Reading: Ch 10.3.

Summary of definitions and main results

Definitions we've covered: Generators of an R–module, the R–submodule RA generated by a set A, finite generation, cyclic module, Noetherian R–module, Noetherian ring, minimal set of generators, direct product, direct sum (externel and internal), R–linear independence.

Main results: Examples of non-Noetherian modules, equivalent definitions of (internal) direct sums, Chinese remainder theorem.

Warm-Up Questions

The "warm-up" questions do not need to be submitted (and won't be graded).

1. Let A be a finite abelian group. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, A) = 0$.
2. Let A and B be R–submodules of an R–module M.
   (a) Prove that the sum $A + B$ is an R–submodule of M.
   (b) Verify that $A + B$ is equal to $R(A \cup B)$, the submodule generated by $A \cup B$, as submodules of M.
   (c) Prove that $A+B$ is the smallest submodule of M containing A and B in the following sense: if any submodule N of M contains both A and B, then N contains $A + B$.
3. (a) Use the first isomorphism theorem to prove that if $x \in R$ then the cyclic module Rx is isomorphic to the R–module $R/\mathrm{ann}(x)$.
   (b) Deduce that if R is an integral domain, then $Rx \cong R$ as R–modules.
   (c) Give an example of a ring R and an element $x \in R$ so that $Rx \ncong R$ as R–modules.
4. Let R be a ring and I a two-sided ideal of R. For each of the following R–modules M indicate whether M is finitely generated, cyclic, or more information is needed:
   $M = R^n$ for $n \in \mathbb{N}$, polynomials $M = R[x]$, series $M = R[[x]]$, $M = I$, and $M = R/I$.
5. (a) Prove that if M is a finitely generated R–module, and $\phi : M \to N$ a map of R–modules, then its image $\phi(M)$ is finitely generated by the images of the generators. Conclude in particular that all quotients of finitely generated modules are finitely generated.
   (b) Suppose that N is a finitely generated R–module, and $\phi : M \to N$ is an R–linear surjective map. Must M be finitely generated?
   (c) Suppose that N is a finitely generated R–module, and $\phi : M \to N$ is an R–linear injective map. Must M be finitely generated?
6. (a) Let $\mathbb{F}$ be a field. Citing results from linear algebra, explain why every finitely generated $\mathbb{F}$–module is Noetherian.
   (b) Citing results from group theory, explain why every finitely generated $\mathbb{Z}$–module is Noetherian.
7. Suppose that V is a finite-dimensional vector space over a field $\mathbb{F}$.
   (a) Explain why every minimal spanning set B for V has the same size. Here we mean *minimal* in the sense that the cardinality of B is smallest among all generating sets for V.
   (b) Show that, if B is a generating set for V that is not minimal in size, then V is spanned by some subset of B.

(c) Show by example that this does not hold for general R–modules: Find an example of a ring R and an R–module M that can be generated by m elements, but has a generating set A of size $n > m$ such that no subset of A generates M, for some n and m.

8. (a) Suppose that V is a vector space over a field $\mathbb{F}$. Prove that the following are equivalent.
   (i) $B = \{b_1, \ldots, b_n\}$ is a basis for V
   (ii) Every element $v \in V$ can be written uniquely as an $\mathbb{F}$-linear combination of elements in B
   (iii) B is a minimal (in cardinality) generating set for V as a $\mathbb{F}$–module
   (iv) B is a maximal (in cardinality) linearly independent subset of V
   (v) $V = \mathbb{F}b_1 \oplus \mathbb{F}b_2 \oplus \cdots \oplus \mathbb{F}b_n$
   (vi) The following map is an isomorphism of $\mathbb{F}$–modules

$$\begin{aligned} \mathbb{F}^n &\longrightarrow V \\ (a_1, a_2, \ldots, a_n) &\longmapsto a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \end{aligned}$$

   (b) Which of these equivalences hold for general R–modules?
   (c) Brainstorm examples to show how the other equivalences may fail for general R–modules.

9. Let U, V, W be vector spaces over a field $\mathbb{F}$. (For simplicity you may assume these vector spaces are finite dimensional. If you do not make this assumption, you should assume the axiom of choice).
   (a) Let $\phi : U \to V$ be an injective linear map, and let $\psi : V \to W$ be a surjective linear map. Prove that both ϕ and ψ have one-sided inverses.
   (b) Show by example that when R is not a field, not all surjective maps of R–modules have (one-sided) inverses, and show that not all injective maps of R–modules have (one-sided) inverses.
   (Later in the course, we will describe this phenomenon by the phrase "Every short exact sequence of vector spaces splits")

10. **(Group theory review)**
   (a) Given the finitely generated abelian group $M = \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_N\mathbb{Z}$, explain how to write M as a product with the minimal number of cyclic factors.
   (b) Find a minimal generating set for the groups

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \qquad \text{and} \qquad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

11. **(Linear algebra review)** Let V, W be vector spaces over a field $\mathbb{F}$ of dimension n and m, respectively.
   (a) Consider a linear map $A : V \to V$ (equivalently, of an $n \times n$ matrix A). Show that the following are equivalent. If A satisfies any of these conditions, it is called *singular*.
      1. A has a nontrivial kernel
      2. $\text{rank}(A) < n$
      3. A is not invertible
      4. The columns of A are linearly dependent
      5. The rows of A are linearly dependent
      6. $\det(A) = 0$
      7. $\lambda = 0$ is an eigenvalue of A
   (b) Let T be a linear transformation on a finite-dimensional $\mathbb{F}$-vector space V. Show that the following are equivalent
      1. λ is an eigenvalue of T
      2. $(\lambda I - T)$ is singular
      3. λ is a root of the *characteristic polynomial* of T, $p_T(x) = \det(xI - T)$.

Assignment Questions

1. Let M be an R–module. Let's call a generating set A for M *minimal* if it has the smallest cardinality among all generating sets for M (to distinguish from being "minimal" under inclusion of sets).

   (a) Suppose an R–module M can be decomposed $M = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n$ for some finite set $A = \{a_1, a_2, \ldots, a_n\} \subseteq M$. Prove or find a counterexample: the following map must define an isomorphism $M \cong R^n$

   $$R^n \longrightarrow M$$
   $$(r_1, r_2, \ldots, r_n) \longmapsto r_1a_1 + r_2a_2 + \cdots + r_na_n$$

   (b) Suppose an R–module M can be decomposed $M = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n$ for some finite set $A = \{a_1, a_2, \ldots, a_n\} \subseteq M$. Prove or find a counterexample: A is a minimal generating set for M.

   (c) Suppose a finitely generated R–module M has a minimal generating set $A = \{a_1, a_2, \ldots, a_n\}$.We saw in class that M need not be the internal direct sum $Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n$. Now suppose that R is a PID, and prove or find a counterexample: $M = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n$.

2. (a) **(Chinese Remainder Theorem)** Let R be any ring, and let $I_1, \ldots I_k$ be two-sided ideals of R such that $I_i + I_j = R$ for any $i \neq j$ (such ideals are called *comaximal*). Prove there is an isomorphism of R–modules

   $$\frac{R}{(I_1 \cap I_2 \cap \cdots \cap I_k)} \cong \frac{R}{I_1} \times \frac{R}{I_2} \times \cdots \times \frac{R}{I_k}.$$

   (b) Conclude that for pairwise coprime integers, $m_1, m_2, \ldots, m_k$, there is an isomorphism of groups

   $$\mathbb{Z}/m_1m_2\cdots m_k\mathbb{Z} \quad \cong \quad \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}.$$

3. Let $\{M_i \mid i \in I\}$ be a (possibly infinite) set of R–modules with index set I. We define the *direct product* of these modules to be

   $$\prod_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in M_i\}$$

   When I is finite or countable, we can express elements as ordered tuples $(m_1, m_2, \ldots, m_n, \ldots)$. The direct product forms an R–module under pointwise addition and scalar multiplication. We define the *direct sum* of the modules $\{M_i \mid i \in I\}$ to be the submodule of $\prod_{i \in I} M_i$

   $$\bigoplus_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in M_i,\ m_i = 0 \text{ for all but at most finitely many } i \in I\}$$

   These definitions coincide when I is finite.

   (a) The direct sum $\bigoplus_{i \in I} M_i$ is a submodule of the direct product $\prod_{i \in I} M_i$, but show by example that these may not be isomorphic. *Hint*: What are their cardinalities?

   (b) Show that $\bigoplus_{i \in I} M_i$ is generated by the set $\bigcup_{i \in I} M_i$, but that $\prod_{i \in I} M_i$ may not be.

4. (a) Let $A_1, A_2, \ldots, A_n$ be R–modules, and $B_i \subseteq A_i$ a submodule for each i. Show that

   $$\frac{A_1 \times A_2 \times \cdots \times A_n}{B_1 \times B_2 \times \cdots \times B_n} \cong \frac{A_1}{B_1} \times \frac{A_2}{B_2} \times \cdots \times \frac{A_n}{B_n}.$$

   (b) Let R be a commutative ring, and let $n, m \in \mathbb{N}$. Prove that that $R^n \cong R^m$ if and only if $n = m$. You may assume without proof that finite-dimensional vector spaces are isomorphic if and only if their dimensions are equal. You may also assume Zorn's Lemma. *Hint:* Dummit–Foote 10.3 # 2.

   (c) Show that this property fails for noncommutative rings – that is, find a ring R which admits an isomorphism of R–modules $R \cong R^2$. Conclude that free R–modules need not have a uniquely defined rank. *Hint:* Dummit–Foote 10.3 # 27.

5. (a) Let M be an R–module. Prove that the following statements are equivalent.
   (i) M is *Noetherian* in the sense that every R–submodule of M is finitely generated.
   (ii) M satisfies the *ascending chain condition* on submodules. This is the condition that every sequences of submodules of M with inclusions

   $$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

   (called an *ascending chain*) eventually stabilizes in the sense that there exists some index k so that

   $$M_k = M_{k+1} = M_{k+2} = \cdots$$

   (b) A ring R is called *Noetherian* if the R–module R is Noetherian.
   (i) Let R be a PID. Show that R is Noetherian.
   (ii) Let R be the ring of polynomials $\mathbb{Q}\langle x, y\rangle$ in **noncommuting** variables x and y. Show that R is not Noetherian.

6. **Bonus (Optional).** Let R be a ring. Show that an arbitrary direct sum of free R–modules is free, but an arbitrary direct product need not be. *Hint:* Dummit–Foote 10.3 # 24.