STRUCTURE THEORY FOR MODULES OVER PRINCIPAL IDEAL DOMAINS AND DEDEKIND DOMAINS

Kyle Mickelson

Last updated: March 2nd, 2025

Contents

Definitions and Examples

1.1 Modules and Submodules

Definition 1.1 (Left R-modules). Let R be a unital ring. A *left R-module* is a set Q equipped with the following data:

1. A binary operation $+$ on Q under which Q is an abelian group;
2. A (ring) action of R on Q given by a map $\bullet : R \times Q \to Q$ sending $(r, q) \mapsto r \bullet q$ for all $r \in R$ and $q \in Q$, which satisfies
   (a) $(r + s) \bullet m = r \bullet m + s \bullet m$, for all $r, s \in R$ and $m \in M$;
   (b) $r \bullet (m + n) = r \bullet m + r \bullet n$, for all $r \in R$ and $m, n \in Q$;
   (c) $(rs) \bullet m = r \bullet (s \bullet m)$, for all $r, s \in R$ and $m \in M$.
   (d) $1 \bullet m = m$, for all $m \in Q$.

From now on we shall forego the symbol $\bullet$ between elements of the ring R and elements of the module Q and instead juxtapose such elements; that is, we write $r \bullet m = rm$ for all $r \in R$ and $m \in Q$.

For a given ring R, we can also consider a completely symmetric construction to the left R-modules defined above: these are, of course, *right R-modules*, objects which differ from left R-modules only in terms of their ring action. Specifically, a right R-module is an abelian group Q (whose operation we again denote by $+$) equipped with a ring action, which is simply a map $\bullet : Q \times R \to Q$ defined by $(m, r) \mapsto m \bullet r$ for all $m \in Q$ and $r \in R$. With respect to this ring action, we require that the following relations are satisfied:

1. $m \bullet (r + s) = m \bullet r + m \bullet s$, for all $r, s \in R$ and $m \in Q$;
2. $(m + n) \bullet r - m \bullet r + n \bullet r$, for all $r \in R$ and $m, n \in Q$;
3. $m \bullet (rs) = (m \bullet r) \bullet s$, for all $r, s \in R$ and $m \in Q$;
4. $m \bullet 1 = m$, for all $m \in Q$.

Note that the relations (1)-(4) above are entirely symmetric with those found in Definition 1.1, the only difference being on which side the ring elements act on the module elements.

Of course, in the case where the ring R is commutative, any left R-module Q can be made into a right R-module by defining $rm = mr$ for all $r \in R$ and $m \in Q$. The converse is true as well, in that right R-modules can be made into left R-modules. For this reason, when considering commutative rings R, we shall refer to left (or right) R-modules simply as R-modules.

Note that when the ring in question R is not commutative, and we are given, say, a right R-module Q, we do not, in general, have that axiom 2(c) in Definition 1.1 holds, since it may not be the case that $rs = sr$ for ring elements $r, s \in R$. In this way, not every right R-module can be considered as well as a left R-module (and conversely).

Already we can see how the theory of modules is intricately tied to the theory of rings. This tight-knit relationship will be explored further in what is to come.

Using the axioms in Definition 1.1, we state a preliminary result. Specifically, we prove that when the zero element of a ring acts on any module element, the resulting module element is 0 (where 0 is the identity element of the underlying abelian group structure of the module). We also show that

Proposition 1.2. Let R be a ring and Q a left R-module. Then $0m = 0$ and $(-1)m = -m$ for all $m \in M$.

Proof. For any $r \in R$, we know that $r - r = 0$, in the ring R, and hence by axiom 2(a) in Definition 1.1 we have:

$$0m = (r - r)m = rm - rm = 0$$

Similarly, since $(-1) \cdot 1 = -1$ in R, axiom 2(c) in Definition 1.1 gives

$$(-1)m = (1 \cdot -1)m = 1(-m) = -m$$

which suffices to show the desired relations. ■

Before we proceed with further structural results and examples of modules, we define the subobjects corresponding to modules.

Definition 1.3 (**R-submodules**)**.** Let R be a ring and let Q be a left R-module. An R-*submodule* of Q is a subgroup T of Q which is closed under the induced ring action of R on Q. That is, we have $rn \in T$ for all $r \in R$ and $n \in T$.

Indeed, submodules of an R-module Q are also themselves R-modules under the same actions and operations inherited from Q. We now prove a short proposition which we shall employ frequently throughout the text; it will serve as a quick way to check whether certain subsets of modules are submodules.

Proposition 1.4 (**The Submodule Criterion**)**.** Let R be a ring and let Q be an R-module. A subset T of Q is an R-submodule of Q if and only if $T \neq \varnothing$ and $x + ry \in T$ for all $r \in R$ and $x, y \in T$.

Proof. Supposing T is an R-submodule of Q, we have $0 \in T$ since T is a subgroup (and so inherits the identity element) of Q, hence $T \neq \emptyset$. Moreover, T is closed under addition (since a subgroup) and ring elements acting on elements of T are carried to T by definition.

Conversely, taking $r = -1$, we see that T is closed under subtraction, hence is a subgroup of Q, hence contains 0. Taking $x = 0$, we have $ry \in T$ for all $r \in R$ and $y \in T$, hence T is sent to itself under the ring action, whence an R-submodule of Q. ■

Since submodules will play an important role in our development, we cover some ground by exhibiting some properties of submodules.

Proposition 1.5 (**Arbitrary intersections of submodules are submodules**)**.** Let R be a ring. The intersection of any non-empty collection of submodules of an R-module is a submodule.

Proof. Let Q be an R-module, and $\mathcal{A}$ be a nonempty collection of R-submodules of Q. Consider the set $\bigcap_{T \in \mathcal{A}} T$. Since each $T \in \mathcal{A}$ is an R-submodule of Q, we have $T \leq Q$ as additive groups. The intersection of any non-empty collection of subgroups of M is once more a subgroup of Q, and thus $\bigcap_{T \in \mathcal{A}} T$ is a subgroup of Q.

What remains is to show that $\bigcap_{T \in \mathcal{A}} T$ is closed under the action of ring elements from R. Let $x \in \bigcap_{T \in \mathcal{A}} T$ and $r \in R$ be arbitrary. In particular, $x \in T$ for all $T \in \mathcal{A}$. Since each T is an R-submodule, we know $rx \in T$ for all $T \in \mathcal{A}$, implying $rx \in \bigcap_{T \in \mathcal{A}} T$ as well. ■

Proposition 1.6 (**Union of ascending chain of submodules is submodule**)**.** Let R be a ring and Q an R-module. If $T_1 \subseteq T_2 \subseteq \cdots$ is an ascending chain of R-submodules of Q, then $\bigcup_{i=1}^{\infty} T_i$ is an R-submodule of Q.

Proof. Take Q an R-module and $T_1 \subseteq T_2 \subseteq \cdots$ a chain of R-submodules of Q. Consider the set $\bigcup_{i=1}^{\infty} T_i$. Since each T_i is an R-submodule of Q, each T_i is a subgroup of Q. From group theory, we know $H \cup K$ is a subgroup of a group G if and only if either $H \subseteq K$ or $K \subseteq H$. It is a simple induction to extend this to the arbitrary case; in our particular case, we have that $T_1 \cup T_2$ is a subgroup of Q since $T_1 \subseteq T_2$. Similarly, we have $\bigcup_{i=1}^{n} T_i \subseteq T_{n+1}$ and so $\bigcup_{i=1}^{n+1} T_i$ is a subgroup. With this induction, we have $\bigcup_{i=1}^{\infty} T_i \leq Q$ is a subgroup. Now let $r \in R$ and $x \in \bigcup_{i=1}^{\infty} T_i$. Then $x \in T_i$ for some $i \in \mathbb{N}$. In particular, $rx \in T_i$ by closure under T_i of the action of R. Thus $rx \in \bigcup_{i=1}^{\infty} T_i$. Thus we have proved $\bigcup_{i=1}^{\infty} T_i$ is an R-submodule of Q. ■

1.2 Examples of Modules

In this section we aim to devise a collection of examples of modules to which we shall turn to frequently in the coming development. In future propositions and theorems, we oftentimes return to these examples for illustrative purposes; either to reiterate key points or to simply showcase the immense diversity and power these constructions possess.

Example 1.7 (**Rings are modules over themselves**). Let R be any ring. Then R has the structure of a left R-module (as well as a right R-module) by defining the ring action to be usual multiplication in the ring R.

Note, however, that when R is not commutative, we may have that the left and right module structures of R over itself do not coincide. That is, it may be the case that R as a left R-module over itself has a different submodule structure than R as a right R-module over itself. To see an example of this, consider Example 1.8 below.

Indeed, we note that *when R is considered as a left R-module, the R-submodules of R are precisely the left ideals of R* (and likewise, when R is considered as a right R-module, the R-submodules of R are precisely the right ideals of R).

Example 1.8 (**Left / right module structures need not coincide**). Let $n \in \mathbb{Z}^+$, $n > 1$ and let R be the ring of $n \times n$ matrices with entries from a field F; that is, let $R = M_n(F)$. Let M be the set of $n \times n$ matrices with arbitrary elements of F in the first column and zeros elsewhere.

We claim that M is a submodule of R when R is considered as a left module over itself, but M is not a submodule of R when R is considered as a right R-module.

Proof. Let R and M be as above. It is trivial to verify that M is an additive subgroup of R. What remains is to check whether the action of R on M remains in M. Take an arbitrary matrix A from R and take an arbitrary B from M. We find that:

$$AB = \begin{pmatrix} x_{11} & x_{21} & \cdots & x_{n1} \\ x_{21} & x_{22} & \cdots & x_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix} \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ a_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^n x_{i1} a_i & 0 & \cdots & 0 \\ \sum_{i=1}^n x_{i2} a_i & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n x_{in} a_i & 0 & \cdots & 0 \end{pmatrix}$$

and clearly the matrix on the right hand side above lies in M as well, hence implying that M is an R-submodule of R considered as a left R-module over itself. However, note that performing the same procedure on the right gives

$$BA = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ a_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} x_{11} & x_{21} & \cdots & x_{n1} \\ x_{21} & x_{22} & \cdots & x_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix} = \begin{pmatrix} a_1 x_{11} & a_1 x_{21} & \cdots & a_1 x_{n1} \\ a_2 x_{11} & a_2 x_{21} & \cdots & a_2 x_{n1} \\ \vdots & \vdots & \ddots & \vdots \\ a_n x_{11} & a_n x_{21} & \cdots & a_n x_{n1} \end{pmatrix}$$

and clearly the matrix above does not, in general, lie in M for all values of x_{ij} above, and hence need not lie in M for all matrices in R. Thus M is not an R-submodule of R considered as a right R-module over itself. ■

Example 1.9. Let $R = F$ be a field. Indeed, as we have seen, every F-vector space is an F-module, and conversely. In particular, letting $n \in \mathbb{Z}^+$, the set

$$F^n = \{(a_1, \ldots, a_n) \mid a_i \in F,\ 1 \leq i \leq n\}$$

is the well-known n-dimensional vector space over the field F, which we shall refer to as *affine n-space over F* henceforth. To recall, we can make F^n into an F-vector space by defining addition and scalar multiplication component-wise:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

$$\alpha(a_1, \ldots, a_n) = (\alpha a_1, \ldots, \alpha a_n)$$

for all $\alpha \in F$ and $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in F^n$.

1.2.1 Abelian Groups as $\mathbb{Z}$-modules

Let A be any abelian group, either finite or infinite, and let $+$ denote the binary operation in A. We now make A into a $\mathbb{Z}$-module by defining an action of $\mathbb{Z}$ on A.

Given any integer $n \in \mathbb{Z}$, we have three cases: either $n > 0$, $n < 0$, or $n = 0$. We define the ring action of $\mathbb{Z}$ on elements $a \in A$ differently depending on these three cases: the proscriptions are as follows:

$$na := \begin{cases} a + \cdots + a & \text{for} \quad n > 0; \\ 0 & \text{for} \quad n = 0; \\ -a - \cdots - a & \text{for} \quad n < 0. \end{cases}$$

where, for instance, there are precisely n different a's which appear in the sum $a + \cdots + a$ (and likewise precisely n different a's which appear in the difference $-a - \cdots - a$). We note that the 0 in the above proscription is the identity element in the abelian group A, not necessarily the integer 0.

The way we have defined the ring action of $\mathbb{Z}$ on A is unique. That is, there is only one possible way that the ring $\mathbb{Z}$ can act on an abelian group A, which can be seen by verifying the axioms for a module given in Definition 1.1. In view of what we have done then, every abelian group may be considered as a $\mathbb{Z}$-module.

Indeed as well, given any $\mathbb{Z}$-module, say Q, we know that, Q is an abelian group (by definition), and hence the above applies. Thus, in a manner of speaking, we have shown that *$\mathbb{Z}$-modules and abelian groups are one in the same*. Moreover, from Definition 1.3, we can see that *$\mathbb{Z}$-submodules and subgroups are one in the same*.

We can see immediately that the left and right $\mathbb{Z}$-module structures on the same abelian group A coincide; that is, there is no distinction between the two.

1.2.2 $k[x]$-modules

Let k be a field and let x be an indeterminate. We now consider the polynomial ring $k[x]$ and modules over this ring.

Let V be a k-vector space and let $T : V \to V$ be a linear operator. Indeed, we have already seen that V may be considered a k-module in the obvious way (since vector spaces are particular examples of modules when the underlying ring is a field). We claim that, in addition to the latent k-module structure on V, we can use the linear operator T to make V into a $k[x]$-module.

To start, we must of course define the ring action: how will $k[x]$ act on elements of the vector space V? The elements of $k[x]$ are polynomials with coefficients in the field k, so let us take some such polynomial $f(x) \in k[x]$, say

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

where $a_0, \ldots, a_n \in k$. For each vector $v \in V$, we define the action of the ring element $f(x)$ on the module element v by

$$\begin{aligned} f(x)v &:= a_0 T^0(v) + a_1 T^1(v) + \cdots + a_n T^n(v) \\ &= a_0 v + a_1 T(v) + \cdots + a_n T^n(v) \end{aligned}$$

In other words, we substitute the indeterminate x in the polynomial $f(x)$ for the linear operator T, so for instance x^n would change to T^n, where T^n denotes the composition of the linear operator n times with itself, which is valid since the domain and codomain of T are the same. We then evaluate the linear transformation T^n at the vector v. We use here, implicitly, the k-vector space structure of the set of all linear transformations from V to itself. That is, we can compose linear transformations from V to itself and scale them by elements from the field k.

It is a simple exercise to check that the module axioms of Definition 1.1 hold for V equipped with the ring action of $k[x]$ defined above.

1.3 Annihilators

Proposition 1.10 (**Submodule of elements annihilated by powers of ideals).** Let R be a ring and I an ideal of R. Let Q' be the subset of elements x of Q that are annihilated by some power, I^k, of the ideal I, where the power may depend on x. Then Q' is a submodule of Q.

Proof. Let Q_k denote the subset of Q consisting of elements x of Q annihilated by I^k. That is, for an integer $k \geq 1$, set $Q_k = \mathrm{Ann}_Q(I^k)$. We claim that $Q_k \subseteq Q_{k+1}$ for all $k \geq 1$. To this end, suppose $x \in Q_k$. Then x is annihilated by I^k. Note that any $r \in I^{k+1} = II^k$ may be written $r = s's$ for $s' \in I$ and $s \in I^k$. Then

$$rx = (s's)x = s'(sx) = s'0 = 0$$

holds since x is annihilated by I^k; hence x is annihilated by I^{k+1}, proving our claim.

Now we have an ascending chain of submodules of Q given by:

$$Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_k \subseteq \cdots ,$$

and by Proposition 1.6, we know $\bigcup_{k=1}^{\infty} Q_k$ is a submodule of Q. Note, however, that this submodule is precisely Q' as defined in the problem description; hence Q' is a submodule of Q. ∎

Proposition 1.11. Let R be a P.I.D., let Q be a torsion R-module, and let p be a prime in R. Prove that if $px = 0$ for some non-zero $x \in B$, then $\text{Ann}_R(Q) \subseteq (p)$.

Proof. Suppose $px = 0$ for some non-zero $x \in Q$. Since $\text{Ann}_R(Q)$ is an ideal of R, and R is a P.I.D., we know $\text{Ann}_R(Q) = (r)$ for some $r \in R$. Consider the ideal $(d) = (r) + (p)$; we know that d is the greatest common divisor of r and p. Since p is a prime element of R, either $d = 1$ or $d = p$. In the former case, there exists $s, t \in R$ such that

$$sr + tp = 1$$

As such, we have

$$x = 1x = (sr + tp)x = (sr)x + (tp)x = s(rx) + t(px) = s0 + t0 = 0 + 0 = 0$$

and hence $x = 0$, a contradiction, for we took $x \in Q \setminus \{0\}$. Thus the latter case holds; that is, $d = p$, so that p divides (r), and hence $\text{Ann}_R(Q) = (r) \subseteq (p)$. ∎

Proposition 1.12. Let R be a ring and let $Q_1, \dots, Q_n$ be R-modules, with T_i a submodule of Q_i for each $i = 1, 2, \dots, n$. Then

$$(Q_1 \times \cdots \times Q_n)/(T_1 \times \cdots \times T_n) \cong (Q_1/T_1) \times \cdots \times (Q_n/T_n).$$

Proposition 1.13. Let R be any ring, and let $Q_1, \dots, Q_n$ be R-modules. Let T_i be a submodule of Q_i, $1 \leq i \leq n$. Then

$$(Q_1 \oplus \cdots \oplus Q_n)/(T_1 \oplus \cdots \oplus T_n) \cong (Q_1/T_1) \oplus \cdots \oplus (Q_n/T_n).$$

Proposition 1.14. The direct sum of any two free modules is free.

1.4 Some basic results

Proposition 1.15. Let R and S be rings and let Q and T be left R-modules. Assume also that Q is an (R, S)-bimodule. Then:

1. If, for $s \in S$ and for $\varphi \in \mathrm{Hom}_R(Q, T)$, we define $(s\varphi) : Q \longrightarrow R$ by $(s\varphi)(x) = \varphi(xs)$, then $s\varphi$ is a homomorphism of left R-modules, and this action of S on $\mathrm{Hom}_R(Q, T)$ makes it into a *left* S-module.

2. Let $S = R$. If, for each $y \in T$, we define $\varphi_y : R \longrightarrow T$ by $\varphi_y(r) = ry$, i.e., φ_y is the unique R-module homomorphism mapping 1_R to n, then $\varphi_n \in \mathrm{Hom}_R(R, T)$. In particular, the map $y \mapsto \varphi_y$ is an isomorphism of left R-modules: $T \cong \mathrm{Hom}_R(R, T)$.

3. If T is a free (respectively, projective, injective, flat) left R-module, then $\mathrm{Hom}_R(R, T)$ is also a free (respectively, projective, injective, flat) left R-module.

❈ Exact Sequences of Modules

We first reframe some familiar notations in a potentially unfamiliar way. Let R be some ring and let A, B, C be R-modules.

The statement that A is isomorphic to a submodule of B is equivalent to the existence of an R-module homomorphism

$$\psi : A \to B$$

which is injective. Then we will have $\ker \psi = 0$, and hence $A \cong \psi(A) \subseteq B$ by the first isomorphism theorem for modules.

In a somewhat similar manner, the statement that C is isomorphic to the quotient module $B/\psi(A)$ is equivalent to the existence of an R-module homomorphism

$$\varphi : B \to C$$

which is surjective with $\ker \varphi = \psi(A)$; then the first isomorphism theorem again will yield that $B/\psi(A) \cong C$.

Collecting the above observations: if A is isomorphic to a submodule of B and C is isomorphic to the resulting quotient, then we have a sequence of R-module homomorphisms

$$A \xrightarrow{\psi} B \xrightarrow{\varphi} C$$

where $\ker \varphi = \operatorname{im} \psi$ holds. Since this situation is a very common one we provide it with a name:

Definition 2.1 (Exactness). Let R be a ring and let A, B, and C be R-modules. Then the sequence

$$A \xrightarrow{\psi} B \xrightarrow{\varphi} C$$

is said to be *exact at B* if $\ker \varphi = \operatorname{im} \psi$.

As may be evident, we can extend this notion to larger sequences, say consisting of more than two R-module homomorphisms.

Definition 2.2 (Exact sequences). Let R be a ring and let $\{Q_n\}$ be any collection of R-modules. Then a sequence

$$\cdots \xrightarrow{\varphi_{n-2}} Q_{n-1} \xrightarrow{\varphi_{n-1}} Q_n \xrightarrow{\varphi_n} Q_{n+1} \xrightarrow{\varphi_{n+1}} \cdots$$

of R-module homomorphisms is said to be an *exact sequence* if it is exact at every Q_n between pairs of R-module homomorphisms; that is, if $\ker \varphi_n = \operatorname{im} \varphi_{n-1}$ holds at every Q_n for all n.

2.1 Short Exact Sequences and Splitting

We cover some basics. As always, we let 0 denote the trivial R-module. Note that for any R-module Q, there are always R-module homomorphisms to and from the trivial R-module. Indeed, these homomorphisms are necessarily unique. For the R-module homomorphism to the trivial module, we have:

$$Q \to 0$$

$$x \mapsto 0.$$

This is the only such homomorphism, for every element of Q must be mapped to some element of 0 by definition of a function, and there is only one such element in 0, namely 0 itself. Likewise, for the R-module homomorphism *from* the trivial module, we have:

$$0 \to Q$$

$$0 \mapsto 0$$

This is the only such homomorphism, for R-module homomorphisms must preserve the identity element of the underlying abelian groups, so must map 0 to 0. Since there is only the 0 element in the trivial module, this is the only possible map.,

Adducing the discussion above, we henceforth write simply $0 \to Q$ and $Q \to 0$ to denote the unique R-module homomorphisms from and to, respectively, the trivial R-module 0.

Proceeding, we can reformulate the notions of injectivity and surjectivity (and hence of bijectivity) in terms of the exactness of a particular sequence.

Proposition 2.3 (**Injective, surjective, bijective maps as exact sequences**)**.** Let A, B, and C be R-modules over some ring R. Then:

1. The R-module homomorphism $\psi : A \to B$ is injective if and only if the sequence $0 \to A \xrightarrow{\psi} B$ is exact at A.
2. The R-module homomorphism $\varphi : B \to C$ is surjective if and only if the sequence $B \xrightarrow{\varphi} C \to 0$ is exact at C.
3. The sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ is exact if and only if ψ is injective, φ is injective, and $\ker \varphi = \operatorname{im} \psi$.

Proof. For (1), as we saw in the discussion preceding the proposition, the unique R-module homomorphism $0 \to A$ has image 0 in A. Thus ψ is injective if and only if $\ker \psi = 0$ if and only if $\ker \psi$ is equal to the image of 0 in A.

Similarly for (2), the unique R-module homomorphism $C \to 0$ has kernel equal to C, since all of C maps to 0. Thus φ is surjective if and only if $\operatorname{im}\varphi = C$ if and only if the kernel of $C \to 0$ is equal to the image of φ.

(3) of the proposition is simply shown using (1) and (2) above. ■

The situation of Proposition 2.3(3) will be crucial to our development, and so we give it a name as well.

Definition 2.4 (Short exact sequences). Let A, B, and C be R-modules for some ring R. Then an exact sequence of the form

$$0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$$

is called a *short exact sequence*.

We remark that any R-module homomorphism, say $\varphi : Q \to T$ for R-modules Q and T, hides an implicit short exact sequence as follows:

$$0 \to \ker\varphi \xrightarrow{i} Q \xrightarrow{\pi} Q/\ker\varphi \to 0$$

where $i : \ker\varphi \to Q$ is the inclusion homomorphism, which is always injective, and $\pi : Q \to Q/\ker\varphi$ is the canonical projection homomorphism, which is always surjective. Moreover, we have that $\ker\pi = \ker\varphi$ automatically; hence by Definition 2.4 the above sequence is a short exact sequence.

2.1.1 Some diagrams

Proposition 2.5. Let R be a ring and suppose that

$$\begin{tikzcd}
A \arrow[r, "\psi"] \arrow[d, "\alpha"] & B \arrow[r, "\varphi"] \arrow[d, "\beta"] & C \arrow[d, "\gamma"] \\
A' \arrow[r, "\psi'"] & B' \arrow[r, "\varphi'"] & C'
\end{tikzcd}$$

is a commutative diagram of R-modules with exact rows (meaning the top row is exact at B and the bottom row is exact at B') Then:

1. If φ and α are surjective, and β is injective then γ is injective.
2. If ψ', α, and γ are injective, then β is injective.
3. if φ, α, and γ are surjective, then β is surjective.
4. If β is injective, α and φ are surjective, then γ is injective.

5. If β is surjective, γ and ψ' are injective, then α is surjective.

Proof. (1) Suppose φ and α are surjective, and that β is injective. Assume $c \in \ker\gamma$. Since $\varphi : B \to C$ is surjective, there exists $b \in B$ for which $\varphi(b) = c$. Since the diagram was assumed to commute, we require that $\varphi'(\beta(b)) = 0$. Thus $\beta(b) \in \ker\varphi'$, and since the bottom row in the diagram is exact, this is equivalent to $\beta(b) \in \operatorname{im}\psi'$. Since $\psi' : A' \to B'$, we know there exists some $a' \in A'$ for which $\psi'(a') = \beta(b)$.

Now, since we assumed $\alpha : A \to A'$ was surjective, there exists some $a \in A$ for which $\alpha(a) = a'$. The commutativity of the diagram once more asserts that $\beta(\psi(a)) = \beta(b)$. Injectivity of β provides $\psi(a) = b$. However, above we saw that $\varphi(b) = c$, and so now we may note that $\varphi(\psi(a)) = c$. But the top row is exact, and so $\operatorname{im}\psi = \ker\varphi$. Since $\psi(a) \in \operatorname{im}\psi$, this means $\psi(a) \in \ker\varphi$, so that $\varphi(\psi(a)) = 0$, and hence $c = 0$. Therefore, $\ker\gamma = \{0\}$; hence γ is injective.

(2) Suppose ψ', α, and γ are injective. Assume $b \in \ker\beta$. We know that $\varphi(b) = c$ for some $c \in C$, and further that $\gamma(c) = 0$ since the diagram commutes, and $\beta(b) = 0$ implies $\varphi'(\beta(b)) = 0$. This means that $c \in \ker\gamma$, and since γ is injective we have $c = 0$. Now $\varphi(b) = 0$, so that $b \in \ker\varphi$, and since the top row is exact, $b \in \operatorname{im}\psi$. Thus there exists $a \in A$ for which $\psi(a) = b$. Since $\beta(b) = 0$, the commutativity of the diagram forces $\psi'(\alpha(a)) = 0$. Since ψ' is injective, this means $\alpha(a) = 0$, and since α is injective, this means $a = 0$. But then $\psi(0) = b$, and so $b = 0$. Thus $\ker\beta = \{0\}$ and so β is injective.

(3) Suppose φ, α, γ are surjective. Let $b' \in B'$. We know that $\varphi'(b') = c'$ for some $c' \in C'$, and furthermore that there exists some $c \in C$ for which $\gamma(c) = c'$ by surjectivity of γ. Since φ is surjective, there exists $b \in B$ for which $\varphi(b) = c$. Now, by commutativity of the diagram, we require $\varphi'(\beta(b)) = c'$ as well, and so $\varphi'(\beta(b)) = \varphi'(b')$. Now

$$\varphi'(\beta(b))\varphi'(b')^{-1} = 0 \iff \varphi'(\beta(b)(b')^{-1}) = 0$$

and so $\beta(b)(b')^{-1} \in \ker\varphi'$. Since the bottom row is exact, this means that $\beta(b)(b')^{-1} \in \operatorname{im}\psi'$ and so there exists $a' \in A$ such that $\psi'(a') = \beta(b)(b')^{-1}$. Since α is surjective, there exists $a \in A$ such that $\alpha(a) = a'$. By commutativity of the diagram, we know that $\beta(\psi(a)) = \beta(b)(b')^{-1}$. Now

$$b' = \beta(\psi(a))^{-1}\beta(b) = \beta(\psi(a)^{-1}b)$$

and since $\psi(a)^{-1}b \in B$, we have found such an element of B which equals b' under β. In particular, this shows that β is surjective, as desired.

(4) Suppose β is injective, α and φ are surjective. Assume $c \in \ker \gamma$. Since φ is surjective, there exists $b \in B$ such that $\varphi(b) = c$. Since the diagram commutes, we know $\varphi'(\beta(b)) = 0$ is required. This means that $\beta(b) \in \ker \varphi'$, and since the bottom row is exact, we have that $\beta(b) \in \text{im } \psi'$ as well. Thus, there exists some $a' \in A'$ for which $\psi'(a') = \beta(b)$. Since $\alpha : A \to A'$ is surjective by assumption, there also exists some $a \in A$ such that $\alpha(a) = a'$.

To summarize: we have $\psi'(\alpha(a)) = \beta(b)$. Furthermore, since the diagram commutes, we require $\beta(\psi(a)) = \beta(b)$. Since β is injective, this implies $\psi(a) = b$. However, it is obvious that $\psi(a) \in \text{im } \psi$, and since the top row is exact, we have $\text{im } \psi = \ker \varphi$, so that $\psi(a) \in \ker \varphi$. Now $\varphi(\psi(a)) = 0$ and so $\varphi(b) = 0$. But we assumed that $\varphi(b) = c$, and so it follows that $c = 0$. Hence $\ker \gamma = \{0\}$, and thus γ is injective.

(5) Suppose β is surjective, γ and ψ' are injective. Let $a' \in A'$ be arbitrary. Obviously $\psi'(a') \in \text{im } \psi'$, and since the bottom row is exact this means $\psi'(a') \in \ker \varphi'$. Hence $\varphi'(\psi'(a')) = 0$.

Now, since β is surjective, there exists some $b \in B$ for which $\beta(b) = \psi'(a')$. From the commutativity of the diagram, we require $\gamma(\varphi(b)) = 0$ to hold as well (since above $\varphi'(\psi'(a')) = 0$ holds). However, since γ is injective by assumpton, this means $\varphi(b) = 0$. In particular, we have $b \in \ker \varphi$. The exactness of the top row implies that $b \in \text{im } \psi$. Hence there exists $a \in A$ for which $\psi(a) = b$.

In particular, $\beta(\psi(a)) = \psi'(a')$ must hold since $\beta(b) = \psi'(a')$, as we saw above. By commutativity of the diagram, we require $\psi'(\alpha(a)) = \psi'(a')$ to hold as well. But injectivity of ψ' assures us that $\alpha(a) = a'$. Thus we have found some $a \in A$ which equals a' under α, and since a' was arbitrary this means α is surjective. ■

Proposition 2.6. Let R be a ring and suppose that

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r, "h"] \arrow[d, "\gamma"] & D \arrow[d, "\delta"] \\
A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r, "h'"] & D'
\end{tikzcd}$$

is a commutative diagram of R-modules with exact rows. Then:

1. If α is surjective, and both β, δ are injective, then γ is injective.
2. If δ is injective, and both α, γ are surjective, then β is surjective.

Proof. (1) Suppose α is surjective and β, δ are injective. Assume $c \in \ker \gamma$. Then $\gamma(c) = 0$, and in particular we know that $h'(\gamma(c)) = 0$ also holds. By the commutativity of the diagram we know $\delta(h(c)) = 0$ as well. Since δ is injective, $h(c) = 0$.

Thus $c \in \ker h$ and so $c \in \text{im } g$ by exactness of the top row. In particular, there exists $b \in B$ such that $g(b) = c$.

Once again, commutativity of the diagram asserts that $g'(\beta(b)) = \gamma(g(b))$ and so $g'(\beta(b)) = 0$. In particular, $\beta(b) \in \ker g'$ and so $\beta(b) \in \text{im } f'$ by exactness of the bottom row. Thus there exists $a' \in A'$ for which $f'(a') = \beta(b)$. Since α is surjective, there exists $a \in A$ for which $\alpha(a) = a'$.

In particular, we kow that $f'(\alpha(a)) = \beta(f(a))$ by commutativity of the diagram. This means $\beta(b) = \beta(f(a))$. Since β was assumed injective, we have $b = f(a)$. With this in mind clearly we have $b = f(a) \in \text{im } f$, and since the top row is exact, we have $b = f(a) \in \ker g$. Hence $g(b) = 0$. However, above we saw that $g(b) = c$, and so we require $c = 0$. Therefore $\ker \gamma = \{0\}$, and hence γ is injective.

(2) Suppose δ is injective, and α, γ are surjective. We aim to show that β is surjective. Refer to the diagram given in part (a). Let $b' \in B'$ be arbitrary. Then $g'(b') \in \text{im } g'$ and by exactness of the bottom row we have $g'(b') \in \ker h'$. Thus $h'(g'(b')) = 0$.

Now, since $g'(b') \in C'$, the surjectivity of γ implies that there exists $c \in C$ for which $\gamma(c) = g'(b')$. Since the diagram commutes, we require that $\delta(h(c)) = h'(g'(b')) = 0$. But since δ is injective by assumption, this means $h(c) = 0$. Thus $c \in \ker h$ and by exactness of the top row we have $c \in \text{im } g$. Now there exists some $b \in B$ for which $g(b) = c$.

Then commutativity of the diagram means $g'(\beta(b)) = \gamma(g(b))$ and so $g'(\beta(b)) = g'(b')$. In particular, we have

$$g'(\beta(b))g'(b')^{-1} = 0 \iff g'(\beta(b)(b')^{-1}) = 0$$

since $g' : B' \to C'$ is a group homomorphism. The above indicates that $\beta(b)(b')^{-1} \in \ker g'$, and so $\beta(b)(b')^{-1} \in \text{im } f'$ by exactness. Thus there exists $a' \in A'$ for which $f'(a') = \beta(b)(b')^{-1}$. Since α is surjective by assumption, there exists $a \in A$ for which $\alpha(a) = a'$ as well. Commutativity of the diagram forces $\beta(f(a)) = f'(\alpha(a))$, which is equivalent to $\beta(f(a)) = \beta(b)(b')^{-1}$. We have

$$\beta(f(a)) = \beta(b)(b')^{-1} \iff b' = \beta(f(a))^{-1}\beta(b) = \beta(f(a)^{-1}b)$$

since $\beta : B \to B'$ is a group homomorphism. However note that we have found an element $f(a)^{-1}b \in B$ which equals b' under β. Since $b' \in B'$ was arbitrary, this proves that β is surjective. ■

2.2 Projective Modules

Theorem 2.7 (Equivalent conditions for projectivity). Let P be an R-module for some ring R. Then the following are equivalent:

1. For any R-modules L, Q, and T, if the following sequence

   $$0 \to L \xrightarrow{\psi} Q \xrightarrow{\varphi} T \to 0$$

   is a short exact sequence, then the sequence

   $$0 \longrightarrow \mathrm{Hom}_R(P, L) \xrightarrow{\psi^*} \mathrm{Hom}_R(P, Q) \xrightarrow{\varphi^*} \mathrm{Hom}_R(P, T) \longrightarrow 0$$

   is also a short exact sequence. In other words, the functor $\mathrm{Hom}_R(P, -)$ is exact; i.e., $\mathrm{Hom}_R(P, -)$ takes short exact sequences to short exact sequences.

2. For R-modules Q and T equipped with a surjective R-module homomorphism $\varphi : Q \to T$, and given any R-module homomorphism $f : P \to T$ we have a lift $F : P \to Q$ such that the diagram

   $$\begin{tikzcd} Q \arrow[r, two heads, "\varphi"] & T \\ & P \arrow[u, "f"'] \arrow[ul, "F"] \end{tikzcd}$$

   commutes.

3. Every short exact sequence $0 \to L \to Q \to P \to 0$ of R-modules splits. In other words, if P is a quotient of Q, then P is isomorphic to a direct summand of Q.

4. P is a direct summand of a free R-module.

Proof. TBD. ■

Definition 2.8 (Projective modules). Let P be an R-module for some ring R. If P satisfies any of the equivalent conditions of Theorem 2.7 then P is said to be *projective*.

Corollary 2.9. Let R be a ring. Then:

1. Free R-modules are projective.

2. A finitely generated R-module is projective if and only if it is a direct summand of a finitely generated free R-module.

3. Every R-module is a quotient of a projective R-module.

Proof. TBD. ■

Proposition 2.10 (Direct sum projective iff summands are projective). Let R be any ring and let P_1 and P_2 be R-modules. Then $P_1 \oplus P_2$ is projective if and only if both P_1 and P_2 are projective.

Proof. Suppose $P_1 \oplus P_2$ is a projective R-module. Then, in view of Theorem 2.7(4), we may write that $P_1 \oplus P_2$ is a direct summand of a free R-module, say $F = P_1 \oplus P_2 \oplus K$ for some R-submodule K of F. In particular, both P_1 and P_2 are direct summands of a free R-module, namely F, since they are in particular direct summands of $P_1 \oplus P_2$.

We prove the converse. Suppose P_1 and P_2 are projective R-modules. Then there exists free R-modules F and F' for which $F = P_1 \oplus K$ and $F' = P_2 \oplus K'$. Since the direct sum of free R-modules is once again free by Proposition 1.14, we know that $F \oplus F'$ is free. Indeed, we have:

$$F \oplus F' = P_1 \oplus K \oplus P_2 \oplus K' = (P_1 \oplus P_2) \oplus (K \oplus K')$$

and so clearly $P_1 \oplus P_2$ is a direct summand of the free R-module $F \oplus F'$, and so is itself projective by Theorem 2.7(4). ■

2.3 Injective Modules

Theorem 2.11 (Equivalent conditions for injectivity). Let Q be an R-module for some ring R. Then the following are equivalent:

1. For any R-modules L, W, and T, if the following sequence

$$0 \to L \xrightarrow{\psi} W \xrightarrow{\varphi} T \to 0$$

is a short exact sequence, then the sequence

$$0 \to \mathrm{Hom}_R(L, Q) \xrightarrow{\psi^*} \mathrm{Hom}_R(W, Q) \xrightarrow{\varphi^*} \mathrm{Hom}_R(T, Q) \to 0$$

is also a short exact sequence. In other words, the functor $\mathrm{Hom}_R(-, Q)$ is exact; i.e., $\mathrm{Hom}_R(-, Q)$ takes short exact sequences to short exact sequences.

2. For R-modules L and T equipped with an injective R-module homomorphism $\psi : L \to T$, and given any R-module homomorphism $f : L \to Q$ we have a lift $F : T \to Q$ such that the diagram

$$\begin{tikzcd} L \arrow[r, "\psi"] \arrow[d, "f"'] & T \arrow[dl, "F"] \\ Q & \end{tikzcd}$$

commutes.

3. Every short exact sequence $0 \to Q \to W \to T \to 0$ of R-modules splits. In other words, if Q is a submodule of W, then Q is a direct summand of W.

Proof. TBD. ■

Definition 2.12 (Injective modules). Let R be a ring and Q an R-module. Then Q is said to be *injective* if any of the equivalent conditions of Theorem 2.11 hold.

Proposition 2.13 (Direct sum injective iff summands injective). Let R be a ring and let Q_1 and Q_2 be R-modules. Then $Q_1 \oplus Q_2$ is injective if and only if both Q_1 and Q_2 are injective.

Proof. Suppose Q_1 and Q_2 are injective. Let L and T be R-modules and suppose $\psi : L \to T$ is injective. Suppose $f \in \operatorname{Hom}_R(L, Q_1 \oplus Q_2)$. We have natural projections given by $\pi_1 : Q_1 \oplus Q_2 \to Q_1$ and $\pi_2 : Q_1 \oplus Q_2 \to Q_2$. In particular, $\pi_1 \circ f \in \operatorname{Hom}_R(L, Q_1)$ and $\pi_2 \circ f \in \operatorname{Hom}_R(L, Q_2)$ since the composition of R-module homomorphisms is an R-module homomorphism. Now, since Q_1 and Q_2 are injective, Theorem 2.11(2) asserts that there exists a lift $F_1 \in \operatorname{Hom}_R(T, Q_1)$ and $F_2 \in \operatorname{Hom}_R(T, Q_2)$ such that

$$\begin{tikzcd}
Q_1 \oplus Q_2 \arrow[r, "\pi_1"] & Q_1 \\
L \arrow[u, "f"] \arrow[r, "\psi"] \arrow[d, "f"'] & T \arrow[u, "F_1"] \arrow[d, "F_2"] \\
Q_1 \oplus Q_2 \arrow[r, "\pi_2"] & Q_2
\end{tikzcd}$$

commutes; i.e., we have $F_1 \circ \psi = \pi_1 \circ f$, and likewise we have $F_2 \circ \psi = \pi_2 \circ f$.

Now we consider the map:

$$\tilde{F} : T \to Q_1 \oplus Q_2$$

$$\tilde{F}(x) = (F_1(x), F_2(x))$$

It is obvious to see that $\tilde{F}$ is an R-module homomorphism, a consequence of F_1 and F_2 being R-module homomorphisms.

We will be done if we can prove that $\tilde{F} \circ \psi = f$, for then we will have a commutative diagram

$$\begin{tikzcd}
L \arrow[r, "\psi"] \arrow[d, "f"'] & T \arrow[dl, "\tilde{F}"] \\
Q_1 \oplus Q_2 &
\end{tikzcd}$$

So take $l \in L$. Assume $f(l) = (q_1, q_2)$ for $q_1 \in Q_1$ and $q_2 \in Q_2$. Then $\pi_1(f(l)) = q_1$ and $\pi_2(f(l)) = q_2$. As above, we have $F_1(\psi(l)) = q_1$ and $F_2(\psi(l)) = q_2$. Now we have

$$\tilde{F}(\psi(l)) = (F_1(\psi(l)), F_2(\psi(l))) = (q_1, q_2) = f(l)$$

and so the diagram commutes. Since the R-module homomorphism $f : L \to Q_1 \oplus Q_2$ was arbitrary, and we found a lift $F : T \to Q_1 \oplus Q_2$ such that $f = F \circ \psi$, by Theorem 2.11(2) we have that $Q_1 \oplus Q_2$ is an injective R-module.

Conversely, suppose $Q_1 \oplus Q_2$ is injective. Let L and T be R-modules and suppose $\psi : L \to T$ is injective. Suppose $f_1 \in \mathrm{Hom}_R(L, Q_1)$ and $f_2 \in \mathrm{Hom}_R(L, Q_2)$. We then have an obvious R-module homomorphism given by $f : L \to Q_1 \oplus Q_2$ defined by $f(l) = (f_1(l), f_2(l))$ for all $l \in L$. By the assumption that $Q_1 \oplus Q_2$ is injective, Theorem 2.11(2) asserts that there exists a lift $F : M \to Q_1 \oplus Q_2$ such that $F \circ \psi = f$. We thus have a diagram

$$\begin{tikzcd}
 & Q_1 \arrow[rrd, bend left, "\iota_1"] & & \\
0 \arrow[r] & L \arrow[u, "f_1"] \arrow[d, dash, "f_2"'] \arrow[r, "\psi"] \arrow[rr, bend right, "f"'] & T \arrow[r, "F"] & Q_1 \oplus Q_2 \\
 & Q_2 \arrow[rru, bend right, "\iota_2"] & &
\end{tikzcd}$$

It is clear that $\pi_1 \circ F : T \to Q_1$ and $\pi_2 \circ F : T \to Q_2$ are both R-module homomorphisms. Furthermore, $(\pi_1 \circ F) \circ \psi = f_1$ and $(\pi_2 \circ F) \circ \psi = f_2$ since if $l \in L$ and $f_1(l) = q_1$ and $f_2(l) = q_2$, then

$$\pi_1(F(\psi(l))) = \pi_1(f(l)) = \pi_1(f_1(l), f_2(l)) = q_1$$

$$\pi_2(F(\psi(l))) = \pi_2(f(l)) = \pi_2(f_1(l), f_2(l)) = q_2$$

and therefore there exists lifts $\pi_1 \circ F \in \mathrm{Hom}_R(T, Q_1)$ and $\pi_2 \circ F \in \mathrm{Hom}_R(T, Q_2)$, which makes Q_1 and Q_2 injective by Theorem 2.11(2). ■

2.3.1 Constructing Injective Modules

Injective modules are slightly harder to contend with than their categorical counterparts, the projective modules.

In order to ameliorate this potential difficulty, we exhibit a recipe by which injective modules can be produced from some relatively simple ingredients. This recipe will fall into place after just two short lemmas.

Lemma 2.14. Let A be a left $\mathbb{Z}$-module and let R be a ring. Then $\mathrm{Hom}_{\mathbb{Z}}(R, A)$ is a left R-module with ring action given by $(r\varphi)(s) = \varphi(rs)$ for all $s, r \in R$ and $\mathbb{Z}$-module homomorphisms $\varphi : R \to A$.

Proof. Any ring R has the structure of an additive abelian group, and hence may be considered a $\mathbb{Z}$-module.. In fact, this means that R is a $(\mathbb{Z}, \mathbb{Z})$-bimodule.

Since A is a left $\mathbb{Z}$-module, we may appeal to Proposition 1.15(1) to write that $\mathrm{Hom}_{\mathbb{Z}}(R, A)$ has the structure of a left R-module (we are taking $S = \mathbb{Z}$ in the notation of that exercise). ■

Lemma 2.15. Let A be a left $\mathbb{Z}$-module. Let R be a ring, Q and T be R-modules, and let $\psi : Q \to T$ be an injective R-module homomorphism. Then if every $\mathbb{Z}$-module homomorphism $f : Q \to A$ lifts to a $\mathbb{Z}$-module homomorphism $F : T \to A$ with $f = F \circ \psi$, then every R-module homomorphism $f^* : Q \to \mathrm{Hom}_{\mathbb{Z}}(R, A)$ lifts to an R-module homomorphism $F^* : T \to \mathrm{Hom}_{\mathbb{Z}}(R, A)$ with $f^* = F^* \circ \psi$.

Proof. Suppose we have some R-module homomorphism $f^* : Q \to \mathrm{Hom}_{\mathbb{Z}}(R, A)$. Consider the map

$$f : Q \to A$$

$$q \mapsto f^*(q)(1_R)$$

So f takes elements of Q to the $\mathbb{Z}$-module homomorphism $f^*(q)$ evaluated at the identity 1_R of R. We now show that f is a $\mathbb{Z}$-module homomorphism. To see this, we need only remark that

$$f(q + q') = f^*(q + q')(1_R) = f^*(q)(1_R) + f^*(q')(1_R) = f(q) + f(q'),$$

which follows since f^* was assumed an R-module homomorphism. Thus, by our assumption, there exists a $\mathbb{Z}$-module homomorphism $F : T \to A$ such that $f = F \circ \psi$.

Now consider the map

$$F^* : T \to \mathrm{Hom}_{\mathbb{Z}}(R, A)$$

$$t \mapsto (r \mapsto F(rt))$$

So in other words, for each $t \in T$, the $\mathbb{Z}$-module homomorphism $F^*(t) : R \to A$ is defined by $F^*(t)(r) = F(rt) \in A$ for all $r \in R$, since the R-module structure of T means that $rt \in T$.

We now show that F^* is an R-module homomorphism that is a lift for f^* above. To see this, we verify the required relations: let $t, t' \in T$ and $r, r' \in R$ be arbitrary.

$$F^*(t + t')(r) = F(r(t + t')) = F(rt + rt') = F(rt) + F(rt') = F^*(t)(r) + F^*(t')(r)$$

$$F^*(r't)(r) = F(r(r't)) = F((rr')t) = F^*(t)(rr') = (r'F^*(t))(r)$$

Note that the last equality in the second line above follows from the specific ring action of R on $\mathrm{Hom}_{\mathbb{Z}}(R, A)$ we covered in Lemma 2.14; the two equations above show that F^* is indeed an R-module homomorphism.

What remains, then, is to show that F^* is a lift of f^*. To prove this, we show that $f^* = F^* \circ \psi$, i.e., that the diagram

$$\begin{tikzcd}
Q \arrow[r, "f^*"] \arrow[d, "\psi"'] & \mathrm{Hom}_{\mathbb{Z}}(R, A) \\
T \arrow[ur, "F^*"'] &
\end{tikzcd}$$

commutes. Taking any $q \in Q$, and letting $r \in R$ be arbitrary, we have the following:

$$\begin{aligned}
f^*(q)(r) &= f^*(q)(1_R \cdot r) \\
&= (r f^*)(q)(1_R) \\
&= f^*(rq)(1_R) \\
&= f(rq) \\
&= (F \circ \psi)(rq) \\
&= F(\psi(rq)) \\
&= F(r\psi(q)) \\
&= F^*(\psi(q))(r) \\
&= (F^* \circ \psi)(q)(r).
\end{aligned}$$

To ease up confusion, we remark that the first equality holds since $r = 1_R \cdot r = r \cdot 1_R$ always holds. Moreover, the second and third equalities hold due to f^* being an R-module homomorphism (see Lemma 2.14). The fourth equality holds by definition of the map f we described above. The fifth since $f = F \circ \psi$ by hypothesis. The sixth is obvious, the seventh is due to ψ being an R-module homomorphism, the eighth is by definition of F^*, and the last is obvious once more.

We make note that the injectivity of $\psi : Q \longrightarrow T$ which was part of our hypothesis serves to ensure that the kernels of f^* and $F^* \circ \psi$ coincide, for instance since ψ must not take non-zero elements of Q to the zero element of T.

Hence F^* is indeed a lift for f^*, and since $f^* : Q \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(R, A)$ was arbitrary, we have the desired statement of the lemma. ■

Now we will employ the two lemmas to delineate a recipe by which injective modules can be made from injective $\mathbb{Z}$-modules.

Proposition 2.16 (**Constructing injective R-modules from injective $\mathbb{Z}$-modules**)**.** Let R be any ring. If Q is an injective $\mathbb{Z}$-module, then $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is an injective R-module.

Proof. Suppose Q is an injective $\mathbb{Z}$-module. Then, in particular, Q is a left $\mathbb{Z}$-module. Suppose also that $\psi : L \longrightarrow T$ is any injective R-module homomorphism.

In particular, since L and T are abelian groups, we may consider L and T as $\mathbb{Z}$-modules in the usual way, and moreover can consider ψ as an injective $\mathbb{Z}$-module homomorphism.

Thus, from Theorem 2.11(2), since Q is injective we know that any $\mathbb{Z}$-module homomorphism $f : L \to Q$ lifts to a $\mathbb{Z}$-module homomorphism $F : T \to Q$ such that $f = F \circ \psi$. But this is precisely the hypothesis of Lemma 2.15, and so we may write that every R-module homomorphism $f^* : L \to \operatorname{Hom}_{\mathbb{Z}}(R, Q)$ lifts to an R-module homomorphism $F^* : T \to \operatorname{Hom}_{\mathbb{Z}}(R, Q)$, with $f^* = F^* \circ \psi$. Note, this is simply Theorem 2.11(2) applied to the R-module $\operatorname{Hom}_{\mathbb{Z}}(R, Q)$ (which, recall, is an R-module via Lemma 2.14). Hence $\operatorname{Hom}_{\mathbb{Z}}(R, Q)$ is an injective R-module by Definition 2.12. ■

2.3.2 Injective Hulls

As we saw in Corollary 2.9, every module can be considered as a quotient of some projective module. In this subsection, we cover an injective analogue of this corollary by introducing the notion of an injective hull of a module.

First we motivate the concept. We have the following lemma, which falls quite easily out of Baer's Criterion for injective modules.

Lemma 2.17 (**Every $\mathbb{Z}$-module is submodule of injective $\mathbb{Z}$-module**)**.** Every $\mathbb{Z}$-module is a submodule of an injective $\mathbb{Z}$-module.

Proof. TBD. ■

We can use the lemma above to prove a more general version of the statement for arbitrary rings.

Theorem 2.18 (**Every module contained in injective module**)**.** Let R be any ring and let W be an R-module. Then W is contained in an injective R-module.

Proof. If W is a left R-module then in particular W is an additive abelian group, and so we may consider W as a $\mathbb{Z}$-module. Now Lemma 2.17 asserts asserts that W is contained as a submodule in an injective $\mathbb{Z}$-module, say Q.

Any R-module homomorphism $f \in \operatorname{Hom}_R(R, W)$ is, in particular, an abelian group homomorphism, and hence $f \in \operatorname{Hom}_{\mathbb{Z}}(R, W)$, to which

$$\operatorname{Hom}_R(R, W) \subseteq \operatorname{Hom}_{\mathbb{Z}}(R, W).$$

Since W is a $\mathbb{Z}$-submodule of Q, we have the inclusion $\mathbb{Z}$-module homomorphism $i : W \to Q$, which we may pre-compose with f to obtain $i \circ f : R \to Q$, a $\mathbb{Z}$-module homomorphism. The maps $\iota \circ f$ and f may be identified by viewing W

as a submodule of Q, and in particular this gives $f \in \operatorname{Hom}_{\mathbb{Z}}(R, Q)$. Thus we have proved

$$\operatorname{Hom}_R(R, W) \subseteq \operatorname{Hom}_{\mathbb{Z}}(R, W) \subseteq \operatorname{Hom}_{\mathbb{Z}}(R, Q)$$

From Proposition 1.15(3), we have that $\operatorname{Hom}_R(R, W) \cong W$ as R-modules. In particular, W is isomorphic to a submodule of $\operatorname{Hom}_{\mathbb{Z}}(R, Q)$ by the containments above. However, from Proposition 2.16, we know that $\operatorname{Hom}_{\mathbb{Z}}(R, Q)$ is an injective R-module since Q is an injective $\mathbb{Z}$-module; hence W is contained in an injective R-module. ■

For a ring R and R-module W, Theorem 2.18 implies the existence of *some* injective R-module containing W. Indeed, a more interesting object to work with would be a *minimal* injective R-module which contains W, one which satisfies a universal property.

Definition 2.19 (**Injective hulls**)**.** Let R be a ring and W an R-module. Then we write $\mathcal{H}(W)$ for the minimal injective R-module containing W; the module $\mathcal{H}(W)$ is minimal in the sense that for any other injective module Q containing W, we have

$$W \subseteq \mathcal{H}(W) \subseteq Q.$$

We call the injective R-module $\mathcal{H}(W)$ the *injective hull* of W.

2.4 Flat Modules

※ Modules over Principal Ideal Domains

3.1 Noetherian Modules

In this section, we define a finiteness condition which shall enable us to get a hold on, so to speak, submodules of certain modules.

Definition 3.1 (**Noetherian modules**)**.** Let R be a ring and Q a left R-module. Then Q is said to be a *Noetherian R-module* if there are no infinite ascending chains of R-submodules of Q. That is, whenever

$$Q_1 \subseteq Q_2 \subseteq Q_3 \subseteq \cdots$$

is an increasing chain of R-submodules of Q, then there exists an $n \in \mathbb{Z}^+$ such that for all $m \geq n$, we have $Q_n = Q_m$. In other words, the ascending chain is eventually stationary at some submodule Q_n.

The definition is also extremely important in the more general theory of rings. In view of this importance, we include the following definition (since it shall also appear later in various situations).

Definition 3.2 (**Noetherian rings**)**.** Let R be a ring. Then R is said to a *Noetherian ring* if R is Noetherian as a left R-module over itself. Since R-submodules of the left R-module R are precisely the left ideals of R, we can also say that R is a Noetherian ring if and only if every ascending chain of ideals is eventually stationary.

We now present a theorem which characterizes Noetherian modules in a more intuitive way; in particular, we find that Noetherian modules are precisely those modules for which all submodules are finitely generated, which will turn out to be quite a strong finiteness condition going forward.

Theorem 3.3 (**Noetherian module equivalence**)**.** Let R be a ring and let Q be a left R-module. Then the following are equivalent:

1. Q is a Noetherian R-module;
2. Every non-empty set of submodules of Q contains a maximal element with respect to inclusion;
3. Every submodule of Q is finitely generated.

Proof. (1) $\implies$ (2). Let $\Sigma \neq \varnothing$ be a set of R-submodules of Q. We may order Σ by set-inclusion; for any chain

$$\cdots \subseteq T_{n-1} \subseteq T_n \subseteq T_{n+1} \subseteq \cdots$$

of R-submodules of Q, we note that $\bigcup_{n=1}^{\infty} T_n$ is an R-submodule

■

With Theorem 3.3 in tow, we can make some fairly inoffensive statements about familiar rings. In particular, an easy corollary is that a familiar class of rings is Noetherian.

Corollary 3.4 (**P.I.D.s are Noetherian**)**.** Let R be a ring. If R is a principal ideal domain, then R is a Noetherian ring.

Proof. Submodules of R considered as a left R-module over itself are precisely the ideals of R. Since every ideal is principal, it is immediate that every submodule is finitely generated, hence by Theorem 3.3 R is a Noetherian ring. ■

3.2 Prelude: Modules over Integral Domains

Linear algebra has a special place in the heart of many mathematicians, both young and old. The myriad reasons for this may be rendered and boiled and poked and prodded, and they all come down to the fact that vector spaces are very well-behaved objects. One of the reasons for their relative placidity (in face of something terribly dirty, say for example, infinite non-abelian groups) is that if we have a finite-dimensional vector space, then subspaces of that vector space must also be finite-dimensional.

Recall that, for modules, things are not as pretty. For instance, it may be the case that a finitely generated R-module Q has a submodule which is not finitely generated. Thus the condition in Definition 3.1, and resulting characterization in Theorem 3.3 is actually quite a strong one. When dealing with Noetherian modules, that is to say, we need not worry about pesky infinitely generated submodules. This is very nice. We explore just how nice this fact is in the remainder of this section (and beyond).

But first we try to emulate some of the things we hold dear in the theory of vector spaces. The notion we aim to emulate is that of linear independence and dependence.

Proposition 3.5. Let R be an integral domain and let Q be a free R-module of rank n. Then any $n+1$ elements of Q are R-linearly dependent; meaning that, for any $m_1, \ldots, m_{n+1} \in Q$, there are elements $r_1, \ldots, r_{n+1} \in R$, with at least one r_i not equal to 0, such that the equation

$$\sum_{i=1}^{n+1} r_i m_i = 0$$

holds in Q.

Proof. One of the nice things about requiring that the underlying ring R be an integral domain is that we can take its field of fractions, call it K. We can then observe that since Q is free of rank n, we have the canonical isomorphism of R-modules $Q \cong R^n$. Combined with the canonical embedding $R \hookrightarrow K$, we can extend via

$$Q \cong R^n = \bigoplus_{i=1}^{n} R \hookrightarrow \bigoplus_{i=1}^{n} K = K^n$$

Thus we may identify Q as a subspace of the n-dimensional K-vector space K^n. Indeed, in K^n, any $n+1$ elements (vectors) of K^n, hence also of Q, are K-linearly dependent. Thus for $m_1, \ldots, m_{n+1} \in Q$ there exists $\alpha_1, \ldots, \alpha_{n+1} \in K$, not all zero, such that

$$\sum_{i=1}^{n+1} \alpha_i m_i = 0$$

Since K is the field of fractions of R, we have that $\alpha_i = a_i/b_i$ for $a_i, b_i \in R$ with $b_i \neq 0$ for each $1 \leq i \leq n+1$. Thus

$$\sum_{i=1}^{n+1} (a_i/b_i) m_i = 0 \iff \sum_{i=1}^{n+1} a_i \left(\prod_{j \neq i} b_j \right) m_i = 0$$

Setting $r_i = a_i(\prod_{j \neq i} b_j)$ for each i gives us elements of R which induce the R-linear dependence on the elements $m_1, \ldots, m_{n+1}$ in Q. ■

In view of Proposition 3.5 above, we now formulate a notion of *rank* for modules which are not necessarily free on their underlying rings. In a sense, we sharpen our previous notion of rank to one that will better suit our purposes, and will generalize the notion of dimension from linear algebra.

Definition 3.6 (**Rank**)**.** Let R be an integral domain. Then the *rank* of an R-module Q is the maximum number of R-linearly independent elements of Q.

We note that if R is a field, then the rank of any R-module as defined in Definition 3.6 above coincides with the familiar notion of dimension from the theory of vector spaces.

Further, using definition above, we can begin to assemble statements which should feel quite natural: for instance, if we take an integral domain R, and any free R-module Q of finite rank, then Proposition 3.5 asserts that any submodule of Q must also have finite rank, which is a sublime statement on its own as well as for its use in our coming developments.

3.2.1 Characterizations on Rank

In order to ameliorate any confusion regarding the definition of rank given prior, we now make further statements about rank and how it pertains to submodules.

To start, we need a result which characterizes modules of finite rank over integral domains. This next result will show that a module over an integral domain has finite rank if and only if it *contains some* free submodule of the same rank such that a certain condition on the quotient is met.

Proposition 3.7 (**Characterization of finite rank**)**.** Let R be an integral domain and Q a left R-module. Then Q has rank n if and only if Q contains a submodule T that is free of rank n such that the quotient Q/T is a torsion R-module.

Proof. Suppose Q has rank n, and let $x_1, \dots, x_n$ be any maximal set of R-linearly independent elements of Q. Let e_i denote the element of R^n with 1 in the ith component and zeroes elsewhere; it is clear that the set of all e_i generate R^n as an R-module. Considering the submodule $T = Rx_1 + \cdots + Rx_n$ of Q, we can construct a mapping $\psi : R^n \to T$ defined by $\psi(e_i) = x_i$ for all $1 \leq i \leq n$. The fact that ψ is an R-module homomorphism is immediate; we also have surjectivity, since for any $y \in T$ we have $y = \sum_{i=1}^n r_i x_i$ for some $r_i \in R$, $1 \leq i \leq n$, and hence $\psi(r_1, \dots, r_n) = y$. Injectivity is also clear, for if $(r_1, \dots, r_n)$ is an element of R^n which is sent to 0 by ψ, then we require $\sum_{i=1}^n r_i x_i = 0$ in T, and by the linear independence of the x_i, this forces $r_i = 0$ for all i; hence $T \cong R^n$ as R-modules.

Now we show that Q/T is torsion. Since Q has rank n, the maximum number of linearly independent elements of Q is n; hence the set $\{y, x_1, \dots, x_n\}$ must be R-linearly dependent, so there exists $r_1, \dots, r_{n+1} \in R$, not all zero, such that

$$r_1 x_1 + \cdots + r_n x_n + r_{n+1} y = 0$$

and hence with

$$r_{n+1} y = -(r_1 x_1 + \cdots + r_n x_n)$$

This of course means $r_{n+1} y \in T$, hence that $\overline{r_{n+1} y} = \overline{0}$ in Q/T, to which $\overline{y} \in \mathrm{Tor}(Q/T)$. Therefore, Q/T is a torsion R-module.

Conversely, suppose that Q contains a submodule $T \cong R^n$ such that Q/T is a torsion R-module. Let $y_1, \dots, y_{n+1}$ be any $n+1$ elements of Q. Since Q/T is torsion, for each equivalence class $\overline{y_i}$ in Q/T there exists some $r_i \in R$ such that $\overline{r_i y_i} = \overline{0}$, which means $r_i y_i \in T$. Thus we have a set

$$\{r_1 y_1, \dots, r_{n+1} y_{n+1}\}$$

of elements of T, and since T is free of rank n, Proposition 3.5 asserts that there exists $s_1, \dots, s_{n+1} \in R$, not all zero, such that

$$s_1(r_1 y_1) + \cdots + s_{n+1}(r_{n+1} y_{n+1}) = 0$$

Letting $t_i = s_1 r_1$, we see that

$$t_1 y_1 + \cdots + t_{n+1} y_{n+1} = 0$$

and hence the set $\{y_1, \dots, y_{n+1}\}$ is R-linearly dependent in Q, so too must be any set of $n+1$ elements of Q, since we chose the y_i arbitrarily. Thus the maximum number of R-linearly independent elements of Q is n, since, for instance, the submodule T of Q has this property. By definition, then, Q is of rank n. ■

We also have the following result, which proves that the rank of a module is the same as the rank of the quotient module obtained modding out the module via its torsion submodule.

Lemma 3.8 (**Rank of torsion submodule is zero).** Let R be an integral domain and Q an R-module. Then the rank of $\text{Tor}(Q)$ is 0.

Proof. Recall that the rank of a module Q over an integral domain R is the maximum number of R-linearly independent elements of Q. If $x \neq 0$ is a torsion element of Q, so that there exists some non-zero $r \in R$ for which $rx = 0$, so then x and 0 are R-linearly dependent; in particular, the maximum number of R-linearly independent torsion elements of Q is 0; hence the rank of $\text{Tor}(Q)$ is 0, and likewise any torsion R-module has rank 0 for the same reason. ■

With this fact in mind, we have the following:

Proposition 3.9 (**Rank of a module modulo torsion).** Let R be an integral domain. For any R-module Q, the rank of Q and the rank of $Q/\text{Tor}(Q)$ coincide.

Proof. In Lemma 3.8 above we showed that $\text{Tor}(Q)$ has rank 0. If the rank of Q and the rank of $Q/\text{Tor}(Q)$ are both finite, say of n and m, respectively, then Theorem 3.11 asserts that

$$n = \text{rank}(Q) = \text{rank}(\text{Tor}(Q)) + \text{rank}(Q/\text{Tor}(Q)) = 0 + m = m$$

hence $n = m$ holds.

So we reduce to analyzing the case where at least one of the ranks of Q or $Q/\text{Tor}(Q)$ is infinite. To this end: let $\overline{x}_1, \ldots, \overline{x}_n$ be R-linearly independent elements of $Q/\text{Tor}(Q)$. Then, if there existed $r_1, \ldots, r_n \in R$, not all zero, such that

$$\sum_{i=1}^{n+1} r_i x_i = 0,$$

i.e., if the $x_1, \ldots, x_n$ were R-linearly dependent in Q, then we would require that:

$$\sum_{i=1}^{n+1} \overline{r_i x_i} = \overline{0} \implies \sum_{i=1}^{n+1} r_i \overline{x}_i = \overline{0}$$

which is a contradiction, for the $\overline{x}_i$ were assumed R-linearly independent; hence the $x_1, \ldots, x_n$ must be R-linearly independent in Q; thus the rank of Q is bounded by the rank of $Q/\text{Tor}(Q)$; hence if Q has infinite rank then $Q/\text{Tor}(Q)$ must also have infinite rank.

Now assume that Q has infinite rank; so there exists elements $x_1, x_2, \ldots$ of Q that are R-linearly independent. We claim that $\overline{x}_1, \overline{x}_2, \ldots$ are R-linearly independent in $Q/\text{Tor}(Q)$. If this is not the case, then there exists $r_1, r_2, \ldots \in R$, not all zero, for which

$$\sum_{n=1}^{\infty} r_i \overline{x}_i = \overline{0} \iff \sum_{i=1}^{\infty} \overline{r_i x_i} = \overline{0},$$

hence $\sum_{i=1}^{\infty} r_i x_i \in \operatorname{Tor}(Q)$ holds, to which there exists some non-zero $s \in R$ for which

$$s\left(\sum_{i=1}^{\infty} r_i x_i\right) = \sum_{i=1}^{\infty}(sr_i)x_i = 0$$

But $sr_i \neq 0$ for all i, since R is an integral domain and $s \neq 0$, and not all of the r_i are zero by assumption. Thus we have found an R-linear dependence relation amongst the $x_1, x_2, \ldots$, which is a contradiction; hence the $\overline{x}_1, \overline{x}_2, \ldots$ are R-linearly independent in $Q/\operatorname{Tor}(Q)$; hence $Q/\operatorname{Tor}(Q)$ has infinite rank as well. ■

3.2.2 Some Theorems on Rank

Armed with Proposition 3.7, we can make the following statement about how rank plays nicely with direct sums.

Proposition 3.10 (**Rank of direct sum is sum of ranks**)**.** Let R be an integral domain and let Q and T be R-modules of ranks m and n, respectively. Then the rank of $Q \oplus T$ is $m + n$.

Proof. From Proposition 3.7 above, we know that Q has a submodule R^m such that Q/R^m is a torsion R-module. Likewise, T has a submodule R^n which is free of rank n such that T/R^n is torsion as an R-module. It is clear to see that $R^m \oplus R^n$ is then a submodule of $Q \oplus T$; we also have that $R^m \oplus R^n \cong R^{m+n}$ via Proposition 1.14. Now, from Proposition 1.12, we know

$$(Q \oplus T)/R^{m+n} \cong (Q \oplus T)/(R^m \oplus R^n) \cong (Q/R^m) \oplus (T/R^n)$$

and since the direct sum of torsion R-modules are torsion once more, we have that $Q \oplus T$ is an R-module with a submodule which is free of rank $m + n$ such that the quotient of $Q \oplus T$ with this submodule is torsion. Thus by Proposition 3.7 once more, $Q \oplus T$ has rank $m + n$. ■

There is also a statement to be made regarding the rank of a module and the rank of its corresponding submodule and quotient module; specifically, when the rank of a module, a submodule, and the resulting quotient module are all finite, we have a somewhat natural equation relating the three.

Theorem 3.11 (**The Rank Theorem**)**.** Let R be an integral domain, Q a left R-module, and T a submodule of Q. If the rank of Q is n, the rank of T is r, and the rank of Q/T is s, then $n = r + s$. In other words,

$$\operatorname{rank}(Q) = \operatorname{rank}(T) + \operatorname{rank}(Q/T)$$

Proof. Let $x_1, \ldots, x_s$ be lifts of a maximal R-linearly independent set of elements of Q/T. Let $x_{s+1}, \ldots, x_{s+r}$ be a maximal set of R-linearly independent elements in T. We claim now that $x_1, \ldots, x_{s+r}$ form a set of R-linearly independent elements in Q. Assume this is not true; that is, there exists $t_1, \ldots, t_{s+r} \in R$, not all zero, such that

$$\sum_{i=1}^{s+r} t_i x_i = 0$$

On passing to the quotient module Q/T, each of the x_i with $s+1 \leq i \leq s+r$ become 0 since these elements lie in T by assumption, hence

$$\sum_{i=1}^{s} \overline{t_i x_i} = \overline{0}$$

holds. But we know that the x_i for $1 \leq i \leq s$ are lifts of a maximal R-linearly independent subset of Q/T, that is, we have $\overline{x_i}$ for $1 \leq i \leq s$ are R-linearly independent in Q/T; hence $t_i = 0$ for all $1 \leq i \leq s$. Thus, our original equation becomes

$$\sum_{i=1}^{s+r} t_i x_i = \sum_{i=s+1}^{s+r} t_i x_i = 0$$

in Q. But note that since each of the x_i for $s+1 \leq i \leq s+r$ lie in T, the whole equation above lies in T since T is closed under the ring action of R, since it is a submodule of Q. In particular, the assumption that x_i for $s+1 \leq i \leq s+r$ form a maximal R-linearly independent set in T implies $t_i = 0$ for all $s+1 \leq i \leq s+r$. In particular, all of the $t_i = 0$ for $1 \leq i \leq s+r$, which is a contradiction, for we assumed at least one of the t_i were non-zero. Hence the original set $x_1, \ldots, x_{s+r}$ of elements of Q is indeed R-linearly independent.

We now show that, for any non-zero element $y \in Q$, there exists $\beta \in R \setminus \{0\}$ such that βy may be written as a linear combination of the $x_1, \ldots, x_{s+r}$. Note that for any such $y \in Q \setminus \{0\}$ we have $\overline{y} \in Q/T$, hence the set $\overline{y}, \overline{x_1}, \ldots, \overline{x_s}$ is R-linearly dependent (since we assumed the set $x_1, \ldots, x_s$ was a lift of a maximal R-linearly independent set in Q/T), and hence there exists $t_i \in R$, not all zero, such that

$$\overline{t_1 x_1} + \cdots + \overline{t_s x_s} + \overline{t_{s+1} y} = \overline{0}$$

Letting $\overline{\alpha} = \overline{t_1 x_1} + \cdots + \overline{t_s x_s} + \overline{t_{s+1} y}$, we have that $\alpha \in T$ holds. Now we know that $\alpha, x_{s+1}, \ldots, x_{s+r}$ is an R-linearly dependent set of elements of T (since, by assumption, $x_{s+1}, \ldots, x_{s+r}$ was a maximal R-linearly independent set in T); hence there exists $u_i \in R$, not all zero, such that

$$u_{s+1} x_{s+1} + \cdots + u_{s+r} x_{s+r} + u_{s+r+1} \alpha = 0$$

in T, and hence also in Q. Upon rewriting what we have so far,

$$0 = \left(\sum_{i=s+1}^{s+r} u_i x_i \right) + u_{s+r+1} \alpha = \left(\sum_{i=s+1}^{s+r} u_i x_i \right) + u_{s+r+1} \left(t_{s+1} y + \sum_{i=1}^{s} t_i x_i \right)$$

Rearranging the above equation, we can isolate the term involving y, getting

$$u_{s+r+1}t_{s+1}y = -\left(\sum_{i=s+1}^{s+r} u_i x_i\right) - u_{s+r+1}\left(\sum_{i=1}^{s} t_i x_i\right)$$

In particular, $\beta := u_{s+r+1}t_{s+1}$ is a non-zero element of R such that βy may be written as a linear combination of $x_1, \ldots, x_{s+r}$.

Now consider the submodule $L = Rx_1 + \cdots + Rx_{s+r}$ of Q. Clearly $L \cong R^{s+r}$ as R-modules, so that L is a free R-module of rank $s + r$. Moreover, the quotient Q/L is a torsion R-module, since for any non-zero $y \in Q$, as above, there exists some non-zero $\beta \in R$ for which $\beta y \in L$. By Proposition 3.7, this occurs if and only if Q has rank $s + r$. Therefore, we have $n = s + r$, as desired. ■

3.3 Structure Theorem for Modules over Principal Ideal Domains

In this section we shall work towards what we refer to as the fundamental theorem for finitely generated modules over principal ideal domains; two forms of the fundamental theorem will interest us, and indeed, both have their uses and applications.

Before we can proceed any further, we shall need a few preliminary results regarding rank, as we discussed in the previous section, and freeness. We would like to place an upper bound on the rank of submodules of free modules with finite rank. We would also like to be able to conveniently choose generators for two modules which are in some way related (such as submodules of a free module).

Theorem 3.12 (Submodules of free modules with finite rank over P.I.D.s are free). Let R be a principal ideal domain and let Q be a free R-module of finite rank n. Let T be a submodule of Q. Then T is free of rank m, where $m \leq n$, and there exists a basis $y_1, \ldots, y_n$ of Q such that $a_1y_1, \ldots, a_my_m$ is a basis of T, where $a_1, \ldots, a_m$ are non-zero elements of R such that

$$a_1 \mid a_2 \mid \cdots \mid a_m$$

In other words, we have the divisibility relations: a_1 divides a_2, a_2 divides a_3, and so on, until a_{m-1} divides a_m.

Proof. In the case where $T = 0$ the theorem is trivial, so we assume $T \neq 0$. Consider the collection of all R-module homomorphisms $\varphi : Q \to R$. For each such homomorphism φ, we know that $\varphi(T)$ is an R-submodule of R, hence an ideal of R. Since R is a P.I.D., it follows that $\varphi(T)$ is a principal ideal of R, so that $\varphi(T) = (a_\varphi)$ for some $a_\varphi \in R$. Now consider the collection

$$\Sigma := \{(a_\varphi) \mid \varphi \in \mathrm{Hom}_R(Q, R)\}$$

Since the trivial R-module homomorphism, which sends all of Q to 0 in R, exists always, we have that $(0) \in \Sigma$, to which $\Sigma \neq \varnothing$. By Corollary 3.4, R is Noetherian, hence Theorem 3.3 applies, to which Σ has a maximal element under inclusion. That is, there exists an R-module homomorphism $\psi : Q \to R$ with $\psi(T) = (a_\psi)$ such that (a_ψ) is not properly contained in any other element of Σ. Define $a_1 := a_\psi$. Since $a_1 \in \psi(T) = (a_1)$, we know that there exists an element $y \in T$ such that $\psi(y) = a_1$.

We now prove that $a_1 \neq 0$.

Let $x_1, \ldots, x_n$ be a basis of Q (which exists since Q is free of rank n). We may write $Q \cong \bigoplus_{i=1}^n Rx_i$, and thus may consider the R-module homomorphisms $\pi_i : Q \to R$ which project the ith coordinate of Q, with respect to this basis, to R. Since $T \neq 0$, there exists some i for which $\pi_i(T) \neq 0$, and hence $\pi_i \in \Sigma$ is an element which contains more than just the trivial ideal (0). Since (a_1) is a maximal element in Σ with respect to inclusion, it follows that $(a_1) \neq (0)$, for if this were the case then the ideal $\pi_i(T)$ of R would contain (a_1), clearly impossible. Since $(a_1) \neq (0)$, we thus have $a_1 \neq 0$, as desired.

Now we claim that $a_1 \mid \varphi(y)$ for all $\varphi \in \mathrm{Hom}_R(Q, R)$.

To this end, note that $(a_1, \varphi(y))$ is an ideal of R, hence principal since R is a P.I.D., so we may take a generator $(d) = (a_1, \varphi(y))$. In particular, then, we have that

$$d = ra_1 + s\varphi(y)$$

for some $r, s \in R$. We may now consider the R-module homomorphism

$$\phi := r\psi + s\varphi \in \mathrm{Hom}_R(Q, R)$$

Indeed, we may observe that

$$\phi(y) = r\psi(y) + s\varphi(y) = ra_1 + s\varphi(y) = d$$

Hence, since $y \in T$, we require that $d \in \phi(T)$. Clearly this means $(d) \subseteq \phi(T)$. By its construction, though, we have $(a_1) \subseteq (a_1, \varphi(y)) = (d)$, to which we have a chain of inclusions

$$(a_1) \subseteq (d) \subseteq \phi(T)$$

Note that $\phi(T) \in \Sigma$ holds, and by the maximality of (a_1) in Σ, we thus have $(a_1) = \phi(T)$, and hence $(a_1) = (d)$ by the chain above. In particular, then, we have shown that

$$(a_1) = (d) = (a_1, \varphi(y))$$

which means $a_1 \mid \varphi(y)$, proving our claim.

In particular, we apply the above to the projections $\pi_i : Q \to R$. We have that $a_1 \mid \pi_i(y)$ for all $1 \leq i \leq n$. Set $\pi_i(y) = a_1 b_i$ for some $b_i \in R$, $1 \leq i \leq n$. Using the basis above, define now

$$y_1 := \sum_{i=1}^n b_i x_i$$

Under this, we have $a_1 y_1 = y$ (since y may be written in terms of the basis $x_1, \ldots, x_n$, and then projected along each component). Since $a_1 \in R$, and ψ is an R-module homomorphism, we have

$$a_1 = \psi(y) = \psi(a_1 y_1) = a_1 \psi(y_1)$$

Since R is an integral domain, and $a_1 \neq 0$ as we saw above, this implies $\psi(y_1) = 1$.

We would now like to verify two claims:

$$Q = Ry_1 \oplus \ker \psi$$

$$T = Ra_1 y_1 \oplus (T \cap \ker \psi)$$

Respectively, these will imply that y_1 can be taken as the first element in some basis of Q, and that $a_1 y_1$ can be taken as the first element in some basis for T.

Towards the first claim, let $x \in Q$ be arbitrary. We may write

$$x = \psi(x) y_1 + (x - \psi(x) y_1)$$

Note, however, that

$$\begin{aligned}\psi(x - \psi(x) y_1) &= \psi(x) - \psi(\psi(x) y_1) \\ &= \psi(x) - \psi(x)\psi(y_1) \\ &= \psi(x) - \psi(x) \cdot 1 \\ &= \psi(x) - \psi(x) \\ &= 0\end{aligned}$$

where the second equality holds since $\psi(x) \in R$ is simply a ring element, as $\psi : Q \to R$. In particular, the above shows that $x - \psi(x) y_1$ lies in the kernel of ψ, and hence that x can be written as the sum of an element in Ry_1 (here being $\psi(x) y_1$) with an element in the kernel of ψ. Therefore $Q = Ry_1 + \ker \psi$. To show that the sum is direct, we must prove that $Ry_1 \cap \ker \psi = 0$. If we have $z \in Ry_1 \cap \ker \psi$ then $z \in Ry_1$ holds, to which $z = ry_1$, and since $ry_1 \in \ker \psi$, we require $\psi(ry_1) = 0$. But $\psi(ry_1) = r\psi(y_1) = r \cdot 1 = r$, and hence $r = 0$ is forced, meaning that $z = 0$. Hence the sum is direct, i.e., $Q = Ry_1 \oplus \ker \psi$.

We proceed to the second claim. Since $(a_1) = \psi(T)$, we know that $a_1 \mid \psi(z)$ for all $z \in T$, since in particular $\psi(z) \in \psi(T) = (a_1)$ holds. Thus we may write $\psi(z) = ba_1$, where $b \in R$ is some ring element. Now:

$$z = \psi(z) y_1 + (z - \psi(z) y_1) = ba_1 y_1 + (z - ba_1 y_1)$$

By the same reasoning as in our first claim, we can easily show that the element $z - ba_1 y_1$ lies in the kernel of ψ, as well as T itself (since z and y_1 both lie in T) and hence that z can be written as a sum of elements in Ra_1y_1 and $T \cap \ker \psi$. Thus we have proven

$$T = Ra_1y_1 + (T \cap \ker \psi)$$

The above sum is direct as a consequence of the directness of the sum $Q = Ry_1 \oplus \ker \psi$, a fact which we proved already.

We finally are able to prove the theorem:

For the first portion, showing that T is free of rank m, where $m \leq n$, we induct on the rank m of T. For our base case, if T has rank $m = 0$, then T is a torsion R-module, hence $T = 0$, since free modules are torsion-free, and T is a submodule of the free R-module Q.

Now suppose $m > 0$. Above we showed that

$$T = Ra_1y_1 \oplus (T \cap \ker \psi)$$

Since the rank of Ra_1y_1 is 1, and the rank of T is m, and R here is an integral domain, we apply Proposition 3.10 to write that the rank of $T \cap \ker \psi$ is $m - 1$. By inductive hypothesis, $T \cap \ker \psi$ is a free R-module of rank $m - 1$. Since Ra_1y_1 is free of rank 1, Proposition 1.14 gives that T is a free R-module of rank m.

Now we prove the second portion of the theorem: we induct on the rank n of Q. The base case $n = 0$ is trivial, so assume $n > 0$. We can apply the first portion of the theorem (proved above) to the submodule $\ker \psi$ of Q; in particular, $\ker \psi$ is free of rank $n - 1$. Now, by inductive hypothesis applied to the R-module $\ker \psi$ and its submodule $T \cap \ker \psi$, there exists a basis $y_2, \ldots, y_n$ of $\ker \psi$ such that $a_2y_2, \ldots, a_my_m$ is a basis of $T \cap \ker \psi$ for some $a_2, \ldots, a_m \in R$ with the divisibility conditions $a_1 \mid a_2 \mid \cdots \mid a_m$. Since Ry_1 is free of rank 1, and we have

$$Q = Ry_1 \oplus \ker \psi$$

we can extend the basis $y_2, \ldots, y_n$ for $\ker \psi$ to a basis $y_1, \ldots, y_n$ for Q. Likewise, we have the direct sum

$$T = Ra_1y_1 \oplus (T \cap \ker \psi)$$

and hence the basis $a_2y_2, \ldots, a_my_m$ for $T \cap \ker \psi$ can be extended to a basis $a_1y_1, \ldots, a_my_m$ for T. To complete the induction, it then remains to show that $a_1 \mid a_2$ holds (for we already have that $a_2 \mid a_3 \mid \cdots \mid a_m$).

Define an R-module homomorphism $\varphi : Q \to R$ by $\varphi(y_1) = \varphi(y_2) = 1$ and $\varphi(y_i) = 0$ for all $2 < i \leq n$ (here we are using that $y_1, \ldots, y_n$ is a basis for Q). Then

$$a_1 = a_1 \cdot 1 = a_1\varphi(y_1) = \varphi(a_1y_1)$$

which means $a_1 \in \varphi(T)$, since $a_1 y_1 \in T$. But $a_1 \in \varphi(T)$ implies $(a_1) \subseteq \varphi(T)$ as ideals in R; by the maximality of (a_1) in Σ, as before, we require then that $(a_1) = \varphi(T)$. Since, in addition, we have

$$a_2 = a_2 \cdot 1 = a_2 \varphi(y_2) = \varphi(a_2 y_2)$$

so that $a_2 \in \varphi(T) = (a_1)$ holds, we have $a_2 \in (a_1)$; in other words, that $a_1 \mid a_2$. This completes the induction for the second portion, and hence concludes our proof of the theorem. ■

The statement of Theorem 3.12 is an important one, both in its own right and in terms of its usefulness in proving a fundamental structure theorems for finitely generated modules over P.I.D.s.

3.3.1 Existence of the Invariant Factor Form

In this section, we prove the existence portion of the fundamental theorem in its so-called invariant factor form. In this way, we shall prove that all finitely generated modules over principal ideal domains are isomorphic to a direct sum of finitely many cyclic modules. That is, we can decompose finitely generated modules over P.I.D.s into direct sums of the simplest modules possible, which will serve us wonderfully in the theory to come.

The existence theorem is as follows:

Theorem 3.13 (**Existence of the Invariant Factor Form**)**.** Let R be a principal ideal domain and let Q be a finitely generated R-module. Then Q is isomorphic to a finite direct sum of cyclic R-modules; that is,

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

for some integer $r \geq 0$ and non-zero, non-unit elements $a_1, \ldots, a_m$ of R which satisfy the following divisibility condition:

$$a_1 \mid a_2 \mid \cdots \mid a_m$$

Proof. The R-module Q is finitely generated, so we may take $x_1, \ldots, x_n$ to be a set of generators for Q. In addition, we may assume that this set of generators is minimal with respect to the cardinalities of generating sets. Now let R^n be the free R-module of rank n, with $b_1, \ldots, b_n$ a set of generators. Define an R-module homomorphism on generators:

$$\pi : R^n \longrightarrow Q$$

$$\pi(b_i) = x_i$$

Immediately, we know π is surjective, since Q is generated by the x_i. By the first isomorphism theorem we thus have $R^n/\ker\pi \cong Q$.

Since R^n is a free R-module of finite rank n, where here R is a P.I.D., we can apply Theorem 3.12 to R^n and its submodule $\ker\pi$. In particular, we may choose a basis $y_1, \dots, y_n$ for R^n such that $a_1y_1, \dots, a_my_m$ is a basis of $\ker\pi$ for some elements $a_i \in R$, $1 \leq i \leq m$, with $a_1 \mid a_2 \mid \cdots \mid a_m$. Thus we have:

$$Q \cong R^n/\ker\pi \cong \left(\bigoplus_{i=1}^{n} Ry_i\right) \Big/ \left(\bigoplus_{i=1}^{m} Ra_iy_i\right)$$

In order to work with the module on the right hand side of the above, we must consider the map:

$$\Phi : \bigoplus_{i=1}^{n} Ry_i \to \left(\bigoplus_{i=1}^{m} (R/(a_i))\right) \oplus R^{n-m}$$

$$(r_1y_1, \dots, r_ny_n) \longmapsto (\overline{r_1}, \dots, \overline{r_m}, r_{m+1}, \dots, r_n)$$

where $\overline{r_i}$ denotes the ring element r_i taken modulo the ideal (a_i) in the components above. Indeed, the map Φ above is a special case of Proposition 1.13: it is a surjective R-module homomorphism with kernel

$$\ker\Phi = \bigoplus_{i=1}^{m} Ra_iy_i$$

Thus, by the first isomorphism theorem once more, we have:

$$\left(\bigoplus_{i=1}^{n} Ry_i\right) \Big/ \left(\bigoplus_{i=1}^{m} Ra_iy_i\right) \cong \left(\bigoplus_{i=1}^{m} (R/(a_i))\right) \oplus R^{n-m}$$

Since we found above that Q is isomorphic as an R-module to the module on the left hand side above, we can set $r := n - m$ and see that:

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

holds, which was precisely the desired decomposition of Q. ■

Note that in Theorem 3.13 above we did *not* prove that the decomposition is unique. This will come later, after we develop the requisite tools. What we can say at this point, however, is that the somewhat strange divisibility condition on the ring elements in Theorem 3.13 is precisely what will give us the desired uniqueness statement.

To justify Theorem 3.13 being called the existence portion of the invariant factor form, it would do well for us to provide a definition for exactly what an invariant factor might be.

Definition 3.14 (Invariant factors and free rank). Let R be a P.I.D. and Q a finitely generated R-module. Then the integer $r \geq 0$ in Theorem 3.13 is called the *free rank* of Q. In addition, the elements $a_1, \ldots, a_m$ satisyfing the divisibility conditions are called the *invariant factors* of Q.

As we mentioned before, we have not yet proved that the decomposition in Theorem 3.13 is unique; that is, we have not proved that a given free rank and set of invariant factors uniquely determine an R-module Q. Thus we cannot quite say that there exists one set of invariant factors (i.e., *the* invariant factors of Q), we must instead refer to any invariant factors as *a* set of invariant factors for Q.

Now we explore some corollaries to Theorem 3.13.

Corollary 3.15 (Torsion-free if and only if free (over a P.I.D.)). Let R be a P.I.D. and let Q be a finitely generated R-module. Then Q is a torsion-free R-module if and only if Q is a free R-module.

Proof. For any such finitely generated R-module Q, Theorem 3.13 gives us a decomposition

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

Note that, for any non-zero ring element $a \in R$, we have that $R/(a)$ is a torsion R-module (indeed, since every element is annihilated by $a \in R$).

In this way, if we assume that Q is torsion-free, then $a_i = 0$ is required for all $1 \leq i \leq m$, in which case:

$$Q \cong R^r \oplus R/(0) \oplus \cdots \oplus R/(0) \cong R^r \oplus R \oplus \cdots \oplus R \cong R^{r+m}$$

and hence Q is a free R-module. The converse is trivial, for free modules are always torsion-free; hence we have the corollary. ■

Corollary 3.16 (Torsion if and only if free rank 0). Let R be a P.I.D. and Q a finitely generated R-module. Then

$$\mathrm{Tor}(Q) \cong R/(a_1) \oplus \cdots \oplus R/(a_m)$$

where $a_1, \ldots, a_m$ are as in the decomposition in Theorem 3.13. In particular, Q is a torsion R-module if and only if $r = 0$, i.e., if and only if Q has free rank 0.

Moreover, in the case where Q is torsion, the annihilator of Q is precisely the ideal (a_m); so in symbols we have $\mathrm{Ann}_R(Q) = (a_m)$.

Proof. The first statement of the corollary is immediate via the decomposition in Theorem 3.13. For the last statement, note that for any non-zero $a \in R$, the annihilator of the torsion module $R/(a)$ is precisely (a). Since the divisibility conditions on the a_i give $a_1 \mid \cdots \mid a_m$, it is clear that $(a_1) \subseteq \cdots \subseteq (a_m)$, and hence that the ideal (a_m) annihilates each element of Q. ■

3.3.2 Existence of the Elementary Divisor Form

The invariant factor form for the fundamental structure theorem for finitely generated modules over principal ideal domains is certainly useful; more, however, can be done in regards to its result. By this we mean that the Chinese Remainder Theorem for modules can be applied to the cyclic modules appearing in the decomposition of Theorem 3.13 to decompose them even further. Indeed, we can actually decompose such a module into a direct sum of cyclic modules whose annihilators are as simple as can be. By simple as can be, we mean that the annihilators can be forced to be either (0), the zero ideal, or alternatively be generated by powers of prime elements in the principal ideal domain.

The process above gives us another decomposition for finitely generated modules over principal ideal domains, which we shall see is also unique.

Theorem 3.17 (**Existence of the Elementary Divisor Form).** Let R be a P.I.D. and let Q be a finitely generated R-module. Then Q is the direct sum of a finite number of cyclic R-modules whose annihilators are either (0) or generated by powers of prime elements in R. That is, we have

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

where $t \geq 0$ is an integer and $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ are positive powers of not necessarily distinct prime elements $p_1, \ldots, p_t$ in R.

Proof. We begin by letting $a \in R$ be arbitrary. Recall that P.I.D.s are U.F.D.s (unique factorization domains), and hence we can write

$$a = up_1^{\alpha_1} \cdots p_s^{\alpha_s}$$

where the p_i are distinct primes in R, the α_i are positive integers, and u is some unit in R. Such a factorization is unique up to units, which means that the ideals $(p_i^{\alpha_i})$, $1 \leq i \leq s$, are uniquely defined by the factorization (since principal ideals are equal up to multiplication by units).

Note that for $i \neq j$, we have $(p_i^{\alpha_i}) + (p_j^{\alpha_j}) = R$, since the sum of these two ideals is the principal ideal generated by their greatest common divisor, which is 1 since $\gcd(p_i, p_j) = 1$ as p_i and p_j are distinct primes in R. This shows that each of the ideals $(p_i^{\alpha_i})$, $1 \leq i \leq s$, are pairwise comaximal. The intersection of principal ideals is the principal ideal generated by the least common multiple of the generators for each ideal; so in our case, we have:

$$\bigcap_{i=1}^{s}(p_i^{\alpha_i}) = (\operatorname{lcm}(p_1, \ldots, p_s)) = (a)$$

Applying the Chinese Remainder Theorem for ideals, one obtains:

$$R/(a) \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_s^{\alpha_s})$$

where the isomorphism above is an isomorphism of rings and also of R-modules.

With this result above, let Q be a finitely generated R-module. Then Theorem 3.13 gives a decomposition

$$Q \cong R^r \oplus \left(\bigoplus_{i=1}^{n} R/(a_i) \right)$$

For each $1 \leq i \leq n$, the R-module $R/(a_i)$ admits a decomposition as we have shown in the first portion of the proof. Extending this for each such $R/(a_i)$, we obtain the desired decomposition of Q into a direct sum of cyclic modules whose annihilators are generated by powers of primes in R. ■

Note the usage of the existence of the invariant factor form of the fundamental theorem in the proof of the existence of the elementary divisor form.

Proceeding directly, we give a definition for so-called elementary divisors.

Definition 3.18 (Elementary divisors). Let R be a P.I.D. and let Q be a finitely generated R-module as in Theorem 3.17. Up to multiplication by units in R, the prime powers $p_1^{\alpha_1}, \dots, p_s^{\alpha_s}$ appearing in the theorem are called the *elementary divisors* of Q.

After the following brief subsection, we shall prove that the elementary divisors of a finitely generated module over a P.I.D. uniquely determine such a module. That is, the decomposition in Theorem 3.17 is unique.

3.3.3 The Primary Decomposition Theorem

We take a slight detour from our main development to cover an important theorem which, in some ways, extends the results we have obtained so far for finitely generated modules over principal ideal domains to those modules which are possibly non-finitely generated.

Let R be a P.I.D. and suppose Q is a finitely generated R-module; referring to the distinct primes $p_1, \dots, p_s$ appearing in the decomposition of Theorem 3.17, we can combine all the cyclic modules corresponding to the same prime p_i (recall that in that theorem the primes were not required to be distinct). Let T_i denote the collection of elements of Q which are annihilated by some power of p_i. We know that each T_i is a submodule of Q via Proposition 1.10. Moreover, each T_i is equal to a direct sum of precisely the cyclic modules in the decomposition which correspond to the same prime p_i. As such, we can write

$$Q = \bigoplus_{i=1}^{s} T_i$$

as a decomposition for Q. The power of this seemingly minor result is that it can be extended to work for potentially non-finitely generated modules.

Theorem 3.19 (The Primary Decomposition Theorem). Let R be a P.I.D. and let Q be a (possibly non-finitely generated) non-zero torsion R-module with non-zero annihilator $\operatorname{Ann}_R(Q) = (a)$ for some $a \in R$. Suppose the prime factorization of a in R is

$$a = up_1^{\alpha_1} \cdots p_n^{\alpha_n},$$

and for each $i \in \{1, \dots, n\}$ set $T_i := \{x \in Q \mid p_i^{\alpha_i} x = 0\}$. Then each T_i is the submodule of Q consisting of all elements of Q annihilated by some power of p_i, and we have $\operatorname{Ann}_R(T_i) = (p_i^{\alpha_i})$. We then have a decomposition

$$Q \cong \bigoplus_{i=1}^{n} T_i.$$

Moreover, if Q is finitely generated then each T_i is the direct sum of finitely many cyclic modules whose annihilators are divisors of $p_i^{\alpha_i}$.

Proof. If Q is such an R-module then indeed, since P.I.D.s are U.F.D.s, we have a prime factorization of the generator for the annihilator of Q into distinct prime powers, so that much is clear. Moreover, the sets T_i for each i are indeed submodules by Proposition 1.10, and have annihilators generated by $p_i^{\alpha_i}$.

The decomposition statement in the theorem is clear in the case where Q is finitely generated, for instance via Theorem 3.17, the existence of the elementary divisor form. In the case where Q is non-finitely generated, we can use the fact that R is a P.I.D., and so for $i \neq j$ we have that the ideals $(p_i^{\alpha_i})$ and $(p_j^{\alpha_j})$ relatively prime; hence, using the Chinese Remainder Theorem for modules, the decomposition result follows immediately. ■

Definition 3.20 (Primary components). Let R be a P.I.D. and let Q be a non-zero torsion R-module. Then the submodule T_i of Theorem 3.19 are called the *p_i-th primary component* of Q.

Under Definition 3.20, we make note that the elementary divisors of a finitely generated module over a P.I.D. are simply the invariant factors of the primary components of that module.

3.3.4 Uniqueness of the Elementary Divisor Form

We now begin the process of proving the uniqueness statement for the elementary divisor form of the fundamental structure theorem for finitely generated modules over principal ideal domains. In effect, we shall show that the elementary divisors, as in Definition 3.18, corresponding to such a finitely generated module uniquely determine the isomorphism class containing that module.

Before we can undertake the statement of interest, we introduce several lemmas. For the first, recall that P.I.D.s have Krull dimension 1; that is, all prime ideals are maximal ideals.

Lemma 3.21. Let R be a P.I.D., p be a prime in R, and $k = R/(p)$. Then, for any integer $n \geq 1$,

$$R^n/pR^n \cong k^n$$

is an isomorphism of R-modules.

Proof. We can extend the canonical projection $R \longrightarrow R/(p) = k$ via the map

$$\pi : R^r \longrightarrow (R/(p))^n = k^n$$

$$(r_1, \ldots, r_n) \longmapsto (\overline{r_1}, \ldots, \overline{r_n})$$

where $\overline{r_i}$ denotes reduction modulo the ideal (p). It is immediate that π is a surjective R-module homomorphism, with kernel consisting of all n-tuples of elements of R which are divisible by p, i.e., $\ker \pi = pR^n$. The first isomorphism theorem then provides the desired isomorphism of R-modules. ■

Lemma 3.22. Let R be a P.I.D., p a prime in R, and $k = R/(p)$. For any non-zero element $a \in R$, let $Q := R/(a)$. There are two cases: either the prime p divides a or p does not divide a. If the former is true, then $Q/pQ \cong k$. If the latter is true, then $Q/pQ \cong 0$.

Proof. We first note that $pQ = p(R/(a))$ is the image of the ideal (p) in the quotient ring $R/(a)$ under the canonical projection $R \longrightarrow R/(a)$. As such, we have that

$$p(R/(a)) = ((p) + (a))/(a).$$

Since R is a P.I.D., the ideal $(p) + (a) = (d)$, where d is the greatest common divisor of p and a; hence if $p \mid a$ then $d = p$, in which case $p(R/(a)) = (p)/(a)$, and so

$$Q/pQ = \frac{R/(a)}{p(R/(a))} = \frac{R/(a)}{(p)/(a)} \cong R/(p) = k$$

where the isomorphism above comes from the third isomorphism theorem for modules.

If, on the other hand, we have $p \nmid a$, then the greatest common divisor of p and a is $d = 1$, since p is a prime in R; hence $(p) + (a) = R$, and so $p(R/(a)) = R/(a)$, to which

$$Q/pQ = \frac{R/(a)}{p(R/(a))} = \frac{R/(a)}{R/(a)} \cong 0.$$

■

Lemma 3.23. Let R be a P.I.D., p a prime in R, and $k = R/(p)$. For any ring elements $a_1, \ldots, a_n \in R$, with each a_i divisible by p, we have $Q/pQ \cong k^n$, where $Q = \bigoplus_{i=1}^{n} R/(a_i)$.

Proof. For each $R/(a_i)$ appearing as a constituent in the direct sum for Q we have $p \mid a_i$, so by Lemma 3.22 we have

$$\frac{R/(a_i)}{p(R/(a_i))} \cong k.$$

Extending the above for Q, and using Proposition 1.13, we find that

$$Q/pQ = \frac{\bigoplus_{i=1}^n R/(a_i)}{p\left(\bigoplus_{i=1}^n R/(a_i)\right)} = \frac{\bigoplus_{i=1}^n R/(a_i)}{\bigoplus_{i=1}^n p(R/(a_i))} \cong \bigoplus_{i=1}^n \frac{R/(a_i)}{p(R/(a_i))} = \bigoplus_{i=1}^n k = k^n,$$

which was the desired statement. ■

With these three lemmas in tow, we state and prove the promised uniqueness.

Theorem 3.24 (Uniqueness of the Elementary Divisor Form). Let R be a P.I.D.. Then two finitely generated R-modules are isomorphic if and only if they share the same free rank and the same list of elementary divisors.

Proof. One direction of the proof is trivial; that is, if two finitely generated modules share the same free rank and list of elementary divisors, then they are isomorphic via the isomorphism in the existence proof of Theorem 3.17. Thus we concern ourselves with the converse statement.

Suppose Q_1 and Q_2 are isomorphic; this means there exists some R-module isomorphism between them, and any such isomorphism is, in particular, an isomorphism on the torsion submodules of Q_1 and Q_2; i.e., $\text{Tor}(Q_1) \cong \text{Tor}(Q_2)$ holds. Using the decomposition in Theorem 3.13, and Corollary 3.16, we thus have

$$R^{r_1} \cong Q_1/\text{Tor}(Q_1) \cong Q_2/\text{Tor}(Q_2) \cong R^{r_2}$$

where r_1 and r_2 denotes the free rank of Q_1 and Q_2, respectively. Now let p be any non-zero prime element of R. The fact that $R^{r_1} \cong R^{r_2}$, combined with Lemma 3.21, gives us the isomorphism

$$k^{r_1} \cong R^{r_1}/pR^{r_1} \cong R^{r_2}/pR^{r_2} \cong k^{r_2}$$

where k is the field $R/(p)$. By vector space theory, an isomorphism of an r_1-dimensional k-vector space with an r_2-dimensional k-vector space implies that $r_1 = r_2$; hence Q_1 and Q_2 share the same free rank.

What remains is to show that Q_1 and Q_2 share the same list of elementary divisors. To this end, since above we showed that the free ranks of Q_1 and Q_2 coincide, it suffices to show that $\text{Tor}(Q_1)$ and $\text{Tor}(Q_2)$ share the same list of elementary divisors; i.e., we may reduce to the case where both Q_1 and Q_2 are torsion R-modules.

To prove the desired result, then, we need only take some fixed non-zero prime p of R, and show that the elementary divisors which are a power of p are the same for both Q_1 and Q_2.

Since we have $Q_1 \cong Q_2$, we know that the p-primary submodule (recall Definition 3.20) of Q_1, i.e., the direct sum of the cyclic factors whose elementary divisors are powers of p, is isomorphic to the p-primary submodule of Q_2. This is because these are the submodules of elements which are annihilated by some power of p, a property which is preserved by the isomorphism between Q_1 and Q_2.

Therefore, in view of the Primary Decomposition Theorem (Theorem 3.19), which allows us to decompose modules into their primary components, we may reduce our inquiry to the case of proving that if two finitely generated modules Q_1 and Q_2 which have annihilator a power of p are isomorphic, then they have the same elementary divisors. As a special case, this will show that the primary components of Q_1 and Q_2 must share the same elementary divisors.

We prove this by induction on the power of p in the annihilator of Q_1, which suffices since $Q_1 \cong Q_2$ implies that $\mathrm{Ann}_R(Q_1) \cong \mathrm{Ann}_R(Q_2)$, i.e., these modules have isomorphic annihilators. We can write $\mathrm{Ann}_R(Q_1) = (p^n)$ since R is a P.I.D.. For our base case, if $n = 0$ then $\mathrm{Ann}_R(Q_1) = (p^0) = (1) = R$, and hence $Q_1 = 0$, and so too must we have $Q_2 = 0$.

Now suppose $n > 0$; the modules Q_1 and Q_2 must then have non-trivial lists of elementary divisors by Theorem 3.17. Since Q_1 has annihilator (p^n), we can write

$$Q_1 \cong \underbrace{R/(p) \oplus \cdots \oplus R/(p)}_{n \text{ times}} \oplus R/(p^{\alpha_1}) \oplus \cdots \oplus R/(p^{\alpha_s})$$

where $2 \leq \alpha_1 \leq \cdots \leq \alpha_s$ are some integers. For brevity, we denote the ordered list of elementary divisors of Q_1 by $\mathcal{E}(Q_1)$, so in this new notation:

$$\mathcal{E}(Q_1) = (\underbrace{p, \ldots, p}_{n \text{ times}}, p^{\alpha_1}, \ldots, p^{\alpha_s})$$

Since each of the modules in the decomposition for Q above are cyclic, we are at liberty to give them generators, say $x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+s}$ with annihilators $(p), \ldots, (p), (p^{\alpha_1}), \ldots, (p^{\alpha_s})$, respectively. So now:

$$Q \cong Rx_1 \oplus \cdots \oplus Rx_n \oplus Rx_{n+1} \oplus \cdots \oplus Rx_{n+s}$$

Given the above, we now consider the submodule pQ_1 of Q_1. We have

$$\begin{aligned} pQ_1 &\cong p(Rx_1 \oplus \cdots \oplus Rx_n \oplus Rx_{n+1} \oplus \cdots \oplus Rx_{n+s}) \\ &= p(Rx_1) \oplus \cdots \oplus p(Rx_n) \oplus p(Rx_{n+1}) \oplus \cdots p(Rx_{n+s}) \\ &= 0 \oplus \cdots \oplus 0 \oplus Rpx_{n+1} \oplus \cdots \oplus Rpx_{n+s} \\ &= Rpx_{n+1} \oplus \cdots \oplus Rpx_{n+s} \end{aligned}$$

Which follows since (p) is the annihilator of the cyclic modules generated by the $x_1, \dots, x_n$ by our assumption. Since the annihilators of the $x_{n+1}, \dots, x_{n+s}$ were taken to be $(p^{\alpha_1}), \dots, (p^{\alpha_s})$, respectively, it follows that the annihilators of the cyclic modules generated by $px_{n+1}, \dots, px_{n+s}$ are $(p^{\alpha_1 - 1}), \dots, (p^{\alpha_s - 1})$, respectively. Thus, letting $\mathcal{E}(pQ_1)$ denote the list of elementary divisors, we have

$$\mathcal{E}(pQ_1) = (p^{\alpha_1 - 1}, \dots, p^{\alpha_s - 1}).$$

Returning to Q_2, and using the same $\mathcal{E}$ notation for elementary divisors, we have, for some $m \in \mathbb{Z}^+$,

$$\mathcal{E}(Q_2) = (\underbrace{p, \dots, p}_{m \text{ times}}, p^{\beta_1}, \dots, p^{\beta_t}),$$

where $2 \le \beta_1 \le \cdots \le \beta_t$ are some integers. In a process analogous to the above carried out for Q_1, we can find that

$$\mathcal{E}(pQ_2) = (p^{\beta_1 - 1}, \dots, p^{\beta_t - 1}).$$

Since $Q_1 \cong Q_2$, we must have $pQ_1 \cong pQ_2$; here, also, we note that the power of p in the annihilator of pQ_1 is one less than the power of p in the annihilator of Q_1. Thus we may apply our inductive hypothesis: the elementary divisors for pQ_1 are the same as the elementary divisors of pQ_2, i.e., $\mathcal{E}(pQ_1) = \mathcal{E}(pQ_2)$, and hence $s = t$ and $\alpha_i = \beta_i$ for all $1 \le i \le s$.

Furthermore, since $Q_1/pQ_1 \cong Q_2/pQ_2$ holds via the isomorphism $Q_1 \cong Q_2$, we may apply Lemma 3.23 to write that

$$k^{n+s} \cong Q_1/pQ_1 \cong Q_2/pQ_2 \cong k^{m+t}.$$

By dimension considerations, we thus have $n + s = m + t$, and since $s = t$ was found already, we get $n = m$. Thus $\mathcal{E}(Q_1) = \mathcal{E}(Q_2)$; the modules Q_1 and Q_2 have the same list of elementary divisors. ■

3.3.5 Uniqueness of the Invariant Factor Form

We now exhibit a proof of the uniqueness of the invariant factor form of the fundamental theorem, Theorem 3.13. In our proof, we will use the uniqueness statement for the elementary divisor form, Theorem 3.24, which we proved in the previous subsection.

Theorem 3.25 (Uniqueness of the Invariant Factor Form). Let R be a P.I.D.. Then two finitely generated R-modules Q_1 and Q_2 are isomorphic if and only if they share the same free rank and the same list of invariant factors.

Proof. One direction is trivial; if Q_1 and Q_2 share the same list of invariant factors, then they are isomorphic by Theorem 3.13, the existence portion of the invariant factor form. Thus we concern ourselves with the converse statement.

Suppose $Q_1 \cong Q_2$. In our proof of Theorem 3.24, we showed that Q_1 and Q_2 must necessarily share the same free rank, so we do not repeat the argument here. Thus it remains to show that Q_1 and Q_2 share the same list of invariant factors.

Let $a_1, \dots, a_n$ be a list of invariant factors for Q_1, with divisibility condition $a_1 \mid \cdots \mid a_n$. We can obtain a list of elementary divisors for Q_1 by taking prime power factors of these elements; i.e., for each a_i, we can obtain a decomposition for $R/(a_i)$ as in the proof of Theorem 3.17, and then combine all prime powers appearing in the decomposition into a list of elementary divisors for Q_1.

Note that, in this way, the divisiblity condition on the invariant factors implies that a_n is the product of the largest of the prime powers among these elementary divisors. If we remove the factors for a_m, then a_{m-1} is the product of the largest prime powers among the remaining elementary divisors, and so on until we reach a_1.

Now let $b_1, \dots, b_m$ be a list of invariant factors for Q_2. We can perform an analogous process to that above, obtaining a list of elementary divisors for Q_2. By Theorem 3.24, the uniqueness proof for the elementary divisor form, the fact that $Q_1 \cong Q_2$ implies that Q_1 and Q_2 share the same list of elementary divisors. Thus $a_n = b_m$, since both are the product of the largest prime powers among the common list of elementary divisors, and so also $a_{n-1} = b_{m-1}$ since these are the product of the largest prime powers of the elementary divisors once the factors corresponding to $a_n = b_m$ have been removed. Continuing this process, we eventually arive at $a_1 = b_1$; the lists of invariant factors are the same. ■

3.3.6 Main Statement, Corollaries, Counterexamples

Now we take a momentary reprieve from our development to reiterate the main statement of the structure theorem for finitely generated modules over P.I.D.s which we have worked so hard to obtain. We also discuss several corollaries of the theorem, foremost among them the fundamental theorem of finitely generated abelian groups. We then present some worked out examples employing the structure theorem.

First, we have a complete statement of the existence and uniqueness of the invariant factor form as follows:

Theorem 3.26 (**Structure Theorem for Modules over P.I.D.s**)**.** Let R be a P.I.D.. Then for any finitely generated R-module Q, we have an isomorphism

$$Q \cong R^n \oplus \mathrm{Tor}(Q), \tag{1}$$

of R-modules, where $n \geq 0$ is the free rank of Q and $\mathrm{Tor}(Q)$ is the torsion submodule of Q. In particular, Q is free if and only if Q is torsion-free, and Q is torsion if and only if Q has free rank 0.

In addition, we can decompose the torsion submodule of Q in two different ways:

1. The **invariant factor form** of the decomposition for Q is that given by

$$\mathrm{Tor}(Q) \cong \bigoplus_{i=1}^{m} R/(a_i),$$

where the $a_1, \ldots, a_m$ are the invariant factors of Q; these are non-zero elements of R which are not units and which satisfy the divisibility relations

$$a_1 \mid a_2 \mid \cdots \mid a_m.$$

2. The **elementary factor form** of the decomposition for Q is given by

$$\mathrm{Tor}(Q) \cong \bigoplus_{i=1}^{t} R/(p_i^{\alpha_i}),$$

where the $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ are the elementary divisors of Q; these are powers of not necessarily distinct prime elements of the ring R.

Moreover, the two decompositions for Q above are unique in that Q is isomorphic to another finitely generated R-module T if and only if Q and T share the same free rank, list of invariant factors, and list of elementary divisors.

Proof. For the invariant factor form we have Theorem 3.13 and Theorem 3.25, which, respectively, give the existence and uniqueness of the invariant factor form decomposition. For the elementary divisor form we have Theorem 3.17 and Theorem 3.24, which give existence and uniqueness, respectively. ∎

Before proceeding to the corollaries of the structure theorem, we exhibit a counterexample to show that such theorems do not extend to the case of non-finitely generated modules over P.I.D.s.

Example 3.27 (Non-finitely generated counterexample to structure theorem). In this example we exhibit an infinitely generated module over $\mathbb{Z}$ whose torsion submodule is not a direct summand. This will illustrate why the assumption of finite generation is crucial in the structure theorem for modules over P.I.D.s.

As stated above, we shall consider the principal ideal domain $\mathbb{Z}$ and the $\mathbb{Z}$-module:

$$M := \prod_{p \text{ a prime}} \mathbb{Z}/(p).$$

It is immediate that M is not finitely generated as a $\mathbb{Z}$-module. First we ascertain the torsion submodule of M; specifically, we shall prove that

$$\operatorname{Tor}(M) = \bigoplus_{p \text{ a prime}} \mathbb{Z}/(p) \tag{2}$$

holds, and then also that $M \neq \operatorname{Tor}(M)$.

Towards this goal: one containment is immediate, for if $\mathbf{x}$ lies in the direct sum on the right hand side of Equation 2 above then $\mathbf{x}$ may be written as $\mathbf{x} = (a_p \pmod{p} \mid p \text{ a prime})$, and we know $a_p \not\equiv 0 \pmod{p}$ holds for only finitely many primes in $\mathbb{Z}$ by the fact that the sum is direct; let these primes be $p_1, \dots, p_k$. Then, taking the product $n := p_1 \cdots p_k \in \mathbb{Z}$, we see that

$$n\mathbf{x} = (na_p \pmod{p} \mid p \text{ a prime}) = (0 \pmod{p} \mid p \text{ a prime}) = \mathbf{0}$$

since each non-zero a_p is killed by some p showing up in the product n; hence $\mathbf{x}$ lies in $\operatorname{Tor}(M)$.

For the reverse containment, if $\mathbf{x} \in \operatorname{Tor}(M)$ then we can write $\mathbf{x} = (a_p \pmod{p} \mid p \text{ a prime})$, and that there exists some non-zero integer $k \in \mathbb{Z}$ for which $k\mathbf{x} = \mathbf{0}$; that is, we have

$$k\mathbf{x} = (ka_p \pmod{p} \mid p \text{ a prime}) = (0 \pmod{p} \mid p \text{ a prime}) = \mathbf{0}$$

In view of the above, note that for any prime p which does not divide the integer k, we require $a_p \equiv 0 \pmod{p}$, following since $k\mathbf{x} = \mathbf{0}$ implies that $ka_p \equiv 0 \pmod{p}$ for all primes p. Since k is an integer, there are only finitely many primes which divide k, and hence only finitely many non-zero components in $\mathbf{x}$; hence $\mathbf{x}$ lies in the direct sum on the right hand side of Equation 2.

Now it is clear that $M \neq \operatorname{Tor}(M)$ since the latter is equal to the direct sum $\bigoplus_p \mathbb{Z}/(p)$, while the former is equal to $\prod_p \mathbb{Z}/(p)$, and these two $\mathbb{Z}$-modules are not equal since there are infinitely many primes in $\mathbb{Z}$; take, for example, the element $\mathbf{1} = (1 \pmod{p} \mid p \text{ a prime})$ of M, which does not lie in $\operatorname{Tor}(M)$.

With the above in mind, we now prove that $M \neq \operatorname{Tor}(M) \oplus N$ for any $\mathbb{Z}$-submodule N of M, i..e, that M cannot be written as a direct sum of its torsion submodule and any other submodule.

So assume, for contradiction, that $M = \operatorname{Tor}(M) \oplus N$. Then $N \cong M/\operatorname{Tor}(M)$ holds, and so, in particular, M has a submodule isomorphic to $M/\operatorname{Tor}(M)$. Our contradiction will be derived through showing that all submodules of M have a certain property, one which $M/\operatorname{Tor}(M)$ lacks.

The property in question is one inherited from M: note that

$$\bigcap_{p \text{ a prime}} pM = 0,$$

holds, which should be clear, for the pth coordinate of any element $\mathbf{x}$ which lies in the intersection on the left hand side above must be $0 \pmod{p}$, and this holds for all p. In particular, we require that

$$\bigcap_{p \text{ a prime}} pN = 0$$

holds for all submodules N of M. Now, as we stated prior, we claim that

$$\bigcap_{p \text{ a prime}} p\,(M/\mathrm{Tor}(M)) \neq 0,$$

which shall give us a contradiction to the original decomposition assumed above.

Let $\mathbf{y} := (1 \pmod{p} \mid p \text{ a prime}) \in M$. Firstly, we see that $\mathbf{y} \notin \mathrm{Tor}(M)$ since there are infinitely many non-zero coordinates of $\mathbf{y}$; hence $\overline{\mathbf{y}} \neq \overline{\mathbf{0}}$ in $M/\mathrm{Tor}(M)$. Now we show that

$$\overline{\mathbf{y}} \in \bigcap_{p \text{ a prime}} p\,(M/\mathrm{Tor}(M))\,.$$

To see this, fix some prime p. For every prime $q \neq p$ we know there exists $z_q \in \mathbb{Z}/(q)$ such that $z_q p \equiv 1 \pmod{q}$; in other words, every p is invertible modulo q for every prime $q \neq p$. Define $z_p = 0 \pmod{p}$. Now we define

$$\mathbf{z} := (z_q \quad (\mathrm{mod}\ q) \mid q \text{ a prime}),$$

which is an element of M. We can see that $p\mathbf{z}$ has $1 \pmod{q}$ in every qth coordinate and has $0 \pmod{p}$ in the pth coordinate. Thus we can write

$$\mathbf{y} = p\mathbf{z} + \mathbf{w}$$

where $\mathbf{w}$ is the element of M having $0 \pmod{q}$ in the qth coordinate and $1 \pmod{p}$ in the pth coordinate for all primes $q \neq p$. Now, of course, we see that $\mathbf{w} \in \mathrm{Tor}(M)$ holds, for instance since $p\mathbf{w} = \mathbf{0}$; hence $\overline{\mathbf{w}} = \overline{\mathbf{0}}$ in $M/\mathrm{Tor}(M)$. Now we have:

$$\overline{\mathbf{y}} = \overline{p\mathbf{z} + \mathbf{w}} = \overline{p\mathbf{z}} + \overline{\mathbf{w}} = \overline{p\mathbf{z}} + \overline{\mathbf{0}} = \overline{p\mathbf{z}} = p\overline{\mathbf{z}}$$

in $M/\mathrm{Tor}(M)$. Since $p\overline{\mathbf{z}} \in p(M/\mathrm{Tor}(M))$ holds, so too must $\overline{\mathbf{y}} \in p(M/\mathrm{Tor}(M))$ hold.

Note that the process above can be repeated the same way for each prime p, and so we must have that $\overline{\mathbf{y}}$ lies in $p(M/\mathrm{Tor}(M))$ for all p, hence

$$\overline{\mathbf{0}} \neq \overline{\mathbf{y}} \in \bigcap_{p \text{ a prime}} p\,(M/\mathrm{Tor}(M))$$

which is a contradiction, for the intersection on the right above is trivial as we stated before. In particular, no such decomposition $M = \mathrm{Tor}(M) \oplus N$ exists for any submodule N of M.

We present another counterexample. This time, we shall show that a torsion-free module over a P.I.D. that is non-finitely generated need not be free.

Example 3.28 (**Non-finitely generated torsion-free over P.I.D. not free**)**.** Consider the ring $\mathbb{Z}$ and the $\mathbb{Z}$-module $\mathbb{Q}$. We easily observe that $\mathbb{Q}$ is not finitely generated as a $\mathbb{Z}$-module and is torsion-free ($\mathbb{Q}$ is a $\mathbb{Q}$-vector space over itself). Clearly, however, $\mathbb{Q}$ is not free as a $\mathbb{Z}$-module.

An obvious question one might ask, and indeed, what will be our first corollary, is how one might go about converting between the elementary divisor and invariant factor form. In other words, is there some algorithmic, or at least, concrete, means by which to go from one form to the other? The final portion of the proof of Theorem 3.25 above suggests the following as an answer to such a question:

Corollary 3.29 (**Conversion between invariant factors and elementary divisors**)**.** Let R be a P.I.D. and let Q be a finitely generated R-module. Then

1. The elementary divisors of Q are exactly the prime power factors of the invariant factors of Q.
2. The largest invariant factor of Q is the product of the largest of the distinct prime powers among the elementary divisors of Q; the next largest invariant factor is the product of the largest of the distinct prime powers among the remaining elementary divisors of Q, and so on.

Proof. The process outlined in (1) above gives one possible list of elementary divisors of Q; the uniqueness statement in Theorem 3.24 asserts that this is the only possible list. The idea for (2) is analogous. ■

Let R be a P.I.D. and Q a finitely generated R-module. For a little additional explanation on the conversion of invariant factors to elementary divisors: if we begin with the invariant factor decomposition, then we obtain a list of invariant factors $a_1, \ldots, a_m$. Choosing any $a := a_i$, we know that a is an element of R, and R is a U.F.D. since P.I.D. implies U.F.D.; hence we can write

$$a = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$$

for prime elements $p_1, \ldots, p_t$ of R. Then via the Chinese Remainder Theorem we get

$$R/(a) \cong R/(p_1^{\alpha_1}) \times \cdots \times R/(p_t^{\alpha_t}).$$

Decomposing each cyclic direct summand $R/(a)$ of Q according to the above process allows us to write Q as a direct sum of a finite number of cyclic modules whose annihilators are quite simple: either (0) or generated by powers of primes in R. This gives us a list of elementary divisors for Q, and by the uniqueness in Theorem 3.26, necessarily we have *the* list of elementary divisors for Q.

As a special case for the structure theorem for finitely generated modules over P.I.D.s, we have the following (major) result in the theory of groups:

Corollary 3.30 (**The Fundamental Theorem for Finitely Generated Abelian Groups**). Let G be a finitely generated abelian group. Then

1. $$G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z},$$

   for some integers $r, n_1, \ldots, n_s$ satisfying the following conditions:

   (a) $r \geq 0$ and $n_i \geq 2$ for all j, as well as

   (b) $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$.

2. The expression in (1) is unique in that if $G \cong \mathbb{Z}^t \times \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_u\mathbb{Z}$, where t and $m_1, \ldots, m_u$ satisfy (a) and (b) above, then $t = r$, $u = s$, and $m_i = n_i$ for all i.

Proof. Take $R = \mathbb{Z}$ in Theorem 3.13 and reverse the order of the invariant factors for (1). For (2), take $R = \mathbb{Z}$ in Theorem 3.25. ■

Note that we have listed the invariant factors in the decomposition of Corollary 3.30 in reverse order; this is prevalent in other sources and is done for computational efficiency.

As an example of the power of the structure theorem for finitely generated modules over P.I.D.s, we classify all abelian groups of a specific order (and find their invariant factors).

Example 3.31 (**Abelian groups of order** 180). Suppose $n = 180 = 2^2 \cdot 3^2 \cdot 5$. We see at once that the order of a finite abelian group is the product of its invariant factors $n_1, \ldots, n_s$, and moreover that $n_s \leq \cdots \leq n_1$ holds, so that n_1 is the largest invariant factor. Also, since each prime divisor of the order divides some n_j, it must divide n_1, hence all prime divisors of the order of the group divide n_1. Thus the possible options for n_1 in our case are

$$n_1 = 2^2 \cdot 3^2 \cdot 5,$$

$$n_1 = 2^2 \cdot 3 \cdot 5,$$

$$n_1 = 2 \cdot 3^2 \cdot 5,$$

$$n_1 = 2 \cdot 3 \cdot 5.$$

For each case above, we must find n_2 such that $n_2 \mid n_1$ and $n_1 n_2 \mid n$, and then we must do the same to find n_3 such that $n_3 \mid n_2$ and $n_1 n_2 n_3 \mid n$, and so on.

If $n_1 = 2^2 \cdot 3^2 \cdot 5$ then obviously the list is complete since $n_1 = n$, and so the list of invariant factors is simply $(2^2 \cdot 3^2 \cdot 5)$, corresponding to the cyclic group Z_{180}.

If $n_1 = 2^2 \cdot 3 \cdot 5$ then since $n_1 n_2 \mid n$ either $n_2 = 1$ or $n_2 = 3$. If $n_2 = 1$ then the list would have to be complete, but this is impossible for $n_1 n_2 \neq n$. Thus we require $n_2 = 3$; in this case, $n_1 n_2 = n$, so the list is complete; hence the list of invariant factors is $(2^2 \cdot 3 \cdot 5, 3)$, corresponding to the group $Z_{60} \times Z_3$.

If $n_1 = 2 \cdot 3^2 \cdot 5$ then since $n_1 n_2 \mid n$ either $n_2 = 1$ or $n_2 = 2$, and clearly $n_2 \neq 1$ for the same reasons as above, forcing $n_2 = 2$ to hold, in which case the list is again complete; hence the list of invariant factors is $(2 \cdot 3^2 \cdot 5, 2)$ corresponding to the group $Z_{90} \times Z_2$.

Finally, if $n_1 = 2 \cdot 3 \cdot 5$ then the only options for n_2 are $n_2 = 2$, $n_2 = 3$, or $n_2 = 2 \cdot 3$. The first two cases are impossible, for instance since if $n_2 = 2$ then $n_1 n_2 \neq n$, so there must be a third invariant factor n_3, and we require $n_3 \mid n_2 = 2$, forcing $n_3 = 1$ or $n_3 = 2$; the case $n_3 = 1$ is impossible since this would imply $n_1 n_2 = n$, which does not hold. Thus $n_3 = 2$ holds; however now $2^3 \mid n$ holds, which is impossible. The case where $n_2 = 3$ is similar. Thus the only valid option is $n_2 = 2 \cdot 3$, in which case the list is complete since now $n_1 n_2 = n$. The list of invariant factors is thus $(2 \cdot 3 \cdot 5, 2 \cdot 3)$, corresponding to the group $Z_{30} \times Z_6$.

Thus all valid abelian groups of order $n = 180$ and their lists of invariant factors are as follows:

Invariant Factors	**Abelian Groups**
$2^2 \cdot 3^2 \cdot 5$	Z_{180}
$2^2 \cdot 3 \cdot 5, 3$	$Z_{60} \times Z_3$
$2 \cdot 3^2 \cdot 5, 2$	$Z_{90} \times Z_2$
$2 \cdot 3 \cdot 5, 2 \cdot 3$	$Z_{30} \times Z_6$

This concludes our analysis of all abelian groups of order 180.

3.3.7 Corollary: Projective and Flat Modules over P.I.D.s

To characterize finitely generated projective modules over P.I.D.s, we need only refer back to one key result made earlier in this section: the result being, of course, Theorem 3.12, which describes submodules of free modules of finite rank as being free themselves.

Theorem 3.32 (Fin. gen. modules over P.I.D. are projective iff free). Let R be a P.I.D.. A finitely generated R-module is projective if and only if it is free.

Proof. Let Q be a finitely generated R-module. If Q is free then Corollary 2.9(1) implies that Q is projective, giving us one direction. If now we assume that Q is projective, then Q is a finitely generated projective R-module, and hence Corollary 2.9(2) asserts that Q is a submodule of a finitely generated free R-module, say F. In particular, Q is a submodule of a free module F of finite rank, and hence by Theorem 3.12, Q is free of rank less than or equal to that of F. Now, of course, Q being free implies that Q is projective by Corollary 2.9(1) once more. ■

3.3.8 Finitely Generated Injective Modules over P.I.D.s

As we have mentioned prior, injective modules are always slightly more involved than their projective counterparts. Unfortunately, this theme remains even in the case where the rings being considered are quite simple and well-behaved. What we mean by this is that we shall have to split our inquiry into finitely generated injective modules over P.I.D.s into two cases: one for P.I.D.s which are not fields and one for P.I.D.s which are fields.

❊ Modules over Dedekind Domains

In this section we will occupy ourselves with modules over certain rings called Dedekind Domains. We begin by introducing these rings and exploring some properties which make them worthy objects of study. Directly proceeding this, we prove a structure theorem for finitely generated modules over Dedekind Domains, which shall in some sense extend the structure theorem for finitely generated modules over P.I.D.s (Principal Ideal Domains) we covered prior. This is of course because, as we shall see very soon, Dedekind Domains are a natural extension of the class of P.I.D.s.

4.1 Dedekind Domains

Readers may be familiar with so-called *discrete valuation rings*, which are local rings that are integrally closed Noetherian integral domains of Krull dimension 1. This is quite a restrictive class of rings, and so one might naturally wonder what sorts of rings might arise from the removal, or relaxing, of some or all of these requirements.

Indeed, in this, our first subsection, we introduce and briefly review the theory of Dedekind Domains, sometimes called Dedekind rings, which are those rings that are not necessarily local, but are integrally closed Noetherian integral domains of Krull dimension 1.

Definition 4.1 (**Dedekind Domains**)**.** A ring R is said to be a *Dedekind Domain* if R is Noetherian, integrally closed in its field of fractions, an integral domain, and has Krull dimension 1.

We make a note that a ring R having Krull dimension 1 means any chain of prime ideals of R has at most two constituents; equivalently, every prime ideal of R is maximal.

To begin with, and, in an effort to orient ourselves, to ensure we are on the right path, we would like to show that the class of Dedekind domains are a quite natural enlargement of the class of principal ideal domains.

Proposition 4.2 (**P.I.D.s are Dedekind Domains**)**.** Every principal ideal domain is a Dedekind domain.

Proof. Recall that a ring R is Noetherian if all of its ideals are finitely generated; clearly if R is a P.I.D., then each ideal is finitely generated (indeed by one element). Moreover, P.I.D.s are U.F.D.s (unique factorization domains), and it is a well-known (and easily verifiable result) that all U.F.D.s are integrally closed in their fields of fractions. What remains, then, is to check that all prime ideals of R are maximal.

Let (p) be a non-zero prime ideal of R. Let $I = (m)$ be any ideal of R containing (p). We must show that either $I = (p)$ or $I = R$. We have $(p) \subseteq I = (m)$, and hence

$p = rm$ for some $r \in R$. However, since $rm = p \in (p)$, and (p) is a prime ideal, we must have either $r \in (p)$ or $m \in (p)$. If $m \in (p)$ then $(m) = I \subseteq (p)$, to which $I = (p)$ holds. On the other hand, if $r \in (p)$, then we may write $r = ps$ for some $s \in R$. Then

$$p = rm = (ps)m = p(sm) \iff p - psm = 0 \iff p(1 - sm) = 0$$

Since R is, in particular, an integral domain, and $p \neq 0$ by assumption that (p) is a non-zero prime ideal, we require that $1 - sm = 0$, hence $sm = 1$. This means that $(m) = I = R$, whence the claim. ■

Now that we have seen we are on the right track in studying Dedekind domains, it will be prudent to develop intuition for them: how do they behave as rings, in what ways are they similar, different. The following theorem will give a number of important equivalent characterizations of Dedekind domains.

Theorem 4.3 (**Dedekind Domain Equivalences**)**.** Let R be an integral domain with field of fractions K such that $R \neq K$. Then the following are equivalent:

1. R is a Dedekind domain. That is, the ring R is Noetherian, integrally closed in K, and every non-zero prime ideal is maximal.

2. The ring R is Noetherian, and for each non-zero prime ideal P of R, the localization R_P of R at P is a DVR.

3. Every non-zero fractional ideal of R in K is invertible.

4. Every non-zero fractional ideal in K is projective as an R-module.

5. Every non-zero proper ideal I of R can be written as a finite product of prime ideals of R, so $I = \prod_{i=1}^{n} P_i$, with each prime ideal not necessarily distinct. Moreover, if the previous statement holds, the set of prime ideals $P_1, \ldots, P_n$ is unique, and hence every non-zero proper ideal I of R can be written (up to reordering) as a product of powers of prime ideals.

Proof. The proof may be found as Theorem 15 in Section 16.3 of [1]. ■

4.1.1 Introducing Fractional Ideals

Definition 4.4 (**Fractional ideals I**)**.** Let R be an integral domain with fraction field K. A *fractional ideal of* R is then an R-submodule A of the R-module K such that $dA \subseteq R$ for some non-zero $d \in R$.

Note that for a fractional ideal A of R, we have that dA is an R-submodule of R for some $d \in R \setminus \{0\}$. Since the submodules of R are precisely the ideals of R, this means that dA is an ideal of R; hence $dA = I$, so that $A = d^{-1}I$. Conversely, for any ideal J of R, and non-zero $d \in R$, we have that $d^{-1}J$ is a fractional ideal of R.

Definition 4.5 (Fractional ideals II). Let R be an integral domain. Then $d^{-1}I$ is a *fractional ideal of* R, where I is some ideal of R and d a non-zero element of R.

What may be obvious, but is certainly worth stating overtly, is that the notion of a fractional ideal of an integral domain R depends entirely on the ring R itself. Phrased differently, we can also consider fractional ideals of R as simply just ideals of R up to multiplication by a fixed denominator $d \in R \setminus \{0\}$.

We broaden our class of examples of fractional ideals considerably in the following example:

Example 4.6 (Every ideal is a fractional ideal). Let R be an integral domain. Taking $d = 1$ in Definition 4.5 above we see that every ideal of R (in the usual sense) can be considered as a fractional ideal of R.

We next determine all of the fractional ideals in the integral domain $\mathbb{Z}$.

Example 4.7 (The fractional ideals of $\mathbb{Z}$). It is easy to check that $\frac{1}{2}\mathbb{Z}$ is a $\mathbb{Z}$-submodule of $\mathbb{Q}$, for instance by using the submodule criterion. In addition, it is trivial to see that

$$2(\frac{1}{2}\mathbb{Z}) = \mathbb{Z} \subseteq \mathbb{Z},$$

where $2 \neq 0$. Therefore $\frac{1}{2}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$. In a similar manner, we can show that all of the $\mathbb{Z}$-submodules $\frac{a}{b}\mathbb{Z}$ of $\mathbb{Q}$, where $a, b \in \mathbb{Z}$ with $b \neq 0$, are fractional ideals of the ring $\mathbb{Z}$. Analyzing Definition 4.5 a little closer, we can see that all fractional ideals of $\mathbb{Z}$ are of the form outlined in this example.

For clarity, we include the following example.

Example 4.8 (Not all fractional ideals are ideals). From Example 4.7, we know $\frac{1}{2}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$. Moreover, we have that $\frac{1}{2}\mathbb{Z}$ is not an ideal of $\mathbb{Z}$; if this were the case then, for example, we would require that $3 \cdot \frac{1}{2} = \frac{3}{2} \in Z$ hold, but clearly this is impossible.

4.1.2 Module Structure of Fractional Ideals

This subsection will consist entirely of auxiliary results which we will use in the proof of the structure theorem for modules over Dedekind Domains.

Let R be a Dedekind Domain. Our first result will be to show that two fractional ideals are isomorphic as R-modules if and only if they lie in the same equivalence class in the ideal class group of R; that is, if and only if the fractional ideals differ by a principal ideal, since, as we recall, the equivalence class of principal ideals of R is the identity element in the ideal class group of R. More precisely:

Lemma 4.9 (Isomorphic fractional ideals differ by a principal ideal). Let R be a Dedekind Domain with field of fractions K. Then two fractional ideals I and J of R are isomorphic as R-modules if and only if I and J differ by a principal ideal; i.e., $I = (a)J$ for some non-zero $a \in K$.

Proof. For the first direction, if $J = (0)$ then the result is trivial, so assume $J \neq (0)$. Then if $I \cong J$ we have $R \cong J^{-1}I$, so there exists some isomorphism of R-modules, say $\phi : R \longrightarrow J^{-1}I$. Set $a := \phi(1)$. Since 1 generates R, we have then that a generates $J^{-1}I$ considered as an R-module via the isomorphism, whence $J^{-1}I = aR$ holds; i.e., we get $J^{-1}I = (a)$, so we have that $I = (a)J$.

Conversely, suppose $I = (a)J$ for some non-zero $a \in K$. We have an obvious R-module isomorphism $\varphi : J \longrightarrow (a)J$ given by $x \mapsto ax$. Thus $I = (a)J \cong J$ are isomorphic as R-modules. ■

While Lemma 4.9 is interesting in its own right, we shall be primarily concerned with its utility in regards to statements about direct sums of fractional ideals; indeed, the next proposition shall turn out to be indispensable to our forthcoming proof of the structure theorem for finitely generated modules over Dedekind Domains.

Proposition 4.10. Let R be a Dedekind Domain with field of fractions K. Then:

1. For non-zero fractional ideals $I_1, \ldots, I_n$ and $J_1, \ldots, J_m$ of R, we have an isomorphism of R-modules
$$\bigoplus_{i=1}^{n} I_i \cong \bigoplus_{i=1}^{m} J_i$$
if and only if $n = m$ and the product ideals $\prod_{i=1}^{n} I_i$ and $\prod_{i=1}^{m} J_i$ differ by a principal ideal:
$$\prod_{i=1}^{n} I_i = (a) \prod_{i=1}^{m} J_i$$
for some non-zero $a \in K$.

2. In particular, we have that
$$\bigoplus_{i=1}^{n} I_i \cong \underbrace{R \oplus \cdots \oplus R}_{n-1 \text{ factors}} \oplus \left(\prod_{i=1}^{n} I_i \right) = R^{n-1} \oplus \left(\prod_{i=1}^{n} I_i \right),$$
and moreover that $I \oplus R^n \cong J \oplus R^n$ if and only if I and J differ by a principal ideal; i.e., if and only if $I = (a)J$ for some non-zero $a \in K$.

Proof. We first show that for any non-zero fractional ideals I and J of R, that $I \oplus J \cong R \oplus IJ$. We can replace the fractional ideals I and J by aI and bJ, for non-zero $a, b \in K$ and integral ideals I and J of R; moreover, we can assume these integral ideals I and J are relatively prime, via Lemma 4.11. Thus, we have $I + J = R$ and $I \cap J = IJ$. We have the surjective R-module homomorphism

$$I \oplus J \longrightarrow I + J$$

$$(x, y) \mapsto x + y,$$

and so in particular since $I + J = R$ we have a short exact sequence

$$0 \longrightarrow IJ \longrightarrow I \oplus J \longrightarrow R \longrightarrow 0$$

of R-modules. Since R is free, hence projective, the above sequence splits, whence

$$I \oplus J \cong R \oplus IJ$$

holds, as we desired to show. Since the sum of two fractional ideals of R is once again a fractional ideal of R, a simple induction argument proves the first statement of part (2) of this proposition. The second statement of (2) is a special case of (1), and we shall indeed occupy ourselves with (1) presently.

For (1), suppose first that $\prod_{i=1}^{n} I_i = (a) \prod_{i=1}^{m} J_i$ for some non-zero $a \in K$ and that $n = m$. Since the product of fractional ideals of R is once again a fractional ideal of R, we can refer to Lemma 4.9 to write that

$$\prod_{i=1}^{n} I_i \cong \prod_{i=1}^{n} J_i$$

where the isomorphism in question is one of R-modules, as per the lemma. Now, by (2) we have above, we have the following isomorphism of R-modules

$$I_1 \oplus \cdots \oplus I_n \cong R^{n-1} \oplus (I_1 \cdots I_n) \cong R^{n-1} \oplus (J_1 \cdots J_n) \cong J_1 \oplus \cdots \oplus J_n,$$

whence the first direction of (1) is proven to hold true.

For the converse, suppose $I_1 \oplus \cdots \oplus I_n \cong J_1 \oplus \cdots \oplus J_m$ as R-modules, where I_i, $1 \leq i \leq n$ and J_i, $1 \leq i \leq m$, are non-zero fractional ideals of R. Bear with us now as we take a little detour into localization.

Now recall from the localization theory of modules that for a multiplicatively closed subset D containing 1 of a ring R and an R-module Q, we have an isomorphism of $D^{-1}R$-modules given via

$$D^{-1}Q \cong Q \otimes_R D^{-1}R.$$

For our current case, we have an R-module I (since I is an R-submodule of K) and a multiplicatively closed subset containing 1 given by $D = R \setminus \{0\}$. Now we have $D^{-1}R = K$ since K is the field of fractions of R, and an isomorphism of K-modules

$$D^{-1}I \cong I \otimes_R K.$$

Note also that since I is a fractional ideal of R, we have that there exists a non-zero $d \in R$ for which $dI \subseteq R$. Thus for some $x \in I$ we have $dx \in R$, and hence $dx/dx = 1 \in D^{-1}I$ holds, whence $D^{-1}I = K$ since $D^{-1}I$ is a K-module. Thus, in particular, we have an isomorphism $K \cong I \otimes_K K$ of K-modules (so K-vector spaces) for all fractional ideals I of R. Applying the above paragraph to our hypothesis, and using the fact that the tensor product commutes with direct sums, we have

$$K^m \cong (J_1 \oplus \cdots \oplus J_m) \otimes_R K \cong (I_1 \oplus \cdots \oplus I_n) \otimes_R K \cong K^n$$

as K-vector spaces, whence $n = m$ is required.

Next we prove that $\prod_{i=1}^n I_i = (a) \prod_{i=1}^n J_i$. Note that, without loss of generality, we may replace the ideal I_1 by the isomorphic fractional ideal $a_1^{-1} I_1$, where $a_1 \in I_1$ is any non-zero element. Our reason for doing this is so that we can assume each of the fractional idealls I_i, J_i being considered contain the ring R (indeed because $a_1^{-1} I_1$ contains R, as can easily be seen).

By assumption, there is some R-module isomorphism ϕ from $I_1 \oplus \cdots \oplus I_n$ to $J_1 \oplus \cdots \oplus J_n$. For each $i \in \{1, \ldots, n\}$, we define

$$\phi((0, \ldots, 0, 1, 0, \ldots, 0)) := (\alpha_{1,i}, \ldots, \alpha_{n,i}) \in \bigoplus_{i=1}^n J_i,$$

where $(0, \ldots, 0, 1, 0, \ldots, 0)$ is the element of $I_1 \oplus \cdots \oplus I_n$ with 1 in the ith coordinate and 0 elsewhere, which is a permissible element since we are assuming each I_i contains the ring R, hence the multiplicative identity element 1 of R. We now claim that for each $j \in \{1, \ldots, n\}$, we have

$$J_j = \alpha_{j,1} I_1 + \cdots + \alpha_{j,i} I_i + \cdots + \alpha_{j,n} I_n.$$

Towards the claim, let $y \in J_j$. Then $(0, \ldots, 0, y, 0, \ldots, 0) \in J_1 \oplus \cdots \oplus J_n$, and so since ϕ is an isomorphism, in particular surjective, there exists some $(x_1, \ldots, x_n) \in I_1 \oplus \cdots \oplus I_n$ mapping to this element under ϕ. Before proceeding, we define

$$\phi(0, \ldots, 0, x_i, 0, \ldots, 0) := (e_{1_i}, \ldots, e_{n_i}) \in \bigoplus_{i=1}^n J_i$$

for each $i \in \{1, \ldots, n\}$. Now we can observe the following sequence of equations:

$$\begin{aligned}(0, \ldots, 0, y, 0, \ldots 0) &= \phi(x_1, \ldots, x_n) \\ &= \phi\left((x_1, 0 \ldots, 0)\right)(1, 0, \ldots 0) + \cdots + (0, \ldots, 0, x_n)(0, \ldots, 0, 1)) \\ &= \phi(x_1, 0, \ldots, 0)\phi(1, 0, \ldots, 0) + \cdots + \phi(0, \ldots, 0, x_n)\phi(0, \ldots, 0, 1) \\ &= (e_{1_1}, \ldots, e_{1_n})(\alpha_{1,1}, \ldots, \alpha_{n,1}) + \cdots + (e_{n_1}, \ldots, e_{n_n})(\alpha_{1,n}, \ldots, \alpha_{n,n}) \\ &= (\alpha_{1,1} e_{1_1} + \cdots + \alpha_{1,n} e_{n_1}, \ldots, \alpha_{n,1} e_{1_n} + \cdots + \alpha_{n,n} e_{n_n}) \\ &= (0, \ldots, 0, \alpha_{j,1} e_{1_j} + \cdots + \alpha_{j,n} e_{n_j}, 0, \ldots, 0).\end{aligned}$$

In particular, after projecting down via $\pi_j : J_1 \oplus \cdots \oplus J_n \longrightarrow J_j$, we require that

$$y = \sum_{i=1}^{n} \alpha_{j,i} e_{i_j} = \sum_{i=1}^{n} \alpha_{j,i} (\pi_j \circ \phi)(0, \ldots, 0, x_i, 0, \ldots, 0)$$

We identify I_i with its homomorphic image in $I_1 \oplus \cdots \oplus I_n$, in particular mapping $x_i \in I_i$ to $\mathbf{x}_i := (0, \ldots, 0, x_i, 0, \ldots, 0)$. In view of this identification, we have

$$y = \sum_{i=1}^{n} \alpha_{j,i} \mathbf{x}_i \in a_{j,1} I_1 + \cdots + \alpha_{j,n} I_n,$$

whence $J_j \subseteq \alpha_{j,1} I_1 + \cdots + \alpha_{j,n} I_n$. The reverse containment is then immediate, and so we have proved our claim.

Using the claim above, we can now see that, for any $\sigma \in S_n$, i.e., any permutation σ of the set $\{1, \ldots, n\}$, we have the containment:

$$(\alpha_{\sigma(1),1} \cdots \alpha_{\sigma(n),n})(I_1 \cdots I_n) \subseteq \prod_{j=1}^{n} \left(\alpha_{j,1} I_1 + \cdots + \alpha_{j,n} I_n \right) = \prod_{j=1}^{n} J_j.$$

Recall now the definition of the determinant of an $n \times n$ matrix; we make such a matrix out of the $a_{i,j}$ and set its determinant as follows:

$$d := \det \begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} & \cdots & \alpha_{1,n} \\ \alpha_{2,1} & \alpha_{2,2} & & \alpha_{2,n} \\ \vdots & & \ddots & \vdots \\ \alpha_{n,1} & \alpha_{n,2} & \cdots & \alpha_{n,n} \end{pmatrix} = \sum_{\sigma \in S_n} \epsilon(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)},$$

where $\epsilon(\sigma)$ is the sign of the permutation σ. Observe now that

$$d(I_1 \cdots I_n) \subseteq (\alpha_{\sigma(1),1} \cdots \alpha_{\sigma(n),n})(I_1 \cdots I_n) \subseteq J_1 \cdots J_n$$

holds true for any $\sigma \in S_n$; in particular, we have $d(I_1 \cdots I_n) \subseteq J_1 \cdots J_n$.

We now repeat the entire process delineated above, but instead defining, for each $j \in \{1, \ldots, n\}$:

$$\phi^{-1}(0, \ldots, 0, 1, 0, \ldots, 0) := (\beta_{1,j}, \ldots, \beta_{n,j}) \in \bigoplus_{i=1}^{n} I_n$$

where the element in the argument of the map ϕ^{-1}, which, recall, exists since ϕ was assumed an isomorphism, is the element of $J_1 \oplus \cdots \oplus J_n$ with 1 in the jth coordinate and 0 elsewhere (which is valid since $R \subseteq J_j$ for all j, as we assumed).

Note now that the product of the two matrices $(\alpha_{i,j})$ and $(\beta_{i,j})$ is the identity matrix (for instance, since these are change of basis matrices to and from the standard basis). Hence $d \neq 0$ and the determinant of the matrix $(\beta_{i,j})$ is precisely

d^{-1} (since the determinant of the $n \times n$ identity matrix is 1). We have, in an exactly analogous process as to the above, that

$$(d^{-1})(J_1 \cdots J_n) \subseteq I_1 \cdots I_n.$$

Hence

$$J_1 \cdots J_n = d(d^{-1})(J_1 \cdots J_n) \subseteq d(I_1 \cdots I_n),$$

which, combined with our previous containment, gives us that

$$d(I_1 \cdots I_n) = J_1 \cdots J_n.$$

Thus, indeed, the products $I_1 \cdots I_n$ and $J_1 \cdots J_n$ differ by a principal ideal, which is precisely what we were attempting to show. ■

After the long discursion above we are nearly done with our preliminary developments; what remains, then, is prove one final proposition, what will come to be the keystone piece, the final touch, in our proof of the structure theorem for modules over Dedekind Domains to come. The proposition in question follows promptly from the next lemma.

Lemma 4.11. Let R be a Dedekind Domain with fractional ideals I_1 and I_2. Then given any non-zero $x_2 \in I_2^{-1}$, there exists a non-zero $x_1 \in I_1^{-1}$ such that the ideals I_1x_1 and I_2x_2 are relatively prime; that is, $I_1x_1 + I_2x_2 = R$.

Proof. Choosing some non-zero $x_2 \in I_2^{-1}$, we have that x_2I_2 is an integral ideal of R. Since R is Dedekind, we let $P_1, \ldots, P_s$ denote the distinct prime ideals dividing I_2x_2. Now, for each i, $1 \leq i \leq s$, we have the containment

$$I_1^{-1}P_1 \cdots P_s \subseteq I_1^{-1}P_1 \cdots P_{i-1}P_{i+1} \cdots P_s$$

so we may choose some $y_i \in (I_1^{-1}P_1 \cdots P_{i-1}P_{i+1} \cdots P_s) \setminus (I_1^{-1}P_1 \cdots P_s)$. Now set

$$x_1 := y_1 + \cdots + y_s$$

Then clearly we have the containment

$$x_1 \in I_1^{-1}\left(\sum_{i=1}^{s} P_1 \cdots P_{i-1}P_{i+1} \cdots P_s\right) \subseteq I_1^{-1},$$

hence $x_1 \in I_1^{-1}$ holds. We next prove that, for each i, $1 \leq i \leq s$, the prime ideal P_i does not divide the integral ideal I_1x_1 of R. Since, in a Dedekind Domain, to contain is to divide, it suffices to show that I_1x_1 is not contained in P_i. We have

$$x_1I_1 = I_1(y_1 + \cdots + y_s) = \{\sum_{i=1}^{s} \alpha y_i \mid \alpha \in I_1\}$$

For each i, $1 \leq i \leq s$, note that for all $\alpha \in I_1$, and for all $j \neq i$, $1 \leq j \leq s$, we have that $\alpha y_j \in P_i$ by closure, as $y_j \in P_i$ since

$$y_j \in I_1^{-1} P_1 \cdots P_{j-1} P_{j+1} \cdots P_s \subseteq P_i$$

following since we took $j \neq i$. In particular, then, $I_1 y_i \nsubseteq P_i$, and hence $I_1 x_1 \nsubseteq P_i$ also holds. Since $I_1 x_1 \nsubseteq P_i$ for all $P_1, \ldots, P_s$ in the prime factorization of $I_2 x_2$, this means that $I_1 x_1$ and $I_2 x_2$ are relatively prime, as desired. ■

Now on to the proposition in question.

Proposition 4.12. Let R be a Dedekind Domain and let I be a non-zero ideal of R. Then for any fractional ideal J of R, we have an isomorphism of R-modules

$$J/JI \cong R/I$$

Proof. We apply Lemma 4.11; in the notation of that lemma, we take $I_1 := J$ and $I_2 := I$, as well as $x_2 := 1$. Thus there exists some non-zero $x \in J^{-1}$ such that the ideals xJ and I are relatively prime; hence $xJ + I = R$. Moreover, the fact that Jx and I are relatively prime also gives that $xJI = xJ \cap I$. We have:

$$J/IJ \cong xJ/xJI \cong xJ/(xJ \cap I) \cong (xJ + I)/I = R/I,$$

where the final isomorphism is a consequence of the second isomorphism theorem for modules. ■

4.1.3 The Chinese Remainder Theorem

Before proceeding, we briefly cover a theorem that will aid us considerably in our proof of the structure theorem for finitely generated modules over Dedekind Domains. While we do not provide a proof here in this text, it will be useful to have a concrete statement of the theorem at hand.

Theorem 4.13 (The Chinese Remainder Theorem). Let R be a Dedekind Domain, $P_1, \ldots, P_n$ distinct prime ideals of R, and $a_i \geq 0$ integers for $1 \leq i \leq n$. Then

$$R/(P_1^{e_1} \cdots P_n^{e_n}) \cong R/P_1^{e_1} \times \cdots \times R/P_n^{e_n}.$$

Equivalently, for any ring elements $r_1, \ldots, r_n \in R$, there exists some element $r \in R$, which is unique up to an element in $P_1^{e_1} \cdots P_n^{e_n}$, for which

$$r \equiv r_i \pmod{P_i^{e_i}}$$

for all $1 \leq i \leq n$.

Proof. A proof may be found as Theorem I.3.6. in [2]. ■

In the next section, we tackle the structure theorem.

4.2 Structure Theorem for Modules over Dedekind Domains

With all of the preliminaries covered, we proceed to considering finitely generated modules over Dedekind domains; in particular, we prove a structure theorem for such modules which shall extend the structure theorems for finitely generated modules over principal ideal domains.

4.2.1 Torsion-Free Modules over Dedekind Domains

For the proof we shall first analyze finitely generated torsion-free modules over Dedekind Domains. As we shall see, all such modules are necessarily projective; this crucial fact will enable us to engage properly with the proof of the structure theorem.

Lemma 4.14 (**Fin. gen. torsion-free modules over Dedekind domains are projective**)**.** Let R be a Dedekind domain. Then any finitely generated torsion-free R-module is projective.

Proof. Suppose Q is a finitely generated R-module with $\mathrm{Tor}(Q) = 0$. Let K be the field of fractions of R, which exists since R is, in particular, an integral domain. Since $\mathrm{Tor}(Q) = 0$, the canonical R-module homomorphism

$$Q \to Q \otimes_R K$$

$$x \mapsto x \otimes 1$$

is injective; hence we may view Q as an R-submodule of the K-vector space $Q \otimes_R K$.

To prove the desired lemma, we shall induct on the rank of Q. If Q has rank 1, then $Q \cong R$ as R-modules, so $Q \cong R = (1)$ is isomorphic to a (trivial) direct sum of ideals; take this as our base case. Now suppose $n > 1$ is the rank of Q. We show that Q is isomorphic to a direct sum of ideals.

Since Q has rank n, we know $Q \otimes_R K$ has dimension n as a K-vector space, as we have seen. As such, take a K-basis $x_1, \ldots, x_n$ for $Q \otimes_R K$ over K. Let $q_1, \ldots, q_n$ be R-module generators for Q. Since Q injects into $Q \otimes_R K$, we can write each q_i as a K-linear combination of $x_1, \ldots, x_n$. For each $1 \leq i \leq n$, take

$$q_i = \sum_{j=1}^{n} a_{i_j} x_j$$

where $a_{i_j} \in K$ for all $1 \leq j \leq n$. Now define d to be the common denominator of

$$a_{1_1}, \ldots, a_{n_n}, a_{2_1}, \ldots, a_{2_n}, \ldots, a_{n_1}, \ldots, a_{n_n}.$$

So d is the common denominator of all of the coefficients in each of the K-linear combinations representing the R-module generators q_i of Q. Now set $y_i := x_i/d$

for all $1 \leq i \leq n$, noting that $d \neq 0$. For any $w \in Q$, we can write

$$w = \sum_{i=1}^{n} r_i q_i = \sum_{i=1}^{n} r_i \left(d \cdot \frac{x_i}{d} \right) = \sum_{i=1}^{n} (r_i d) \left(\frac{x_i}{d} \right) = \sum_{i=1}^{n} (r_i d) y_i$$

for some $r_i \in R$, $1 \leq i \leq n$. In particular, we have $w \in Ry_1 + \cdots + Ry_n$, and hence that

$$Q = Rx_1 + \cdots + Rx_n \subseteq Ry_1 + \cdots + Ry_n \subset Kx_1 + \cdots + Kx_n = Q \otimes_R K$$

Since $Ry_1 + \cdots + Ry_n$ is a free R-submodule of $Q \otimes_R K$ of rank n, every element $w \in Q$ can be written

$$w = \sum_{i=1}^{n} a_i y_i$$

for $a_i \in R$, $1 \leq i \leq n$. Now since the R-module homomorphsim

$$\Phi : Q \to R$$

$$\sum_{i=1}^{n} a_i y_i \longmapsto a_n$$

is surjective, we have an exact sequence

$$0 \to \ker \Phi \to Q \xrightarrow{\Phi} \Phi(Q) \to 0$$

Set $I_1 := \Phi(Q)$. Since $I_1 \subseteq R$ is an R-submodule of R, it follows that I_1 is an ideal of R. Now the submodule $\ker \Phi$ is a torsion-free R-module with rank less than or equal to $n - 1$, as

$$\ker \Phi \subseteq Ry_1 + \cdots + Ry_{n-1}$$

and the R-module on the right has rank $n - 1$. Since $Q/\ker \Phi \cong I_1$, Theorem 3.11 implies that the rank of I_1 is one and $\ker \Phi$ has rank $n - 1$. In particular, $I_1 \neq (0)$. Now Theorem 4.3(4) asserts that I_1 is projective; hence the short exact sequence above splits, to which

$$Q \cong I_1 \oplus \ker \Phi.$$

Since $\ker \Phi$ has rank $n - 1$, we may apply our inductive hypothesis to write $\ker \Phi$ as the direct sum of non-zero ideals of R. Thus we can, in particular, write Q as a direct sum of non-zero ideals of R, so

$$Q \cong I_1 \oplus \cdots \oplus I_n$$

Since each I_i is a projective R-module by Theorem 4.3(4) once again, and the direct sum of projective modules is projective, we have thus proved that Q is a projective R-module. ■

We have successfully shown that finitely generated modules over Dedekind Domains which are torsion-free are necessarily projective. Recall, also, that finitely generated modules which are free are always projective (indeed, even non-finitely generated free modules are always projective). Thus, for finitely generated modules over Dedekind Domains, both of the properties of freeness and torsion-freeness imply projectivity. After we have obtained the structure theorem, we will be able to make a stronger assertion: namely, that finitely generated modules over Dedekind Domains which are projective must also be torsion-free; in particular, we will have exhibited a simple characterization of projectivity in the case of finite generation over Dedekind Domains.

4.2.2 Main Statement of the Structure Theorem

On towards the structure theorem.

Theorem 4.15 (**Structure Theorem for Modules over Dedekind Domains).** Let R be a Dedekind Domain and let Q be a finitely generated R-module of rank n. Then

$$Q \cong \left(\bigoplus_{i=1}^{n-1} R \right) \oplus I \oplus \mathrm{Tor}(Q)$$

for some ideal I of R, and

$$\mathrm{Tor}(Q) \cong R/P_1^{\alpha_1} \times \cdots \times R/P_s^{\alpha_s}$$

for some integers $s, \alpha_1, \ldots, \alpha_s \geq 0$ and not necessarily distinct prime ideals P_i for $1 \leq i \leq s$. Moreover, the decomposition for Q above is unique, in that the ideal I is unique up to multiplication by a principal ideal in R, and that the prime ideals $P_i^{\alpha_i}$ are unique for $1 \leq i \leq s$.

Proof. Let Q be a finitely generated R-module. Then the quotient $Q/\mathrm{Tor}(Q)$ is finitely generated and torsion-free; hence projective by Lemma 4.14. Thus by Theorem 2.7(3), the exact sequence

$$0 \longrightarrow \mathrm{Tor}(Q) \longrightarrow Q \longrightarrow Q/\mathrm{Tor}(Q) \longrightarrow 0$$

splits, and hence we have a decomposition:

$$Q \cong (Q/\mathrm{Tor}(Q)) \oplus \mathrm{Tor}(Q)$$

Additionally, since $Q/\mathrm{Tor}(Q)$ is isomorphic to a direct sum of ideals $I_1, \ldots, I_m$ of R, as we saw in the induction proof of Lemma 4.14, we have

$$Q/\mathrm{Tor}(Q) \cong \bigoplus_{i=1}^{m} I_i$$

Since ideals of R are fractional ideals (Example 4.6), we may apply Proposition 4.10(2) from the previous section to write that

$$Q/\mathrm{Tor}(Q) \cong \left(\bigoplus_{i=1}^{m-1} R\right) \oplus \left(\prod_{i=1}^{m} I_i\right)$$

Now set $I := \prod_{i=1}^{m} I_i$. Then, with our initial decomposition for Q in mind, we have that:

$$Q \cong \left(\bigoplus_{i=1}^{m-1} R\right) \oplus I \oplus \mathrm{Tor}(Q)$$

We note that the uniqueness of the ideal I in the statement of the theorem is now a consequence of the uniqueness of the ideals $I_1, \dots, I_m$ of R from the final statement of Proposition 4.10(2).

What remains then is to analyze $\mathrm{Tor}(Q)$ and prove the requisite statements in the theorem regarding this submodule. Let $I = \mathrm{Ann}_R(\mathrm{Tor}(Q))$ be the annihilator of $\mathrm{Tor}(Q)$ in R. Since R is a Dedekind Domain, we can factorize the ideal I as follows:

$$I = \prod_{i=1}^{t} P_i^{e_i}$$

for distinct prime ideals $P_1, \dots, P_t$ of R and $t, e_1, \dots, e_t \geq 0$ are integers. Now we may consider $\mathrm{Tor}(Q)$ as an R/I-module in the usual way. We note that

$$R/I \cong R/P_1^{e_1} \times \cdots \times R/P_t^{e_t}$$

as rings by the Chinese Remainder Theorem (Theorem 4.13). Therefore, for our R/I-module $\mathrm{Tor}(Q)$, we have an isomorphism of R-modules:

$$\mathrm{Tor}(Q) \cong \bigoplus_{i=1}^{t} \left(\mathrm{Tor}(Q)/P_i^{e_i}\mathrm{Tor}(Q)\right)$$

We now analyze each direct summand of the decomposition above separately.

Set $P := P_i$ and $e := e_i$ for any $1 \leq i \leq t$. Since $\mathrm{Tor}(Q)$ is finitely generated over R, we know each $\mathrm{Tor}(Q)/P^e\mathrm{Tor}(Q)$ is finitely generated over the quotient ring R/P^e. We have an isomorphism of rings:

$$R/P^e \cong R_P/P^eR_P,$$

where R_P is the localization of R at the prime ideal P. Since R is a Dedekind Domain, we know each localization R_P is a P.I.D., even a DVR.

Now we can consider each $\mathrm{Tor}(Q)/P^e\mathrm{Tor}(Q)$ as a finitely generated R_P-module, noting that P^eR_P is the annihilator of $\mathrm{Tor}(Q)/P^e\mathrm{Tor}(Q)$ via the ring homomorphism above (so in particular we can extend the ring action R_P/P^eR_P to R_P by letting ring elements of P^eR_P kill elements of $\mathrm{Tor}(Q)/P^e\mathrm{Tor}(Q)$).

But now we may invoke the structure theorem for finitely generated modules over P.I.D.s, in particular the elementary divisor form, Theorems 3.24 and 3.17, to write that each $\mathrm{Tor}(Q)/P^e\mathrm{Tor}(Q)$ is isomorphic as an R_P-module to a finite direct sum of modules of the form R_P/P^fR_P, where $f \leq e$. By the ring isomorphism

$$R_P/P^fR_P \cong R/P^f$$

once more, each $\mathrm{Tor}(Q)/P^e\mathrm{Tor}(Q)$ is thus isomorphic as an R-module to a finite direct sum of modules of the form R/P^f, where again $f \leq e$.

In conclusion, then, each direct summand in the original for $\mathrm{Tor}(Q)$ may be decomposed according to the above paragraph, and hence $\mathrm{Tor}(Q)$ has a decomposition

$$\mathrm{Tor}(Q) \cong R/P_1^{\alpha_1} \oplus \cdots \oplus R/P_s^{\alpha_s}$$

for some integers $s, \alpha_1, \ldots, \alpha_s \geq 0$. Next we shall prove this decomposition is unique.

So suppose we have integers $t, \beta_1, \ldots, \beta_t \geq 1$ and prime ideals $P'_1, \ldots, P'_t$ of R such that

$$\mathrm{Tor}(Q) \cong \bigoplus_{i=1}^{s} \left(R/P_i^{\alpha_i}\right) \cong \bigoplus_{j=1}^{t} \left(R/(P')_j^{\beta_j}\right)$$

Set $P := P_i$ and $\alpha := \alpha_i$ for some $1 \leq i \leq s$. Also, set $S := R_P/P^\alpha R_P$. We know, like in previous paragraphs, that S is a P.I.D., and moreover that $\mathrm{Tor}(Q)$ may be considered as an S-module, hence we may apply the Primary Decomposition Theorem to write $\mathrm{Tor}(Q)$ as a direct sum of its primary components. Let M denote the P-primary component of $\mathrm{Tor}(Q)$. Then we require

$$M \cong \bigoplus_{P_i = P} \left(R/P_i^{\alpha_i}\right) \cong \bigoplus_{P'_j = P} \left(R/P_j^{\beta_j}\right)$$

In other words, M is isomorphic to the direct sum of all $R/P_i^{\alpha_i}$ where $P_i = P$ since M is the P-primary component of $\mathrm{Tor}(Q)$, and hence consists of all those elements of $\mathrm{Tor}(Q)$ which are annihilated by some power of P. Likewise, M must too be isomorphic to the direct sum of all $R/(P')_j^{\beta_j}$ for those $(P')_j$ with $(P')_j = P$.

Thus our inquiry reduces to proving that the powers α_i and β_j are the same, for then the Primary Decomposition Theorem will allow us to carry out the process for each primary component, which will suffice to show the uniqueness of the decomposition for $\mathrm{Tor}(Q)$.

Re-indexing and rewriting each P_i and P'_j which are equal to P as simply P, we can write that

$$M \cong \bigoplus_{i=1}^{s} (R/P^{\alpha_i}) \cong \bigoplus_{j=1}^{t} (R/P^{\beta_j})$$

Now, since we have the isomorphism of R-modules:

$$PM \cong P\left(\bigoplus_{i=1}^{s}(R/P^{\alpha_i})\right) \cong \bigoplus_{i=1}^{s}(P/P^{\alpha_i})$$

We have the following sequence of isomorphisms:

$$\begin{aligned} M/PM &\cong \left(\bigoplus_{i=1}^{s}(R/P^{\alpha_i})\right) \Big/ \left(\bigoplus_{i=1}^{s}(P/P^{\alpha_i})\right) \\ &\cong \bigoplus_{i=1}^{s}((R/P^{\alpha_i})/(P/P^{\alpha_i})) \\ &\cong \bigoplus_{i=1}^{s}(R/P) \end{aligned}$$

where the final isomorphism is a consequence of the third isomorphism theorem for modules, and the second isomorphism is due to Proposition 1.13. Since P is a prime ideal of R, we know R/P is a field; hence M/PM is a vector space over R/P of dimension s.

However, an analogous process may be carried out with the $P^{\beta_1}, \dots, P^{\beta_t}$; that is, we can replace s with t and α_i with β_j in the above sequence of isomorphisms. In particular, then, M/PM also has dimension t as an (R/P)-vector space, which means that $s = t$ is required.

Given this fact, to get our uniqueness we need only prove that each α_i has a corresponding β_j for which $\alpha_i = \beta_j$.

Note that $\mathrm{Ann}_R(M) = P^k$ for some integer $k \geq 0$, since M is annihilated by powers of P. Thus we may consider the common integer:

$$k := \max\{\alpha_1, \dots, \alpha_s\} = \max\{\beta_1, \dots, \beta_s\}$$

We argue by induction on k above that each α_i has a corresponding β_j for which $\alpha_i = \beta_j$.

For our base case take $k = 1$, where the result is obvious, for then $\alpha_i = \beta_j$ for all i and j, as we took each as integers $\alpha_i, \beta_j \geq 1$; hence $\alpha_i = \beta_j = 1$ for all possible i and j, and there are the same number of α_i and β_j.

Now suppose $k > 1$. Then we can see that, in view of Proposition 4.12, the following isomorphism of R-modules holds:

$$PM \cong \bigoplus_{i=1}^{s}(P/P^{\alpha_i}) \cong \bigoplus_{i=1}^{s}\left(R/P^{\alpha_i - 1}\right)$$

Applying our inductive hypothesis to the decomposition on the right yields the desired conclusion.

Therefore there are a fixed number of direct summands of Tor(Q) isomorphic to R/P^{α}, corresponding to a fixed number of direct summands of each P-primary component of Tor(Q) isomorphic to R/P^{α}. In essence, then, the number of such direct summands is uniquely determined by Tor(Q) via the Primary Decomposition Theorem ; hence the integers $s, \alpha_1, \dots, \alpha_s \geq 1$ are unique, proving the last statement of the theorem. ■

Indeed, if Q is a finitely generated module over a Dedekind Domain R, as in the structure theorem above, then the isomorphism type of Q is determined by the rank n of Q as an R-module, the prime ideal powers $P_1^{e_1}, \dots, P_s^{e_s}$, and the class of the ideal I in the ideal class group of R.

Definition 4.16 (Steinitz class). Let R be a Dedekind Domain and let Q be a finitely generated R-module. Then the equivalence class of the ideal I appearing in decomposition of Q in Theorem 4.15 is called the *Steinitz class* of Q.

4.2.3 Corollary: Projective Modules over Dedekind Domains

Lemma 4.17. If P is a nonzero prime ideal in the Dedekind Domain R then R/P^n is not a projective R-module for any $n \geq 1$.

Proof. If we assume, for contradiction, that R/P^n is projective as an R-module, then we have that R_P/P^nR_P is a projective R_P-module, since the localization of a projective R-module is a projective module over the localized ring.

Moreover, since the localization of a Dedekind Domain at a prime ideal is, in particular, a P.I.D., via Theorem 4.3(2), we have that R_P/P^nR_P is a finitely generated projective R_P-module; hence R_P/P^nR_P is free by Theorem 3.32. This is clearly a contradiction, for freeness implies torsion-freeness for integral domains, and we obviously have $\text{Tor}(R_P/P^nR_P) = P^nR_P \neq 0$ since by assumption $P \neq 0$. Therefore R/P^n is not a projective R-module for any $n \geq 1$. ■

With Lemma 4.17 in mind, we have the following statement:

Proposition 4.18 (Projective iff torsion-free over Dedekind Domain). A finitely generated module over a Dedekind Domain is projective if and only if it is torsion-free.

Proof. In the proof of Theorem 4.15 we showed explicitly that a finitely generated torsion-free R-module is projective. By the decomposition in the same theorem, we have that Q is projective as an R-module if and only if (by Proposition 2.10) Tor(Q) is projective. Note, however, that

$$\text{Tor}(Q) \cong \bigoplus_{i=1}^{s} \left(R/P_i^{e_i}\right)$$

for some not necessarily distinct prime ideals $P_1, \ldots, P_s$ and some integers $e_1, \ldots, e_s \geq 1$. As we saw in the Lemma 4.17, $R/P_i^{e_i}$ is not a projective R-module for any e_i and prime ideal P_i; hence Q is not a projective R-module by Proposition 2.10 once more. ■

4.3 Applications to Algebraic Number Theory

We now apply some of the results we obtained in the previous sections to modules over a specific class of Dedekind Domains which are of special interest to many mathematicians. These are, of course, the rings of integers of number fields.

Recall that a *number field* is a finite extension K of $\mathbb{Q}$. To such a number field K we associate a ring $\mathcal{O}_K$, said to be the *ring of integers* of K, which contains $\mathbb{Z}$ as a subring and is the integral closure of $\mathbb{Z}$ in K (i.e., any element of K which is integral over $\mathbb{Z}$ is contained in $\mathcal{O}_K$; that is, any element of K which satisfies some polynomial with integer coefficients is contained in $\mathcal{O}_K$).

Our present discussion (and indeed, much of modern algebraic number theory) hinges on the following crucial fact.

Proposition 4.19 (**Rings of integers of number fields are Dedekind Domains**)**.** The ring of integers of a number field is a Dedekind Domain.

Proof. A proof of this inordinately important fact can be found in many introductory texts or notes on algebraic number theory. One such example is in [3]. ■

4.3.1 $\mathbb{Z}$-module Structure of Rings of Integers

Let K be a number field and let $\mathcal{O}_K$ denote its ring of integers. The purpose of this section is to prove that $\mathcal{O}_K$ as a finitely generated $\mathbb{Z}$-module; in fact, we claim that $\mathcal{O}_K$ is a finitely generated free $\mathbb{Z}$-module. Why is this the case? First and foremost, we showcase the finite generation.

Proposition 4.20. Let A be an integrally closed integral domain with field of fractions K. Let B be the integral closure of A in A in a separable extension L of K of degree m. Then there exists free A-submodules M and M' of L such that

$$M \subseteq B \subseteq M'.$$

Therefore if A is Noetherian, then B is finitely generated as an A-module. If, in addition, A is a P.I.D., then B is free of rank m.

Proof. A proof of this fact can be found on page 36 as Proposition 2.29 of J.S. Milne's note on algebraic number theory. ■

Corollary 4.21. The ring of integers of a number field K is the largest subring of K that is finitely generated as a $\mathbb{Z}$-module.

Proof. We have just seen in Proposition 4.20 that $\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module. This follows since $\mathcal{O}_K$ is a Dedekind Domain, hence an Noetherian integrally closed integral domain with field of fractions K. If now B is some other subring of K which is finitely generated as a $\mathbb{Z}$-module then every element of B is integral over $\mathbb{Z}$, hence $B \subseteq \mathcal{O}_K$. ■

There we have the first step: $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module. Next, we note that the ring $\mathbb{Z}$ is a P.I.D., and so we may apply our results on modules over P.I.D.s from previous sections; specifically, we recall that a module over a P.I.D. is torsion-free if and only if it is free (see Corollary 3.15). Since $\mathcal{O}_K$ is a subspace of the $\mathbb{Q}$-vector space K we know that $\mathcal{O}_K$ is torsion-free as a $\mathbb{Q}$-vector space, hence obviously torsion-free as a $\mathbb{Z}$-module; thus $\mathcal{O}_K$ is free as a $\mathbb{Z}$-module, as claimed.

In view of the fact that rings of integers are always finitely generated over $\mathbb{Z}$, we introduce the following definition which we shall expound on further in the next section.

Definition 4.22 (Integral basis). Let K be a number field with ring of integers $\mathcal{O}_K$. Then a basis $\alpha_1, \ldots, \alpha_m$ of $\mathcal{O}_K$ as a $\mathbb{Z}$-module is called an *integral basis* for K.

Indeed, the corollary exhibited above shows that rings of integers always have such a basis; that is, integral bases always exist.

4.3.2 Relative Integral Bases

We can push the line of inquiry we have been following further by exploring how rings of integers which are related by intermediate field extension behave with respect to one another. More precisely, for any intermediate extension of fields $\mathbb{Q} \subseteq F \subseteq K$, we have the picture

$$\begin{tikzcd}
\mathcal{O}_K \arrow[r, hook] & K \\
\mathcal{O}_F \arrow[r, hook] \arrow[u, hook] & F \arrow[u, hook] \\
\mathbb{Z} \arrow[r, hook] \arrow[u, hook] & \mathbb{Q} \arrow[u, hook]
\end{tikzcd}$$

and hence may consider $\mathcal{O}_K$ as an $\mathcal{O}_F$-module in the usual way, for instance by extending scalars from $\mathbb{Z}$ from the inclusion $\mathbb{Z} \hookrightarrow \mathcal{O}_F$. Now, since $\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module, so too must $\mathcal{O}_K$ be finitely generated as an $\mathcal{O}_F$-module (again via extending scalars). It is not true in general, however, that $\mathcal{O}_K$ need have a basis as an $\mathcal{O}_F$-module, as we shall see.

We are primarily interested in the case where $\mathcal{O}_K$ is free as a $\mathcal{O}_F$-module. In this case, there exists a $\mathcal{O}_F$-basis for $\mathcal{O}_K$. We give such a basis a special name which highlights its relative nature:

Definition 4.23 (Relative integral basis). Let K/F be an extension of number fields and let $\mathcal{O}_K$ and $\mathcal{O}_F$ denote the rings of integers of K and F, respectively. If $\mathcal{O}_K$ is free as a $\mathcal{O}_F$-module, then K is said to possess a *relative integral basis* over F.

We note that if $\mathcal{O}_F$ is a P.I.D. then $\mathcal{O}_K$ is a free $\mathcal{O}_F$-module. This follows since, as we saw previously, $\mathcal{O}_K$ is a finitely generated $\mathcal{O}_F$-module which is torsion-free (another instance of the power of Corollary 3.15). So the case where $\mathcal{O}_F$ is a P.I.D. is quite simple to dispense with. The obvious next question, then, is what might occur when $\mathcal{O}_F$ is not a P.I.D.

A common colloquialism (in certain circles) is that the ideal class group of a Dedekind Domain R measures the extent to which R is close to being a P.I.D.; that is, how far away is R from being a P.I.D. Thus we might naturally relate the notion of ideal class group of rings of integers with the question of the existence of a relative integral basis.

For now, we involve ourselves with some examples. We maintain the same setting as previously, so K/F an extension of number fields. The first example shows that $\mathcal{O}_K$ being free as a $\mathcal{O}_F$-module does not imply that $\mathcal{O}_F$ is a P.I.D.

Example 4.24. Let $K = \mathbb{Q}(i, \sqrt{-5})$ and $F = \mathbb{Q}(\sqrt{-5})$. Quadratic rings of integers are somewhat nice; we immediately have that $\mathcal{O}_F = \mathbb{Z}[\sqrt{-5}]$ (see any introductory algebraic number theory text). The ring $\mathcal{O}_K$, on the other hand, is not so simple to determine.

$$\begin{tikzcd}
\mathcal{O}_K \arrow[r, hook] & K = \mathbb{Q}(i, \sqrt{-5}) \\
\mathcal{O}_F = \mathbb{Z}[\sqrt{-5}] \arrow[u, hook] \arrow[r, hook] & F = \mathbb{Q}(\sqrt{-5}) \arrow[u, hook]
\end{tikzcd}$$

Clearly $\mathcal{O}_F = \mathbb{Z}[\sqrt{-5}]$ is not a P.I.D., for instance we have the ideal $(2, 1 + \sqrt{-5})$. However, $\mathcal{O}_K$ is a free $\mathcal{O}_F$-module since we have a relative integral basis for K over F given by

$$\{1, \frac{i + \sqrt{-5}}{2}\},$$

as can be verified by a lengthy computation.

Example 4.25. Let $K = \mathbb{Q}(\sqrt{-15}, \sqrt{26})$ and $F = \mathbb{Q}(\sqrt{-15})$. It can be found that the ideal class group of F is cyclic of order 2, hence $\mathcal{O}_F$ is not a P.I.D. However, we have

$$\mathcal{O}_K = \mathcal{O}_F \oplus \sqrt{26} \cdot \mathcal{O}_F.$$

We now invoke the structure theorem for finitely generated modules over Dedekind Domains to prove stronger results above rings of integers of number fields, as promised in the preamble to this section. We shall use both the structure theorem and one of our main results from the theory of fractional ideals in the next theorem.

Theorem 4.26. Let K/F be an extension of number fields and let $\mathcal{O}_K$ and $\mathcal{O}_F$ denote the rings of integers of K and F, respectively. If $[K : F] = n$ then

$$\mathcal{O}_K \cong \mathcal{O}_F^{n-1} \oplus I$$

is an isomorphism of $\mathcal{O}_F$-modules, where I is some non-zero ideal of $\mathcal{O}_F$.

Proof. Since, as previously mentioned, $\mathcal{O}_K$ is a finitely generated torsion-free $\mathcal{O}_F$-module, and $\mathcal{O}_F$ is a Dedekind Domain, we refer to Theorem 4.15, the structure theorem, to write that

$$\mathcal{O}_K \cong \mathcal{O}_F^{d-1} \oplus I \oplus \mathrm{Tor}(\mathcal{O}_K) = \mathcal{O}_F^{d-1} \oplus I,$$

where $d \geq 1$ is the rank of $\mathcal{O}_K$ as an $\mathcal{O}_F$-module. Now let $m = [F : \mathbb{Q}]$. Then both $\mathcal{O}_F$ and I are of rank m over $\mathbb{Z}$, and $\mathcal{O}_K$ is of rank mn over $\mathbb{Z}$. Since isomorphisms preserve rank, and by Proposition 3.10, we have

$$mn = \mathrm{rank}(\mathcal{O}_K) = \mathrm{rank}(\mathcal{O}_F^{d-1}) + \mathrm{rank}(I) = m(d-1) + m = md.$$

But now we require that $mn = md$, and hence that $n = d$ hold, finishing up the proof of the theorem. ■

Theorem 4.26 shows us that when K/F is an extension of number fields, the ring of integers of K, $\mathcal{O}_K$, is very nearly a free $\mathcal{O}_F$-module. In fact, when the ideal class group of F is trivial, that is, when $\mathcal{O}_F$ is a P.I.D., we have $I \cong \mathcal{O}_F$ as $\mathcal{O}_F$-modules for all non-zero ideals I of $\mathcal{O}_F$, and hence we have $\mathcal{O}_K \cong \mathcal{O}_F^{n-1} \oplus \mathcal{O}_F = \mathcal{O}_F^n$ when $[K : F] = n$, which means that $\mathcal{O}_K$ is a free $\mathcal{O}_F$-module of rank n.

Generally speaking, for any two non-zero ideals I and J of $\mathcal{O}_F$, we may refer to Proposition 4.12(2) to write that there is an isomorphism

$$\mathcal{O}_F^{n-1} \oplus I \cong \mathcal{O}_F^{n-1} \oplus J$$

of $\mathcal{O}_F$-modules if and only if I and J differ by a principal ideal in $\mathcal{O}_F$; that is, if and only if I and J lie in the same class in the ideal class group of F. Thus the $\mathcal{O}_F$-module isomorphism class of $\mathcal{O}_K$ depends entirely upon the ideal class group of F in a convenient way. We make the recollection that the ideal class in the ideal class group which corresponds to $\mathcal{O}_K$ as an $\mathcal{O}_F$-module is the Steinitz class of $\mathcal{O}_K$.

We now present an example to illustrate a small instance of the power of what we have covered so far.

Example 4.27. Let $K = \mathbb{Q}(\sqrt{-3}, \sqrt{-6})$ and $F = \mathbb{Q}(\sqrt{-6})$. The ideal class group of F is cyclic of order 2, certainly not trivial, and hence $\mathcal{O}_F = \mathbb{Z}[\sqrt{-6}]$ is not a P.I.D. Letting $P = (3, \sqrt{-6})$ and setting

$$\alpha := \frac{1+\sqrt{-3}}{2}$$

and

$$\beta := \frac{1}{\sqrt{-3}},$$

we can find that

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \alpha\mathbb{Z}[\sqrt{-6}] \oplus \beta(3, \sqrt{-6}) = \alpha\mathcal{O}_F \oplus \beta P.$$

Since $\beta P \cong P$ and $\alpha\mathcal{O}_F \cong \mathcal{O}_F$ as $\mathcal{O}_F$-modules, the equation above implies that we have an isomorphism

$$\mathcal{O}_K \cong \mathcal{O}_F \oplus P$$

of $\mathcal{O}_F$-modules. We claim that $\mathcal{O}_K$ is not a free $\mathcal{O}_F$-module. If this were the case, then we would require $\mathcal{O}_K \cong \mathcal{O}_F^2$ since $[K : F] = 2$, which would force

$$\mathcal{O}_F^2 = \mathcal{O}_F \oplus \mathcal{O}_F \cong \mathcal{O}_F \oplus P,$$

which would occur if and only if $\mathcal{O}_F \cong P$ as $\mathcal{O}_F$-modules, by Theorem 4.26 above. This implies that P is a principal ideal of $\mathcal{O}_F$, which is absolutely not the case, hence we have a contradiction. Therefore $\mathcal{O}_K$ is not a free $\mathcal{O}_F$-module.

❊ References

References

[1] D. Dummit, R. Foote, *Abstract Algebra*. 3rd Edition, John Wiley & Sons, Inc., 2004.

[2] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin, Heidelberg, 1999.

[3] Serge Lang, *Algebraic Number Theory*, Springer New York, New York City, 1994.