Abstract Algebra II Homework 2

Carson Connard

Section 10.3

2 Assume R is commutative. Prove that $R^n \cong R^m$ if and only if $n = m$, that is two free R-modules of finite rank are isomorphic if and only if they have the same rank.

Proof. ($\Longleftarrow$) Note that if $|M| = |N|$, then the free modules $F(M) \cong F(N)$. So, assuming that two modules are of the same rank, then they must be isomorphic.
($\Longrightarrow$) First, we shall prove the following lemma: if $M \cong N$ as R-modules, and $I \trianglelefteq R$, then $M/IM \cong N/IN$.

Proof. Take $\varphi : M \to N$ to be an R-module isomorphism. Also, consider the induced map $\varphi' : M/IM \to N/IN$ defined as $m + IM \mapsto \varphi(m) + IN$. This is well defined since we are taking a quotient of each module by the action of I. It is surjective too: taking $n + IN \in N/IN$, the preimage is $\varphi^{-1}(n) + IM \in M/IM$. We also have that the inverse induced map, $(\varphi')^{-1} : N/IN \to M/IM$ is well defined. We see that $(\varphi')^{-1} \circ \varphi'$ acts as the identity on M/IM:

$$(\varphi')^{-1}(\varphi'(m + IM)) = (\varphi')^{-1}(\varphi(m) + IN) = \varphi^{-1}(\varphi(m)) + IM = m + IM.$$

Therefore we have that φ' is injective, and so φ' is an isomorphism as desired. $\square$

Suppose now that $R^n \cong R^m$. Also, take I to be a maximal ideal. We have from the problem statement of 10.2.12 that $(R/IR)^n \cong R^n/IR^n \cong R^m/IR^m \cong (R/IR)^m$, with the middle isomorphism being the induced isomorphism which was used in the lemma. But, this means that two modules of dimension m and n are isomorphic, which means that we must have $m = n$. $\square$

4 An R-module M is called a *torsion* module if for each $m \in M$ there is a nonzero element $r \in R$ such that $rm = 0$, where r may depend on m (i.e. $M = \text{Tor}(M)$ in the notation of §1 Ex. 8). Prove that every finite abelian group is a torsion $\mathbb{Z}$-module. Give an example of an infinite abelian group that is a torsion $\mathbb{Z}$-module.

Proof. Take G to be an abelian group. Then the nonzero element $g = |G| \in \mathbb{Z}$ annihilates G, and therefore G is a torsion module. $\square$

Example: Consider the group $\mathbb{Q}/\mathbb{Z}$. Each element is of finite order and therefore is annihilated by some $a \in \mathbb{Z}$.

5 Let R be an integral domain. Prove that every finitely generated torsion R-module has a nonzero annihilator, that is, there is a nonzero element $r \in R$ such that $rm = 0$ for all $m \in M$ – here r does not depend on m. Give an example of a torsion R-module whose annihilator is the zero ideal.

Proof. Take $M = RA$ for $A = \{a_1, ..., a_n\}$. For each a_i, take $r_i \neq 0$, such that $r_i a_i = 0$. We claim now that $r_1 r_2 \cdots r_n =: r$ is a nonzero element of $\text{Ann}_R(M)$. Since R is an integral domain, we have that $r \neq 0$. Now notice that by the commutativity of R, we have that r annihilates each a_i, and therefore $r \in \text{Ann}_R(M)$. Since r annihilates a generating set for M we must have that r annihilates M. $\square$

Example: Notice every element of $\bigoplus_{i \in \mathbb{N}} \mathbb{Z}_2$ has order 1 or 2, and therefore it is certainly torsion and infinite.

6 Prove that if M is a finitely generated R-module that is generated by n elements then every quotient of M may be generated by n or fewer elements. Deduce that quotients of cyclic modules are cyclic.

Proof. Take $\{a_1, \cdots, a_n\}$ to be a generating set for M. We claim that $\{a_1 + N, \cdots, a_n + N\}$ generates the R-module M/N. Indeed, we see that we can write any $m + N \in M/N$ as

$$m + N = \left(\sum_i r_i a_i\right) + N = \sum_i r_i(a_i + N).$$

This shows the result. Therefore we have that the quotient of cyclic module can be generated by 0 or 1 elements and still be cyclic. $\square$

7 Let N be a submodule of M. Prove that if both M/N and N are finitely generated then so is M.

Proof. Take $\{a_1, ..., a_n\}$ to be the finite generating set of N. Also take $\{b_1 + N, ..., b_m + N\}$ to be the finite generating set of M/N. We claim now that the set $S := \{a_1, ..., a_n, b_1, ..., b_m\}$ generates the R-module M. Let us take $\pi : M \to M/N$ to be the projection map. Then for some arbitrary $m \in M$, take $x_1, ..., x_m$ to be such that

$$m + N = \sum_i x_i(b_i + N) = \left(\sum_i x_i b_i\right) + N.$$

We see that $m - \sum x_i b_i \in \ker \pi$, therefore $m - \sum x_i b_i \in N$. So, there must exist $y_1, ..., y_n$ such that

$$m - \sum_i x_i b_i = \sum_j y_j a_j, \text{ implying } m = \sum_i x_i b_i + \sum_j y_j a_j \in RA.$$

Therefore $RA = M$ and A finitely generates M. $\square$

9 An R-module M is called *irreducible* if $M \neq 0$ and if 0 and M are the only submodules of M. Show that M is irreducible if and only if $M \neq 0$ and M is a cyclic module with any nonzero element as generator. Determine all the irreducible $\mathbb{Z}$-modules.

Proof. ($\Longrightarrow$) Suppose M is irreducible. By definition, we know then that $M \neq 0$. So taking some nonzero $m \in M$, we have that Rm is a nonzero submodule of M, and therefore $Rm = M$ since M is irreducible. Therefore M is generated by any nonzero element.

($\Longleftarrow$) Suppose now $M \neq 0$ and M is cyclic with a nonzero element as a generator. Take now N to be some nonzero submodule of M. Take $n \in N$ to be nonzero, and notice then $M = Rn \subset N$, and so therefore $M = N$. Therefore the only nonzero submodule of M is M, and so M is irreducible. $\square$

Classification: In order to classify the irreducible $\mathbb{Z}$-modules, consider just cyclic modules. If a cyclic module is not a torsion module then it must be isomorphic to $\mathbb{Z}$. However, this is not irreducible since it contains a submodule isomorphic to $n\mathbb{Z}$ for $n \in \mathbb{N}$. So we have only cyclic torsion modules of $\mathbb{Z}$, which in fact are just finite cyclic groups. We know that the only irreducible finite cyclic groups are those of the form $\mathbb{Z}_p$ for p prime.

10 Assume R is commutative. Show that an R-module M is irreducible if and only if M is isomorphic (as an R-module) to R/I where I is a maximal ideal of R.

Proof. ($\Longrightarrow$) Suppose that M is an irreducible R-module. Fixing some nonzero $m \in M$, we know that $Rm = M$. Take now $\varphi : R \to M$ to be defined as $r \mapsto rm$. This is a homomorphism of R-modules, and moreover, it is surjective. So, we have that $M \cong R/\ker\varphi$. It now suffices to show that $\ker\varphi$ as a submodule is a maximal ideal of R. So, first since $\ker\varphi$ is a submodule of R, we know that $\ker\varphi$ is an ideal. Next, notice that $\ker\varphi = \mathrm{Ann}_R(m)$. Therefore any ideal I which strictly contains $\ker\varphi$ must contain some r such that $rm \neq 0$. But, this means that $IM \neq 0$, and therefore $IM = M$ since M is irreducible. So, I must contain some element s such that $sm = m$, or equivalently $(s - 1)m = 0$. Clearly then $s - 1 \in \ker\varphi$, but $\ker\varphi \subset I$ and therefore we have that $s, s - 1 \in I$ which gives that $1 \in I$. Therefore we have that $I = R$ and so I is maximal as desired.

($\Longleftarrow$) Suppose that $M \cong R/I$ for some maximal ideal I. We want to show that $Rm = M$ for all nonzero $m \in M$. Indeed, we can write any $m \neq 0$ as $a + I$ with $a \notin I$ since we assumed the above isomorphism. But, then we have$R(a+I) = Ra + RI = Ra + I$. Notice now that $Ra + I$ is an ideal which strictly contains I, and therefore $Ra + I = R$ since I was taken to be maximal. Therefore we have that $R(a + I) = R/I$ in R/I as desired. □

11 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 irreducible then $\mathrm{End}_R(M)$ is a division ring (this result is called *Schur's lemma*).

Proof. Take $\varphi : M_1 \to M_2$ to be a nonzero R-module homomorphism We know that $\ker \varphi \neq M_1$, and therefore we have that $\ker \varphi$ is trivial. However, we know that $\varphi(M_1) \neq \{0\}$, and so $\varphi(M_1) = M_2$. Therefore we have that φ is both injective and surjective, and since it is a homomorphism, we have that φ is an isomorphism.

We want to show that $\mathrm{End}_R(M)$ is a division ring, that is it is a ring which every nonzero element has an inverse such that $rr^{-1} = r^{-1}r = 1$. Notice though that the objects of $\mathrm{End}_R(M)$ are functions, and so if M is irreducible, then every element in $\mathrm{End}_R(M)$ is an isomorphism by the above result, which implies that M contains multiplicative inverses as desired. □

12 Let R be a commutative ring and let A, B, M be R-modules. Prove the following isomorphisms of R-modules:

(a) $\hom_R(A \times B, M) \cong \hom_R(A, M) \times \hom_R(B, M)$.

Proof. For brevity, let us define $H := \hom_R(A \times B, M)$, $H_A := \hom_R(A, M)$, and $H_B := \hom_R(B, M)$. Let us define a map $F : H_A \times H_B \to H$ by $(a, b) \mapsto \varphi_1(a) + \varphi_2(b)$, where $\varphi_1 \in H_A$ and $\varphi_2 \in H_B$. We must show that F is well defined: indeed, let us take $(a, b), (c, d) \in A \times B$ and take $r \in R$. Since the φ_i are homomorphisms, we have that

$$\begin{aligned}
F((\varphi_1, \varphi_2))(r(a, b) - (c, d)) &= \varphi_1(ra - c) + \varphi_2(rb - d) \\
&= r\varphi_1(a) - \varphi_1(c) + r\varphi_2(b) - \varphi_2(d) \\
&= rF((\varphi_1, \varphi_2))(a, b) - F((\varphi_1, \varphi_2))(c, d).
\end{aligned}$$

Indeed, F is well defined. We aim to show that F is an isomorphism, so first a homomorphism. Take $(\varphi_1, \varphi_2), (\psi_1, \psi_2) \in H_A \times H_B$ and let $r \in R$. Also, take some $(a, b) \in A \times B$. Then we have that

$$\begin{aligned}
F(r(\varphi_1, \varphi_2) - (\psi_1, \psi_2))(a, b) &= (r\varphi_1 - \psi_1)(a) + (r\varphi_2 - \psi_2)(b) \\
&= r\varphi_1(a) - \psi_1(a) + r\varphi_2(b) - \psi_2(b) \\
&= rF(\varphi_1, \varphi_2) - F(\psi_1, \psi_2).
\end{aligned}$$

F is a homomorphism. Finally, we need to show that F is bijective. Injectivity is clear, as if $(\varphi_1, \varphi_2) = (0, 0)$ then we have that $F((\varphi_1, \varphi_2))(a, b) = \varphi_1(a) + \varphi_2(b) = 0$ for any $(A, b) \in A \times B$. For surjectivty, consider some $\Phi \in H$. Also, take again some $(\varphi_1, \varphi_2) \in H_A \times H_B$, such that for any $(a, b) \in A \times B$, they are defined as $\varphi_1(a) = \Phi(a, 0)$ and $\varphi_2(b) = \Phi(0, b)$. Notice that Φ is just an R-module homomorphism restricted to $A \times \{0\}$ and $\{0\} \times B$ respectively, and therefore we have that $\varphi_1(a) \in H_A$ and $\varphi_2 \in H_B$. So, we have that $F((\varphi_1, \varphi_2))(a, b) = \Phi(a, 0) + \Phi(0, b) = \Phi(a, b)$. This shows surjectivity, and therefore F is an isomorphism. The congruence has been shown. □

(b) $\hom_R(M, A \times B) \cong \hom_R(M, A) \times \hom_R(M, B)$.

Proof. For brevity, let us define $H := \hom_R(M, A \times B)$, $H_A := \hom_R(M, A)$, and $H_B := \hom_R(M, B)$. Let us define a map $F : H_A \times H_B \to H$ by $(\varphi_1, \varphi_2) \mapsto \varphi$, where $\varphi(m) = (\varphi_1(m), \varphi_2(m))$ for $m \in M$. We must show that F is well defined: indeed, take $m, n \in M$ and $r \in R$. Then we have that

$$\varphi(rm - n) = (\varphi_1(rm - n), \varphi_2(rm - n)) = (r\varphi_1(m) - \varphi_1(n), r\varphi_2(m) - \varphi(n)) = r\varphi(m) - \varphi(n).$$

So $\varphi \in H$ and F is well defined. We aim to show that F is an isomorphism, so first we show that it is a homomorphism. Let us take $(\varphi_1, \varphi_2), (\psi_1, \psi_2) \in H_A \times H_B$ and let $r \in R$. Then for any $m \in M$, we see

$$\begin{aligned} F(r(\varphi_1, \varphi_2))(m) &= ((r\varphi_1 - \psi_1)(m), (r\varphi_2 - \psi_2)(m)) \\ &= r(\varphi_1(m) - \psi_1(m), r\varphi_2(m) - \psi_2(m)) \\ &= r(\varphi_1(m), \varphi_2(m)) - (\psi_1(m), \psi_2(m)) \\ &= rF((\varphi_1, \varphi_2))(m) - F((\psi_1, \psi_2))(m). \end{aligned}$$

F is a homomorphism. Finally, we need to show that F is an isomorphism. If we let $F((\varphi_1, \varphi_2)) = 0$, then for any $m \in M$ we have that $(\varphi_1(m), \varphi_2(m)) = (0, 0)$. Therefore we have that $\varphi_1 = \varphi_2 = 0$. Suppose now $\Phi \in H$, then for any $m \in M$ we have that $\Phi(m) = (a_m, b_m)$ for some $a_m = a(m) \in A$ and $b_m = b(m) \in B$. Let now φ_1 be defined as $m \mapsto a_m$. Then if $m, n \in M$ and $r \in R$, we have that $\varphi_1(rm - n) = a_{rm-n}$. Now since $\Phi(rm - n) = r\Phi(m) - \Phi(n)$ since Φ is a homomorphism, we have that $a_{rm-n} = ra_m - a_n$. Therefore $\varphi_1 \in H_A$. We can repeat this exact process for ϕ_2 mapping $m \mapsto b_m$, giving $\varphi_2 \in H_B$. Therefore, $F(\varphi_1, \varphi_2) = \Phi$, and so F is an isomorphism. The congruence has been shown. □

15 An element $e \in R$ is called a *central idempotent* if $e^2 = e$ and $er = re$ for all $r \in R$. If e is a central idempotent in R, prove that $M = eM \oplus (1-e)M$.

Proof. Suppose first that e is a central idempotent. Define $\varphi : M \to eM \oplus (1-e)M$ by $m \mapsto (em, (1-e)m)$. We claim that φ is an R-module homomorphism. Indeed, take $r \in R$ and $m_1, m_2 \in M$. We have the following:

$$\varphi(rm_1 - m_2) = (e(rm_1 - m_2), (1-e)(rm_1 - m_2)) = (e(rm_1), (1-e)(rm_1)) - (em_2, (1-e)m_2).$$

Moreover, since $er = re$, we have that $(1-e)r = r - er = r - re = r(1-e)$, and so indeed we have that φ is an R-module homomorphism since

$$\varphi(rm_1 - m_2) = r(em_1, (1-e)m_1) - (em_2, (1-e)m_2) = r\varphi(m_1) - \varphi(m_2).$$

We now show that φ is an isomorphism. First note that if $\varphi(m) = 0$, we clearly have that $(em, (1-e)m) = (0, 0)$, so $(1-e)m = 0$. Equivalently, we see $m - em = 0$, and since $em = 0$ we have that $m = 0$, giving that φ is injective. If we consider some element $(a, b) \in eM \oplus (1-e)M$, then we see $a = ea'$ and $b = (1-e)b'$ for $a', b' \in M$. Therefore we have that $ea' + (1-e)b' \in M$, and so applying φ yields

$$\varphi(ea' + (1-e)b') = (e(ea), (1-e)((1-e)b)) = (ea', (1-e)b').$$

This gives that φ is surjective, and therefore we have that φ is an isomorphism. This means that indeed, $M = eM \oplus (1-e)M$ as desired. □

16 For any ideal I of R, let IM be the submodule defined as

$$IM = \left\{ \sum_{\text{finite}} a_i m_i : a_i \in I,\ m_i \in M \right\}.$$

Let $A_1, ..., A_k$ be any ideals in the ring R. Prove that the map $\varphi : M \to M/A_1M \times \cdots \times M/A_kM$ defined by $m \mapsto (m + A_1M, \cdots, m + A_kM)$ is an R-module homomorphism with kernel $A_1M \cap A_2M \cap \cdots \cap A_kM$.

Proof. Notice that $\ker \varphi$ is the set of all $m \in M$ such that $m \in A_iM$ for all i by definition of quotient. By definition of intersection, this is equivalent to $A_1M \cap A_2M \cap \cdots \cap A_kM$, and we have the desired result. □

17 In the notation of the previous exercise, assume further that the ideals $A_1, \cdots, A_k$ are pairwise comaximal, that is $A_i + A_j = R$ for all $i \neq j$. Prove that $M/(A_1 \cdots A_k)M \cong M/A_1M \times \cdots \times M/A_kM$.

Proof. We mirror the proof for the Chinese remainder theorem for rings, and modify for modules. First, we aim to show that $A_1M \cap \cdots \cap A_kM = (A_1 \times \cdots \times A_k)M$.

First let us note that the product of all $A_1 \times \cdots \times A_k$ is contained in any A_i since each A_i is an ideal, and multiplication is absorbed on both sides by definition of an ideal. Therefore we have that $A_1M \cap \cdots \cap A_kM \supset (A_1 \times \cdots \times A_k)M$.

For the reverse inclusion, we induct over k. For our base case, take $k = 1$, and we have an obvious inclusion since we only have one ideal. For our inductive hypothesis, let us assume that $A_2M \cap \cdots \cap A_kM = (A_2 \cdots A_k)M$. Certainly then we have that $A_1M \cap A_2M \cap \cdots \cap A_kM = A_1M \cap (A_2 \cdots A_k)M$. Notice now that the assumption regarding comaximality in the problem statement implies that A_1 and $A_2 \cdots A_k$ are comaximal due to the behavior of ideals. Therefore we can write $1 = a + a'$ for some $a \in A_1$ and $a' \in A_2 \cdots A_k$. This implies that $A_1 \cap A_2 \cap \cdots \cap A_k \subset A_1A_2 \cdots A_k$, since for $b \in A_1 \cap A_2 \cap \cdots \cap A_k$ we have that $b = 1 \cdot b = (a + a')b = ab + a'b = ab + ba' \in A_1(A_2 \cdots A_k)$. Combining everything gives the following:

$$\begin{aligned} A_1M \cap A_2M \cap \cdots \cap A_kM &= A_1M \cap (A_2 \cdots A_k)M \\ &\subset A_1M \cap (A_2 \cap A_3 \cap \cdots \cap A_k)M \\ &\subset A_1M \cap A_2M \cap \cdots \cap A_kM. \end{aligned}$$

We have shown both containments and therefore we have that indeed, $A_1M \cap \cdots \cap A_kM = (A_1 \times \cdots \times A_k)M$.

We now need to show surjectivity of the map $\varphi : M \to M/A_1M \times \cdots \times M/A_kM$ defined by $m \mapsto (m + A_1M, \cdots, m + A_kM)$. We again induct over k. Taking a base case of $k = 2$, we see that since A_1 and A_2 are comaximal, we have that there must exist some $a_1 \in A_1$ and some $a_2 \in A_2$ such that $a_1 + a_2 = 1$. It suffices to show then that there exists some preimage of $(m + A_1, 0)$ and of $(0, m + A_2)$ for all $m \in M$ in order to show surjectivity. Indeed, notice that

$$\begin{aligned} &\varphi(a_1m) = (0, a_1m + A_2) = (0, (1 - a_2)m + A_2) = (0, m - a_2m + A_2) = (0, m + A_2), \text{ and} \\ &\varphi(a_2m) = (a_2m + A_1, 0) = ((1 - a_1)m + A_1, 0) = (m - a_1m + A_1, 0) = (m + A_1, 0). \end{aligned}$$

Indeed, the map is surjective for the base case. For the inductive step, the inductive hypothesis gives that φ is surjective on all elements of the form $(m_1 + A_1, m_2 + A_2M \cdots, a_k + A_kM)$, where all values of $m_2, \cdots, m_k$ are acquired, but not necessarily the same for the values of m_1. So, we must show preimages for $(m_1 + A_1, 0, \cdots, 0)\ \forall m_1$. Note that since A_1 and $A_2 \cdots A_k$ are comaximal, we can say $a + a' = 1$ for some $a \in A_1$ and $a' \in A_2 \cdots A_k$. We have the following:

$$\begin{aligned} \varphi(a'm_1) &= (a'm_1 + A_1M, a'm_1 + A_2M, \cdots, a'm_1 + A_kM) \\ &= (m_1 - am_1 + A_1M, 0 \cdots, 0) \\ &= (m_1 + A_1M, 0, \cdots, 0). \end{aligned}$$

Indeed, $\varphi(M)$ is all of $M/A_1M \times \cdots \times M/A_kM$. By the first isomorphism theorem for modules we have that $M/\ker\varphi \cong M/A_1M \times \cdots \times M/A_kM$. However, we know that $\ker\varphi = A_1M \cap \cdots \cap A_kM$, and as we showed earlier, $A_1M \cap \cdots \cap A_kM = (A_1 \times \cdots \times A_k)M$. Therefore we have that $M/(A_1 \cdots A_k)M \cong M/A_1M \times \cdots \times M/A_kM$ as desired. □

18 Let R be a PID and let M be an R-module that is annihilated by the nonzero, proper ideal (a). Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the unique factorization of a into distinct prime powers in R. Let M_i be the annihilator of $p_i^{\alpha_i}$ in M, that is M_i is the set $\{m \in M : p_i^{\alpha_i} m = 0\}$ – called the *p_i-primary component of* M. Prove that $M = M_1 \oplus \cdots \oplus M_k$.

Proof. We claim first that $M_1 + \cdots + M_k$ is indeed a direct sum. To do so, we aim to show that $M_i \cap (\sum_{j \neq i} M_j) = 0$ for all i. So take some $m_i \in M_i$ and let us assume that $m_i \in \sum_{j \neq i} M_j$ as well. We see that m_i is annihilated by both $p_i^{\alpha_i}$ and $\prod_{j \neq i} p_j^{\alpha_j}$ by definiton of M_i. Therefore we have that $p_i^{\alpha_i}$ and $\prod_{j \neq i} p_j^{\alpha_j}$ are elements of the same ideal which annihilates m_i. This ideal must then contain $\gcd(p_i^{\alpha_i}, \prod_{j \neq i} p_j^{\alpha_j})$, which since these are coprime numbers, must be equal to 1. So, $m_i = 1m_i = 0$, and therefore indeed $M_1 + \cdots + M_k = M_1 \oplus \cdots \oplus M_k$.

We now want to show that $M = M_1 \oplus \cdots \oplus M_k$. Problem 17 gives the following congruences:

$$M \cong M/(a)M \cong M/(p_1^{\alpha_1})M \times \cdots \times M/(p_k^{\alpha_k})M.$$

This is because $(a)M = 0$ and any two $(p_i^{\alpha_i})$ are pairwise comaximal. Recall now from Problem 17 the isomorphism $\varphi(m) = (m + p_1^{\alpha_1}M, \cdots, m + p_k^{\alpha_k}M)$. We want to show that this map restricted to $M_1 \oplus \cdots \oplus M_k \subset M$ is surjective. To do so, we will show that φ^{-1} maps into $M_1 \oplus \cdots \oplus M_k$. We can show this for only $x_i := (0, \cdots, 0, m + (p_i^{\alpha_i})M, 0, \cdots, 0)$, where the nonzero term is in the ith position. This works since elements of this form generate $M_1 \oplus \cdots \oplus M_k$. Indeed, the image of x_i will be some $m' \in M$, which is congruent to 0 mod $p_j^{\alpha_j}$ for $j \neq i$. In particular, for some $m'' \in M$, we have that $m' = (a/p_i^{\alpha_i})m''$ for some other $m'' \in M$. Certainly then $m' \in M_i$ since $p_i^{\alpha_i}m = p_i^{\alpha_i}(a/p_i^{\alpha_i})m'' = am'' = 0$. Therefore we have that indeed φ^{-1} maps into $\bigoplus M_i$, and therefore $M = M_1 \oplus \cdots \oplus M_k$ as desired. $\square$