $\phi^*(M) = M$ with a different action, $\phi^*(f : M \to N)$ is also the same mapping $f : M \to N$ considered as a homomorphism of S-modules.

The other fact that we used in the last example was our knowledge of linear algebra over any field. I decided to go over some of that.

8.3. **finite dimensional vector spaces.** Recall that a module over a field F is the same as a vector space. So I called it V. Suppose V is finitely generated with generators $v_1, v_2, \cdots, v_n$. In linear algebra we say that these vectors *span* V and every element of V is a linear combination of these vectors:

$$(\forall x \in V)(\exists x_1, \cdots, x_n \in F) \quad x = x_1v_1 + x_2v_2 + \cdots + x_nv_n$$

This is equivalent to saying that we have an epimorphism

$$\phi : F^n \to V$$

$$(x_1, \cdots, x_n) \mapsto \sum x_iv_i$$

The set $\{v_1, \cdots, v_n\}$ is a *basis* for V if this mapping is an isomorphism.

8.3.1. *existence of a basis.*

Lemma 8.9. *If the epimorphism $\phi : F^n \to V$ is not an isomorphism then V is generated by $n-1$ elements.*

This lemma implies the existence of a basis for a finitely generated vector space. (The word "dimension" is not yet justified. Since this is defined to be the number of elements in a basis, we need to show that this number is unique to show that dimension is well-defined.)

Theorem 8.10. *Any minimal finite spanning set for a vector space V is a basis.*

As I pointed out the next day, this implies the following.

Corollary 8.11. *Every finite spanning set for a vector space contains a basis.*

Proof of Lemma. Suppose that $\phi : F^n \to V$ is not an isomorphism. Then $\ker\phi \neq 0$. So, there is a nonzero element $x \in \ker\phi$. But $x = (x_1, \cdots, x_n)$ being nonzero means one of the coordinates is nonzero. Say $x_1 \neq 0$. Then $x_1^{-1} \in F$. So,

$$v_1 = \sum_{i=2}^{n} \frac{x_i v_i}{x_1}$$

which means that the $n-1$ vectors $v_2, \cdots, v_n$ span V as claimed. □

8.3.2. *dimension.* On the next day, I showed that the number of elements in a finite basis is uniquely determined.

Theorem 8.12. *If V is a finitely generated vector space over a field F then any two bases for V have the same number of elements.*

Proof. By Theorem 8.10, V has a finite basis. The proof will be by induction on n, the size of the smallest basis for V.

Suppose the theorem were not true. Then $F^n \cong V \cong F^m$ where $m > n$. Let $v_1, \cdots, v_m \in V$ be a basis with the larger number of elements. Let $W = Fv_m$. Then $V/W \cong F^{m-1}$ since $v_1 + W, \cdots, v_{m-1} + W$ form a basis. The homomorphism

$$\phi : F^n \cong V \twoheadrightarrow V/W$$

is onto with nontrivial kernel $\ker\phi = W$. So, by Lemma 8.9, V/W is generated by $n-1$ elements. By Corollary 8.11, this implies that V/W has a basis with $\leq n-1$ elements. By induction on n, all bases for V/W have the same size. This is a contradiction since we know that V/W has a basis with $m-1$ elements. □