Basic module theory

October 14, 2010

1 Basic definitions

Let R be a ring, which will often be assumed to have an identity 1.

Definition 1.1. A *left R-module* is an abelian group M and an "external law of composition" $\mu : R \times M \to M$, subject to the conditions that for all $r, s \in R$ and $m, n \in M$ we have

(a) $\mu(r, m+n) = \mu(r, m) + \mu(r, n)$

(b) $\mu(r+s, m) = \mu(r, m) + \mu(s, m)$

(c) $\mu(rs, m) = \mu(r, \mu(s, m))$

(d) if $1 \in R$, then $\mu(1, m) = m$.

We shall usually omit the notation of μ and simply write $r \cdot m$ for $\mu(r, m)$. Thus axiom (c) would be written $(rs) \cdot m = r \cdot (s \cdot m)$, etc.

Exercise 1. We denote by $\mathrm{End}_{\mathrm{Grp}}(M)$ the set of group endomorphisms of M: An element $\varphi \in \mathrm{End}_{\mathrm{Grp}}(M)$ is a group homomorphism $\varphi : M \to M$. $\mathrm{End}_{\mathrm{Grp}}(M)$ is naturally a ring, with addition and multiplication defined by

$$(\varphi + \psi)(m) := \varphi(m) + \psi(m) \qquad \text{and} \qquad (\varphi\psi)(m) := \varphi \circ \psi(m).$$

$\mathrm{End}_{\mathrm{Grp}}(M)$ has an identity element $1 = \mathrm{id}_M$.

Show that the data of a left R-module structure on M is equivalent to giving a (unital, if $1 \in R$) ring-map $R \to \mathrm{End}_{\mathrm{Grp}}(M)$.

Remark 1.2. As the name "*left* R-module" suggests, there is also the notion of a *right* R-module: A right R-module is an abelian group M together with an external law of composition $\mu : M \times R \to M$, satisfying the same axioms of Definition 1.1 but with the places of the ring and the abelian group switched.

Exercise 2. Can a right R-module structure on M be thought of as a map $R \to \mathrm{End}_{\mathrm{Grp}}(M)$? What conditions must be placed on R or the map $R \to \mathrm{End}_{\mathrm{Grp}}(M)$ for this to be true? In general, formulate a definition of right R-modules in the spirit of Exercise 1.

Remark 1.3. Unless we explicitly state otherwise, all of our R-modules will be left R-modules, so we will not explicitly state the handedness if there is no chance of confusion.

Example 1.4. If R is a field, an R-module is the same thing as a vector space over R. In this case, basic linear algebra tells us many things about the structure of R-modules, so that we actually have quite a good understanding of them. For instance, the notion of "dimension" sets up a bijection between the natural numbers and an important class of R-vector spaces (the finite dimensional ones). That the module theory of a field is so simple is related to the fact that fields are the simplest examples of rings, at least in an ideal-theoretic sense. In fact, the study of modules over R is often a very good way of understanding the structure of the ring R itself.

Example 1.5. R is naturally a left (resp., right) R-module, with action given by left (resp., right) multiplication: If $r \in R$ is thought of as a ring element, while $s \in R$ is thought of as being an element of the underlying abelian group of R, we have $r \cdot s = rs$. This is the *regular (left) R-module*, and is often denoted ${}_RR$ (or R_R for the regular right R-module) to distinguish it from ring version of R. Studying this module version of R is another good way to start to understand R as a ring.

Exercise 3. What does it mean to be a $\mathbb{Z}$-module?

Definition 1.6. If M and N are R-modules, a map $f : M \to N$ is a *morphism of R-modules* if f is a homomorphism of the underlying abelian groups and if for all $r \in R$ and $m \in M$ we have $f(r \cdot m) = r \cdot f(m)$.

Exercise 4. Express the notion of morphism of R-modules in the language of Exercise 1.

Remark 1.7. Suppose that M is an S-module, and $\alpha : R \to S$ is a map of rings. Then M is also naturally an R-module, via the action $r \cdot m := \alpha(r) \cdot m$. This is often called the *restriction of M along α*. In particular, any ring map $R \to S$ makes the regular S-module ${}_SS$ into an R-module.

Definition 1.8. If $f : M \to N$ is an R-module morphism such that there is another R-module morphism $g : N \to M$ with $gf = \mathrm{id}_M$ and $fg = \mathrm{id}_N$, we say that f is an *isomorphism of R-modules* and g is the *inverse of f*.

Exercise 5. Show that if $f : M \to N$ is a morphism of R-modules that is a bijection on the underlying sets, then f is an isomorphism of R-modules. (Note: If this seems like something that should obviously be true, construct a continuous map of topological spaces that is a set-bijection but not a homeomorphism.)

Definition 1.9. It is clear that the composition of R-module maps is again an R-module map (and if it's not, prove it). Thus the collection of R-modules together with R-modules morphisms form a category, denoted R-mod.

Definition 1.10. A subset N of the R-module M is a *submodule* if it is a subgroup that is closed under the R-action: For all $r \in R$ and $n \in N$, we have $r \cdot n \in N$.

Definition 1.11. Let $N \subseteq M$ be an inclusion of R-modules. The *quotient of M by N* is an R-module, which we denote M/N. As an abelian group, M/N is the quotient of M by N, so the elements of M/N are equivalence classes $m + N$, where $m + N = m' + N$ iff $m - m' \in N$. Moreover, M/N naturally inherits the structure of an R-module from the R-module structure on M: For all $r \in R$ and $m \in M$, we set $r \cdot (m + N) = r \cdot m + N$.

Exercise 6. If G is a group and $H \leq G$ a subgroup, it is not always true that the set of equivalence classes (called "left H-cosets") G/H inherits a group structure from G. In order for this to be the case we must have that H is normal in G. Show that in the case of modules, "normality" is a condition that is always satisfied. In other words for any submodule $N \subseteq M$, show that the R-module structure on M/N of Definition 1.11 is well-defined.

Exercise 7. For M an R-module, set $\mathrm{Ann}(M) = \{r \in R | aM = 0\}$. Show that $\mathrm{Ann}(M)$ is an ideal of R, and that M is naturally an $(R/\mathrm{Ann}(M))$-module. $\mathrm{Ann}(M)$ is called the *annihilator of M*.

Exercise 8. What are the submodules of the regular module ${}_RR$? What are the submodules of a $\mathbb{Z}$-module?

Definition 1.12. Let $f : M \to N$ be a morphism of R-modules. The *kernel of f*, denoted $\ker(f)$, is the set of $m \in M$ such that $f(m) = 0$. The *image of f*, denoted $\mathrm{im}(f)$, is the set of $n \in N$ such that there is some $m \in M$ with $f(m) = n$. Finally, the *cokernel of f* is the quotient R-module $\mathrm{coker}(f) := N/\mathrm{im}(f)$.

Exercise 9. Show that for any morphism of R-modules $f : M \to N$, we have $\ker(f) \subseteq M$ and $\mathrm{im}(f) \subseteq N$ are inclusions of R-submodules.

Lemma 1.13. *For every morphism of R-modules $f : M \to N$, there is a canonical isomorphism of R-modules* $\mathrm{im}(f) \cong M/\ker(f)$.

Exercise 10. Prove Lemma 1.13. Conclude that $f : M \to N$ is an isomorphism of R-modules iff $\ker(f) = 0$ and $\mathrm{coker}(f) = 0$. *Hint*: For the last statement, use Exercise 5.

Lemma 1.13 should look like a familiar isomorphism theorem from your study of groups. In fact, all of the basic isomorphism theorems of groups have module-theoretic analogues. Proving the following would be a good test of your understanding of both groups and modules:

Lemma 1.14. *Let M be an R-modules with submodules $N, N' \subseteq M$.*

1. *$(N + N')/N' \cong N/(N \cap N')$.*
2. *If $N' \leq N$ then $(M/N')/(N/N') \cong M/N$.*
3. *There is an inclusion-preserving bijection between submodules of M containing N' and submodules of M/N', given by $N \mapsto N/N'$.*

Remark 1.15. In Item 1., $N + N'$ denotes the smallest submodule of M containing both N and N', and implicit in the statement is that $N \cap N'$ is actually a submodule of M.

2 New modules from old

In this section we describe a few important constructions that allow us to create new R-modules from given ones.

2.1 External products and sums

Definition 2.1 (Products of R-modules)**.** Let I be an indexing set and $\{M_i\}_{i\in I}$ a collection of left R-modules indexed on I. The *(external) direct product of the* M_i is the R-module $\prod_{i\in I} M_i$ whose elements are collections $\{m_i\}_{i\in I}$ where $m_i \in M_i$. The group structure of $\prod_{i\in I} M_i$ is componentwise addition, and the R-module structure comes from R's acting "diagonally":

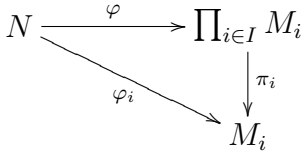
$$\{m_i\}_{i\in I} + \{m_i'\}_{i\in I} = \{m_i + m_i'\}_{i\in I} \qquad \text{and} \qquad r\cdot\{m_i\}_{i\in I} = \{r\cdot m_i\}_{i\in I}$$

If I is finite of order n (or countable), we will often write $(m_1, m_2, \ldots, m_n)$ (or $(m_1, m_2, \ldots)$) for an element of $\prod_{i=1}^{n} M_i$ (or $\prod_{i=1}^{\infty} M_i$), with the understanding that I has been given a specified ordering.

Definition 2.2 (Sums of R-modules)**.** Again let I be an indexing set and $\{M_i\}_{i\in I}$ a collection of left R-modules. The *(external) direct sum of the* M_i is the R-module $\bigoplus_{i\in I} M_i$ whose elements are colelctions $\{m_i\}_{i\in I}$ such that for all but finitely many i, $m_i = 0$. Again, the group structure of $\bigoplus_{i\in I} M_i$ is componentwise and R acts diagonally.

Remark 2.3. Of course, if $I = \{1, 2, \ldots, n\}$ is finite, the direct sum and direct product of $M_1, \ldots, M_2$ coincide. Why then do we introduce two different concepts that amount to the same thing in the case in which we will be most interested? Mainly for the sake of completeness, as the following exercise shows how these two constructions fulfill different categorical roles.

Exercise 11. Show that for each indexing $i \in I$ there is a canonical R-module surjection $\pi_i : \prod_{i\in I} M_i \to M_i$. Moreover, show that if N is any R-module, the data of a R-module map $\varphi : N \to \prod_{i\in I} M_i$ are the same as giving an R-module map $\varphi_i : N \to M_i$ for each $i \in I$. By "the same as" we mean that given such a collection of $\{\varphi_i\}_{i\in I}$, there is a unique $\varphi : N \to \prod_{i\in I} M_i$ such that

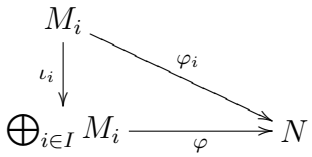


commutes for all i. In other words, for any R-module N, there is a natural bijection

$$\mathrm{Hom}_{R-\mathrm{mod}}\left(N, \prod_{i\in I} M_i\right) \cong \prod_{i\in I} \mathrm{Hom}_{R-\mathrm{mod}}(N, M_i).$$

Here, the product on the right hand side is meant to be the product in sets, which we already understand. This result is alluding to the fact that the product of R-modules is an example of a *limit* in the category R-mod.

Similarly, show that for each indexing $i \in I$ there is a canonical R-module injection $\iota_i : M_i \to \bigoplus_{i\in I} M_i$ such that for any R-module N and collection of R-maps $\varphi_i : M_i \to N$, there is a unique R-module map $\bigoplus_{i\in I} M_i \to N$ such that



is a commutative diagram of R-modules, and we consequently have natural bijections

$$\mathrm{Hom}_{R-\mathrm{mod}}\left(\bigoplus_{i\in I} M_i, N\right) \cong \prod_{i\in I} \mathrm{Hom}_{R-\mathrm{mod}}(M_i, N).$$

The sum of R-modules is an example of a *colimit* in the category R-mod.

Example 2.4 (Free R-modules). One of the most important examples of R-modules are those built out of the regular R-module ${}_RR$. If for each $i \in I$, the R-module M_i is isomorphic to ${}_RR$, the direct sum of the M_i is called a *free R-module*. We shall be primarily concerned with the direct sum of finitely many copies of ${}_RR$, in which case the direct sum and direct product coincide. The notation R^n will be understood to mean the sum of n copies of ${}_RR$, viewed as an R-module.

Notation 2.5. We will primarily be interested in taking external direct products or sums over a finite indexing set, in which case both notions coincide. We shall generally use the symbol $\oplus$ to denote this common value, but it would be a good exercise to pay attention to whether we're using properties coming from the direct sum or direct product nature of $M \oplus N$ in what follows.

2.2 Tensor products (Optional!)

The last example of creating new R-modules from old will not play much of a role later in these notes, but it is a very important concept so it seem natural to include it at this point. This is the notion of tensor product of R-modules; we begin by defining the tensor product of abelian groups (which we recall should be thought of as $\mathbb{Z}$-modules).

Definition 2.6. Let M and N be abelian groups. The *tensor product* of A and B is the abelian group $M \otimes N$ obtained by taking the free abelian group[1] on the symbols $m \otimes n$

[1] If the concept of free abelian group is unfamiliar to you, think of this as the free $\mathbb{Z}$-module and refer to the results of Section 3.2.

for all $m \in M$ and $n \in N$ and quotienting out by the relations so that for all $m, m' \in M$, $n, n' \in N$, and $z \in \mathbb{Z}$:

$$\begin{aligned}(m + m') \otimes n &= m \otimes n + m' \otimes n, \\ m \otimes (n + n') &= m \otimes n + m \otimes n', \\ (z \cdot m) \otimes n &= m \otimes (z \cdot n) \\ &= z \cdot (m \otimes n)\end{aligned}$$

Now we are prepared to define tensor product of two R-modules. Note that we are not assuming R is commutative here, and we are *not* taking the tensor product of two *left* R-modules.

Definition 2.7. Let M be a right R-module and N a left R-module. The *tensor product of M and N as R-modules* is the abelian group $M \otimes_R N$, which is obtained by quotienting the tensor product of M and N as abelian groups by the relation that for all $m \in M$, $n \in N$, and $r \in R$, we have

$$m \cdot r \otimes n = m \otimes r \cdot n.$$

Exercise 12. Show that for abelian groups M and N, we have $M \otimes N = M \otimes_{\mathbb{Z}} N$. In other words, our way of thinking of abelian groups as $\mathbb{Z}$-modules, and conversely, makes sense in the context of tensor products.

There's something a bit odd about this construction. On the one hand, we've seen that the tensor product of $\mathbb{Z}$-modules carries the structure of a $\mathbb{Z}$-module, but on the other hand, for an arbitrary ring R and R-modules M_R and ${}_R N$ (here the subscript is meant to indicate the handedness of the R-module), $M \otimes_R N$ is only an abelian group, or $\mathbb{Z}$-module. Moreover, when constructing the tensor product of $\mathbb{Z}$-modules, we did not have to specify that one be a left module and the other a right module. What's going on?

There are two things to take note of here. First, if R is commutative (e.g., $R = \mathbb{Z}$), then any left R-module M can be made into a right R-module by defining $m \cdot r = r \cdot m$, where the right-hand side is understood to mean the given left action of r on M. The converse is also true. Note, however, that if R is not commutative, this definition need not turn a left R-module into a right R-module (cf. Exercise 2).

Second, when we form the tensor product of R-modules $M \otimes_R N$, we are effectively "dividing out" the R-action on both M and N, and there is no natural way to assign an R-action on the result. If R is commutative, then we can view M as both a left and right R-module, simultaneously, in a coherent manner, which allows us to still act on the the tensor product after dividing out one of the R-actions.

Definition 2.8. If R and S are rings, an abelian group ${}_R M_S = M$ is an (R, S)-*bimodule* if M has the structure of a left R-module and a right S-module in such a way that the actions commute: For all $m \in M$, $r \in R$, and $s \in S$, we require that $(r \cdot m) \cdot s = r \cdot (m \cdot s)$.

Exercise 13. Show that if R is commutative and M is a left R-module, there is a natural way to think of M as an (R, R)-bimodule.

Exercise 14. Suppose that M is an (R, S)-bimodule and N is a left S-module. Show that there is a natural R-module structure that can be given to $M \otimes_S N$.

Exercise 15. Apparently it is important to think about both left and right R-modules. If we were octopuses, would we have eight different types of modules to worry about?

3 Generation of modules

Let M be an R-module.

Definition 3.1. A subset $X \subset M$ is said to *generate M as an R-module* if for every $m \in M$ there exist $x_1, \ldots, x_n \in X$ and $r_1, \ldots, r_n \in R$ such that $m = \sum_{i=1}^{n} r_i \cdot x_i$. Note that the sum is finite, as it must be for this definition to make sense.

More generally, for any subset $Y \subset M$, the *R-submodule of M generated by Y* is the submodule $R \cdot Y$ that consists of all finite sums of the form $\sum_{i=1}^{n} r_i \cdot y_i$ for $r_i \in R$ and $y_i \in Y$.

Exercise 16. If N_1 and N_2 are submodules of M, denote by $N_1 + N_2$ the set of all elements of the form $r_1 \cdot n_1 + r_2 \cdot n_2$ for $r_i \in R$ and $n_i \in N_i$. Show that $N_1 + N_2$ is a submodule, and that in fact it is the submodule generated by $N_1 \cup N_2$. Show that an equivalent definition would be that $N_1 + N_2$ is the smallest submodule of M that contains N_1 and N_2 (and more generally, that the submodule generated by a set $X \subset M$ is the smallest submodule containing X).

Definition 3.2. If there exists a finite subset $X \subset M$ such that M is generated by X, we say that M is *finitely generated*. If $X = \{x\}$ is a single element set such that $M = R \cdot x$, we say that M is *cyclic with generator x*.

Note that there is no assumption of uniqueness for generating sets, even in the cyclic case.

Exercise 17. Show that if M is generated by an n-element set, then every quotient of M can be generated by at most n elements.

Exercise 18. Let N be a submodule of M. Show that if N and M/N are finitely generated, then M is as well. Show that the converse is not true in general.

Definition 3.3. If M is finitely generated, there exists a generating set of minimal order. Such a generating set is called *minimal*.

Remark 3.4. Note that the notion of minimal generating set is defined purely in terms of the number of generators, not any sort of containment statement. Your intuition from dealing with vector spaces may lead you astray here: It is not in general true that any set of nonzero elements of M is contained in a minimal generating set. Find a counterexample.

3.1 Internal products and sums

We've already seen how we can take separate R-modules and piece them together with the product and sum operations to get new R-modules. We now turn this process around and examine how a given R-module M can be broken up into submodules such that M is isomorphic to the external direct sum of these submodules. We will only concern ourselves with considering finitely man submodules, so recall that the sum and product are are in fact the same for us.

Exercise 19. Let $N_1, \ldots, N_r$ be submodules of M such that M is generated by the N_i. Show that the following are equivalent:

1. The map $N_1 \oplus \ldots \oplus N_r \to M : (n_1, \ldots, n_r) \mapsto n_1 + \ldots + n_r$ is an isomorphism of R-modules. (Here $N_1 \oplus \ldots \oplus N_r$ is the external direct sum of the N_i.)

2. For each $1 \leq i \leq r$, the intersection of N_i with the submodule of M generated by all the other N_j is trivial.

3. Every element of M can be written *uniquely* as an R-linear combination of elements of the N_i.

Definition 3.5. If M and $\{N_i\}$ satisfy the condition of Exercise 19, we say that M is the *internal direct sum* of the N_i.

Remark 3.6. We could just as easily have replaced every instance of $\oplus$ with $\times$ in Exercise 19 and called the result the *internal direct product*. As the indexing set is finite, there is no difference.

Definition 3.7. A nonzero R-module M is said to be *irreducible* (or *simple*) if it contains no nonzero proper submodules. M is *indecomposable* if there do not nonzero submodules $N_1, N_2 \subset M$ such that M is the internal direct sum of N_1 with N_2.

Exercise 20. Show that every simple module is indecomposable, but that the converse is false in general.

Exercise 21. What are the irreducible $\mathbb{Z}$-modules? Formulate a guess as to what the indecomposable finitely generated $\mathbb{Z}$-modules might be.

Exercise 22 (Schur's Lemma)**.** If M is an R-module, let $\mathrm{End}_R(M)$ denote the set of R-module endomorphisms of M. There is a natural ring structure on $\mathrm{End}_R(M)$, where addition is defined pointwise and multiplication is given by composition. Show that if M is irreducible then $\mathrm{End}_R(M)$ is a division ring (so that every nonzero element is invertible, but it is not necessarily commutative). *Hint*: What can be said about the kernel and cokernel of an endomorphism of M? What does this imply?

3.2 Free modules

We have already encountered the free modules R^n; in this section we investigate their properties further.

Definition 3.8. Suppose that M is generated by the subset X. We say that M is *freely generated by* X if for each $m \in M$ there are *unique* $\{x_1, \ldots, x_n\} \subseteq X$ and $\{r_1, \ldots, r_n\} \subseteq R$ such that $m = \sum_{i=1}^{n} r_i \cdot x_i$.

Exercise 23. Suppose that M is freely generated by X and X is finite. For each $x \in X$, let $R \cdot x$ denote the R-module spanned (i.e., generated) by x. Show that M is the internal direct product of the $R \cdot x$ as x ranges over all elements of X. (In general, M is the internal direct sum of such submodules. Formulate and prove this result.)

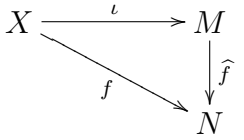
Exercise 24. If M is freely generated by a *finite* subset X of order n, show that M is isomorphic with R^n. In general if M is freely generated by X, show that M is isomorphic with a (possibly infinite) direct *sum* of copies of ${}_RR$.

Proposition 3.9. *For any set X, there is a free R-module generated by X.*

Exercise 25. Prove it. *Hint*: Consider formal finite R-linear combinations of elements of X.

Free modules have the following important *universal property*:

Proposition 3.10. *Suppose that M is freely generated by X and N is an arbitrary R-module. For every set-map $f : X \to N$, there is a unique map of R-modules $\widehat{f} : M \to N$ such that*



commutes as a map of sets.

Exercise 26. Prove it.

Remark 3.11. There is a natural "forgetful functor" from R-mod to *Set* that sends any R-module to its underlying set. Propositions 3.9 and 3.10 then tell us that there is a "free R-module" functor going in the opposite direction, that sends a set to the free R-module generated by it. The universal property then implies that the free R-module functor is left adjoint to the forgetful functor.

Exercise 27. Show that an R-module M is finitely generated if and only if there is a surjective map from a finitely generated free R-module to M.

For the remainder of this section assume that R is an integral domain, so that R is commutative and has no zero divisors.

Definition 3.12. The *rank* of a finitely generated R-module R^n is the integer n.

In general the *rank* of an R-module M is the maximal rank of a free submodule N.

Of course, even if M is finitely generated there is no reason to assume that any submodule is, so it is possible that the rank of M might be infinite even for seemingly easy examples. In order to get a better handle on the notion of rank, we must impose further structural conditions on R itself; we shall return to this point soon. But first, it is unclear that the two definitions of rank are consistent: Is it possible that R^n contains a copy of R^m for $m > n$?

Definition 3.13. A collection of elements $\{m_1, \ldots, m_n\} \subset M$ is *R-linearly dependent* if there exist elements $r_1, \ldots, r_n \in R$, not all zero, such that $\sum_{i=1}^{n} r_i \cdot m_i = 0$. If there are no such elements of R, the m_i are *R-linearly independent*.

Note that, unlike in the case of linear dependence of elements of a vector space over a field, the statement that some collection of elements $\{m_i\}$ of M are R-linearly dependent does *not* imply that some m_j can be written as an R-linear combination of the other m_i, simply because we can't divide in a general integral domain.

Proposition 3.14. *For R an integral domain, any collection of $n+1$ elements of R^n is R-linearly dependent.*

Proof. As R is a domain, it embeds in its field of fractions F. As F^n is n-dimensional over F, for any $n+1$ elements there must be some F-linear relationship amongst them. Taking this relationship and multiply through by the least common multiple of the denominators and one obtains an R-linear relationship amongst the same elements. □

Exercise 28. Show that if R is an integral domain, the two definitions of the rank of R^n coincide (and equal n). *Hint*: Another possible definition of the rank of a module M is the maximal number of R-linearly independent elements. Use Proposition 3.14.

Exercise 29. If R is commutative, show that $R^n \simeq R^m$ if and only if $n = m$. *Hint*: Let I be a maximal ideal of R and show that we can "reduce mod I" to turn R^n into a finite dimensional vector space over the field R/I. Use your knowledge of how dimension classifies vector spaces up to isomorphism.

Exercise 30. Special challenge: Find an example of a ring R and natural numbers $n \neq m$ such that $R^n \cong R^m$ as R-modules.

3.3 Torsion, annihilators, and the Chinese Remainder Theorem

In this subsection take R to be an integral domain, and let M be an R-module.

Definition 3.15. An element $m \in M$ is *torsion* if there is some nonzero $r \in R$ such that $r \cdot m = 0$. The set of all torsion elements of M is denoted $\mathrm{Tor}(M)$, and is called the *torsion submodule* of M.

More generally, a submodule N of M is a *torsion* submodule if every element of n is annihilated by some nonzero element of R, or equivalently, if $N \subseteq \mathrm{Tor}(M)$.

Finally, M is *torsion free* if $\mathrm{Tor}(M) = 0$.

Exercise 31. Show that $\mathrm{Tor}(M)$ is indeed a submodule of M. Give an example of a ring R (necessarily not a domain) and R-module M where this is not true.

Exercise 32. Show that if M is a torsion module, then every nonempty subset of elements of M is R-linearly dependent. Conclude that the rank of a torsion module is 0.

Exercise 33. Show that any finite $\mathbb{Z}$-module is torsion. Find a finite R-module M that is torsion free.

If there is torsion in M it makes sense to consider the subsets of R that annihilate the torsion elements. We've already introduced this concept in Exercise 7, but we recall the definition here for completeness.

Definition 3.16. Given a subset $X \subseteq M$, the *annihilator of* X is the set of elements $\mathrm{Ann}(X) \subseteq R$ such that $r \cdot m = 0$ for all $r \in \mathrm{Ann}(X)$ and $m \in M$.

Remark 3.17. Generalizing Exercise 7, $\mathrm{Ann}(X)$ is an ideal of R.

Recall that the module M is *cyclic* if it is generated by a single element (though perhaps not a unique single element).

Exercise 34. If M is cyclic with generator m, show that $\mathrm{Ann}(m) = \mathrm{Ann}(M)$. Moreover, show that there is an R-module map ${}_RR \to M$ sending $1 \mapsto m$ with kernel the R-submodule $\mathrm{Ann}(m)$. Thus every cyclic R-module can be thought of as a quotient of the regular R-module. Classify the cyclic R-modules

Exercise 35. Show that if R is a domain and M is a finitely generated torsion module, $\mathrm{Ann}(M) \neq 0$. Give an example that shows that both assumptions are necessary.

We will return to questions of torsion and annihilators shortly. First, we finish this section with an important structure theorem that relates the ideal-structure of R to its module theory. Recall that if M is an R-modules and I is an ideal of R, the set $I \cdot M$ denotes the submodule of M consisting of all finite sums $\sum i \cdot m$ for $i \in I$ and $m \in M$.

Theorem 3.18 (Chinese Remainder Theorem)**.** *Let R be a commutative ring with 1. For any R-module M and all ideals $I_1, \ldots, I_n \subset R$, the natural map*

$$\varphi : \quad M \to M/I_1 \cdot M \oplus \ldots \oplus M/I_n \cdot M : \quad m \mapsto (m + I_1 \cdot M, \ldots, m + I_n \cdot M)$$

is a morphism of R-modules with kernel $\bigcap_{j=1}^n I_j \cdot M$. If moreover the I_j are pairwise comaximal, so that $I_j + I_{j'} = R$ for all $j \neq j'$, then this map in fact induces an isomorphism of R-modules

$$M/(I_1 I_2 \ldots I_n \cdot M) \cong M/I_1 \cdot M \oplus \ldots M/I_n \cdot M$$

Proof. That this is a map of R-modules is obvious, and the identification of the kernel is left as an exercise. We will show that if $n = 2$ and $I_1 + I_2 = R$, we have that this map is surjective and $I_1 \cdot M \cap I_2 \cdot M = (I_1 I_2) \cdot M$; the rest of the result will follow by induction.

Since we assume that I_1 and I_2 are comaximal, we must have that there exist elements $x \in I_1$ and $y \in I_2$ such that $1 = x + y \in R$. Thus for any $m \in M$, $1 \cdot m = (x + y) \cdot m$ and therefore $\varphi(m) = (y \cdot m + I_1 \cdot M, x \cdot m + I_2 \cdot M)$ since $x \cdot m \in I_1 \cdot M$, etc. On the other hand, by definition $\varphi(m) = (m + I_1 \cdot M, m + I_2 \cdot M)$, so we see that for any element $(m_1 + I_1 \cdot M, m_2 + I_2 \cdot M)$ in the target, φ maps $y \cdot m_1 + x \cdot m_2$ to this element. Thus the comaximality of I_1 and I_2 implies that φ is surjective.

Now, since I_1 and I_2 are ideals of R it is immediate that we have $I_1 I_2 \subseteq I_1 \cap I_2$. On the other hand, for any $r \in I_1 \cap I_2$, we have $r = (x + y)r = xr + yr \in I_1 I_2$. Thus comaximality also implies $I_1 I_2 = I_1 \cap I_2$, and thus $I_1 I_2 \cdot M = (I_1 \cap I_2) \cdot M$, and all we have to do is show $(I_1 \cap I_2) \cdot M = I_1 \cdot M \cap I_2 \cdot M$.

Clearly we have $(I_1 \cap I_2) \cdot M \subseteq I_1 \cdot M \cap I_2 \cdot M$. Now let us pick an element $m = i_1 \cdot m_1 = i_2 \cdot m_2$ in the intersection, with $i_1 \in I_1$ and $i_2 \in I_2$. Then $m = (x+y) \cdot m = x i_2 \cdot m_2 + y i_1 \cdot m_1 \in I_1 I_2 \cdot M$ and the result is proved. □

Note in particular that the Chinese Remainder theorem implies that the direct sum of two cyclic R-modules R/I and R/J need *not* be cyclic. Thus the order of a minimal generating set of modules over a commutative ring is not nearly as nicely behaved as the notion of dimension for vector spaces over a field.

Exercise 36. Find such an example.

4 Modules over a PID

In this section we investigate the structure of finitely generated modules over a PID. We are able to prove a very strong classification theorem in ideal-theoretic terms.

4.1 Noetherian modules, noetherian rings

In this subsection let R be commutative.

Definition 4.1. An R-module M is said to satisfy the *ascending chain condition* if every chain of submodules

$$M_1 \subseteq M_2 \subseteq M_2 \subseteq \dots$$

stabilizes. This means that there is some $n \in \mathbb{N}$ such that for all $i \geq n$, $M_i = M_n$.

Exercise 37. Show that for an R-module M, the following are equivalent:

1. M satisfies the ascending chain condition.
2. Every collection of submodules of M contains a maximal element, ordered by inclusion. In other words, if M_0 is in our collection of submodules, we say that M_0 is *maximal* if whenever M_1 is also in the collection and contains M_0, we must have $M_0 = M_1$. Note that this does not mean that M_0 contains every submodule of our collection.

3. Every submodule of M is finitely generated.

Hint: Show that 1. $\Rightarrow$ 2. $\Rightarrow$ 3. $\Rightarrow$ 1.: If we assume that 2. does not hold, construct an infinite chain of submodules of M that does not stabilize. Given a submodule $N \subset M$, look at the collection of finitely generated submodules of N and ask what it would mean for a maximal such submodule to not equal N. Finally, given an arbitrary ascending chain, consider the union of modules in that chain and ask what it would mean for the union to be finitely generated (after showing that it is a submodule of M).

Definition 4.2. An R-module that satisfies any of the equivalent conditions of Exercise 37 is called *noetherian*. The ring R itself is called *noetherian* if the regular module ${}_RR$ is noetherian.

Remark 4.3. From the definition it is clear that if M is noetherian then so is any submodule and any quotient module of M, and in particular M is finitely generated. If it is not clear, prove it. Note that while it is in general true that any quotient module of a finitely generated module is finitely generated, it is not true that any submodule must be as well (or else there would be no point to making this definition). Find an example of this.

Exercise 38. Show that if R is a PID, then R is noetherian.

Proposition 4.4. *If the ring R is noetherian, then any finitely generated module M over R is noetherian as well.*

Proof. It will be enough to show that R^n is noetherian for all $n \in \mathbb{N}$, as any finitely generated module is a quotient of a free module. We prove this by induction; the case $n = 1$ is the definition of R's being noetherian in the first place.

Let M be a submodule of R^n; we wish to show that M is finitely generated. Recall that $\pi_1 : R^n \to R$ denotes the projection onto the first coordinate. π_1 is an R-module map, so its image is an R-submodule of ${}_RR$, and thus is finitely generated by assumption. Let $\{m_1, \ldots, m_r\}$ be elements of M such that the set $\{\pi_1(m_i)\}$ generates $\pi_1(M)$. The m_i span an R-submodule N of M, and moreover it is clear that any element of M can be written as a sum of some $n \in N$ and some m' such that $\pi_1(m') = 0$. The collection of elements of R^n whose projection onto the first coordinate is zero is an R-submodule of R^n which can be identified with R^{n-1}. Thus we've seen that we can write M as being generated by the m_i and $M \cap R^{n-1}$. By inductive hypothesis, $M \cap R^{n-1} \subseteq R^{n-1}$ is finitely generated, and the result is proved. $\square$

Corollary 4.5. *Any finitely generated module over a PID is noetherian.*

4.2 Splitting off the free part

In this section, let R be a PID. We examine the structure of free R-modules in greater detail, in particular the structure of their submodules.

Exercise 39. A submodule M of R^n has rank less than or equal to n.

As R is noetherian, any submodule of R^n is finitely generated, but we do not yet know that it must be free.

Proposition 4.6. *If M is a submodule of R^n, M is free.*

Proof. Fix a free basis $\{e_1, \ldots, e_n\}$ of R^n, identify R^i with the (necessarily free) submodule generated by $\{e_1, \ldots, e_i\}$, and set $M_i := M \cap R^i$. We wish to show by induction that M_i is free for all i.

In the case $i = 1$, $M_i = M \cap R \subseteq R$ is an ideal of R, say generated by r. As R is a domain, either $r = 0$ or the ideal it generates is free of rank 1. (*Exercise*: Prove this.) The zero module can be thought of as the free R-module on the empty set (why is this?), so we've established the base case of the induction.

Suppose now that for $i < j$, M_i is free, and consider M_j. $R \cdot e_j$ is isomorphic to the regular R-module ${}_R R$, so $M_j \cap (R \cdot e_j)$ can again be thought of as an ideal of of R, say generated by an element $r \in R$. If $r = 0$, then M_j can be identifies with a submodule of M_{j-1}, and we're done. So assume $r \neq 0$.

Let $m \in M_j$ be such that m can be written as $\sum_{i=1}^{j-1} r_i \cdot e_i + r \cdot e_j$. In other words, m is an element of M_j that maps to the generator of $M_j \cap (R \cdot e_j)$, which description shows that it must exist. Clearly $M_{j-1} \cap (R \cdot m) = 0$, as every nonzero element in the submodule generated by m projects to a nonzero multiple of e_j, while no element of M_{j-1} does. On the other hand, it is easy to see that M_{j-1} and m generated M_j, so we have a decomposition of M_j as the direct sum of two free groups. The result follows. □

Corollary 4.7. *If M is a finitely generated torsion free R-module, M is free.*

Proof. Let n be the rank of M, and pick a finite set of generators $\{m_1, \ldots, m_\ell\}$ of M such that $\{m_1, \ldots, m_n\}$ is a basis for a free submodule of M of maximal rank. (*Exercise*: Why do we know there exists such a submodule?) Note that we are not requiring that the $\{m_i\}$ are a *basis* for M, meaning that they would be R-linearly independent, but merely that they generate M.

Because n was chosen to be the maximal number of R-linearly independent elements of R (by one of our equivalent notions of rank), for each $i \in \{1, \ldots, \ell\}$ we have that there exists a nonzero $r_i \in R$ such that r_i can be written as a R-linear combination of $\{m_1, \ldots, m_n\}$. Setting $r = \prod_{i=1}^{\ell} r_i$, we see that $r \cdot m_i$ is in the R-span of $\{m_1, \ldots, m_n\}$ for all $i \in \{1, \ldots, \ell\}$. In other words, left multiplication by ℓ sends M into a free submodule. Finally, since $r \neq 0$ and M is torsion free, we see that $r \cdot M \cong M$ as R-modules, and we've embedded M as a submodule of a free R-module. Proposition 4.6 finishes the proof. □

Exercise 40. Show by example that the assumption that M be finitely generated is necessary in Corollary 4.7.

Now let us use the fact that submodules of free modules are free to obtain our first piece of structure for finitely generated modules over a PID.

Proposition 4.8. *For any finitely generated R-module M, the quotient module $M/\operatorname{Tor}(M)$ is torsion free. Consequently, there is a (non-canonical) decomposition $M \cong \operatorname{Tor}(M) \oplus R^n$ of M as a torsion R-module with a free R-module.*

Proof. Suppose that $m \in M$ is such that the image $\overline{m} \in \overline{M} := M/\operatorname{Tor}(M)$ is a torsion element. Then there is some $r \in R$ such that $r \cdot \overline{m} = 0$, or equivalently $r \cdot m \in \operatorname{Tor}(M)$, so by definition there is some $r' \in R$ such that $r'r \cdot m = 0$ (in M). Thus m itself is a torsion element of M, and $\overline{m} = 0 \in \overline{M}$.

Therefore $\overline{M}$ is a finitely generated torsion free R-module, and so is free by Corollary 4.7. Let $\{\overline{m_1}, \ldots, \overline{m_n}\}$ be a free basis over $\overline{M}$, and pick elements $\{m_1, \ldots, m_n\} \subset M$ that map to this basis. As $\overline{M}$ is free, the set map sending $\overline{m_i}$ to m_i extends uniquely to an R-module map $f : \overline{M} \to M$. We wish to show that this map is injective.

Suppose that $\sum_{i=1}^n r_i \cdot \overline{m_i}$ is in the kernel of f, so that $\sum_{i=1}^n r_i \cdot m_i = 0$ in M. By projecting back down to $\overline{M}$, we see that $\sum_{i=1}^n r_i \cdot \overline{m_i} = 0$ in $\overline{M}$, so the fact that the $\overline{m}_i$ form a free basis for $\overline{M}$ implies that $r_i = 0$ for all i.

Thus we have embedded the free R-module $\overline{M} \cong R^n$ as a submodule of R. The proof that this decomposes M as $\operatorname{Tor}(M) \oplus R^n$ is left as an exercise. □

Remark 4.9. There are two things to note with the proof of Proposition 4.8. First, even though we are able to embed a copy of R^n in M there was a choice involved in how this was done: The construction of the map required picking preimages of the basis elements of $\overline{M}$. Thus, even though the submodule $\operatorname{Tor}(M)$ is uniquely defined (as simply the set of all torsion elements of M, which we've seen carries an R-module structure), the "free part" of M is not canonical.

Second, the idea of the proof relied on finding a submodule of M that is isomorphic to a given quotient of M. For an arbitrary quotient, there is absolutely no reason to assume that such a submodule should exist, and indeed, it often does not. (*Exercise*: Find some counterexamples.) The key piece of information we used to construct this submodule was the universal property for free modules. This actually hints at important concept in module-theory: Free modules are an example of *projective* modules, which are defined basically by taking the situation of the proof of Proposition 4.8 and asserting that there exists some (not necessarily unique) map splitting the quotient $M \to \overline{M}$. This is a very important definition, which we will unfortunately not have time to explore in this course.

Thus we've seen that for any finitely generated R-module M, there is a well-defined natural number n such that $M \cong \operatorname{Tor}(M) \oplus R^n$. Perhaps it would be a good exercise to check that n is the rank of M, defined either in terms of maximal free submodules or maximal sets of R-linearly independent elements.

Exercise 41. Do this. Conclude that the rank of $M \oplus N$ is the rank of M plus the rank of N, for M and N finitely generated. Note the difference between rank and minimal sets of generators.

4.3 Decomposing torsion R-modules

In this section assume that M is a finitely generated torsion module.

Definition 4.10. Let $p \in R$ be a prime. The *generalized p-torsion* of M is the set of elements $M(p) \subseteq M$ that are annihilated by some power of of p.

Exercise 42. Show that $M(p)$ is a submodule of M.

Exercise 43. Show that if $p \neq q$ are primes of R, then $M(p) \cap M(q) = 0$.

Hint: Use the fact that if $p \neq q$ then for any natural numbers a, b there are elements $r, s \in R$ such that $rp^a + sq^b = 1$. What can you say about $m = 1 \cdot m$ for $m \in M(p) \cap M(q)$?

Exercise 44. Show that there are only finitely many primes $p \in R$ such that $M(p) \neq 0$.

Hint: We already know that $Ann(M)$ is a nonzero ideal of R, and thus is generated by a single element as $r \in R$ (since R is a PID). Show that if $M(p) \neq 0$ then $p|r$.

Further hint: Use the fact that if $p \nmid r$, the ideal generated by p and r is all of R, and thus we can write 1 as an R-linear combination of p and r. Use this to prove that $M(p) = 0$.

Remark 4.11. In fact, the converse to the hint of Exercise 44 is also true: The prime $p \in R$ divides the generator of $\mathrm{Ann}(M)$ iff $M(P) \neq 0$. This result will fall out naturally from our classification of finitely generated modules over a PID, but perhaps it would be good to try to prove the converse implication now.

Proposition 4.12. *There is a natural decomposition $M \cong \bigoplus M(p)$, where the sum runs over the primes of R.*

Exercise 45. Prove Proposition 4.12.

Hint: Most of the work has already been done in the previous three exercises. All that we have left to do is prove that $M \subseteq \sum M(p)$, or that every element of M can be written as a sum of generalized p-torsion elements of M (why is this all we have to do?). To see this, pick a finite generating set $m_1, \ldots, m_n$ and for each $1 \leq i \leq n$, consider the submodule of M generated by m_i. Use the Chinese Remainder Theorem to finish the proof.

Thus classifying finitely generated torsion R-modules has been reduced to classifying such modules, all of whose elements have annihilators a power of a given prime $p \in R$. Our goal is to find a minimal generating set that will allow us to further decompose such generalized p-torsion modules.

Definition 4.13. The elements $m_1, \ldots, m_n \in M$ are *independent* if whenever we have $\sum_{i=1}^n r_i \cdot m_i = 0$ for $r_i \in R$, we must have each $r_i \cdot m_i = 0$.

Remark 4.14. Note that this is *not* the same as saying that the m_i are R-linearly independent, which is a stronger statement (find an example to illustrate the difference). However, if the m_i are independent, then the submodule of M generated by the m_i is isomorphic with the *direct* sum of the cyclic modules the m_i generate.

Lemma 4.15. *Let M be a finitely generated generalized p-torsion module. Then there is some integer k such that p^k annihilates M. Moreover, if $\{m_1, \ldots, m_n\}$ generate M and p^{k_i} is the minimal power of p that annihilates m_i, $k = \max\{k_i\}$.*

Proof. To state it is to prove it. □

Notation 4.16. For an element $r \in R$, the ideal generated by r will be denoted (r). For an element $m \in M$, the submodule $R \cdot m$ will be denote $\langle m \rangle$.

The following is a sort of analogue of our work on free modules to the world of generalized p-torsion modules.

Lemma 4.17. *Let M be a finitely generated generalized p-torsion module with maximal p-power annihilator k and $m \in M$ such that p^k is the minimal power of p that annihilates m. If $y_1, \ldots, y_n \in M/\langle m \rangle$ are independent and y_i has annihilator (p^{k_i}), there are elements $x_i \in M$ such that x_i is sent to y_i by the natural projection map and (p^{k_i}) is the annihilator of x_i. Moreover, the collection of x_i together with m is independent.*

Proof. We begin by picking an arbitrary z_i that lies over y_i for each i. Since $z_i + \langle m \rangle = y_i$ and $p^{k_i} \cdot y_i = 0$, we conclude that $p^{k_i} \cdot z_i \in \langle m \rangle$. , Therefore there are a natural number s_i and an element $r_i \in R$ such that $p \nmid r_i$ and $p^{k_i} \cdot z_i = r_i p^{s_i} \cdot m$. If $s_i < k_i$, we'd have $p^k \cdot z_i = p^{k-k_i} \cdot (p^{k_i} \cdot z_i) = r_i p^{k-k_i+s_i} \cdot m \neq 0$, contrary to our assumption that k was chosen to be maximal among the exponents of the annihilators of elements of M. Therefore $s_i \geq k_i$, and setting $x_i = z_i - r_i p^{s_i - k_i} \cdot m$ yields an element in the preimage of y_i that by construction has annihilator (p^{k_i}).

We just have to show that these x_i form, together with m, an independent set. Suppose that we have some relation $b \cdot m + \sum_{i=1}^n a_i \cdot x_i = 0$. Reducing mod $\langle m \rangle$ this becomes $\sum_{i=1}^n a_i \cdot y_i = 0$. Because the x_i were chosen to have the same annihilators of the corresponding y_i, the assumption that the y_i are independent forces $a_i \cdot y_i = 0$ and thus $a_i \cdot x_i = 0$. Clearly this implies $b \cdot m = 0$, and the result is proved. □

Remark 4.18. Note that an immediate corollary of Lemma 4.17 is that the submodule of M generated b the x_i maps *isomorphically* to the submodule of $M/\langle x \rangle$ generated by the y_i, so that we are able to embed a subquotient of M in M itself. As you may recall, the main property of free R-modules that we came down to a similar sort of trick (which was achieved there through a universal property, and consequently was much cleaner to prove); this is what I mean by Lemma 4.17 is a torsion module analogue of our free module work.

Proposition 4.19. *Let M be a finite generated generalized p-torsion module. Then there exist natural numbers $k_1 \geq k_2 \geq \ldots \geq k_n$ such that*

$$M \cong \bigoplus_{i=1}^{n} R/(p^{k_i})$$

Proof. We induct on the the order of a minimal generating set for M. If M is cyclic, our classification of cyclic modules gives the result immediately. Assume now that M has minimal generating set of order ℓ; pick a generating set $\{x_1, z_2, \ldots, z_\ell\}$. Let p^k be the minimal power of p that annihilates M; without loss of generality assume that the annihilator of x_1 is (p^k). The quotient module $M/\langle x_1\rangle$ can certainly be generated by $\ell-1$ elements, namely the images of the z_i for $1 < i \leq \ell$, though it is possible that a minimal generating set will have strictly smaller order. By inductive hypothesis, we have an independent generating set $\{y_2, \ldots, y_n\}$ of $M/\langle x_1\rangle$ with $\mathrm{Ann}(y_i) = (p^{k_i})$. Applying Lemma 4.17, we get elements $x_2, \ldots, x_n$, with x_i lying over y_i, having the same annihilator, and such that the set of elements $\{x_1, x_2, \ldots, x_n\}$ is independent. By construction, an arbitrary element of M differs from an element of the submodule spanned by $\{x_2, \ldots, x_n\}$ by a multiple of x_1, so we've given a generating set of M consisting of independent generators with the desired properties. The result follows. □

4.4 Classification Theorems

We can now assemble all our work on the structure of finitely generated modules over a PID to state our first Classification Theorem:

Theorem 4.20 (Elementary Factor Decomposition Theorem)**.** *If M is a finitely generated module over the PID R, there exist natural number $b, k_1, \ldots, k_n$ and primes $p_1, \ldots, p_n \in R$ (not necessarily distinct) such that*

$$M \cong R^b \oplus \bigoplus_{i=1}^{n} R/(p_i^{k_i})$$

Proof. Split M into free and torsion parts according to Proposition 4.8 to get the R^b factor. $\mathrm{Tor}(M)$ splits as a direct sum of generalized p-torsion submodules by Proposition 4.12, and each $M(p)$ splits as claimed by Proposition 4.19. □

Remark 4.21. As suggested by the name of Theorem 4.20, the cyclic modules $R/(p_i^{k_i})$ in the decomposition are the *elementary factors* of M. Of course, we haven't yet shown uniqueness of these factors, but we will, don't worry.

In order to prove uniqueness of this decomposition it will be helpful formulate another version of the Classification Theorem, which is useful in its own right.

Theorem 4.22 (Invariant Factor Decomposition Theorem)**.** *If M is a finitely generated module over the PID R, there exists a natural number b and elements $a_1, a_2, \ldots, a_\ell \in R$ such that $a_\ell | a_{\ell-1} | \ldots | a_1$ and*

$$M \cong R^b \oplus \bigoplus_{i=1}^{\ell} R/(a_i)$$

Proof. Clearly it suffices to show that if M is torsion, the result holds with $b = 0$. Take a set of elementary factors for M, and use it to construct a grid of natural numbers as follows:

Let p_i for $1 \leq i \leq q$ be the distinct primes of R with $M(p_i) \neq 0$; these will index the rows of the grid. For a given p_i, arrange the exponents of the elementary factors corresponding to p_i in descending order; fill out the row corresponding to p_i with these descending exponents, defining the entries to be zero once you've run out of factors. The finite generation assures that we end up with a finite array of nonzero numbers:

$$\begin{array}{c|cccc} p_1 & k_1^1 & k_1^2 & \dots & 0 \\ p_2 & k_2^1 & k_2^2 & \dots & 0 \\ \vdots & & \ddots & & \\ p_q & k_q^1 & k_q^2 & \dots & 0 \end{array}$$

Set $a_1 = p_1^{k_1^1} p_2^{k_2^1} \dots p_q^{k_q^1}$, $a_2 = p_1^{k_1^2} p_2^{k_2^2} \dots p_q^{k_q^2}$, etc., where the element a_j is defined by looking along the jth column of our array, and where a_ℓ is by definition the last identity element so constructed. By our arrangement, it is clear that $a_\ell | a_{\ell-1} | \dots | a_1$, and finally, the Chinese Remainder Theorem gives $R/(a_j) \cong \sum_{i=1}^q R/(p_i^{k_i^j})$ and the result is proved. □

We conclude this section by showing that we really have classified all the finitely generated modules over the PID R; in order to do so, we must see that our descriptions of a module M are uniquely determined by the isomorphism class of M. By this we mean that if M has two elementary factor decompositions $M \cong R^b \oplus \bigoplus_{i=1}^n R/(p_i^{k_i}) \cong R^{b'} \oplus \bigoplus_{j=1}^{n'} (R/q_j^{k'_j})$ then $b = b'$, $n = n'$, and, after suitable reordering, $p_i = q_i$ (up to choice of unit) and $k_i = k'_i$.

Similarly, for uniqueness of invariant factor forms, we must show that if we have two decompositions $M \cong R^b \oplus \bigoplus_{i=1}^\ell R/(a_i) \cong R^{b'} \oplus \bigoplus_{j=1}^{\ell'} R/(a'_j)$ with $a_\ell | a_{\ell-1} | \dots | a_1$ and $a'_{\ell'} | a'_{\ell'-1} | \dots | a'_1$, then $b = b'$ and $a_i = a'_i$ up to a unit.

Exercise 46. Reduce both cases to proving the result for torsion modules. In the case of the elementary factor decomposition, reduce to the case of a generalized p-torsion module.

Exercise 47. Prove the uniqueness of the elementary factor decomposition in the case that M is generalized p-torsion.

Hint: Induct on the minimal power of p that annihilates M. For the base case, note that if $p \cdot M = 0$, then M is naturally a module over $R/(p)$, which is a field (why?), so our knowledge of finite dimensional vector spaces over fields will give the result. For the inductive step, consider the submodule $p \cdot M$ to use as a stepping stone.

Exercise 48. Prove the uniqueness of the invariant factor decomposition in the case that M is a torsion R-module.

Hint: Begin by exploring the submodule annihilated by (p), denoted M_p. In the case of an invariant factor $N = R/(pa)$ (where p may possibly divide a), what is N_p? As above, M_p is a vector space over $R/(p)$; express its dimension in terms of an invariant factor decomposition; by clever choice of p, conclude that any two invariant factor decompositions of M must have the same length. Finish off the proof by induction on the minimal power of p (for our cleverly chosen p) that annihilates M. That such a power should exist is also a hint as to what p should be chosen.