Math 114 Homework 9
(due Thursday, 16 April)

1. Let R be a ring with identity, I a nonempty index set (possibly infinite), $(M_\alpha)_{\alpha\in I}$ a list of R-modules indexed by I. Prove that the direct product $\prod_{\alpha\in I} M_\alpha$ (together with, for each $\beta \in I$, the projection map $p_\beta : \prod_{\alpha\in I} M_\alpha \to M_\beta$ given by $(m_\alpha) \mapsto m_\beta$) has the following universal property:

   Let N be any R-module, and for each $\beta \in I$ let $f_\beta : N \to M_\beta$ be an R-module homomorphism. Then there is a unique R-module homomorphism $f : N \to \prod_{\alpha\in I} M_\alpha$ such that $p_\beta \circ f = f_\beta$ for every $\beta \in I$.

   (Try doing this without looking at the corresponding proof for direct sums, which we did in class. The definition of the direct product is given in Exercise 20 in §10.3.)

   Proof. Define $f : N \to \prod_{\alpha\in I} M_\alpha$ by
   $$n \mapsto \prod_{\beta\in I} f_\beta(n)$$
   for all $n \in N$.

   First, we will show that f is a homomorphism. For any $a, b \in N$ and $r \in R$, we have
   $$f(a + rb) = \prod_{\beta\in I} f_\beta(a + rb) = \prod_{\beta\in I} f_\beta(a) + r \prod_{\beta\in I} f_\beta(b) = f(a) + rf(b)$$
   where the middle equality is given by the fact that the addition in and action of R on the direct product is componentwise.

   Now, for any $n \in N$, we have
   $$p_\beta \circ f(n) = p_\beta \left(\prod_{\beta\in I} f_\beta(n) \right) = f_\beta(n)$$
   so $p_\beta \circ f = f_\beta$.

   Now, suppose g is any map $N \to \prod_{\alpha\in I} M_\alpha$ such that $g \neq f$. So g differs from f at some point $n \in N$, i.e. $g(n) \neq f(n)$. Let (a_α) be the function such that $g(n) = \prod_{\alpha\in I} a_\alpha$. Since f and g differ at n, there must be some $\beta \in I$ such that $a_\beta \neq f_\beta(n)$ (by our definition of f). But then
   $$p_\beta \circ g(n) = p_\beta \left(\prod_{\alpha\in I} a_\alpha \right) = a_\beta \neq f_\beta(n)$$
   thus $p_\beta \circ g \neq f_\beta$. So our choice of f is the unique map with this property. □

2. (Exercise 5 in DF §10.3.) Let R be an integral domain (a commutative ring with 1 in which $1 \neq 0$ and there are no zero-divisors). An R-module M is *torsion* if for each $m \in M$ there is a nonzero element $r \in R$ such that $rm = 0$. Prove that if M is any finitely generated torsion R-module, then there is a nonzero element $r \in R$ such that $rm = 0$ for every $m \in M$ (i.e., the annihilator of M in R (defined in Exercise 9 of §10.1) is nonzero).

   Give an example of an integral domain R and a torsion R-module M (necessarily not finitely generated) whose annihilator in R is the zero ideal. (Hint: see Exercise 20 in §10.3.)

   Proof. Let $\{a_1, \ldots, a_n\}$ be a generating set for M over R. Then there exist nonzero $r_1, \ldots, r_n \in R$ such that $r_i a_i = 0$ for each i. Any element of M is of the form $s_1a_1 + \cdots + s_na_n$ for some $s_1, \ldots, s_n \in R$, so for any element of M we have
   $$\begin{aligned} r_1 \cdots r_n(s_1a_1 + \cdots + s_na_n) &= (s_1r_2 \cdots r_n)(r_1a_1) + \cdots + (s_nr_1 \cdots r_{n-1})(r_na_n) \\ &= (s_1r_2 \cdots r_n)(0) + \cdots + (s_nr_1 \cdots r_{n-1})(0) \\ &= 0 \end{aligned}$$

because R is commutative. However, $r_1 \cdots r_n \neq 0$ because R contains no zero divisors, and each r_i is nonzero. Therefore, since $r_1 \cdots r_n \in \mathrm{Ann}_R(M)$, we know that $\mathrm{Ann}_R(M) \neq 0$.

For the example, let $R = \mathbb{Z}$ and let $M = \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \cdots$ (over $\mathbb{Z}$). Any $x \in M$ is of the form $r_1 x_1 + \cdots r_n x_n$ for some $r_1, \ldots, r_n \in \mathbb{Z}$ and $x_1 \in \mathbb{Z}/k_1\mathbb{Z}, \ldots, x_n \in \mathbb{Z}/k_n\mathbb{Z}$ for some positive integers $k_1, \ldots, k_n$. Letting l be the least common multiple of $k_1, \ldots, k_n$, we see that

$$rx = r_1 \left(\frac{l}{k_1}\right)(k_1 x_1) + \cdots + r_n \left(\frac{l}{k_n}\right)(k_n x_n) = r_1 \left(\frac{l}{k_1}\right)(0) + \cdots + r_n \left(\frac{l}{k_n}\right)(0) = 0.$$

So M is a torsion R-module. However, given any $r \in R$, we may consider its action on the identity element 1_{r+1} of $\mathbb{Z}/(r+1)\mathbb{Z}$, which we know is contained in M. This action $r \cdot 1_{r+1}$ is the element r in $\mathbb{Z}/(r+1)\mathbb{Z}$, which is nonzero. Therefore, the annihilator of M in $\mathbb{Z}$ is the zero ideal. □

3. (Exercise 9 in DF §10.3. WILL NOT BE GRADED.) Let R be a ring with 1. An R-module M is called *irreducible* if $M \neq \{0\}$ and the only submodules of M are $\{0\}$ and M. Show that M is irreducible if and only if $M \neq \{0\}$ and $M = Rm$ (that is, M is generated by the element m) for any nonzero $m \in M$.

   Determine all the irreducible $\mathbf{Z}$-modules.

   Proof. Suppose M is an irreducible $\mathbb{Z}$-module. First, assume M contains an element x of finite order $n > 1$ in the underlying group. Then x generates a cyclic subgroup H of order n, so we must have $H = G$. However, if n is not prime, then some prime p is a proper divisor of n; thus, by Cauchy's Theorem, H contains a proper subgroup of order p, a contradiction. So G has prime order, thus is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

   Next, assume every non-identity element of M has infinite order. Given any $x \in M$, $2x$ will generate a proper subgroup of M (since it cannot generate the element x). This contradicts the irreducibility of M, so the only option is the previous case.

   Therefore, $M \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p. So these are all the irreducible $\mathbb{Z}$-modules. □

4. (Exercise 11 in DF §10.3.) Let R be a ring with 1. Show that if M_1 and M_2 are irreducible R-modules, then any nonzero R-module homomorphism from M_1 to M_2 is an isomorphism. Deduce that if M is an irreducible R-module, then $\mathrm{End}_R(M)$ (defined on p. 347 of DF) is a division ring. (This result is called *Schur's lemma*.)

   Proof. Let $\varphi : M_1 \to M_2$ be a nonzero R-module homomorphism of the irreducbile R-modules M_1 and M_2. Since φ is nonzero, $\ker \varphi \neq M_1$. By the First Isomorphism Theorem, $\ker(\varphi)$ is a submodule of M_1, thus it must be $\{0\}$ since M_1 is irreducible. Since φ is a group homomorphism as well (module homomorphisms respect the structure of the underlying group), φ is injective.

   The First Isomorphism Theorem also tells us that the image of φ is a submodule of M_2. If it were $\{0\}$, then φ would be the zero map. Thus the image must be all of M_2, since M_2 is irreducible. So φ is surjective, and thus an isomorphism.

   If M is an irreducible R-module, and $\varphi \in \mathrm{End}_R(M)$, then $\varphi : M \to M$ is an R-module homomorphism from an irreducible module to an irreducible module, thus by this exercise it is an isomorphism. Therefore, it has a unique inverse isomorphism $\varphi^{-1} \in \mathrm{End}(M)$ as well. So $\mathrm{End}(M)$ is a division ring. □

5. (Exercise 23 in DF §10.3.) Let R be a ring with 1. Show that any direct sum of free R-modules is free.

   Proof. Let I be an index set. For each $\alpha \in I$, let M_α be an R-module. Let M be the direct sum $\oplus_{\alpha \in I} M_\alpha$. Let A be the disjoint union $\bigsqcup_{\alpha \in I} A_\alpha$, meaning we may consider it to be the union of the sets $\overline{A_\alpha} = \{(a, \alpha) : a \in A_\alpha\}$. (From this point on, we will assume that the A_α are disjoint.)

   For each $\alpha \in I$, let $\iota_\alpha : M_\alpha \to M$ be the natural inclusion of M_α into M. Now, define a map $\iota : A \to M$ by $\iota(a) = \iota_\alpha(a)$ if $a \in A_\alpha$ and $\iota(a) = 0$ otherwise. Clearly, ι restricts to ι_α on A_α. By the

universal property of free modules, there is a unique homomorphism $\Phi : F(A) \to M$ that restricts to ι on A, and thus also to ι_α on A_α.

We will now show that Φ is injective. Assume there is some nonzero $x \in \ker(\Phi)$. Since A is a basis for $F(A)$, and A is the disjoint union of the A_α, x has a unique representation of the form

$$x = r_{1,1}a_{1,1} + \cdots + r_{1,k_1}a_{1,k_1} + \cdots + r_{n,1}a_{n,1} + \cdots + r_{n,k_n}a_{n,k_n}$$

where $r_{i,j} \in R$ is nonzero for all i, j, and $a_{i,j} \in A_{\alpha_i}$ for some $\alpha_i \in I$ such that $\alpha_s \neq \alpha_t$ whenever $s \neq t$. So

$$\begin{aligned}
\Phi(x) &= \Phi(r_{1,1}a_{1,1} + \cdots + r_{1,k_1}a_{1,k_1} + \cdots + r_{n,1}a_{n,1} + \cdots + r_{n,k_n}a_{n,k_n}) \\
&= r_{1,1}\iota(a_{1,1}) + \cdots + r_{1,k_1}\iota(a_{1,k_1}) + \cdots + r_{n,1}\iota(a_{n,1}) + \cdots + r_{n,k_n}\iota(a_{n,k_n}) \\
&= r_{1,1}\iota_{\alpha_1}(a_{1,1}) + \cdots + r_{1,k_1}\iota_{\alpha_1}(a_{1,k_1}) + \cdots + r_{n,1}\iota_{\alpha_n}(a_{n,1}) + \cdots + r_{n,k_n}\iota_{\alpha_n}(a_{n,k_n}) \\
&= \iota_{\alpha_1}(r_{1,1}a_{1,1} + \cdots + r_{1,k_1}a_{1,k_1}) + \cdots + \iota_{\alpha_n}(r_{n,1}a_{n,1} + \cdots + r_{n,k_n}a_{n,k_n}) \\
&= \prod_{\alpha \in I} m_\alpha \\
&= 0_M.
\end{aligned}$$

where $m_\alpha = r_{i,1}a_{i,1} + \cdots + r_{i,k_1}a_{i,k_i}$ if $\alpha = \alpha_i$ for some $i \in \{1, \ldots, n\}$, and $m_\alpha = 0$ otherwise.

Since addition in a direct sum is componentwise, we must have $m_\alpha = 0_{M_\alpha}$ for all α. This means that $m_{\alpha_i} = r_{i,1}a_{i,1} + \cdots + r_{i,k_1}a_{i,k_i} = 0_{M_{\alpha_i}}$ for all i. However, A_{α_i} forms a basis for M_{α_i}, thus $0_{M_{\alpha_i}}$ cannot take this form with nonzero $r_{i,j}$. Therefore, $x \neq 0_{F(A)}$, a contradiction. So $\ker(\Phi) = \{0\}$, thus Φ is injective. (Note: Just to make sure I do not take this for granted, if B is a basis for an R-module N and we have some nonzero $r_1, \ldots, r_n \in R$ such that $r_1a_1 + \cdots + r_na_n = 0$ for some distinct $a_1, \ldots, a_n \in A$, then $r_1a_1 + \cdots + r_{n-1}a_{n-1} = (-r_n)a_n$ gives two separate representations of $-r_na_n$ as an R-linear combination of basis elements, a contradiction. This is obvious, but we have not explicitly proven it up to this point).

Next, we will show that Φ is surjective. Let $x \in M$, so that $x = \prod_{\alpha \in I} m_\alpha$ where $m_\alpha \in M_\alpha$ for each α and $m_\alpha \neq 0$ for finitely many $\alpha \in I$. Each nonzero m_α is of the form $m_\alpha = r_{1,\alpha}a_{1,\alpha} + \cdots + r_{n,\alpha}a_{n,\alpha}$ where $r_{1,\alpha}, \ldots, r_{n,\alpha} \in R$ and $a_{1,\alpha}, \ldots, a_{n,\alpha} \in A_\alpha$. Let

$$y = \sum_{\{\alpha : m_\alpha \neq 0\}} r_{1,\alpha}a_{1,\alpha} + \cdots + r_{n,\alpha}a_{n,\alpha} \in F(A).$$

Then

$$\begin{aligned}
\Phi(y) &= \Phi\left(\sum_{\{\alpha : m_\alpha \neq 0\}} r_{1,\alpha}a_{1,\alpha} + \cdots + r_{n,\alpha}a_{n,\alpha} \right) \\
&= \sum_{\{\alpha : m_\alpha \neq 0\}} r_{1,\alpha}\Phi(a_{1,\alpha}) + \cdots + r_{n,\alpha}\Phi(a_{n,\alpha}) \\
&= \sum_{\{\alpha : m_\alpha \neq 0\}} r_{1,\alpha}\iota_\alpha(a_{1,\alpha}) + \cdots + r_{n,\alpha}\iota_\alpha(a_{n,\alpha}) \\
&= \sum_{\{\alpha : m_\alpha \neq 0\}} \iota_\alpha(r_{1,\alpha}a_{1,\alpha} + \cdots + r_{n,\alpha}a_{n,\alpha}) \\
&= \sum_{\{\alpha : m_\alpha \neq 0\}} \iota_\alpha(m_\alpha) \\
&= \prod_{\alpha \in I} m_\alpha \\
&= x
\end{aligned}$$

therefore, Φ is surjective and thus an isomorphism.

We have now shown that $F(A) \cong M$. All that remains to show is that, for any R-modules M and N such that $M \cong N$, if M is free, then N is free. Let M and N be congruent R-modules such that M is free on a set A. Let $\varphi : M \to N$ be an isomorphism, and let $y \in N$ be nonzero. There is a unique nonzero element $x \in M$ such that $\varphi(x) = y$. Since M is free on A, there are unique nonzero $r_1, \ldots, r_n \in R$ and unique $a_1, \ldots, a_n \in A$ such that $x = r_1 a_1 + \cdots + r_n a_n$. Thus $y = \varphi(x) = \varphi(r_1 a_1 + \cdots + r_n a_n) = r_1 \varphi(a_1) + \cdots + r_n \varphi(a_n)$. Since φ is injective, $\varphi(a_1), \ldots, \varphi(a_n)$ are distinct. Thus y has a representation as an R-linear combination of distinct elements of the set $\varphi(A)$ with nonzero coefficients.

Now, assume that $y = s_1\varphi(b_1) + \cdots + s_n\varphi(b_n)$ for nonzero $s_1, \ldots, s_n \in R$ and distinct $\varphi(b_1), \ldots, \varphi(b_n) \in \varphi(A)$ (where $b_1, \ldots, b_n \in A$). Note that, since φ is injective, $b_1, \ldots, b_n$ must also be distinct. We have

$$\begin{aligned} x &= r_1\varphi(a_1) + \cdots + r_n\varphi(a_n) \\ &= s_1\varphi(b_1) + \cdots + s_n\varphi(b_n) \\ &= \varphi(s_1 b_1 + \cdots + s_n b_n) \\ &= s_1 b_1 + \cdots + s_n b_n. \end{aligned}$$

Since A forms a basis for M over R, the coefficients $s_1, \ldots, s_n$ are nonzero, and $b_1, \ldots, b_n$ are distinct, we must have $a_i = b_i$ and $r_i = s_i$ for every $i \in \{1, \ldots, n\}$, up to reordering the indices. Therefore, the representation of x of this form is unique, so N is free on $\varphi(A)$.

□

6. (Exercise 27 in DF §10.3.) For each $i \in \mathbf{N}$, let $M_i = \mathbf{Z}$ (viewed as a $\mathbf{Z}$-module). Let M be the direct product $\prod_{i \in \mathbf{N}} M_i$, and let $R = \mathrm{End}_{\mathbf{Z}}(M)$ (defined on p. 347 of DF).

Define $\phi_o, \phi_e \in R$ by

$$\begin{aligned} \phi_o(a_1, a_2, a_3, \ldots) &= (a_1, a_3, a_5, \ldots), \\ \phi_e(a_1, a_2, a_3, \ldots) &= (a_2, a_4, a_6, \ldots). \end{aligned}$$

(a) Prove that $\{\phi_o, \phi_e\}$ is a basis of the left R-module R. (Hint: Define elements $\psi_o, \psi_e \in R$ by

$$\begin{aligned} \psi_o(a_1, a_2, a_3, \ldots) &= (a_1, 0, a_2, 0, \ldots), \\ \psi_e(a_1, a_2, a_3, \ldots) &= (0, a_1, 0, a_2, \ldots). \end{aligned}$$

Verify that $\phi_o\psi_o = \phi_e\psi_e = 1$, $\phi_o\psi_e = \phi_e\psi_o = 0$, and $\psi_o\phi_o + \psi_e\phi_e = 1$. Deduce from these relations that $\{\phi_o, \phi_e\}$ is a basis.)

Proof. We will verify that the relations hold:

$$\begin{aligned} \phi_o\psi_o(a_1, a_2, a_3, \ldots) &= \phi_o(a_1, 0, a_2, 0, \ldots) = (a_1, a_2, a_3, \ldots) \\ \phi_e\psi_e(a_1, a_2, a_3, \ldots) &= \phi_e(0, a_1, 0, a_2, \ldots) = (a_1, a_2, a_3, \ldots) \\ \phi_o\psi_e(a_1, a_2, a_3, \ldots) &= \phi_o(0, a_1, 0, a_2, \ldots) = (0, 0, 0, \ldots) \\ \phi_e\psi_o(a_1, a_2, a_3, \ldots) &= \phi_e(a_1, 0, a_2, 0, \ldots) = (0, 0, 0, \ldots) \\ (\psi_o\phi_o + \psi_e\phi_e)(a_1, a_2, a_3, \ldots) &= \psi_o(a_1, a_3, a_5, \ldots) + \psi_e(a_2, a_4, a_6, \ldots) \\ &= (a_1, 0, a_3, 0, a_5, 0, \ldots) + (0, a_2, 0, a_4, 0, a_6, \ldots) \\ &= (a_1, a_2, a_3, a_4, a_5, a_6, \ldots) \end{aligned}$$

Since $\psi_o\phi_o + \psi_e\phi_e = 1$, left multplying by any $\varphi \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z})$ gives

$$(\varphi\psi_o)\phi_o + (\varphi\psi_e)\phi_e = \varphi(\psi_o\phi_o + \psi_e\phi_e) = \varphi$$

thus every element has a representation as a linear combination of elements of this basis.

Now, assume for some $f, g \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z})$ that $f\phi_o + g\phi_e = 0$. Right multiplication by ψ_o and left multiplication by ψ_e gives

$$\begin{aligned}\psi_e f &= (\psi_e f) \cdot 1 + (\psi_e g) \cdot 0 \\ &= (\psi_e f)(\phi_o \psi_o) + (\psi_e g)(\phi_e \psi_o) \\ &= \psi_e (f\phi_o)\psi_o + \psi_e (g\phi_e)\psi_o \\ &= \psi_e (f\phi_o + g\phi_e)\psi_o \\ &= 0.\end{aligned}$$

Right multiplication by ψ_e and left multiplication by ψ_o gives

$$\begin{aligned}\psi_o g &= (\psi_o f) \cdot 0 + (\psi_o g) \cdot 1 \\ &= (\psi_o f)(\phi_o \psi_e) + (\psi_o g)(\phi_e \psi_e) \\ &= \psi_o (f\phi_o)\psi_e + \psi_o (g\phi_e)\psi_e \\ &= \psi_o (f\phi_o + g\phi_e)\psi_e \\ &= 0.\end{aligned}$$

Left multiplying by ϕ_e and ϕ_o, respectively, gives

$$\begin{aligned}f &= (\phi_e \psi_e) f = \phi_e (\psi_e f) = \phi_e \cdot 0 = 0 \\ g &= (\phi_o \psi_o) g = \phi_o (\psi_o g) = \phi_o \cdot 0 = 0.\end{aligned}$$

Now, if any element of M has two equal representations $a\phi_0 + b\phi_e$ and $c\phi_0 + d\phi_e$ as an R-linear combination of these generators, then we have

$$\begin{aligned}& a\phi_0 + b\phi_e = c\phi_0 + d\phi_e \\ \implies & (a-c)\phi_0 + (b-d)\phi_e = 0.\end{aligned}$$

So by the result of the previous paragraph, $a - c = b - d = 0$, so $a = c$ and $b = d$. Thus these representations are unique, so $\{\phi_o, \phi_e\}$ is a basis of the left R-module R. □

(b) Use part (a) to prove that $R \cong R^2$. Deduce that $R \cong R^n$ for every $n \in \mathbf{N}$.

Proof. The universal property given in Theorem 6 implies that $R \cong R^2$. Since R is free on $A = \{\phi_o, \phi_e\}$, the set map $\phi_o \mapsto (1_R, 0)$, $\phi_e \mapsto (0, 1_R)$ naturally and uniquely extends to an isomorphism between $R = R\phi_o \oplus R\phi_e$ and R^2. Thus $R \cong R^2$.

Now, assume for some $n \in \mathbb{N}$ that $R \cong R^n$. Then $R^{n+1} \cong R \oplus R^n \cong R \oplus R \cong R^2 \cong R$, so the desired result follows by induction. □