Reading: Dummit–Foote Ch 12.1, 18.1

Summary of definitions and main results

Definitions we've covered: ACC (Ascending chain condition), Noetherian R–module, Noetherian ring, Smith normal form, group ring, (linear) representation, degree of a representation, faithful representation, trivial representation, permutation representation, regular representation, homomorphism and isomorphism of representations, G-equivariant map, intertwiner, simple (or irreducible) module, decomposable module, completely reducible module

Main results: Equivalent definitions of Noetherian module, Proof outline of structure theorem for finitely generated modules over PID (existence, uniqueness), equivalent definitions of a group representation, properties of the averaging map

Warm-Up Questions

1. Explain why all PIDs are Noetherian rings.
2. Let R be a Euclidean domain and M a finitely generated submodule. To prove the invariant factor decomposition for M, we first constructed a surjection φ

$$0 \longrightarrow \ker(\varphi) \longrightarrow R^n \xrightarrow{\varphi} M \longrightarrow 0$$

and then computed the *Smith normal form* of the $m \times n$ *relations matrix* between a basis $x_1, \ldots, x_n$ for R^n and a generating set $y_1, \ldots y_m$ for $\ker(\varphi)$.

   (a) Define the relations matrix. Explain the sense in which the rows of the relations matrix correspond to generators y_i of $\ker(\varphi)$, and the columns of the matrix correspond to basis elements x_j of R^n.

   (b) Explain how column operations on the relations matrix correspond to operations on the basis $\{x_j\}$, and how row operations correspond to operations on the generators $\{y_i\}$.

   (c) Verify that for each row and column operation, the modified set $\{x_j\}$ will still be a basis for R^n, and the modified set $\{y_i\}$ will still be a generating set for $\ker(\varphi)$.

   (d) Describe what it means for the relations matrix to be in *Smith normal form*, and the structure of the basis for R^n and generating set of $\ker(\varphi)$ constructed in the process of putting the matrix in this form.

   (e) Explain how to compute the invariant factor decomposition of $M \cong R^n/\ker(\varphi)$ from the Smith normal form of the matrix.

3. Assume the same set up as in the previous question, with $R = \mathbb{Z}$.

   (a) For each of the matrices in Smith normal form, concretely describe the short exact sequence

$$0 \longrightarrow \ker(\varphi) \longrightarrow \mathbb{Z}^n \xrightarrow{\varphi} M \longrightarrow 0$$

   and state the free rank and invariant factors for M.

$$A = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \end{bmatrix} \quad C = \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix} \quad D = \begin{bmatrix} 2 & 0 \\ 0 & 4 \\ 0 & 0 \end{bmatrix} \quad E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{bmatrix}$$

   (b) Explain how the rows of zeroes in matrices A and D correspond to a redundancy in our choice of generators $\{y_1, \ldots, y_m\}$ for the kernel $\ker(\varphi)$.

   (c) Explain how the column of zeroes in matrices A and B corresponds to the free part of M.

(d) Explain how the unit 1 in E corresponds to a redundancy in our choice of generators $\{\varphi(x_1), \ldots, \varphi(x_n)\}$ for M.

4. Fill in the details of the following result from class: Let R be a PID, $p \in R$ prime, and denote by $\mathbb{F}$ the field $R/(p)$.
   (a) $R^r/p(R^r) \cong \mathbb{F}^r$.
   (b) Let $M = R/(a), a \neq 0$. Then M/pM is isomorphic to $\mathbb{F}$ if p divides a, and zero otherwise.
   (c) If $M \cong R/(a_1) \oplus \cdots \oplus R/(a_k)$ where p divides each a_i, then $M/pM \cong \mathbb{F}^k$.

5. Let G be a group and V an $\mathbb{F}$-vector space. Show that the following are all equivalent ways to define a (linear) representation of G on V.
   i. A group homomorphism $G \to \mathrm{GL}(V)$.
   ii. A group action (by linear maps) of G on V.
   iii. An $\mathbb{F}[G]$–module structure on V.

6. (a) Describe the canonical representation on $\mathbb{F}^n$ of the symmetric group S_n by permutation matrices.
   (b) Let $\langle e_1, \ldots, e_n \rangle$ be the standard basis for $\mathbb{F}^n$. Show that if S_n acts by permuting the basis

$$\sigma e_i \mapsto e_{\sigma(i)} \qquad \text{for all } \sigma \in S_n, i = 1, \ldots, n,$$

   then σ acts on a vector $(v_1, v_2, \ldots, v_n) := v_1 e_1 + \ldots + v_n e_n$ in $\mathbb{F}^n$ by

$$\sigma(v_1, v_2, \ldots, v_n) \mapsto (v_{\sigma^{-1}(1)}, v_{\sigma^{-1}(2)}, \ldots, v_{\sigma^{-1}(n)}).$$

   (c) Verify that $\mathbb{F}^n$ decomposes into the direct sum $D \oplus U$ of two invariant subspaces under this action: the diagonal

$$D = span_{\mathbb{F}}(e_1 + e_2 + \ldots + e_n) = \{(a, a, \ldots, a) \in \mathbb{F}^n \mid a \in \mathbb{F}\},$$

   and the subspace with coefficient-sum-zero

$$U = span_{\mathbb{F}}(e_1 - e_2,\ e_1 - e_3,\ \ldots,\ e_1 - e_n) = \{(a_1, a_2, \ldots, a_n) \in \mathbb{F}^n \mid a_1 + a_2 + \ldots + a_n = 0\}.$$

7. (a) Compute the sum and product of the elements $(1 + 3e_{(1\,2)} + 4e_{(1\,2\,3)})$ and $(4 + 2e_{(1\,2)} + 4e_{(1\,3)})$ in the group ring $\mathbb{Q}[S_3]$.
   (b) Compute the sum and product of $(2 + e_2 + e_3)$ and $(3 - e_1 - 3e_2)$ in the group ring $\mathbb{Q}[\mathbb{Z}/4\mathbb{Z}]$. (Explain why it is prudent to denote group elements by e_g instead of g in situations like this one).

8. Let R be a commutative ring. Show that the group ring $R[\mathbb{Z}] \cong R[x, x^{-1}]$. What is the group ring $R[\mathbb{Z}^n]$? The group ring $R[\mathbb{Z}/n\mathbb{Z}]$?

9. Let G be a group and R a commutative ring. Show that the group ring $R[G]$ is commutative if and only if G is abelian.

10. Prove that if $\phi : G \to GL(V)$ is any representation, then ϕ defines a faithful representation of the group $G/\ker(\phi)$.

11. Let $\rho : G \to GL(V)$ be a representation of a finite group G, and let $V \cong U \oplus W$ be a decomposition of V into G-invariant subspaces. Show that, in a suitably chosen basis for V, every matrix $\rho(g)$ will be block diagonal, with a block acting on U and a block acting on V.

12. (a) Find an explicit isomorphism T between the following two representations of S_2.

$$S_2 \to GL(\mathbb{R}^2) \qquad\qquad S_2 \to GL(\mathbb{R}^2)$$
$$(1\ 2) \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad\qquad (1\ 2) \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$
$$id \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad\qquad id \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Give a geometric description of the action and the two bases for $\mathbb{R}^2$ associated to each matrix group.

(b) Prove that the following two representations of S_2 are not isomorphic.

$$S_2 \to GL(\mathbb{R}^2) \qquad\qquad S_2 \to GL(\mathbb{R}^2)$$
$$(1\ 2) \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad\qquad (1\ 2) \mapsto \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$
$$id \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad\qquad id \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

13. Given representations $G \to GL(V)$ and $G \to GL(U)$, construct a representations $G \to GL(V \oplus U)$ and $G \to GL(V \otimes U)$.

14. Show that a representation of a group G is equivalent to the data of a functor from the category $\mathcal{G}$ (with one object and morphisms G) to the category $\text{Vect}_{\mathbb{F}}$ of $\mathbb{F}$–vector spaces. Conclude that (by composing functors) any representation of G on vector space V and covariant functor $\mathcal{F} : \text{Vect}_{\mathbb{F}} \to \text{Vect}_{\mathbb{F}}$ will define a G–representation $\mathcal{F}(V)$.

Assignment Questions

1. Define a ring R to be *(left) Noetherian* if R is Noetherian as a left module over itself. In this question we will show this definition is equivalent to our earlier definition of a Noetherian ring: R is *(left) Noetherian* if every finitely generated left R–module is Noetherian.

   (a) Suppose R is Noetherian as a left R–module. Let M be a submodule of R^n. Prove that

   $$\{\ r \mid r \text{ appears as a first coordinate in an element of } M\} \subseteq R \qquad \text{and} \qquad M \cap (\{0\} \times R^{n-1}) \subseteq R^n$$

   are R–modules.

   (b) Using part (a) and induction on n, prove that R^n is a Noetherian R–module.
   Hint: Consider the relationship between M and the short exact sequence

   $$0 \longrightarrow \{0\} \times R^{n-1} \longrightarrow R^n \xrightarrow{\pi_1} R \longrightarrow 0.$$

   (c) Prove that an R–module N is finitely generated if and only if it is quotient of a finite rank free R–module R^n.

   (d) Prove that a quotient of a Noetherian R–module is Noetherian.

   (e) Conclude that any finitely generated R–module is Noetherian.

2. In class, we sketched a proof of the structure theorem for finitely generated modules over a Euclidean domain R. Reference: Dummit–Foote Ch 12.1 Exercises 17–19.

   (a) Let K be a submodule of R^n. Since R^n is Noetherian, K is finitely generated. Show that the result of our proof-sketch from class in fact showed that K is a free R–module of rank at most n, with the following property: there exists a basis $x_1, \ldots, x_n$ for R^n such that K is free on the basis $a_1x_1, a_2x_2, \ldots, a_kx_k$ for some nonzero $a_i \in R$ satisfying $a_1|a_2|\cdots|a_k$.
   (You do not need to re-prove the arguments from the class, you can just quote the conclusion concerning the relations matrix in Smith normal form).
   Remark: This property holds for all PID's. Those interested should refer to 12.1 Theorem 4.

(b) Let $\mathbb{Z}^4$ be the free abelian group on the standard basis $e_1 = (1,0,0,0), \ldots, e_4 = (0,0,0,1)$. Let M be the submodule generated by the elements

$$M = \left\langle \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \\ 3 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 4 \\ -2 \end{bmatrix}, \begin{bmatrix} 6 \\ 0 \\ -4 \\ -6 \end{bmatrix} \right\rangle$$

Find bases for $\mathbb{Z}^4$ and M as described in part (a), by performing row and column operations to put an appropriately defined matrix into Smith normal form. (You can optionally use computer software to do these computations, but include a print-out of your computer work).

(c) What is the invariant factor decomposition for $\mathbb{Z}^4/M$?

3. Let G be a finite group, and $\mathbb{F}$ a field. A *permutation representation* of G on a finite-dimensional $\mathbb{F}$-vector space V is a linear representation $\rho : G \to GL(V)$ in which elements act by permuting some basis $B = \{b_1, \ldots b_m\}$ for V.

   (a) Show that, with respect to the basis $\{b_1, \ldots, b_m\}$, for each element $g \in G$, $\rho(g)$ is represented by an $m \times m$ *permutation matrix*, a square matrix that has exactly one entry 1 in each row and each column, and zero elsewhere. Use this description of matrices $\rho(g)$ to show that the trace of $\rho(g)$ is equal to the number of basis elements b_i fixed by $\rho(g)$.

   (b) The group ring of $\mathbb{F}[G]$ is a left module over itself. Show that this corresponds to permutation representation of the group G on the underlying vector space $\mathbb{F}[G]$, called the *(left) regular representation* of G. Find the degree of this representation. In what basis is this a permutation representation, and how many G-orbits does this basis have?

   (c) For any $g \in G$, compute the trace of the matrix representing g in the regular representation.

4. **(Schur's Lemma).** Let R be a ring, and let V, U be simple R–modules.

   (a) Prove that every nonzero R–module homomorphism from V to U is either an isomorphism or the zero map. Conclude that $\mathrm{Hom}_R(V,V)$ is a *division ring*, a ring (not necessarily commutative) in which every nonzero element has a multiplicative inverse.

   (b) Suppose R is an algebraically closed field. Show that any R–module map $\phi : V \to V$ is equal to the scalar map λI for some $\lambda \in R$.

5. Let G be a finite **abelian** group, and V a finite-dimensional complex representation of G. Show that V decomposes into a direct sum of 1-dimensional G–representations. Conclude that the image of G in $GL(V)$ is *simultaneously diagonalizable*, that is, there is some basis for V with respect to which every matrix is diagonal.