Honors Algebra IV – MATH 371

Course Notes by Dr. Eyal Goren

McGill University

Winter 2005

Last updated: September 4, 2009.

©All rights reserved to the author, Eyal Goren, Department of Mathematics and Statistics, McGill University.

Contents

1. Introduction

2. Modules

2.1. **Definition of modules, submodules, module homomorphism and quotient modules.**

Let R be a ring, always associative with 1.

Definition 2.1.1. An abelian group M is a (left) R-module if one is given a map

$$R \times M \longrightarrow M, \qquad (r, m) \mapsto rm,$$

such that:

(1) $(r+s)m = rm + sm$.
(2) $r(sm) = (rs)m$.
(3) $r(m_1 + m_2) = rm_1 + rm_2$.
(4) $1 \cdot m = m$.

(This holding for any $r, s \in R, m, m_1, m_2 \in M$).

We note two basic facts. Firstly, the definition of the map $R \times M \to M$ is part of the definition of an R-module. An abelian group could sometimes be an R module in many different ways.

Secondly, if R is a field then an R-module is just a vector space. It is a good case to keep in mind, but one must remember that R needs not be a field, not even commutative!

Here are some easy consequences of the definition:

(1) $0_R \cdot m = 0_M$.
(2) $-1 \cdot m = -m$.
(3) $r \cdot 0_M = 0_M$.

Definition 2.1.2. Let M be an R-module. A subset $N \subseteq M$ is an R-submodule if N is a subgroup of M and

$$\forall r \in R, n \in N, \quad rn \in N.$$

We note that in this case N is an R-module in its own right. Trivial examples are $N = \{0\}$ and $N = M$. It is easy to verify the following Lemma.

Lemma 2.1.3. *N is a submodule if and only if: 1) $N \neq \emptyset$ and 2) for all $n_1, n_2 \in N$, for all $r \in R$, $n_1 + rn_2 \in N$.*

Definition 2.1.4. Let M_1, M_2 be R-modules. An R-module homomorphism from M_1 to M_2 is a function,

$$f : M_1 \to M_2,$$

such that f is a group homomorphism and, in addition,

$$f(rm) = rf(m), \qquad r \in R, m \in M_1.$$

Furthermore, f is called an isomorphism if f is a bijective function.

It is easy to check that in that case $g = f^{-1}$ is also an R-module homomorphism. Also, a composition of R-module homomorphisms is an R-module homomorphism.

Let us say that M_1 is isomorphic to M_2 if there exists an R-module isomorphism $f : M_1 \to M_2$. We write $M_1 \cong M_2$. It follows from our remarks that being isomorphic is an equivalence relation on R-modules.

Lemma 2.1.5. *Let $f : M_1 \to M_2$ be an R-module homomorphism. Let*

$$\mathrm{Ker}(f) := \{m \in M_1 : f(m) = 0\}.$$

Then $\mathrm{Ker}(f)$, called the kernel of f, is a submodule of M_1. The map f is injective if and only if $\mathrm{Ker}(f) = \{0\}$.

Proof. Most of the lemma is clear because f is a group homomorphism. We only need to verify that $m \in \mathrm{Ker}(f), r \in R$ implies $rm \in \mathrm{Ker}(f)$ and indeed: $f(rm) = rf(m) = r \cdot 0 = 0$. □

Proposition 2.1.6. *Let M be an R-module and $N \subseteq M$ an R-submodule. Then M/N (the quotient abelian group) has a natural structure of an R-module given by*

$$r(m+N) = rm + N, \qquad r \in R, m \in M,$$

or, in more compact notation,

$$r\,\overline{m} = \overline{rm}.$$

Proof. The action is well-defined: if $m + N = m' + N$ then $m' = m + n$ for some $n \in N$ and so $r(m' + N) = rm + rn + N = rm + N = r(m + N)$, because $rn \in N$ implies $rn + N = N$.

The axioms now follow automatically from the fact they hold in N. For example,

$$\begin{aligned} r(\overline{m_1} + \overline{m_2}) &= r\,\overline{m_1 + m_2} \\ &= \overline{r(m_1 + m_2)} \\ &= \overline{rm_1 + rm_2} \\ &= \overline{rm_1} + \overline{rm_2} \\ &= r\,\overline{m_1} + r\,\overline{m_2}. \end{aligned}$$

□

2.2. **Examples.** The following are key examples. Every concept and theorem we will learn should be studied by you first for these examples.

2.2.1. $R = \mathbb{Z}$. Every abelian group M has a unique structure of an R module. Indeed, if M is an R-module, since $1 \cdot m = m$ then $2 \cdot m = (1+1) \cdot m = m + m$ and inductively we find that $n \cdot m = m + m + \cdots + m$ (n-times). Since $(-n)m = (-1 \cdot n)m = -1 \cdot (nm) = -nm$, also $(-n)m$ is uniquely determined and in fact $(-n)m = -(nm)$.

Conversely, for any abelian group M just define $n \cdot m = m + m + \cdots + m$ (n-times) for $n > 0$, $0 \cdot m = 0_M$, and $(-n) \cdot m = -(n \cdot m)$. This gives M a $\mathbb{Z}$-module structure. We have the following dictionary.

$\mathbb{Z}$-module	=	abelian group
$\mathbb{Z}$-submodule	=	subgroup
$\mathbb{Z}$-module homomorphism	=	group homomorphism
quotient module	=	quotient subgroup

2.2.2. $R = \mathbb{F}$, a field. We have the following dictionary.

$\mathbb{F}$-module	=	vector space
$\mathbb{F}$-submodule	=	subspace
$\mathbb{F}$-module homomorphism	=	linear transformation
quotient module	=	quotient space

2.2.3. $R = \mathbb{F}[x]$, the ring of polynomials in the variable x over a field F. Let V be an $\mathbb{F}[x]$-module. Since $\mathbb{F} \subset \mathbb{F}[x]$ we get that V is a vector space over $\mathbb{F}$. Let

$$T : V \longrightarrow V, \qquad T(v) := xv,$$

where xv is the multiplication of the ring element x with the module element v, provided by the module structure. Then T is a linear transformation. The knowledge of the vector space structure and T gives the module structure, because

$$(a_n x^n + \cdots + a_1 x + a_0)v = a_n T^n v + \cdots + a_1 T v + a_0 v.$$

(As usual T^n just means $T \circ T \circ \cdots \circ T$ (n-times).)

Conversely, let V be a vector space over $\mathbb{F}$ and T any linear map. Define an $\mathbb{F}[x]$-module structure on V by

$$(a_n x^n + \cdots + a_1 x + a_0)v := a_n T^n v + \cdots + a_1 T v + a_0 v.$$

It is easy to verify that the axioms hold.

We have the following dictionary.

$\mathbb{F}[x]$-module V	$=$	vector space V over $\mathbb{F}$ and a linear map $T : V \to V$
$\mathbb{F}[x]$-submodule	$=$	T-invariant subspace
$\mathbb{F}[x]$-module homomorphism $f : V_1 \to V_2$	$=$	linear transformation $f : V_1 \to V_2$ such that $f \circ T_1 = T_2 \circ f$
quotient module	$=$	quotient space by a T-invariant subspace

2.2.4. R and ring, $M = R$. Then a submodule is the same thing as a left ideal. We remark here that R/I (the cosets $r + I, r \in R$) is always a quotient module if I is a left ideal. Only if we want R/I to be a ring we need to require that I be a two-sided ideal.

2.2.5. Now, quite generally, if M_1, M_2 are R-modules so is

$$M_1 \oplus M_2 := \{(m_1, m_2) : m_1 \in M_1, m_2 \in M_2\},$$

under the usual group operations and where we let

$$r(m_1, m_2) = (rm_1, rm_2), \qquad r \in R.$$

In a similar way we may form the direct sum $M_1 \oplus M_2 \oplus \cdots \oplus M_n$. In particular, for any ring R,

$$R^n := \{(r_1, \ldots, r_n) : r_i \in R, i = 1, \ldots, n\},$$

is an R-module where $r(r_1, \ldots, r_n) = (rr_1, \ldots, rr_n)$.

Let M be an R-module and let $S = \{m_\alpha : \alpha \in I\}$ be a collection of elements of M indexed by a set I. Define the submodule generated by S, denoted $\langle S \rangle$, to be the set of finite sums

$$\{\sum r_i s_i : r_i \in R, s_i \in S\}.$$

It is not hard to check the following fact: if $M_1, \ldots, M_n$ are submodules of M and $S = M_1 \cup \cdots \cup M_n$ then

$$\langle S \rangle = M_1 + \cdots + M_n,$$

where

$$M_1 + \cdots + M_n := \{m_1 + \cdots + m_n : m_i \in M_i, i = 1, \ldots, n\}.$$

If $M_1, \dots, M_n$ are submodules of M then so is $M_1 \cap \cdots \cap M_n$.

If M is an R-module and I is a left ideal of R then the set

$$IM := \{\sum i_\alpha m_\alpha : i_\alpha \in I, m_\alpha \in M\}$$

(finite sums) is in fact already an R-module. Let $N \subseteq M$ be a submodule. Let the annihilator of N be

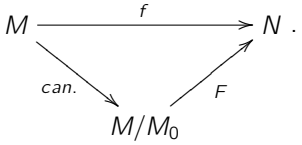
$$\mathrm{Ann}(N) := \{r \in R : rn = 0, \forall n \in N\}.$$

Then $\mathrm{Ann}(N)$ is a two sided ideal of R and N is naturally an $R/\mathrm{Ann}(N)$-module (more generally, an R/I module for any two-sided idea $I \subset \mathrm{Ann}(N)$). For example, for any two sided ideal I the annihilator of M/IM contains I and so M/IM is naturally an R/I module.

2.3. **The isomorphism theorems.** The isomorphism theorems for groups hold for modules as well, provided all subgroups are submodules. In particular, if $f\colon M \to N$ is an R-module homomorphism then $f(M)$ is an R-submodule of N. We have

$$M/\mathrm{Ker}(f) \cong f(M).$$

More generally, if $M_0 \subseteq \mathrm{Ker}(f)$ is an R-submodule then there is a unique R-module homomorphism, $F\colon M/M_0 \to N$, such that the diagram is commutative:



The kernel of F is $\mathrm{Ker}(f)/M_0$.

In the same manner as for groups one deduces

(1) If A, B, are submodules of M then

$$(A + B)/B \cong A/(A \cap B).$$

(2) If $A \subset B$ then

$$(M/A)/(B/A) \cong M/B.$$

(3) There is a bijection $B \mapsto B/A$ between submodules of B of M containing A and submodules of M/A.

Here are some examples:

(1) The map

$$p_i : M_1 \oplus \cdots \oplus M_n \to M_i, \qquad p_i(m_1, \dots, m_n) = m_i,$$

is an R-module homomorphism with kernel $M_1 \oplus \cdots \oplus \widehat{M_i} \oplus \cdots \oplus M_n$. Therefore,

$$(M_1 \oplus \cdots \oplus M_n)/(M_1 \oplus \cdots \oplus \widehat{M_i} \oplus \cdots \oplus M_n) \cong M_i.$$

(2) If $N_i \subseteq M_i$ are submodules then

$$(M_1 \oplus \cdots \oplus M_n)/(N_1 \oplus \cdots \oplus N_n) \cong (M_1/N_1) \oplus \cdots \oplus (M_n/N_n).$$

The isomorphism is induced from the homomorphism $M_1 \oplus \cdots \oplus M_n \to (M_1/N_1) \oplus \cdots (M_n/N_n)$ given by $(m_1, \dots, m_n) \mapsto (m_1 + N_1, \dots, m_n + N_n)$.

(3) Let M be an R-module and $m \in M$. Let $f : R \to M$ be the R-module homomorphism $r \mapsto rm$. The image of such f is called a cyclic module. We have

$$\mathrm{Im}(f) \cong R/\mathrm{Ann}(m),$$

where $\mathrm{Ann}(m) = \{r \in R : rm = 0\}$ is a left ideal of R.

2.3.1. *Exact sequences.* Let M_i be R-modules and $f_i : M_i \to M_{i+1}$ be R-module homomorphism. Consider the diagram (possibly infinite in each direction)

$$\cdots \longrightarrow M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \longrightarrow \cdots$$

Such a diagram is called a complex if $f_{i+1} \circ f_i = 0$ for all i. Namely, for every i we have $\mathrm{Im}(f_i) \subseteq \mathrm{Ker}(f_{i+1})$. Such a sequence is called exact if for every i we have $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$. A short exact sequence is an exact sequence of the form

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0 \ .$$

This is equivalent to saying: (i) f_1 is injective and f_2 is surjective, and (ii) $\mathrm{Im}(f_1) = \mathrm{Ker}(f_2)$.

We note that for a short exact sequence we have $M_3 \cong M_2/M_1$.

By a long exact sequence we mean an exact sequence of the form

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \cdots \longrightarrow M_n \longrightarrow 0 \ .$$

That means that f_1 is injective, f_{n-1} is surjective and for every i we have $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$.

Exercise 2.3.1. Prove that if $R = \mathbb{Z}$ and M_i are finite abelian groups then $\prod_i |M_i|^{(-1)^i} = 1$. Prove that if $R = \mathbb{F}$ is a field and M_i are finite dimensional vector spaces over $\mathbb{F}$ then $\sum_{i=1}^{n} (-1)^i \dim_{\mathbb{F}}(M_i) = 0$.

2.3.2. *Chinese Remainder Theorem.*

Theorem 2.3.2. *Let R be a commutative ring with* 1*. Let $I_1, \ldots, I_k$ be relatively prime ideals of R and let M be an R module. The natural R-module homomorphism $M \to M/I_1M \oplus \cdots \oplus M/I_kM$ induces an isomorphism*

$$M/(I_1 I_2 \ldots I_k)M \cong M/I_1M \oplus \cdots \oplus M/I_kM,$$

and, in particular,

$$(I_1 I_2 \ldots I_k)M = I_1M \cap \cdots \cap I_kM.$$

The proof the Chinese Remainder Theorem is almost verbatim the proof for rings and is left as an exercise. Here is an example: Let V be an $\mathbb{F}[x]$-module, where $\mathbb{F}$ is a field. Let m be the minimal polynomial of the linear transformation $T : V \to V, T(v) = xv$. Then V is in fact an $\mathbb{F}[x]/(m(x))$-module. Suppose that

$$m(x) = f_1(x)^{m_1} \cdots f_r(x)^{m_r}$$

is the decomposition into irreducible factors in $\mathbb{F}[x]$. Let $I_i = (f_i(x)^{m_i})$ then $(m(x)) = I_1 I_2 \cdots I_k$ and the ideals I_i are relatively prime. It follows from the Chinese Remainder Theorem that

$$V \cong V/(m(x))V \cong V/I_1V \oplus \cdots \oplus V/I_kV,$$

is a decomposition into T-invariant subspaces and it is also easy to deduce that the minimal polynomial of T on V/I_iV is $f_i(x)^{m_i}$ (it certainly divides $f_i(x)^{m_i}$ and so of the form $f_i(x)^{m_i'}$, but now calculate that $f_1(x)^{m_1'}\cdots f_r(x)^{m_r'}$ annihilates V...)

2.4. **Finitely generated modules and free modules.** Let M be an R-module. We say that M is **finitely generated** if there exist $x_1,\dots,x_n\in M$ such that the module generated by $\{x_1,\dots,x_n\}$ is M, that is, every element $m\in M$ can be expressed as $r_1x_1+\cdots+r_nx_n$ for some $r_i\in R$ (the r_i need not be unique).

Note that if R is a field that means that M is a finite dimensional vector space over R and the dimension is at most n.

An R-module M is called cyclic if it is generated by one element, say x. Then the R-module homomorphism

$$R\to M,\qquad r\mapsto rx,$$

is surjective and shows that

$$M\cong R/\mathrm{Ann}(x).$$

Conversely, for any left ideal I the module $M=R/I$ is cyclic (generated by 1).

Example 2.4.1. (1) $\mathbb{Z}/n\mathbb{Z}$ is a cyclic $\mathbb{Z}$-module generated by 1, as is $\mathbb{Z}$ itself. Every cyclic $\mathbb{Z}$-module, or (what amount to the same) every cyclic group, is one of these.

(2) Let $\mathbb{F}[x]$ act on $\mathbb{F}^2$ by x acting through

$$T\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}0&0\\1&0\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}0\\a\end{pmatrix}.$$

Then $\mathbb{F}^2$ is cyclic; $xe_1=e_2$ etc. It follows that $\mathbb{F}^2\cong\mathbb{F}[x]/\mathrm{Ann}(e_1)$. Since $T^2=0, x^2\in\mathrm{Ann}(e_1)=(f(x))$. Since $x\notin\mathrm{Ann}(x)$ it follows that $\mathrm{Ann}(x)=(x^2)$ and $\mathbb{F}^2\cong\mathbb{F}[x]/(x^2)$, as modules, for the given $\mathbb{F}[x]$ action.

Exercise 2.4.2. Let V be an $\mathbb{F}[x]$-module, finite dimensional over $\mathbb{F}$. Find a necessary and sufficient condition on the action of x for V to be a cyclic module.

The following definition is the analogue of the notion of a basis for vector spaces. A R-module M is called **free** on a set $X=\{x_1,x_2,\dots x_n\}$ of elements of M if every element $m\in M$ can be expressed uniquely in the form $r_1x_1+\cdots+r_nx_n$ for some $r_i\in R$.

Proposition 2.4.3. *M is free on a set X containing n elements if and only if $M\cong R^n$ (as R-modules).*

Proof. Suppose M is free on $X=\{x_1,\dots,x_n\}$. Define

$$\varphi: R^n\to M,$$

by

$$\varphi((r_1,\dots,r_n))=r_1x_1+\cdots+r_nx_n.$$

It is easy to check it's an isomorphism ("surjective" reduces to the fact that X is generating, "injective" follows from the uniqueness of expression).

Conversely, given an isomorphism,

$$\varphi: R^n\to M,$$

let $x_i = \varphi(e_i)$, where as usual $e_i = (0, \dots, 0, \underset{i}{1}, 0 \dots, 0)$. Let $m \in M$ then $\varphi^{-1}(m) = (r_1, \dots, r_n)$, for some r_i, and it follows that $m = r_1x_1 + \cdots + r_nx_n$. If also $m = r_1'x_1 + \dots r_n'x_n$ then $\varphi(r_1, \dots, r_n) = \varphi(r_1', \dots, r_n')$. Since φ is injective, $(r_1, \dots, r_n) = (r_1', \dots, r_n')$. □

Corollary 2.4.4. *If M is free on $X = \{x_1, \dots, x_n\}$ and N is free on $Y = \{y_1, \dots, y_n\}$ then $X \cong Y$ and, in fact, the proof gives that there is such an isomorphism taking x_i to y_i for all i.*

Our definition of a free module was quite straightforward; the following proposition shows that a free module has a certain "universal property". One can show, that any module with such universal property is free.

Proposition 2.4.5. *Let M be a free module on a set $X = \{x_1, \dots, x_n\}$ and let N be any R-module. Given any function $f : X \to N$ there exists a unique R-module homomorphism $F : M \to N$ such that $F(x_i) = f(x_i)$.*

(This should be compared with Lemma **??** in MATH 251.)

Proof. We define

$$F(r_1x_1 + \cdots + r_nx_n) = r_1f(x_1) + \cdots + r_nf(x_n).$$

The point is that this is well defined because M is free on X. It's easy to check that F has the desired properties. □

Remark 2.4.6. One can ask if M is free on X , N is free on Y and $M \cong N$ implies that $\sharp X = \sharp Y$?! We know that this holds for vector spaces. It turns out that in general the answer is no, but such examples exist only for non-commutative rings. If R is a commutative ring then indeed $\sharp X = \sharp Y$. The argument is as follows. It is easy to reduce to the case of $M = R^m, N = R^n$. First, one shows it is true if R is a field. Next, pick a maximal ideal I in R (such exists by Zorn's lemma) and prove that $R^m/IR^m \cong (R/I)^m$ and that $R^m \cong R^n$ implies that $(R/I)^m \cong (R/I)^n$ as R/I-modules. Since I is maximal R/I is a field and so we conclude that $m = n$.

3. Modules over a PID

3.1. **Some general notions, once more.**

3.1.1. *Torsion.* Let R be an integral domain. As you recall that means R is a non-zero commutative ring with 1 in which there are no zero-divisors. Let M be an R-module. Define the **torsion** of M,

$$\mathrm{Tors}(M) := \{m \in M : \exists r \in R, r \neq 0, rm = 0\}.$$

We say that M is **torsion free** if $\mathrm{Tors}(M) = \{0\}$.

Proposition 3.1.1. $\mathrm{Tors}(M)$ *is a submodule of* M.

Proof. First, $0_M \in \mathrm{Tors}(M)$ because $1 \neq 0$ in R and $1 \cdot 0M = 0_M$. Now, suppose that $x, y \in \mathrm{Tors}(M)$ and say $r_x x = r_y y = 0$ for some nonzero elements $r_x, r_y \in R$. Then, for every $r \in R$, $r_x r_y(x + ry) = r_y(r_x x) + r_x r(r_y y) = 0$. Since $r_x r_y \neq 0$, $x + ry \in \mathrm{Tors}(M)$ too. □

Example 3.1.2. Let $R = \mathbb{Z}$. $\mathrm{Tors}(M)$ is then the elements of finite order in the abelian group M.

Example 3.1.3. Let $R = \mathbb{F}[x]$ and V an R-module, finite dimensional over $\mathbb{F}$, x acting through the linear transformation T. Let $m(x)$ be the minimal polynomial of T. Then, for every $v \in V$, $m(x)v = 0$. It follows that $\mathrm{Tors}(V) = V$. In fact, $\mathrm{Ann}(V) = (m(x))$.

Let us now consider V as an $\mathbb{F}[x]/(m(x))$-module. Note that $\mathbb{F}[x]/(m(x))$ is not a domain in general and so $\mathrm{Tors}(V)$ need not be a submodule (the proof breaks down and also there are easy counter examples. Can you give one? for example when the minimal polynomial is $x(x-1)$?). However, we can still say that $\mathrm{Tors}(V) \neq 0$ (as an $\mathbb{F}[x]/(m(x))$-module) implies that there is a non-trivial T-invariant subspace $U \subsetneq V$. Indeed, if $v \in \mathrm{Tors}(V)$ is a non-zero vector then $U = \mathrm{Span}_{\mathbb{F}}(\{v, Tv, T^2v, \dots\})$ is such a subspace.

Proposition 3.1.4. *If* M *is a free* R*-module (of finite rank) then* M *is torsion-free.*

Proof. Suppose that M is free on $X = \{x_1, \dots, x_n\}$, $m \in M$ and $rm = 0$ for some nonzero $r \in R$. Write $m = r_1x_1 + \cdots + r_nx_n$ then $0 = rr_1x_1 + \cdots + rr_nx_n$ and, of course, $0 = 0_Rx_1 + \cdots + 0_Rx_n$. Since M is free on X, we must have $rr_i = 0_R$ for all i and since R is an integral domain, $r_i = 0$ for all i. Thus, $m = 0$. □

The following proposition gives us a canonical way to pass to a torsion free module, which is useful in many situations.

Proposition 3.1.5. *Let* M *be an* R*-module then* $M/\mathrm{Tors}(M)$ *is torsion-free.*

Proof. Let $\bar{m} \in M/\mathrm{Tors}(M)$ and $r \in R$ a non-zero element such that $r\bar{m} = \bar{0}$. This implies that $rm \in \mathrm{Tors}(M)$ and so there a non-zero element $r_1 \in R$ such that $r_1 rm = 0$. Then $a = r_1 r$ is a non-zero element, because R is an integral domain, such that $am = 0$. This implies that $m \in \mathrm{Tors}(M)$ and so $\bar{m} = \bar{0}$. □

Remark 3.1.6. To remark on the connection between torsion-free and free modules, we first extend our definitions. One says that an R-module M is free on a set $X \subset M$ if every element in M can be written uniquely as $r_1x_1 + \cdots + r_nx_n$ where $x_i \in X$ and $r_i \in R$; equivalently, if every function $f : X \to N$ from X to an R-module N can be extended uniquely to an R-module homomorphism $M \to N$. M is called free if it is free on some set X.

It is easy to show that if M is free then M is torsion free in the same way we did it above. On the other hand, a torsion free module need not be free. For example, $\mathbb{Q}$ is a torsion free $\mathbb{Z}$-module which is not free on any set $X \subset \mathbb{Q}$ (finite or infinite). We leave that as an exercise.

Even if M is a finitely generated module, namely $M = \langle X \rangle$ for some finite set $X \subset M$, and torsion free then M need not be free. For example, one can prove that the ideal $(2, 1 + \sqrt{-5})$ of $\mathbb{Z}[\sqrt{-5}]$ is a torsion free $\mathbb{Z}[\sqrt{-5}]$-module, which is not free.

3.1.2. *Rank.* As before, R is an integral domain. A set of elements $x_1, \ldots, x_n$ of M are called **linearly dependent** over R if there exist $r_1, \ldots, r_n$ in R, not all zero, such that $r_1x_1 + \cdots + r_nx_n = 0$. We define the **rank** of M to be the size of a maximal set of elements $x_1, \ldots, x_n$ that are linearly independent over R ($r_1x_1 + \cdots + r_nx_n = 0 \Rightarrow r_i = 0, \forall i$). We denote this number by $\mathrm{rank}(M)$.

Proposition 3.1.7. *We have* $\mathrm{rank}(M) = \mathrm{rank}(M/\mathrm{Tors}(M))$.

Proof. Let $x_1, \ldots, x_n$ be linearly independent elements of M. Suppose that $r_1\overline{x_1} + \cdots + r_n\overline{x_n} = \bar{0}$ in $M/\mathrm{Tors}(M)$. Then, for some $m \in \mathrm{Tors}(M)$ we have $r_1x_1 + \cdots + r_nx_n = m$. Let $r \in R$ be a nonzero element such that $rm = 0$. Then $rr_1x_1 + \cdots + rr_nx_n = 0$. It follows that $rr_i = 0$ for all i and so that $r_i = 0$ for all i. That shows $\overline{x_1}, \ldots, \overline{x_n}$ are linearly independent and so $\mathrm{rank}(M/\mathrm{Tors}(M)) \geq \mathrm{rank}(M)$.

On the other hand, suppose that $y_1, \ldots, y_s \in M/\mathrm{Tors}(M)$ are linearly independent and $x_i \in M$ are elements such that $\overline{x_i} = y_i$. If $r_1x_1 + \cdots + r_sx_s = 0$ then, via the homomorphism $M \to M/\mathrm{Tors}(M)$, also $r_1y_1 + \cdots + r_sy_s = 0$ and so all the r_i are zero. It follows that $\mathrm{rank}(M) \geq \mathrm{rank}(M/\mathrm{Tors}(M))$. □

Example 3.1.8. R^n has rank n. It is easy to see that the rank is at least n by considering the set $e_1, \ldots, e_n$ and a standard argument.

Suppose now that $x_1, \ldots, x_m$ are linearly independent elements of R^n and consider R^n as a subset of $\mathbb{F}^n$, where $\mathbb{F}$ is the field of fractions of R. If $m > n$ then, from the theory of vector spaces, for some $f_i \in \mathbb{F}$, not all zero, we have $f_1x_1 + \cdots + f_mx_m = 0$. Find $r \in R$ such that $r \neq 0$ and $rf_i \in R$ for all i. Then $rf_1x_1 + \cdots + rf_mx_m = 0$ and we have a contradiction.

Example 3.1.9. The rank of the ideal $(2, 1 + \sqrt{-5})$ of $\mathbb{Z}[\sqrt{-5}]$ is 1, when considered as a $\mathbb{Z}[\sqrt{-5}]$-module, though it is not generated by any single element. The rank of the ideal $(2, 1 + \sqrt{-5})$ of $\mathbb{Z}[\sqrt{-5}]$ is 2, when considered as a $\mathbb{Z}$-module; in fact 2 and $1 + \sqrt{-5}$ generate it also as a $\mathbb{Z}$-module.

3.1.3. *Internal direct sums.* Here R is not necessarily an integral domain. Let M be an R-module and $M_1, \ldots, M_n$ submodules of M.

Proposition 3.1.10. *The following are equivalent:*

(1) *The natural map* $M_1 \oplus \cdots \oplus M_n \to M$, $(m_1, \ldots, m_n) \mapsto m_1 + \cdots + m_n$, *is an isomorphism.*
(2) $M = M_1 + \cdots + M_n$ *and each* $m \in M$ *has a unique expression in the form* $m = m_1 + \cdots + m_n$ *with* $m_i \in M_i$.
(3) $M = M_1 + \cdots + M_n$ *and each* i *we have* $M_i \cap (M_1 + \cdots + \widehat{M_i} + \cdots + M_n) = \{0\}$.

The proof is almost identical to the proof of Proposition **??** of MATH 251 and so we omit it.

3.2. **The elementary divisors theorem.**

Theorem 3.2.1 (Elementary divisors theorem)**.** *Let R be a PID and N a free R-module of rank n. Let $M \subset N$ be a non-zero submodule. Then:*

(1) *M is free of some rank m, $1 \leq m \leq n$.*

(2) *There is a basis $y_1, \dots, y_n$ of N and non-zero elements $a_1|a_2|\dots|a_m$ of R such that $a_1y_1, \dots, a_my_m$ is a basis of M.*

Corollary 3.2.2. *Let $f : L \to N$ be an R-module homomorphism between two free R-modules. There exist bases $y_1, \dots, y_n$ of N and $z_1, \dots, z_t$ of L such that with respect to these bases f is given by the matrix*

$$\begin{pmatrix} a_1 & & 0 & & & \\ & \ddots & & & & \\ 0 & & a_m & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix},$$

where the a_i are not zero and $a_1|a_2|\dots|a_m$.

Proof. (Of Corollary) Let $M = f(L)$ and choose $y_1, \dots, y_n$, $a_1|a_2|\dots|a_m$ as in the EDT. Let $z_i \in L$ such that $f(z_i) = a_iy_i$, $i = 1, \dots, m$. Let $z_{m+1}, \dots, z_t$ be a basis for $\mathrm{Ker}(f)$ (which is free by the EDT). The proof is complete if we show that $z_1, \dots, z_t$ is a basis for L. Let $I = \langle z_1, \dots, z_m \rangle$, $K = \mathrm{Ker}(f) = \langle z_{m+1}, \dots, z_t \rangle$. Then:

(1) $I \cap K = \{0\}$. Indeed, if $\sum_{i=1}^m b_iz_i \in K$ then $f(\sum_{i=1}^m b_iz_i) = 0$, but $f(\sum_{i=1}^m b_iz_i) = \sum_{i=1}^m (b_ia_i)y_i$ and so every $a_ib_i = 0$. Since the a_i are non-zero and R is a domain, every b_i is zero.
(2) $I + K = L$. Indeed, given $\ell \in L$ we can write $f(\ell) = \sum_{i=1}^m b_i(a_iy_i)$ for some $b_i \in R$. Therefore, $\ell - \sum_{i=1}^m b_iz_i \in \mathrm{Ker}(f) = K$ and so for some b_i, $i = m+1, \dots, t$ we have $\ell - \sum_{i=1}^m b_iz_i = \sum_{i=m+1}^t b_iz_i$ and it follows that $\ell \in I + K$.
(3) Therefore $L = I \oplus K$ and it follows, by the usual arguments, that $z_1, \dots, z_t$ is a basis for L.

□

Exercise 3.2.3. Let $f : \mathbb{Z}^n \to \mathbb{Z}^n$ be a group homomorphism, represented by a matrix M. Prove that if $\det(M) \neq 0$ then $|\det(M)| = |\mathbb{Z}^n / f(\mathbb{Z})^n|$.

*** PROOF READ UNTIL HERE ***

Before commencing the proof of the EDT we discuss the main idea behind it. Supposing that the theorem is true, one can ask "well, what is a_1?" Supposing a basis such as the EDT promises, we can see that we can project N onto R such that the image of N is the ideal generated by a_1. Indeed, send $b_1y_1 + \dots + b_ny_n$ to b_1. This gives a well-defined R-module homomorphism

$$f : N \to R,$$

which is surjective, in fact. The image of M is thus a submodule of R, that is, an ideal, which is principal and contains a_1. Moreover, since every element in M has the form $c_1a_1y_1 + \dots + c_ma_my_m$, we see that the image is exactly the ideal a_1.

It is a bit more subtle, but in fact for every homomorphism

$$\phi : N \to L$$

we have that $\mathrm{Im}(f) \subseteq (a_1)$. Indeed, we have

$$\phi(\sum_{i=1}^{m} b_i \cdot a_i y_i) = \sum_{i=1}^{m} a_i b_i \phi(y_i) \in (a_1),$$

because of the condition $a_1|a_2|\ldots|a_m$.

This discussion motivate the following key lemma, which is the first part of the proof of the EDT (and thus does not use the EDT at all):

Lemma 3.2.4. *Let the notation be as in the EDT. There is a non-zero element $a_1 \in R$ and $y \in M$ such that for every homomorphism $\phi : N \to R$ we have $a_1|\phi(y)$. Moreover, if $\phi(M) \supseteq (a_1)$ then $\phi(M) = (a_1)$.*

Proof. Consider the set $\Sigma = \{\phi(M) : \phi \in \mathrm{Hom}_R(N, R)\}$. Then Σ is a collection of ideals of R, which is non-empty because $(0) \in \Sigma$ (coming from the zero homomorphism, for example). For every ϕ choose a_ϕ such that $\phi(M) = (a_\phi)$. We note that Σ is partially ordered with respect to inclusion. Suppose that Σ doesn't have a maximal element. Then we can find $\phi_1, \phi_2, \cdots \in \mathrm{Hom}_R(N, R)$ such that

$$(a_{\phi_1}) \subsetneqq (a_{\phi_2}) \subsetneqq \ldots$$

But $\cup_{i=1}^{\infty}(a_{\phi_i})$ is also an ideal, say equal to (a). We must have $a \in (a_{\phi_i})$ for some i and that gives $(a_{\phi_{i+1}}) \subseteq (a) \subseteq (a_{\phi_i})$, which is a contradiction. Therefore, there is a homomorphism $f : N \to R$ such that $f(M)$ is a maximal element of Σ. Let $a_1 = a_f$ and let $y \in M$ be such that $f(y) = a_1$.

Choose an isomorphism $g : N \to R^n$. The R-module homomorphisms $p_i \circ g : N \to R$, where p_i is the projection on the i-th coordinate, show that that for some i, $p_i \circ g(M) \neq 0$. It follows that $a_1 \neq 0$.

Let $\phi \in \mathrm{Hom}_R(N, R)$ and let $d = \gcd(f(y), \phi(y)) = \alpha f(y) + \beta\phi(y)$, for some $\alpha, \beta \in R$. Then $g = \alpha f + \beta\phi \in \mathrm{Hom}_R(N, R)$ and $d = g(y) \in g(M)$ and therefore $g(M) \supseteq (f(y))$. It follows from maximality of $(f(y))$ that $(d) = (f(y))$, that is $d \sim f(y)$, and so that $f(y)$, i.e., a_1, divides $\phi(y)$. □

It follows from the lemma that $a_1|(p_i \circ g)(y)$ for all i and so that there is a $y_1 \in N$ such that $y = a_1 y_1$. Now, since $f(N) = R$ and is generated by $f(y_1)$ and $f(M) = (a_1)$ and is generated by $f(a_1 y_1)$, we conclude as in the proof of the corollary that:

$$N = \langle y_1 \rangle \oplus \mathrm{Ker}(f), \qquad N = \langle a_1 y_1 \rangle \oplus (\mathrm{Ker}(f) \cap M) = \langle a_1 y_1 \rangle \oplus (\mathrm{Ker}(f|_M)).$$

We now prove part (1) of the EDT by induction on the rank m of M. Consider $\mathrm{Ker}(f) \cap M$. It it has rank ℓ then M has rank at least $\ell + 1$. It follows that $\ell \leq m - 1$. We may now apply induction to $\mathrm{Ker}(f) \cap M$ (if $\ell = 0$ then, since M is torsion free, it means that every element of $\mathrm{Ker}(f) \cap M$ is zero) to conclude that $\mathrm{Ker}(f) \cap M$ is free of rank ℓ and so M is free of rank $\ell + 1$. It now follows that $\ell + 1 = m$.

We next prove part (2) of the EDT, this time by induction on $n = \mathrm{rank}(N)$. By the above, and since we already know part (1), we have the situation

$$M \cap \mathrm{Ker}(f) \subseteq \mathrm{Ker}(f),$$

inclusion of free modules of rank $m - 1$ and $n - 1$, respectively. Therefore, by induction, there exists a basis $y_2, \ldots, y_n$ of $\ker(f)$ (and so $y_1, \ldots, y_n$) is a basis of N and non-zero elements $a_2|a_3|\ldots|a_m$ of R such that $M \cap \mathrm{Ker}(f)$ is free on $a_2 y_2, a_3 y_3, \ldots, a_m y_m$ and so M is free on $a_1 y_1, a_2 y_2, a_3 y_3, \ldots, a_m y_m$. It only remains to show that $a_1|a_2$.

Apply the lemma to the R-module homomorphism $\phi := (p_1 + p_2) \circ g$. Then $\phi(a_1 y_1) = a_1$ and this implies that $\phi(M) \supseteq (a_1)$, hence that $\phi(M) = (a_1)$. It follows that $\phi(a_2 y_2) = a_2 \in (a_1)$ and so that $a_1 | a_2$.

3.3. **The structure theorem for finitely generated modules over a PID.**

Theorem 3.3.1 (Existence of decomposition in invariant factors form)**.** *Let R be a PID and M a finitely generated R-module. Then:*

(1) *$M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$, for $r \geq 0$, equal to the rank of M, and some non-zero $a_i \in R$ satisfying $a_1 | a_2 | \ldots | a_m$.*
(2) *M is torsion free if and only if M is free. In fact, $\mathrm{Tors}(M) = R/(a_1) \oplus \cdots \oplus R/(a_m)$. M is torsion if and only if $r = 0$ and then $\mathrm{Ann}(M) = (a_m)$.*

Proof. Let $x_1, \ldots, x_n$ be generators for M. The map,

$$R^n \to M, \qquad (r_1, \ldots, r_n) \mapsto r_1 x_1 + \cdots + r_n x_n,$$

is thus a surjective R-homomorphism. Let K be its kernel and apply the EDT to the pair $K \subseteq R^n$. There is a basis $y_1, \ldots, y_n$ to R^n and non-zero elements of R, $a_1 | a_2 | \ldots | a_m$, such that $a_1 y_1, \ldots, a_m y_m$ are a basis for K. Then

$$\begin{aligned} M &\cong R^n / K \\ &\cong (Ry_1 \oplus \cdots \oplus Ry_n) \,/\, (Ra_1 y_1 \oplus \cdots \oplus Ra_m y_m \oplus \{0\} \oplus \cdots \oplus \{0\}) \\ &\cong \oplus_{i=1}^m R/(a_i) \oplus R^{n-m}. \end{aligned}$$

Since $\mathrm{Ann}(R/(a_i)) = (a_i)$ we see that $\mathrm{Tors}(M) \cong \oplus_{i=1}^m R/(a_i)$; we find that M is torsion free implies that m is zero and so M is free. Since $\mathrm{rank}(M) = \mathrm{rank}(M/\mathrm{Tors}(M)) = n - m$ (Proposition 3.1.7) it follows that $r = n - m$ is the rank of M. We know in general (Proposition 3.1.4) that a free module is torsion free. Finally, M is torsion implies that $r = 0$ and we then have $\mathrm{Ann}(M) = (a_m)$. □

Remark 3.3.2. If any of the a_i are units then $R/(a_i) \cong \{0\}$ and so we may remove them. Thus, one may assume that none of the a_i are units. Then, as we shall see, the ideals (a_i) are uniquely determined by M (and is r, being the rank of M, is determined by M). The elements $a_1, \ldots, a_m$ (up to units) are called the invariant factors of M.

Corollary 3.3.3. *Let M be a finitely generated abelian group then*

$$M \cong \mathbb{Z}^r \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_m\mathbb{Z},$$

where r is the rank of M and the a_i are integers such that $1 < a_1 | a_2 | \ldots | a_m$ (uniquely determined by M, as we shall see).

Corollary 3.3.4. *Let V be a finite dimensional vector space over a field $\mathbb{F}$. Let $T : V \to V$ be a linear map and view this way V as an $\mathbb{F}[x]$-module. Since $\mathbb{F}[x]$ is infinite dimensional over $\mathbb{F}$ the rank of V is zero and so*

$$V \cong \sum_{i=1}^m \mathbb{F}[x]/(a_i(x)),$$

for some non-constant polynomials $a_i(x)$ such that $a_1(x) | a_2(x) | \ldots | a_m(x)$. The minimal polynomial of T is $a_m(x)$.

Note that each $\mathbb{F}[x]/(a_i(x))$ corresponds to a T invariant subspace $V_i \subset V$. In fact it is a cyclic space: if $1 \in \mathbb{F}$ corresponds to $v_i \in V_i$ then a basis for V_i consists of $v_i, Tv_i, T^2v_i, \ldots, T^{\deg(a_i)-1}v_i$. Let $a_i(x) = b_0 + b_1x + \cdots + b_{s-1}x^{s-1} + x^s$. The map T acts on V_i, relative to this basis, by the $s \times s$ matrix

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -b_0 \\ 1 & 0 & \ldots & 0 & -b_1 \\ & 1 & & \vdots & \vdots \\ & & & 0 & -b_{s-2} \\ & & & 1 & -b_{s-1} \end{pmatrix},$$

whose minimal polynomial is $a_i(x)$.

We also remark that this theorem clarifies exactly the information held in the minimal polynomial $a_m(x)$. Also, note that $\Delta_T(x) = a_1(x) \cdot a_2(x) \cdots a_m(x)$ and we conclude that $m_T(x)|\Delta_T(x)$ but also, since each $a_i(x)|a_m(x)$, that Δ_T and m_T have the same irreducible factors.

Corollary 3.3.5 (Existence of decomposition in elementary divisors form)**.** [1] *Let M be a finitely generated module over a PID R. Then, there are irreducible elements p_i of R, not necessarily distinct, and integers $\alpha_i \geq 1$, such that*

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

Proof. Using the EDT we may assume that $M = R/(a)$. Let $a = p_1^{b_1} \cdots p_d^{b_d}$ be the prime decomposition of a. Then by CRT we have

$$R/(a) \cong R/(p_1^{b_1} \oplus \cdots \oplus R/(p_d^{b_d}).$$

□

We remark that in turn existence of decomposition in elementary divisors form implies existence of decomposition in invariant factors form. The idea is rather simple. List the elementary divisors in a form of a table

$$\begin{matrix} p_1^{b_1^1} & p_1^{b_2^1} & \ldots & p_1^{b_n^1} \\ p_2^{b_1^2} & p_2^{b_2^2} & \ldots & p_2^{b_n^2} \\ & & \vdots & \\ p_s^{b_1^s} & p_s^{b_2^s} & \ldots & p_s^{b_n^s} \end{matrix}$$

where to simplify notation we allow here some of the b_i^j to be zero (but for at least one j we have $b_1^j > 0$. We order the powers so that for every j we have $b_1^j \leq b_2^j \leq \cdots \leq b_j^n$. We now let

$$c_1 = p_1^{b_1^1} p_2^{b_1^2} \cdots p_s^{b_1^s}, \quad c_2 = p_1^{b_2^1} p_2^{b_2^2} \cdots p_s^{b_2^s}, \ldots, \quad c_s = p_1^{b_s^1} p_2^{b_s^2} \cdots p_s^{b_s^s}.$$

Then we have $c_1|c_2|\ldots|c_s$ and, by CRT $M \cong \oplus_{i=1}^s R/(c_i)$. We leave it to you to verify that in fact this is the only way one can pass from elementary divisors to invariant factors, assuming uniqueness for elementary divisors. Therefore, to prove uniqueness of decomposition in invariant factors form it is enough to prove uniqueness of decomposition in elementary divisors form, which we now do.

[1] Note that the terminology is a bit confusing when compared with the elementary divisors theorem!

Theorem 3.3.6 (Uniqueness of decomposition in elementary divisors form)**.** *Suppose that* $R^{r_1} \oplus \oplus_i R/(p_i^{a_i}) \cong R^{r_2} \oplus \oplus_j R/(q_j^{b_j})$*, where* p_i, q_j *are primes and* a_i, b_j *are positive integers. Then, after reindexing, there is the same number of summands,* $r_1 = r_2$ *and* $p_i \sim q_i$ *and* $a_i = b_i$ *for every* i*.*

Proof. The proof begins by a series of reductions. First, let M_1 denote the left hand side and M_2 the right hand side. Then, $M_1 \cong M_2$ implies that $\mathrm{Tors}(M_1) \cong \mathrm{Tors}(M_2)$ and so that

$$R^{r_1} \cong M_1/\mathrm{Tors}(M_1) \cong M_2/\mathrm{Tors}(M_2) \cong R^{r_2}.$$

it follows that $r_1 = r_2$.

We may then just examine $\mathrm{Tors}(M_1) \cong \mathrm{Tors}(M_2)$ and so we may assume that $M_1 = \oplus_i R/(p_i^{a_i}), M_2 = \oplus_j R/(q_j^{b_j})$. We now perform a second reduction step. Let p be any prime of R and M any R-module, the p-**primary component** of M is

$$M_p := \{m \in M : \exists b > 0, p^b m = 0\}.$$

This of course depends only on p modulo units, namely on (p). It is a submodule of M. One also checks the following facts:

- $(M \oplus M')_p = M_p \oplus M'_p$. The proof here is "automatic".
- If q is a prime and q and p are not associates then $(R/(q^a))_p = \{0\}$ for $a > 0$. Indeed, let $x \in (R/(q^a))_p$ then we have for some $b > 0$, $p^b x = q^a x = 0$. Since $(p^b, q^a) = 1$ we have $1 = \alpha p^b + \beta q^a$ for some $\alpha, \beta \in R$ and so also $1 \cdot x = 0$. Thus, $x = 0$.
- $(R/(p^a))_p = R/(p^a)$ as clearly every element of $R/(p^a)$ is killed by p^a.

Since $M_1 \cong M_2$, we conclude that $(M_1)_p \cong (M_2)_p$ and $(M_1)_p \cong \oplus_{i:p_i=p} R/(p^{a_i})$, $(M_2)_p \cong \oplus_{j:q_j=p} R/(p^{b_j})$. We conclude that it is enough to prove that if

$$\oplus_i^{n_1} R/(p^{a_i}) \cong \oplus_j^{n_2} R/(p^{b_j}),$$

for positive integers a_i, b_j, such that $0 < a_1 \leq a_2 \leq \ldots$, $0 < b_1 \leq b_2 \leq \ldots$, then $n_1 = n_2$ and $a_i = b_i$ for all i.

Consider the R-module $R/(p^c)$ and let $r \geq 0$. We have a surjective R module homomorphism $M \to p^r M/p^{r+1}M$ with kernel $\{m \in M : p^r m = 0\}$. The kernel is isomorphic to pM if $r < c$ and to M if $r \geq c$. Therefore

$$p^r M/p^{r+1}M \cong \begin{cases} 0 & r \geq c \\ R/pR & r < c. \end{cases}$$

Let $\mathbb{F} := R/pR$, a field. We have

$$p^r M_1/p^{r+1}M_1 = \mathbb{F}^{m(r)}, \quad m(r) = \sharp\{a_i : r < a_i\},$$

and

$$p^r M_2/p^{r+1}M_2 = \mathbb{F}^{m'(r)}, \quad m'(r) = \sharp\{b_i : r < b_i\}.$$

It follows from considering dimensions over $\mathbb{F}$ that $m(r) = m'(r)$ for every r. It follows from that the sequences $a_1 \leq a_2 \leq$ and $b_1 \leq b_2 \leq$ are equal. □

As we have remarked, using the CRT and some combinatorics, the following uniqueness statement follows.

Theorem 3.3.7 (Uniqueness in invariant factors form)**.** *If*

$$R^{r_1} \oplus \oplus_{i=1}^{n_1} R/(a_i) \cong R^{r_2} \oplus \oplus_{i=1}^{n_2} R/(b_i),$$

with $0 \neq a_1|a_2|\dots|a_{n_1}$, $0 \neq b_1|b_2|\dots|b_{n_2}$, *with* a_i, b_j *not units then* $r_1 = r_2, n_1 = n_2$ *and* $a_i \sim b_i$ *for every* i.

3.4. **Applications of the structure theorem for modules over a PID.** We repeat here the applications already mentioned previously, with a more detailed discussion.

3.4.1. $R = \mathbb{Z}$. .

Theorem 3.4.1 (The fundamental theorem of abelian groups)**.** *Every finitely generated abelian group* M *is isomorphic to*

$$\mathbb{Z}^r \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_n\mathbb{Z},$$

for a unique r*, called the rank of* M*,* $n \geq 0$ *and unique integers* $1 < a_1|a_2|\dots|a_n$.

Alternately, it is isomorphic to a group of the form

$$\mathbb{Z}^r \oplus \mathbb{Z}/p_1^{b_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/{p_s}^{b_s}\mathbb{Z},$$

for primes p_i *and integers* $b_i > 0$. *The primes and the exponents are uniquely determined by* M.

Exercise 3.4.2. Recall the **partition function** $p(n)$. For every positive integer n, $p(n)$ is the numbers of ways one can express n as $a_1 + \cdots + a_r$ where the $a_i \geq 1$ are integers (any such sequence $(a_1, \dots, a_r)$ is called a partition of n). Here are some examples:

n	partitions of n	$p(n)$
1	(1)	1
2	$(1,1), (2)$	2
4	$(1,1,1,1), (1,1,2), (1,3), (2,2), (4)$	5
7	$(1,1,1,1,1,1,1), (1,1,1,1,1,2), (1,1,1,1,3),$ $(1,1,1,2,2), (1,1,1,4), (1,1,2,3), (1,1,5), (1,2,2,2),$ $(1,2,4), (1,3,3), (1,6), (2,2,3), (2,5), (3,4), (7)$	14

Let $n = p_1^{a_1} \cdots p_r^{a_r}$, product of distinct primes to positive exponents. Prove that the number of abelian groups of order n, up to isomorphism, is the product $p(a_1)p(a_2)\cdots p(a_r)$.