Reading: Ch 10.3 & pp 911–913.

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, minimal set of generators, direct product, direct sum (externel and internal), R–linear independence, free module, basis, rank of a free module, universal property, category, object, morphism, functor, coproduct, abelianization.

Main results: Examples of non-Noetherian modules, equivalent definitions of (internal) direct sums, Chinese remainder theorem, universal property for free modules, construction of the free module $F(A)$, verification that $F(A)$ satisfies the universal property, universal properties define objects up to unique isomorphism.

Warm-Up Questions

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

1. 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 $A+B$.
2. Use the first isomorphism theorem to prove that if $x \in R$ then the cyclic module Rx is isomorphic to the R–module $R/\text{ann}(x)$. Deduce that if R is an integral domain, then $Rx \cong R$ as R–modules.
3. 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 $M = R/I$.
4. 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.
5. (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.
6. (a) Suppose a finitely generated R–module M has a minimal generating set $A = \{a_1, a_2, \ldots, a_n\}$. Prove or find a counterexample: $M \cong Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n$.
   (b) Suppose an R–module M can be decomposed $M \cong Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n$ 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.
7. (a) Let A be any finite set of n elements. Show that the free R–module on A is isomorphic as an R–module to R^n.
   (b) For R commutative, are the polynomial rings $R[x]$ and $R[x, y]$ free R–modules? What about Laurent polynomials $R[x, x^{-1}]$? Rational functions in x?
   (c) Do these arguments work for series $R[[x]]$?
8. Show that $M = \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ is a free $\mathbb{Z}/10\mathbb{Z}$–module by finding a basis. Show that the element $(2, 2)$ cannot be an element of any basis for M. Is the submodule $N = \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ also free?

9. Show that $M = \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ is a rank-2 free module over $\mathbb{Z}/6\mathbb{Z}$, and find necessary and sufficient conditions on a pair of elements $\{a, b\} \subset M$ to be a basis for M.

10. (a) Show that A is a basis for the R–module RA it generates if and only if A is R–linearly independent.
    (b) Find a counterexample to the following false statement: If M is a free R–module and $A \subseteq M$ is an R–linearly independent subset of M, then A can be extended to a basis for M.
    (c) **(Challenge)** Show that a $\mathbb{Z}$–linearly independent subset B of the free abelian group $\mathbb{Z}^N$ can be extended to a basis for $\mathbb{Z}^N$ if and only if $\mathbb{Z}B$ is *splittable* in the sense of Homework #1 Bonus.

11. (a) Let F be the free R–module on a set A. Show that if R has no zero divisors and $N \subseteq M$ is any nonzero submodule, then $\operatorname{ann}(N) = \{0\}$.
    (b) Let $R = \mathbb{Z}/10\mathbb{Z}$ and let $F \cong R^2$ be the free R–module of rank 2. Compute the annihilator of the submodule $2F$.

12. In class (and in Dummit-Foote 10.3 Theorem 6) we gave a construction of a free module $F(A)$ on a set A. Verify that this construction is in fact a free module with basis A (as given in the definition on p354). Show moreover that $F(A) \cong \bigoplus_A R$.

13. (a) Citing results from linear algebra, explain why every vector space over a field $\mathbb{F}$ is a free $\mathbb{F}$–module.
    (b) When $\mathbb{F}$ is a field, any minimal finite generating set $B = \{a_1, \dots, a_n\}$ of an $\mathbb{F}$–module must be linearly independent and therefore a basis. Prove that in general, if an R–module has a minimal generating set $B = \{a_1, \dots, a_n\}$, then R need not be free on B.
    (c) Suppose that M is an R–module containing elements $\{a_1, a_2, \dots, a_n\}$ such that $M = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n$. Explain how $A = \{a_1, a_2, \dots a_n\}$ could fail to be a basis for M. What conditions on the elements a_i could ensure that A is a basis?

14. Let R be a ring, M and R–module and N an R–submodule of N.
    (a) Show that M/N satisfies the following universal property: If $\varphi : M \to Q$ is any map of R–modules satisfying $\phi(n) = 0$ for all $n \in N$, then φ factors uniquely through M/N.
    (b) Show that this universal property defines the quotient M/N uniquely up to unique isomorphism.

15. **(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

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

16. **(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. $\operatorname{rank}(A) < n$
    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

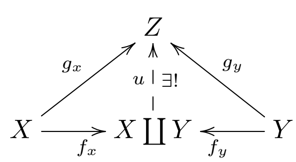
1. (a) **(Chinese Remainder Theorem)** Let R be any ring, and let $I_1, \dots I_k$ be two-sided ideals of R such that $I_i + I_j = R$ for any $i \neq j$ (such ideals are called *comaximal*). Prove there is an isomorphism of R–modules
$$\frac{R}{(I_1 \cap I_2 \cap \cdots \cap I_k)} \cong \frac{R}{I_1} \times \frac{R}{I_2} \times \cdots \times \frac{R}{I_k}.$$

   (b) Conclude that for pairwise coprime integers, $m_1, m_2, \dots, m_k$, there is an isomorphism of groups
$$\mathbb{Z}/m_1 m_2 \cdots m_k \mathbb{Z} \quad \cong \quad \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}.$$

2. (a) Let $A_1, A_2, \dots, A_n$ 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.

3. **(Coproducts).** Let $\mathcal{C}$ be a category with objects X and Y. The *coproduct* of X and Y (if it exists) is an object $X \coprod Y$ in $\mathcal{C}$ with maps $f_x : X \to X \coprod Y$ and $f_y : Y \to X \coprod Y$ satisfying the following universal property: whenever there is an object Z with maps $g_x : X \to Z$ and $g_y : Y \to Z$, there exists a unique map $u : X \coprod Y \to Z$ that makes the following diagram commute:



   (a) Let X and Y be objects in $\mathcal{C}$. Show that, if the coproduct $(X \coprod Y, f_x, f_y)$ exists in $\mathcal{C}$, then the universal property determines it uniquely up to unique isomorphism.

   (b) Prove that in the category of R–modules, the coproduct of R–modules $X \coprod Y$ is $X \oplus Y$ with the canonical inclusions of X and Y. In other words, this universal property defines the direct sum operation on R–modules.

   (c) Explain how to reinterpret this universal property for the direct sum of R–modules as a bijection of sets
$$\mathrm{Hom}_R(X \oplus Y, Z) \cong \mathrm{Hom}_R(X, Z) \times \mathrm{Hom}_R(Y, Z)$$
   for R–modules X, Y, Z.

   (d) Prove that in the category of groups, the univeral property for the coproduct $X \coprod Y$ of groups X and Y does *not* define the direct product of those groups along with their canonical inclusions. (It is a construction called the *free product* of groups).

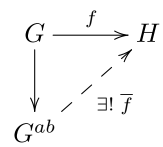
   (e) Prove that in the category of sets, the coproduct $X \coprod Y$ of sets X and Y is their disjoint union.

4. **(Abelianization).** Let $\underline{\mathrm{Grp}}$ denote the category of groups and group homomorphisms, and let $\underline{\mathrm{Ab}}$ denote the category of abelian groups and group homomorphisms. Define the *abelianization* G^{ab} of a group G to be the quotient of G by its *commutator subgroup* $[G, G]$, the subgroup normally generated by *commutators*, elements of the form $ghg^{-1}h^{-1}$ for all $g, h \in G$.

   (a) Define a map of categories $[-, -] : \underline{\mathrm{Grp}} \to \underline{\mathrm{Grp}}$ that takes a group G to its commutator subgroup $[G, G]$, and a group morphism $f : G \to H$ to its restriction to $[G, G]$. Check that this map is well defined (ie, check that $f([G, G]) \subseteq [H, H]$) and verify that $[-, -]$ is a functor.

(b) Show that G^{ab} is an abelian group. Show moreover that if G is abelian, then $G = G^{ab}$.

(c) Show that the quotient map $G \to G^{ab}$ satisfies the following universal property: Given any **abelian** group H and group homomorphism $f : G \to H$, there is a unique group homomorphism $\overline{f} : G^{ab} \to H$ that makes the following diagram commute:



This universal property shows that G^{ab} is in a sense the "largest" abelian quotient of G.

(d) Show that the map ab that takes a group G to its abelianization G^{ab} can be made into a functor $ab : \underline{\text{Grp}} \to \underline{\text{Ab}}$ by explaining where it maps morphisms of groups $f : G \to H$, and verifying that it is functorial.

(e) The category $\underline{\text{Ab}}$ is a subcategory of $\underline{\text{Grp}}$. Define the functor $\mathcal{A} : \underline{\text{Ab}} \to \underline{\text{Grp}}$ to be the inclusion of this subcategory; $\mathcal{A}$ takes abelian groups and group homomorphisms in $\underline{\text{Ab}}$ to the same abelian groups and the same group homomorphisms in $\underline{\text{Grp}}$. Briefly explain why the universal property in Part (c) can be rephrased as follows: Given groups $G \in \underline{\text{Grp}}$ and $H \in \underline{\text{Ab}}$, there is a natural bijection between the sets of morphisms:

$$\text{Hom}_{\underline{\text{Grp}}}(G, \mathcal{A}(H)) \cong \text{Hom}_{\underline{\text{Ab}}}(G^{ab}, H)$$

Remark: Since this bijection is "natural" (a condition we won't formally define or check) it means that $\mathcal{A} : \underline{\text{Ab}} \to \underline{\text{Grp}}$ and $ab : \underline{\text{Grp}} \to \underline{\text{Ab}}$ are what we call a pair of *adjoint functors*.

5. **Bonus Warm-up Question (Optional, not for credit).** 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.

6. **Bonus (Optional).**

(a) 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 (definitions in Problem (5)). *Hint:* Dummit–Foote 10.3 # 24.

(b) In Problem (2) we saw that if R is commutative and $R^n \cong R^m$, then $n = m$. Show that this property fails for noncommutative rings – that is, free R–modules need not have a uniquely defined rank. *Hint:* Dummit–Foote 10.3 # 27.