STRUCTURE THEOREM FOR FINITELY GENERATED MODULES OVER A PID

ALBERT TAM

1. Introduction

In this paper, we will prove the structure theorem for finitely generated modules over a principal ideal domain. Sections 2 and 3 will define and provide examples of rings, ideals, quotient rings, and ring homomorphisms. Section 4 will define more specific types of rings, including principal ideal domains, which are the main focus of this paper. Sections 5 and 6 will introduce modules, submodules, quotient modules, and module homomorphisms. Section 7 will define special properties of modules. Section 8 will prove preliminary results, and Section 9 will contain the actual proof of the structure theorem. Section 10 will discuss consequences of the structure theorem, such as the classification of finitely generated abelian groups.

2. An introduction to rings

Definition 2.1.

(1) A ring is a set R with two binary operations $+$ and $\times$, which are addition and multiplication respectively, satisfying the following axioms:
   (a) $(R, +)$ is an abelian group.
   (b) $\times$ is associative, so $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$.
   (c) The distributive law holds, so for all $a, b, c \in R$:

$$a \times (b + c) = a \times b + a \times c$$

   and

$$(a + b) \times c = a \times c + b \times c.$$

(2) The ring R has an *identity* if there exists an element $1 \in R$ such that $1 \times a = a \times 1 = a$ for all $a \in R$.

Remark 2.2. From now on, we will assume that all rings have an identity unless stated otherwise.

Notice that multiplicative inverses and a multiplicative identity are not guaranteed for rings, like they are for fields.

Now, let's consider some examples of rings.

(1) The prototypical example of a ring is the integers $\mathbb{Z}$. They form an abelian group under addition and have a well-defined multiplication operation, under which inverses are not guaranteed. However, $\mathbb{Z}$ has significant structure over a typical ring; for example, multiplication in $\mathbb{Z}$ is commutative, and there is an identity in $\mathbb{Z}$.
(2) All fields are rings under the same addition and multiplication operations.

(3) The ring of $n \times n$ matrices with entries in a ring R form a *matrix ring*, denoted by $M_n(R)$, where addition is defined componentwise and multiplication is defined by normal matrix multiplication. This ring is *not* commutative.
(4) Let R be a ring with identity and commutative multiplication and $x_1, \ldots, x_n$ be variables. Then $R[x_1, \ldots, x_n]$, the set of polynomials of $x_1, \ldots, x_n$ with coefficients in R, forms a ring, which also has identity and commutative multiplication.
(5) The integers modulo any integer n, or $\mathbb{Z}/n\mathbb{Z}$, always forms a ring with identity and commutative multiplication.

Notice that in $\mathbb{Z}/n\mathbb{Z}$ for composite n, nonzero elements can multiply to 0 (for example, take $2 \cdot 3$ in $\mathbb{Z}/6\mathbb{Z}$). We give such elements a special name:

Definition 2.3. Let R be a ring. An element $a \in R$ is called a *zero divisor* if there is another nonzero element $b \in R$ such that $ab = 0$.

Example. In the matrix ring $M_2(\mathbb{Z})$, the matrix $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is a zero divisor, since:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

.

Let's consider $M_2(\mathbb{Z})$ again. While not every element has a multiplicative inverse in this ring, some elements do. For example, $\begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 3 & -5 \\ -1 & 2 \end{bmatrix} = I$, where I is the identity matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. These elements also have a special name:

Definition 2.4. Let R be a ring with identity. An element $a \in R$ is called a *unit* if there is an element $b \in R$ such that $ab = 1$.

There is also another class of elements in rings that generalizes primes in $\mathbb{Z}$.

Definition 2.5. Let R be a ring, and let $a, b \in R$. A non-unit element $r \in R$ is *prime* if, whenever r divides ab, either r divides a or r divides b.

Remark 2.6. This is just one way to generalize the primes in $\mathbb{Z}$; the other way gives rise to the class of irreducible elements, which are elements that can only be expressed as the product of a unit and another element. Primes and irreducibles do not always coincide. They only represent the same elements if the ring is an *integral domain*, which we will define later.

3. Subrings, ideals, quotient rings, and ring homomorphisms

Naturally, we consider next substructures of rings, quotients of rings, and ring homomorphisms.

3.1. **Subrings and ideals.**

Definition 3.1. Let R be a ring. A subset $S \subseteq R$ is a *subring* if S is a ring under the same operations ($+$ and $\times$) as R.

To see some examples of subrings, let us take the most familiar ring, $\mathbb{Z}$. Notice that $5\mathbb{Z}$, all of the multiples of 5 in $\mathbb{Z}$, is almost a ring. It is closed under addition and multiplication as defined over $\mathbb{Z}$, but it doesn't contain the identity. However, $5\mathbb{Z}$ has another important property: when any element of $\mathbb{Z}$ is multiplied by an element of $5\mathbb{Z}$, it is also an element of $5\mathbb{Z}$. As a result, it seems like $5\mathbb{Z}$ is still a useful substructure to consider. It turns out that the structure of an *ideal* captures the important properties of $5\mathbb{Z}$:

Definition 3.2. Let R be a ring. A subset $I \subseteq R$ is a left *ideal* if it is nonempty and satisfies the following properties:

(1) If $a, b \in I$, then $a + b \in I$.
(2) If $r \in R$ and $a \in I$, then $ra \in I$.

The definition of a right ideal is the same, except the order of the terms in the second property is switched. If an ideal is both a left ideal and a right ideal, then it is a *two-sided ideal*. For the remainder of this paper, if an ideal is not specified to be left or right, it is assumed to be two-sided.

We provide some examples of ideals, which the reader can verify:

(1) In $\mathbb{Z}$, the set $n\mathbb{Z}$ is a left ideal for any integer n. Since multiplication in $\mathbb{Z}$ is commutative, $n\mathbb{Z}$ is a two-sided ideal.
(2) In $M_2(\mathbb{Z})$, the set of matrices in the form $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$ for all integers a and b forms a left ideal. The set of matrices in the form $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ for all integers a and b forms a right ideal.
(3) For any ring R, the set of polynomials with a constant coefficient of 0 forms a two-sided ideal in $R[x]$.

We say that an ideal is *generated* by a subset $S = \{s_1, \ldots, s_n\}$ if is of the form $\{r_1 s_1 + r_2 s_2 + \cdots + r_n s_n \mid r_1, \ldots, r_n \in R\}$. Such an ideal is denoted by (S). For example, the ideal $n\mathbb{Z}$ for an integer n is just all the multiples of n, so it can be written as (n).

We can "compose" two ideals into other ideals in a number of ways:

Proposition 3.3. *Let I and J both be two-sided ideals in R. Then the following are two-sided ideals:*

(1) *$I + J$, which is defined as $\{a + b \mid a \in I, b \in J\}$*
(2) *$I \cap J$*
(3) *IJ, which is defined as all finite sums $a_1 b_1 + \cdots + a_n b_n$, where $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_n \in J$*

Some types of ideals are special enough that they deserve special terminology:

Definition 3.4. Let I and J be ideals in a ring R.

(1) I is *maximal* if there is no ideal of R, other than R itself and I, that contains I.
(2) I and J are *comaximal* if $I + J = R$.
(3) I is *principal* if $I = (r)$ for some $r \in R$.

Here are some examples of ideals with these special properties:

(1) The ideal $p\mathbb{Z}$, or (p), is maximal in $\mathbb{Z}$. It is also principal, since it is generated by a single element.
(2) For two relatively prime integers m and n, the ideals $m\mathbb{Z}$ and $n\mathbb{Z}$ in $\mathbb{Z}$ are comaximal, since there is a solution to $mx + ny = 1$, and every element in $\mathbb{Z}$ is a multiple of 1.
(3) In the ring $\mathbb{Z}[x]$, the ideal (x) is maximal. However, the ideal $(x - 1)$ is not maximal, since $(x - 1)$ is properly contained in the ideal $(1, x)$.

3.2. **Ring homomorphisms.**

Definition 3.5. Let R and S be rings. A function $\phi : R \to S$ is a *homomorphism* if it satisfies the following properties:

(1) For any $x, y \in R$, $\phi(x + y) = \phi(x) + \phi(y)$.
(2) For any $x, y \in R$, $\phi(xy) = \phi(x) + \phi(y)$.

Example. There is a homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $a \mapsto a \pmod{n}$ for any integer n.

Example. The map $\phi : \mathbb{R}[x] \to \mathbb{R}$ given by $p(x) \mapsto p(a)$ for any real number a is a homomorphism.

For a ring homomorphism, we can also define its kernel and image in a familiar manner:

Definition 3.6. Let R and S be rings, and let $\phi : R \to S$ be a ring homomorphism.

(1) The *kernel* of ϕ, or $\ker \phi$, is defined by $\ker \phi = \{r \in R \mid \phi(r) = 0_S\}$.
(2) The *image* of ϕ, or $\operatorname{im} \phi$, consists of all the elements s in S such that there exists some $r \in R$ with $\phi(r) = s$.

The kernel and image of ring homomorphisms also share familiar properties:

Proposition 3.7. *Let R and S be rings, and let $\phi : R \to S$ be a ring homomorphism. Then* $\ker \phi$ *is an ideal of R, and* $\operatorname{im} \phi$ *is a subring of S.*

Proposition 3.8. *Let R and S be rings, and let $\phi : R \to S$ be a ring homomorphism. Then* $\operatorname{im} \phi = S$ *if and only if ϕ is surjective, and* $\ker \phi = 0_R$ *if and only if ϕ is injective.*

A bijective homomorphism, as always, is an *isomorphism*.

3.3. **Quotient rings.**

Definition 3.9. Let R be a ring and I an ideal in R. Let r be an element of R. The *coset* of r is the set $r + I = \{r + a \mid a \in I\}$.

Cosets in rings work very similar to cosets in groups; for example, just like in groups, if $a + I = b + I$, the element $a - b$ is in I.

Now, we can define quotient rings:

Definition 3.10. Let R be a ring and I an ideal in R. Then the *quotient ring* R/I is the set consisting of all the cosets of I in R. Addition is defined such that $(a+I)+(b+I) = (a+b)+I$, and multiplication is defined such that $(a + I)(b + I) = ab + I$.

We will not prove that this, in fact, does form a ring.

Example. Recall that $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$ for any integer n. There exists the quotient ring $\mathbb{Z}/n\mathbb{Z}$, which consists of the elements $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n - 1) + n\mathbb{Z}$.

Just like how there is a natural projection homomorphism from $G \to G/H$, where G is a group and H a normal subgroup, there is also a natural homomorphism from R to R/I that sends each element in R to its coset in R/I. Like the group projection, this map is also surjective and has a kernel of I.

Now, we can prove a key result about ring homomorphisms that involves quotient rings:

Theorem 3.11 (First Isomorphism Theorem for rings)**.** *Let $\phi : R \to S$ be a ring homomorphism. Then $R/\ker \phi \cong \operatorname{im} \phi$.*

Proof Sketch. The isomorphism $f : R/\ker\phi \to \operatorname{im}\phi$ is given by $r + \ker\phi \mapsto \phi(r)$. The rest of the proof proceeds very similarly to the proof of the group-theoretic version. ■

Using the First Isomorphism Theorem, we can now prove a familiar theorem, generalized for rings.

Theorem 3.12 (Chinese Remainder Theorem for rings)**.** *Let R be a ring, and let $I_1, I_2, \dots I_n$ be comaximal ideals in R. Then $R/(I_1 \cap I_2 \cap \dots \cap I_n) \cong R/I_1 \oplus R/I_2 \oplus \dots \oplus R/I_n$.*

Proof Sketch. It suffices to prove the theorem for two comaximal ideals I and J and extend the theorem to n comaximal ideals with induction. Consider the homomorphism $\phi : R \to R/I \oplus R/J$ defined by $x \mapsto (x + I, x + J)$. Check that this is a ring homomorphism. There is always a solution to the equations $x \equiv r \pmod I$ and $x \equiv s \pmod J$, so ϕ is surjective. Then show that the kernel of ϕ is $(I \cap J)$. By Theorem 3.11, $R/(I \cap J) \cong R/I \oplus R/J$. ■

4. Specific classes of rings

Recall the ring $\mathbb{Z}$. Though not a field, it holds much more structure than our definition of a ring. For example, multiplication is commutative, and there are no nonzero zero divisors. It turns out that these properties (and more) define more specific classes of rings:

Definition 4.1.
(1) A *commutative ring* is a ring where multiplication is commutative.
(2) An *integral domain* is a commutative ring with no nonzero zero divisors.
(3) A *unique factorization domain* is an integral domain where any element can be expressed as the product of a unit and a number of prime elements. This expression is unique, up to the choice of unit and the order of the prime elements.
(4) A *principal ideal domain* is a unique factorization domain where every ideal is generated by a single element, i.e. every ideal can be expressed as the set of multiples of a single element.

Here are some examples of these special types of rings:

(1) An example of a noncommutative ring is the matrix ring $M_2(\mathbb{Z})$.
(2) The ring $\mathbb{Z}[\sqrt{-5}]$, where elements are of the form $a + b\sqrt{-5}$ for integers a, b, is an integral domain but not a unique factorization domain. For example, $6 = 2 \cdot 3$, but 6 is also $(1 + \sqrt{-5})(1 - \sqrt{-5}$. In both cases, the factors of 6 are irreducible (which can be checked), so 6 does not have unique factorization.
(3) Let F be a field. Then the polynomial ring $F[x_1, \dots, x_n]$ is a unique factorization domain, but not a principal ideal domain, when $n \geq 2$. (This is nontrivial.)
(4) The ring $\mathbb{Z}$ is a principal ideal domain. To see why, notice that if I is an ideal of $\mathbb{Z}$, the abelian group $(I, +)$ is a subgroup of the group $(\mathbb{Z}, +)$. Since $(\mathbb{Z}, +)$ is cyclic, so is $(I, +)$. Let $(I, +) = \langle n \rangle$, where n is an integer. Then $I = \{mn \mid m \in \mathbb{Z}\}$, so $I = (n)$. Therefore, all ideals in $\mathbb{Z}$ are principal.

Clearly, principal ideal domains have much more structure than standard rings. For example:

Theorem 4.2. *Let R be a principal ideal domain and $p \in R$ be a prime. Then (p) is maximal.*

Proof. Assume there is an ideal $\mathfrak{m}$ in R such that $(p) \subset \mathfrak{m}$. Since R is a principal ideal domain, we can write $\mathfrak{m} = (m)$ for some $m \in R$. Since $(p) \subset (m)$, we must have $p \in (m)$. Let $p = am$ for some $a \in R$. Since p is a prime, p divides either a or m, so $am \in (p)$.

If p divides a, then write $a = bp$ for some $b \in R$. Then $p = bpm$, so $p(1 - bm) = 0$. Since R is an integral domain, either p or $1 - bm$ is 0. Since p is nonzero, $bm = 1$. Therefore, 1 is in (m), so $(m) = R$.

If p divides m, then let $m = cp$ for some $c \in R$. For every $x \in (m)$, we can write $x = dm$ for some $d \in R$, so every x can also be written as dcp. Therefore, $(m) \subseteq (p)$, so $(m) = (p)$. Thus, if an ideal contains (p), it is either R or (p) itself. Therefore, (p) is maximal. ■

5. Introduction to modules

As a mnemonic, modules can be thought of as vector spaces, but defined over rings.

Definition 5.1. Let R be a ring. A *left R-module*, or a *left module over R*, is a set M together with two operations: a binary operation of M, and an action of R on M (equivalent to a map $R \times M \to M$) that satisfies the following properties:

(1) M is an abelian group under $+$.
(2) Let $r \in R$ and $m \in M$. Then the action of R on M is denoted rm, and it satisfies the following for all $r, s \in R$ and $m, n \in M$:
  (a) $(r + s)m = rm + sm$.
  (b) $r(sm) = (rs)m$.
  (c) $r(m + n) = rm + rn$.
  (d) $1_R m = m$.

A right module over R can be defined analogously. If the underlying ring R is commutative, a right module can be defined for each left module by setting $rm = mr$, and vice versa. Since we primarily concern ourselves with commutative rings in this paper, we will not specify whether a module is left or right, due to this relation between left and right modules over commutative rings.

We give the following examples of modules.

(1) Let R be a ring. Then R is a left R-module over itself, where the action is just left multiplication.
(2) Let R be a ring, and let n be a positive integer. Define $R^n = \{(r_1, r_2, \ldots, r_n) \mid r_i \in R\}$ for all i. Then R^n is a left R-module, where addition is defined componentwise, and the action of R on R^n is componentwise left multiplication.
(3) Let $R = \mathbb{Z}$, and let G be an abelian group whose operation is written as $+$. Then G forms a $\mathbb{Z}$-module as follows. Let $n \in \mathbb{Z}$ and $g \in G$. If n is positive, then let $ng = g + g + \cdots + g$, where there are n copies of g. If n is zero, let $ng = 0$. If n is negative, let $ng = -g - g \cdots - g$, where there are n copies of g.
(4) Let F be a field and V be a vector space of F. Then V is also an F-module.
(5) Let F be a field, V be a vector space over F, and T be a linear transformation from V to V. There is an $F[x]$-module associated with V, given by T. Let T^n denote the function created by composing T for n number of times, with T^0 being the identity. Take the vector space's normal addition operation. Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$. The action of $p(x)$ on V is defined as

$$a_n T^n(v) + a_{n-1} T^{n-1} V + \cdots + a_1 T(v) + a_0.$$

This forms an $F[x]$-module.

Definition 5.2. A subset $N \subseteq M$ is a *submodule* if N is a module under the operations of M.

Example. Let R be a ring, and let $M = R$ be a left R-module where the action is defined by left multiplication. The left ideals of R form submodules of M. Likewise, if M is a right R-module where the action is right multiplication, the right ideals of R form submodules of M.

Example. Let G be an abelian group. As we saw earlier, G forms a left $\mathbb{Z}$-module. The submodules of G as a left module are the same as subgroups of G as a group.

6. Quotient modules and module homomorphisms

Once again, we consider quotients of modules by their substructures and module homomorphisms.

6.1. Module homomorphisms.

Definition 6.1. Let M and N be R-modules. A function $\phi : M \to N$ is a *homomorphism* if it satisfies the following properties:

(1) For any $a, b \in M$, $\phi(a + b) = \phi(a) + \phi(b)$.
(2) For any $r \in R$ and $a \in M$, $\phi(ra) = r\phi(a)$.

Example. There is a projection homomorphism $\pi_i : R^n \to R$ for $1 \leq i \leq n$, defined by $(x_1, \ldots, x_n) \mapsto x_i$. These homomorphisms are surjective, and their kernel consists of the elements with a 0 in position i.

Example. Let G be a $\mathbb{Z}$-module. Since multiplication by an element of $\mathbb{Z}$ is the same as addition of elements in G, the second condition in our definition of module homomorphisms is a result of the first. It follows that homomorphisms of G as a $\mathbb{Z}$-module are the same as group homomorphisms of G.

We can also define notions of kernel and image for module homomorphisms:

Definition 6.2. Let M and N be rings, and let $\phi : M \to N$ be a module homomorphism.

(1) The *kernel* of ϕ, or $\ker \phi$, is defined by $\ker \phi = \{m \in M \mid \phi(m) = 0_N\}$.
(2) The *image* of ϕ, or $\operatorname{im} \phi$, consists of all the elements n in N such that there exists some $m \in M$ with $\phi(m) = n$.

The kernel and image of module homomorphisms also share familiar properties:

Proposition 6.3. *Let M and N be modules, and let $\phi : M \to N$ be a module homomorphism. Then $\ker \phi$ is a submodule of M, and $\operatorname{im} \phi$ is a submodule of N.*

Proposition 6.4. *Let M and N be modules, and let $\phi : M \to N$ be a module homomorphism. Then $\ker \phi = 0_M$ if and only if ϕ is injective, and $\operatorname{im} \phi = N$ if and only if ϕ is surjective.*

6.2. **Quotient modules.**

Definition 6.5. Let R be a ring, let M be an R-module, and let N be a submodule of M. The quotient group $(M,+)/(N,+)$ can be made into an R-module by defining, for all $r \in R$ and $x + N \in M/N$:

$$r(x+N) = rx + N.$$

Notice that $(M,+)/(N,+)$ indeed has group structure, since $(M,+)$ is abelian, so all its subgroups are normal. We will not prove that quotient modules form modules, though.

As always, there is a natural projection homomorphism from a module M to its quotient module M/N given by $m \mapsto m + N$. This homomorphism is also surjective, and its kernel is N.

Theorem 6.6 (First Isomorphism Theorem for modules)**.** *Let M, N be R-modules, and let $\phi : M \to N$ be an R-module homomorphism. Then $R/\ker\phi \cong \operatorname{im}\phi$.*

The proof of this is very similar to the First Isomorphism Theorem for groups and rings, and the reader is invited to prove this as an exercise.

7. Properties of modules

Definition 7.1. Let A be a subset of M. Let $RA = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_1, \ldots, r_n \in R, a_1, \ldots, a_n \in A\}$.

(1) The set RA is called the *submodule* of M *generated by* A. (Proving that this is a submodule is left to the reader.)
(2) Let N be a submodule of M (possibly M itself). Then N is *finitely generated* if there is a finite subset A of M such that $N = RA$.
(3) Let N be a submodule of M (possibly M itself). Then N is *cyclic* if there is an element $a \in M$ such that $N = Ra$.

Definition 7.2. Let M be an R-module.

(1) A subset $m_1, \ldots, m_n$ is *linearly independent* if the only solution to the equation $\sum r_im_i = 0$, where each $r_i \in R$, is when all the r_i are 0.
(2) The rank of M is the maximum number of linearly independent elements in M.

Definition 7.3. Let M be an R-module.

(1) A subset S of M is called a *basis* if S is linearly independent and generates M.
(2) A module M is called *free* if it has a basis.

Remark 7.4. Not every module is free. Let R be the polynomial ring $F[x,y]$ for a field F. Then the ideal (x,y) is a module (since all ideals form modules over their rings), but it is not free. Its generators are x and y, but $(y)x + (-x)y = 0$, so its generators are not linearly independent. Thus, (x,y) is not free.

Definition 7.5. Let $M_1, \ldots, M_k$ be a collection of R-modules. The set of k-tuples $(m_1, \ldots, m_k)$, where each $m_i \in M_i$ and addition and action by R are defined componentwise, is called the *direct sum* of $M_1, \ldots, M_k$, and denoted $M_1 \oplus \cdots \oplus M_k$.

Remark 7.6. There is another condition; in a direct sum of modules, all but finitely many of the entries must be nonzero. This distinction is not relevant in direct sums of finitely many modules.

Proposition 7.7. *Let $N_1, \dots, N_k$ be submodules of an R-module M. Let $N_1 + \cdots + N_k$ be the submodule defined by $\{n_1 + \cdots + n_k \mid n_i \in N_i\}$. Then $N_1 \oplus \cdots \oplus N_k \cong N_1 + \cdots N_k$ if and only if, for every N_j, we have that $N_j \cap \{N_1, \dots, N_{j-1}, N_{j+1}, \dots, N_k\} = \{0\}$.*

Remark 7.8. Therefore, whenever we want to show that a module M is isomorphic to the direct sum of some modules $M_1, \dots, M_k$, it suffices to show that every element in M can be expressed as a linear combination of elements in $M_1, \dots, M_k$, and that $M_j \cap \{M_1, \dots, M_{j-1}, M_{j+1}, \dots, M_k\} = \{0\}$ for every M_j.

Definition 7.9. Let M be a module.

(1) We say that M is a *torsion* module if there exists $m \in M$ such that $am = 0$ for some nonzero $a \in R$.
(2) Likewise, we say that M is *torsion-free* if there are no such elements.
(3) The *torsion submodule* of M consists of the elements $m \in M$ such that there exists $m \in M$ such that $am = 0$ for some nonzero $a \in R$.

8. Preliminary results

This section will prove the many preliminary results that are necessary to show the structure theorem. Many of these results have proofs that are long and not particularly enlightening. For proofs that are not in this section, they can be found in the appendix at the end of this paper.

Proposition 8.1. *Let M be a finitely generated, free module over a principal ideal domain R, and let N be a submodule of M. Then N is free, and its rank is less than or equal to the rank of M.*

Remark 8.2. The theorem also holds true when M does not have a finite basis, but that results is not necessary for our purposes.

The structure theorem essentially decomposes every finitely generated module into a direct sum of some smaller modules. The following result gives us a way to begin doing so, which we will eventually relate later to the torsion submodule of a module.

Lemma 8.3. *Let M and M' be modules over a principal ideal domain R, and assume that M' is free. Let $\phi : M \to M'$ be a surjective R-module homomorphism. Then there exists a free submodule N of M such that the restriction of ϕ to N, or $\phi\big|_N$, induces an isomorphism of N and M', and such that $M \cong N \oplus \ker \phi$.*

Proof. Let $x'_1, \dots, x'_n$ be a basis of M'. For each $1 \leq i \leq n$, let x_i be an element of M such that $\phi(x_i) = x'_i$. Let N be the submodule of M generated by $x_1, \dots, x_n$. Since $x'_1, \dots, x'_n$ are linearly independent, so are $x_1, \dots, x_n$. Therefore, N is free, and ϕ induces an isomorphism $N \cong M'$.

It suffices to show now that $M \cong N \oplus \ker \phi$. Let x be an element of M. Then $\phi(x) \in M'$, so it can be expressed as $\sum a_i x'_i$ for some elements $a_i \in R$. But $\phi(\sum a_i x_i)$ is also equal to $\sum a_i x'_i$, so $x - \sum a_i x_i$ must lie in the kernel of ϕ. Therefore, x can be written as $\sum a_i x_i + (x - \sum a_i x_i)$. The first term lies in N, and the second lies in $\ker \phi$, so $M = N + \ker \phi$. Since ϕ is an isomorphism, its kernel is 0, so $N \cap \ker \phi = 0$. Therefore, $M \cong N \oplus \ker \phi$. ∎

Proposition 8.4. *A finitely generated torsion-free module over a principal ideal domain is free.*

Proof. Let M be a finitely generated torsion-free module over a principal ideal domain R. If $M = 0$, then the statement is trivial, so assume that $M \neq 0$. Let $X = \{x_1, \dots, x_n\}$ be a finite set of generators of M. Let $S = \{x_1, \dots, x_k\}$ be a maximal subset of X with the property that whenever $r_1x_1 + \cdots + r_kx_k = 0$ for elements $r_1, \dots, r_k \in R$, $r_1 = \cdots = r_k = 0$. Since M is torsion-free, any subset of size 1 satisfies this property, so S is nonempty.

Consider the submodule F generated by S. Now let y be an element of X that is not in S. Since S is maximal, there must be $r, r_1, \dots, r_k$ that are not all 0 such that $ry + r_1x_1 + \cdots + r_kx_k = 0$. Therefore, $ry = -\sum_{i=1}^{k} r_ix_i$, so $ry \in F$. If $r = 0$, then all the r_i on the right hand side must also be 0, so r must be nonzero. Let R be the product of all such r for all elements of X that are not in S. Then every element of $RX = \{Rx \mid x \in X\}$ is contained in F. Since X generates M, every element of RM is contained in F. Therefore, there is an R-module homomorphism $\phi : M \to M$ given by $a \mapsto Ra$. Since M is torsion-free, if $Ra = 0$, then either R or a must be 0. If R is 0, then there are no elements in X that are not in S, so $X = S$. This would mean that X is linearly independent, so M is free. If R is nonzero, then the kernel of ϕ is 0. Notice also that the image of ϕ is RM. By Theorem 6.6, $M \cong RM$. Notice that F is generated by a linearly independent set, so F is free. Since RM is contained in F, RM must also be free by Theorem 8.1. Therefore, M is free. ∎

Not every finitely generated module is free, but it would be useful to decompose each finitely generated module into the direct sum of some free module and some other module. By the previous result, we know that this other module has to be a torsion module. Indeed, there is a way to decompose every finitely generated module into a direct sum of its torsion module and some other module:

Lemma 8.5. *Let M be a finitely generated module. Then M/M_{tors} is free, and there exists a free submodule N of M such that $M = M_{tors} \oplus N$.*

Proof. Consider the surjective homomorphism $\phi : M \to M/M_{tors}$. The kernel of ϕ is clearly M_{tors}. By Lemma 8.3, M is isomorphic to $M_{tors} \oplus M/M_{tors}$. Now, we prove that M/M_{tors} is torsion-free.

Let $x \in M$ and $\bar{x}$ be its residue class mod M_{tors}. Let b be a nonzero element in R such that $b\bar{x}$ is 0. Then $\overline{bx} = 0$, so bx is in M_{tors}. Therefore, there exists a nonzero $c \in R$ such that $cbx = 0$. Therefore, $x \in M_{tors}$, so $\bar{x} = 0$. Therefore, M/M_{tors} is torsion-free. By Theorem 8.4, M/M_{tors} is also free. By Theorem 8.3, since M/M_{tors} is the image of ϕ, it is isomorphic to some submodule of M. Let N be this submodule. N must be free, giving us the desired decomposition $M = M_{tors} \oplus N$. ∎

So how does taking a direct sum affect the rank of the resulting module? The following three results give us a way to characterize how ranks and direct sums are related.

Lemma 8.6. *Let A and B be free modules over a principal ideal domain R with ranks m and n respectively. Then $A \oplus B$ is free, and it has rank $m + n$.*

Proof Sketch. Let $a_1, \dots, a_m$ be a basis for A and $b_1, \dots, b_n$ be a basis for B. Showing that $(a_1, 0), \dots, (a_m, 0), (0, b_1), \dots, (0, b_n)$ forms a basis for $A \oplus B$ is not too difficult. ∎

Lemma 8.7. *Let M be a module over a principal ideal domain R and N a free module with rank n such that M/N is torsion. Then M has rank n.*

Lemma 8.8. *Let R be a principal ideal domain, and let A and B be modules over R with ranks m and n respectively. Then $A \oplus B$ has rank $m + n$.*

All the above theorems help us prove the following result, which is key in proving the structure theorem:

Lemma 8.9. *Let R be a principal ideal domain, let M be a free R-module with finite rank n, and let N be a submodule of M. Then there exists a basis $y_1, \ldots, y_n$ of M such that there is a basis $a_1y_1, \ldots, a_my_m$ of N, where $a_1 \mid a_2 \mid \cdots a_m$.*

Recall that a module C is cyclic if there is some $x \in C$ such that $C = Rx$. We can then define a homomorphism $\phi : R \to C$ by $\phi(r) = rx$. Since $C = Rx$, ϕ is surjective. The kernel of ϕ is merely all the elements $a \in R$ such that $ax = 0$. The set of these elements is given a special name:

Definition 8.10. Let M be a module over a ring R. The *annihilator* of an element $x \in M$ is the set consisting of all elements a such that $ax = 0$ denoted by $\operatorname{ann} x$. The *annihilator* of a module M is the set consisting of all elements a such that $am = 0$ for every $m \in M$, denoted by $\operatorname{ann} M$.

Notice that the annihilator of a cyclic module C is equivalent to the kernel of the homomorphism we defined that maps r to rx. Therefore, by Theorem 6.6, $R/\operatorname{ann} C \cong C$.

In fact, annihilators are always ideals. Therefore, in a principal ideal domain R, we can write $\operatorname{ann} C = (a)$ for some $(a) \in R$. Thus, $R/(a) \cong C$. The structure theorem holds that we can write any finitely generated module over a principal ideal domain as a finite direct sum of cyclic modules, which are bound by certain relations.

9. Structure theorem

Theorem 9.1 (Structure theorem, invariant factors form, existence)**.** *Let M be a finitely generated module over a principal ideal domain R.*

(1) *M is isomorphic to the following direct sum:*

$$M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

for some nonnegative integer r and nonzero, nonunit elements $a_1, a_2, \ldots a_m \in R$ such that $a_1 \mid a_2 \mid \cdots \mid a_m$.

(2) *In the above decomposition, $M_{tors} \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$.*

Proof. Let $x_1, \ldots, x_n$ be a finite set of generators for M with minimal size. Let R^n be the free R-module of rank n with basis $b_1, \ldots, b_n$. Define a homomorphism $\phi : R^n \to M$ by defining $\phi(b_i) = x_i$ for each $1 \leq i \leq n$. Since the x_i generate M, ϕ is surjective. By Theorem 6.6, we have that $R^n/\ker\phi = M$. By applying 8.9 to R^n, with $\ker\phi$ as the submodule, there is another basis $y_1, \ldots, y_n$ of R^n such that $a_1y_1, \ldots, a_my_m$ form a basis for $\ker\phi$ with $a_1 \mid \cdots \mid a_m$. Therefore, since $M \cong R^n/\ker\phi$:

$$M \cong (Ry_1 \oplus \cdots \oplus Ry_n)/(Ra_1y_1 \oplus \cdots \oplus Ra_1y_m)$$

.

Define a R-module homomorphism $\phi : (Ry_1 \oplus \cdots \oplus Ry_n) \to (R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m})$ by $(b_1y_1, \ldots, b_ny_n) \mapsto (b_1 \pmod{(a_1)}, b_2 \pmod{(a_2)}, \ldots, b_m \pmod{(a_m)}, b_{m+1}, \ldots, b_n)$.

The kernel of ϕ is clearly the elements such that a_i divides b_i for all $1 \leq i \leq m$. This is just $Ra_1y_1 \oplus \cdots \oplus Ra_my_m$. By Theorem 6.6, therefore, M is isomorphic to the image of ϕ. Since ϕ is clearly surjective, $M \cong (R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m})$. This gives our desired decomposition in part (1).

Now, we will prove part (2). Since $a_1 \mid \cdots \mid a_m$, (a_m) annihilates the module $R/(a_1) \oplus \cdots \oplus R/(a_m)$. Therefore, $R/(a_1) \oplus \cdots \oplus R/(a_m)$ is a torsion submodule of M. Since M is isomorphic to the direct sum of R^r and this torsion module, by Theorem 8.7, the rank of M is r. Therefore, the dimension of the free module in the decomposition given in Theorem 8.5 is uniquely determined. Thus, in the decomposition $M \cong M_{tors} \oplus F$, where F is a free module, F must have rank r. Thus, $F \cong R^r$, so $M = M_{tors} \oplus R^r$. Thus, $M_{tors} \cong R/(a_1) \oplus \cdots \oplus R/(a_m)$. ∎

Definition 9.2. In Theorem 9.1, the integer r is called the *free rank* of M, and the factors $a_1, \ldots, a_n$ are called the *invariant factors* of M.

Theorem 9.3 (Structure theorem, elementary divisors form, existence)**.** *Let M be a finitely generated module over a principal ideal domain R. Then M is isomorphic to the following direct sum:*

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_t^{\alpha_t})$$

where r is a nonnegative integer and $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_t^{\alpha_t}$ are powers of primes in R.

Remark 9.4. The primes $p_1, p_2, \ldots, p_t$ need not be distinct.

Proof. Since R is a principal ideal domain, it is also a unique factorization domain. Therefore, for every invariant factor $a_1, \ldots, a_m$, we can write $a_i = uq_1^{\beta_1} \ldots q_k^{\beta_k}$ for a unit u, primes $q_1, \ldots, q_k$, and positive integers $\beta_1, \ldots, \beta_k$. Notice that the ideal $(a_i) = (q_1^{\beta_1}) \cap \cdots \cap (q_k^{\beta_k})$. Therefore, by Theorem 3.12, each $R/(a_i)$ is isomorphic to $R/(q_1^{\beta_1}) \oplus \cdots \oplus R/(q_k^{\beta_k})$ as rings and therefore also as R-modules. Decomposing this way for every a_i gives our desired decomposition. ∎

To prove uniqueness, we need to introduce some lemmas:

Theorem 9.5. *Let R be a principal ideal domain and $p \in R$ be a prime. Then $R/(p)$ is a field.*

Proof. We will actually show a more general result: that if I is a maximal ideal, then R/I is a field. Our result will follow by Theorem 4.2, which states that (p) is maximal.

To show that R/I is a field if I is maximal, we need to show that there are multiplicative inverses for every nonzero element of R/I. Let $a + I$ be a nonzero element in R/I. Consider the set $A = \{ar + s \mid r \in r, s \in I\}$. We claim that A is an ideal (showing this is left to the reader). Since $a \in A$, but $a \notin I$, A properly contains I. Since I is maximal, A must be the whole ring R. Therefore, $1 \in A$, so $1 = ar + s$ for some $r \in R$ and some $s \in I$. Thus, $ar - 1 = -s$ is also in I. Therefore, $(ar - 1) + I = 0$, so $ar + I = 1 + I$. From this, we have $(a + I)(r + I) = 1 + I$, so $a + I$ and $r + I$ are multiplicative inverses. Multiplicative inverses therefore exist for every nonzero element of R/I, so R/I is a field. Since (p) is maximal, $R/(p)$ is a field. ∎

Lemma 9.6. *Let R be a principal ideal domain and $p \in R$ be a prime. Let F be the field $R/(p)$, and let $M = R^r$. Then $M/pM \cong F^r$.*

Proof. Consider the map from R^r to F^r such that $(a_1, \ldots, a_r) \mapsto (a_1 \pmod{(p)}, \ldots, a_r \pmod{(p)})$. Clearly, this is surjective. The kernel is all the elements in R^r where each entry in the r-tuple is divisible by p. This just pR^r. By Theorem 6.6, $R^r/pR^r = F^r$. ∎

Lemma 9.7. *Let R be a principal ideal domain and $p \in R$ be a prime. Let F be the field $R/(p)$. Let $M = R/(a_1) \oplus \cdots \oplus R/(a_k)$, where each a_i is divisible by p. Then $M/pM \cong F^k$.*

Proof. Here, we will assume the Third Isomorphism Theorem of rings, which states that if R is a ring, and I and J are ideals of R with $I \subseteq J$, then J/I is an ideal, and $(R/I)/(J/I) \cong R/J$.

Let $N = R/(a)$, where a is some element of $a_1, \dots, a_k$. Then elements in pN are of the form $p(k + (a)) = pk + (a)$ for some $k \in R$. These elements can be characterized by the ideal $(p) + (a)$. Therefore, $pN \cong ((p) + (a))/(a)$. Since p divides a, $(a) \subseteq (p)$. Therefore, $(p) + (a)$ is just (p), so $pN \cong (p)/(a)$. Therefore, $N/pN \cong (R/(a))/((p)/(a))$. By the Third Isomorphism Theorem, this is isomorphic to $R/(p) = F$. This applies for each copy of $R/(a)$, so $M \cong F^k$. ■

Theorem 9.8 (Structure theorem, elementary divisors, uniqueness)**.** *Let M_1 and M_2 be finitely generated modules over a principal ideal domain R. If they are isomorphic, then they share the same free rank and the same list of elementary divisors (up to ordering).*

Proof. Since M_1 and M_2 are isomorphic, their torsion modules are isomorphic to each other, too. Let M_1 and M_2 have free ranks r_1 and r_2, respectively. Then $R^{r_1} \cong M_1/\operatorname{Tor} M_1 \cong M_2/\operatorname{Tor} M_2 \cong R^{r_2}$. Thus, for any nonzero prime in $p \in R$, $R^{r_1}/pR^{r_1} \cong R^{r_2}/pR^{r_2}$. By Theorem 9.6, $R^{r_1}/pR^{r_1} \cong F^{r_1}$, and $R^{r_2}/pR^{r_2} \cong F^{r_2}$. Therefore, $F^{r_1} \cong F^{r_2}$. Since any two isomorphic vector spaces have the same dimension, $r_1 = r_2$. Since the free ranks of M_1 and M_2 are equal, we only need to show that their torsion modules, which are isomorphic, share the same elementary divisors. Therefore, we can assume that M_1 and M_2 are both torsion modules.

We can work for a fixed prime p, since if M_1 and M_2 have the same elementary divisors that are a power of p for every p, they share the same elementary divisors. Let the p-primary submodule of a module M be the direct sum of all the cyclic module factors of M whose elementary divisors are a power of p. Since M_1 and M_2 are isomorphic, their p-primary submodules are isomorphic, since they are the submodules that are annihilated by the same power of p, and annihilators are invariant under isomorphism. Therefore, it suffices to show that two isomorphic p-primary submodules share the same elementary divisors.

We use induction on the power of p in the annihilator of the two p-primary submodules (which are isomorphic). Let P_1 be the p-primary submodule of M_1, and let P_2 be the p-primary submodule of M_2. If the power of p in the annihilator of P_1 and P_2 is 0, then P_1 and P_2 are both 0 and we are done. Otherwise, let the elementary divisors of P_1 be $p, \dots, p, p^{a_1}, p^{a_2}, \dots, p^{a_s}$, where there are m copies of p, and $2 \le a_1 \le a_2 \le \cdots \le a_2$. Let the elementary divisors of P_2 be $p, \dots, p, p^{b_1}, p^{b_2}, \dots, p^{b_t}$. Similarly, let there be n copies of p, and let $2 \le b_1 \le b_2 \le \cdots \le b_t$.

Consider the module pP_1. Since every element in the module $pR/(p^x)$ can be expressed in the form $p(k + (p^x)) = pk + (p^x) = (p^{x-1})$, each submodule with elementary divisor p^x in P_1 becomes a submodule with elementary divisor p^{x-1}. Therefore, the elementary divisors of pP_1 are $p^{a_1-1}, p^{a_2-1}, \dots, p^{a_s-1}$. Similarly, the elementary divisors of pP_2 are $p^{b_1-1}, p^{b_2-1}, \dots, p^{b_t-1}$. Since $P_! \cong P_2$ (by $M_1 \cong M_2$), we have that $pP_1 \cong pP_2$. Since the power of p in the annihilator of pP_1 is one less than the power of p in the annihilator of P_1, by induction, we have that the elementary divisors of pP_1 and pP_2 are the same. Therefore, $s = t$, and each $a_i = b_i$.

Notice that P_1/pP_1 and P_2/pP_2 are also isomorphic. Therefore, by Theorem 9.7, $P_1/pP_1 \cong (R/(p))^{m+s}$ and $P_2/pP_2 \cong (R/(p))^{n+t}$ are also isomorphic. Since isomorphic vector spaces share the same dimension, $m+s = n+t$. We already know that $s = t$, so $m = n$. Therefore, the elementary divisors of P_1 and P_2 are equal for any prime p, so the elementary divisors of M_1 and M_2 are equal too.

Therefore, since any two isomorphic modules share the same free rank and elementary divisors, any modules with different free rank or a different list of elementary divisors are not isomorphic. As a result, elementary divisors and free rank admit a unique decomposition of every finitely generated module over a principal ideal domain. ■

Theorem 9.9 (Structure theorem, invariant factors, uniqueness). *Let M_1 and M_2 be finitely generated modules over a principal ideal domain R. If they are isomorphic, then they share the same free rank and the same list of invariant factors (up to ordering).*

Proof. Once again, as we showed in the proof that elementary divisors formed a unique decomposition, we can assume that M_1 and M_2 are isomorphic torsion modules.

Let $a_1 \mid \cdots \mid a_m$ be the invariant factors of M_1, and let $b_1 \mid \cdots \mid b_n$ be the invariant factors of M_2. Since R is a unique factorization domain, the prime power factors of M_1 uniquely give a list of elementary divisors for M_1. Notice that we can uniquely reconstruct invariant factors from a list of elementary divisors: a_m is the product of the largest prime powers for each prime, a_{m-1} is the product of the next-largest prime powers for each prime, and so on. We can do the same for M_2 and $b_1, \ldots, b_n$. Since M_1 and M_2 share the same elementary divisors, they share the same invariant factors. Therefore, invariant factors also admit a unique decomposition. ■

10. Consequences of the structure theorem

Theorem 10.1 (Classification of finitely generated abelian groups). *Every finitely generated abelian group can be expressed as the direct sum of the cyclic groups*

$$A = \mathbb{Z}^n \oplus \mathbb{Z}_{p_1^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{r_k}}$$

where $p_1, \ldots, p_k$ are primes and $r_1, \ldots, r_k$ are positive integers. The group can also be expressed as

$$A = \mathbb{Z}^n \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m}$$

for positive integers $d_1, \ldots, d_m$ such that $d_1 \mid \cdots \mid d_m$.

These decompositions are unique up to ordering.

Proof. Since every abelian group is a $\mathbb{Z}$-module, this result follows from the structure theorem. ■

Corollary 10.2. *Let V be a finitely generated vector space over a field F. As an F-module, $V \cong F^t$ for some nonnegative integer t.*

Proof. Vector spaces are clearly PIDs. For any ideal (x) in F, the ideal must include the entire field, since any $y \in F$ can just be written as $(yx^{-1})x$. Therefore, $F/(x)$ for any $x \in F$ must be 0. Thus, by the structure theorem, $V \cong F^t$ for a nonnegative integer t. ■

The existence of the Jordan canonical form for matrices, a special representation of a linear transformation as an upper triangular matrix with many other interesting properties, also follows from the structure theorem. We will not go into detail here, but a proof of this can be found in Chapter 12 of [1].

References

[1] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2003.

Appendix A. Full proofs of preliminary results

Proposition. *Let M be a finitely generated, free module over a principal ideal domain R, and let N be a submodule of M. Then N is free, and its rank is less than or equal to the rank of M.*

Proof. We use strong induction on the rank of M, which we will denote by n. This is trivial if $n = 0$, since then both M and N must simply be 0. Assume now that $n > 0$ and that the result holds true for all submodules of free modules with rank $n - 1$. Let M have a finite basis $(e_1, \ldots, e_n)$. Let M' be the submodule generated by $(e_2, \ldots, e_n)$. If N is a submodule of M', then the inductive assumption shows that N is free with rank less than or equal to $n - 1$. Therefore, we may assume that N is not a submodule of M'.

Consider the set I of elements a for which there is an element in N of the form $f_1 = ae_1 + y$, where $y \in M'$. In fact, I is an ideal. To see why, let a, b be elements in I. Then there exist $f_1 = ae_1 + y$ and $f_1' = be_1 + y'$. Adding these together gives $f_1 + f_1' = (a + b)e_1 + (y + y')$. Since $(y + y') \in M'$, and $(f_1 + f_2) \in N$, $a + b$ is in I. A similar argument can be used to show that I is closed under multiplication by R. Therefore, I is an ideal.

Since R is a principal ideal domain, I is generated by some element d. Let $f_1 = de_1 + y_1$, where $f_1 \in N$ and $y_1 \in M'$. Consider $L = N \cap M'$. This is a submodule of M', which is free of rank $n - 1$. Therefore, by induction, it has a basis $(f_2, \ldots, f_m)$ of size $m - 1 \leq n - 1$. We will show that $(f_1, f_2, \ldots, f_m)$ forms a basis for N. This has size m, and since $m - 1 \leq n - 1$, we have that $m \leq n$. This will prove our theorem.

Let x be an arbitrary element in N. Since $x \in M$, too, it can be expressed as $be_1 + y$, where $y \in M'$. This implies that $y \in M'$, so in this expression of x, b must be in the ideal I. Since I is generated by d, let $b = k_1 d$, where $k_1 \in R$. Therefore, $x - k_1 f_1 = k_1 de_1 + y - k_1(de_1 + y_1) = y - k_1 y_1$. Since x and f_1 are in N, this term is also in N. Since y and y_1 are in M', this term is also in M'. Therefore, $x - k_1 f_1 \in N \cap M' = L$. Since L is generated by $(f_2, \ldots, f_m)$, we can write $x - k_1 f_1$ as $k_2 f_2 + \cdots + k_m f_m$. Therefore, $x = k_1 f_1 + k_2 f_2 + \cdots + k_m f_m$, so N is generated by $(f_1, \ldots, f_m)$.

Now, we will show that $(f_1, \ldots, f_m)$ are linearly independent. Suppose that $k_1 f_1 + \cdots k_m f_m = 0$. Then $k_1 de_1 + k_1 y_1 + k_2 f_2 + \cdots + k_m f_m = 0$. Since y_1 and each of $f_2, \ldots, f_m$ are all in M', we can rewrite this relation as $k_1 de_1 + l_2 e_2 + \cdots + l_n e_n = 0$, where $e_2, \ldots, e_n$ form a basis for M'. Since $e_1, \ldots, e_n$ are a basis for M, $k_1 d = 0$. Since $d \neq 0$, $k_1 = 0$. Therefore, $k_2 f_2 + \cdots + k_m f_m = 0$. Since $(f_2, \ldots, f_m)$ are a basis for L, all the coefficients $k_2, \ldots, k_m$ are 0. Therefore, $(f_1, \ldots, f_m)$ are linearly independent, so they form a basis for N. ∎

Lemma. *Let M be a module over a principal ideal domain R and N a free module with rank n such that M/N is torsion. Then M has rank n.*

Proof. Let S be a basis of N (of size n). Clearly, S must also be linearly independent in M, so the rank of M is at least n. Let $T = \{t_1, \ldots, t_{n+1}\}$ be a set of $n + 1$ elements in M. Since M/N is torsion, for every t_i, there must be a nonzero $r_i \in R$ such that $r_i t_i$ is the zero element in M/N. This implies that $r_i t_i \in N$.

If any two r_i, r_j are equal, then T is linearly dependent (since then, $r_i t_i = r_j t_j$). Assume that no two r_i, r_j are equal. Then the set $\{r_i t_i\}$, which is contained within N, contains $n + 1$ elements. Since the rank of N is n, there exist coefficients s_i that are not all zero such that $\sum s_i r_i t_i = 0$. Therefore, T is linearly dependent in M, so the rank of M is at most n. As a result, M has rank n. ∎

Lemma. *Let R be a principal ideal domain, and let A and B be modules over R with ranks m and n respectively. Then $A \oplus B$ has rank $m+n$.*

Proof. By Theorem 8.5, there are free submodules A_1 and B_1 of A and B, respectively, such that $A = A_1 \oplus A_{tors}$ and $B = B_1 \oplus B_{tors}$. By Lemma 8.6, $A_1 \oplus B_1$ is free. Now, we will prove that $(A \oplus B)/(A_1 \oplus B_1) \cong (A/A_1) \oplus (B/B_1)$. Let $\phi_1 : A \to A/A_1$ and $\phi_2 : B \to B/B_1$ denote the canonical projections. Both ϕ_1 and ϕ_2 are surjective, so $\phi_1 \oplus \phi_2$ is also surjective. The kernels of ϕ_1 and ϕ_2 are A_1 and B_1 respectively, so the kernel of $\phi_1 \oplus \phi_2$ is $A_1 \oplus B_1$. Therefore, by Theorem 6.6, $(A \oplus B)/(A_1 \oplus B_1) \cong (A/A_1) \oplus (B/B_1)$.

Since A and B have ranks m and n respectively, and A/A_1 and B/B_1 are both torsion, A_1 and B_1 have ranks m and n by Lemma 8.7. Since $(A \oplus B)/(A_1 \oplus B_1) \cong (A/A_1) \oplus (B/B_1)$, we have that $A \oplus B = (A_1 \oplus B_1) \oplus ((A/A_1) \oplus (B/B_1))$. Since both A/A_1 and B/B_1 are torsion modules, their direct sum is also torsion. Once again, invoking Lemma 8.7, the rank of $A_1 \oplus B_1$ is equal to the rank of $A \oplus B$. By Lemma 8.6, the rank of $A_1 \oplus B_1$ is $m+n$. Therefore, the rank of $A \oplus B$ is $m+n$. ∎

Lemma. *Let R be a principal ideal domain, let M be a free R-module with finite rank n, and let N be a submodule of M. Then there exists a basis $y_1, \dots, y_n$ of M such that there is a basis $a_1y_1, \dots, a_my_m$ of N, where $a_1 \mid a_2 \mid \cdots a_m$.*

Proof. If $N = 0$, then the theorem is trivial.

Assume $N \neq 0$. For each R-module homomorphism from M to R, the image $\phi(N)$ of N is a submodule of R. Since submodules are closed under addition and multiplication by any element in R, every submodule of R, including $\phi(N)$ is an ideal. Since R is a principal ideal domain, write $\phi(N) = (a_\phi)$ for some $a_\phi \in R$. Let Σ be the collection of all these ideals (a_ϕ). Clearly, Σ is nonempty, since taking ϕ to be the trivial homomorphism implies that (0) is in Σ. Thus, Σ has a maximal element, or an element such that (a_ϕ) is not contained in any other element of Σ. Let this maximal element be (a_1). Let $(a_1) = \phi(N)$, and let $y \in N$ be the element such that $\phi(y) = a_1$.

Let $x_1, \dots, x_n$ be a basis of M, and define π_i to be the natural projection homomorphism such that $\pi_i : a_1x_1 + \cdots + a_nx_n \mapsto a_i$. Since N is nonzero, there must be some π_i such that $\pi_i(N) \neq (0)$, so Σ cannot contain only (0). Since (0) is included in every other ideal, (0) cannot be the maximal element of Σ. Because (a_1) is maximal, $a_1 \neq 0$.

We will now show that a_1 divides $f(y)$ for every homomorphism f from M to R. Let g be a generator for the principal ideal generated by a_1 and $f(y)$. Since g must itself be in this ideal, g can be written as $r_1a_1 + r_2f(y)$ for some $r_1, r_2 \in R$. Now, consider the homomorphism $\psi : M \to R$ given by $\psi : x \mapsto r_1\phi(x) + r_2f(x)$. We have that $\psi(y) = r_1a_1 + r_2f(y) = g$, so $g \in \psi(N)$. Since a_1 is in the ideal generated by g, we have that g divides a_1. Therefore, $(a_1) \subseteq (g)$. Since $g \in \psi(N)$, and $\psi(N)$ is itself an ideal, we must have $(g) \subseteq \psi(N)$. Therefore, we have a chain of inclusions $(a_1) \subseteq (g) \subseteq \psi(N)$. Since (a_1) is maximal, these inclusions must be equalities, so $(a_1) = (g) = \psi(N)$. Since $f(y)$ is also in (g), g must divide $f(y)$. Therefore, a_1 must divide $f(y)$.

Now, we apply this result to the projection homomorphisms π_i we defined earlier. Since a_1 must divide $\pi_i(y)$, we can write $\pi_i(y) = a_1b_i$ for some $b_i \in R$ for all $1 \leq i \leq n$. Define $y_1 = \sum_{i=1}^n b_ix_i$. Notice that $a_1y_1 = \sum_{i=1}^n a_1b_ix_i = \sum_{i=1}^n \pi_i(y)x_i = y$. Therefore, $a_1 = \phi(y) = \phi(a_1y_1) = a_1\phi(y_1)$. Therefore, $\phi(y_1) = 1$.

We claim the following:

(1) $M = Ry_1 \oplus \ker\phi$

(2) $N = Ra_1y_1 \oplus (N \cap \ker\phi)$.

To prove (1), let $x \in M$. Write $x = \phi(x)y_1 + (x - \phi(x)y_1)$. Let us evaluate $\phi(x - \phi(x)y_1)$:

$$\begin{aligned}\phi(x - \phi(x)y_1) &= \phi(x) - \phi(\phi(x)y_1)\\ &= \phi(x) - \phi(x)\phi(y_1)\\ &= \phi(x) - \phi(x)\\ &= 0.\end{aligned}$$

Therefore, $(x - \phi(x)y_1)$ is in $\ker\phi$. Clearly, $\phi(x)y_1 \in Ry_1$, so $M = Ry_1 + \ker\phi$. To show that this sum is direct, it suffices to show that $Ry_1 \cap \ker\phi = 0$. Let $b \in Ry_1$, and write $b = ay_1$. Then $\phi(ay_1) = a\phi(y_1) = a$, so if $b \in \ker\phi$, $a = 0$, so b must also be 0. Therefore, $M = Ry_1 \oplus \ker\phi$.

To prove (2), let $x' \in N$. Notice that a_1 divides $\phi(x')$, since a_1 is a generator of $\phi(N)$. Let $\phi(x') = ba_1$ for some $b \in R$. Write $x' = \phi(x')y_1 + (x' - \phi(x')y_1)$. Substituting ba_1 for $\phi(x')$ gives us that $x' = ba_1y_1 + (x' - ba_1y_1)$. As we showed before, the second term is in the kernel of ϕ. Since $a_1y_1 = y$, and $y \in N$, the second term is also in N. Therefore, $N = Ra_1y_1 + (N \cap \ker\phi)$. Since $Ra_1y_1 \subseteq Ry_1$, and $(N \cap \ker\phi) \subseteq \ker\phi$, the intersection of $Ra_1y_1 and (N \cap \ker\phi)$ is also 0 by the method we used in our proof of part (1). Therefore, $N = Ra_1y_1 \oplus (N \cap \ker\phi)$.

Now, we can prove our theorem. We use induction on the rank of M, which is n. Since $\ker\phi$ is a submodule of M, it must be free. Notice that Ry_1 is generated by y_1, so it has rank 1. Therefore, since $M = Ry_1 \oplus \ker\phi$, by 8.8, the rank of $\ker\phi$ is $n-1$. By induction, there is a basis $y_2, \ldots, y_n$ of $\ker\phi$ such that $a_2y_2, \ldots, a_my_m$ is a basis of $N \cap \ker\phi$ (which is a submodule of $\ker\phi$) for $a_2, \ldots, a_m \in R$ such that $a_2 \mid \cdots \mid a_m$. Because $M = Ry_1 \oplus \ker\phi$, $y_1, y_2, \ldots, y_n$ form a basis for M. Since $N = Ra_1y_1 \oplus (N \cap \ker\phi)$, $a_1y_1, a_2y_2, \ldots, a_my_m$ form a basis for N. Now, we merely need to show that $a_1 \mid a_2$. Define a homomorphism $f : M \to R$ such that $f(y_1) = f(y_2) = 1$ and $f(y_i) = 0$ for $2 < i \leq n$. Then, $a_1 = a_1f(y_1) = f(a_1y_1)$, so $a_1 \in f(N)$. Therefore, (a_1) is also in $f(N)$. Since (a_1) is maximal in Σ, $(a_1) = f(N)$. Since $a_2 = a_2f(y_2) = f(a_2y_2)$, a_2 is also in $f(N)$. Therefore, a_1 divides a_2, completing our induction. ■