Modules Over Principal Ideal Domains

Brian Whetter

University of Puget Sound

4/30/2014
# Table of Contents

1. Introduction
2. Defining a Module
3. Module Properties
4. Modules Over Principle Ideal Domains
5. Conclusion
6. References
Introduction

A module, in short is a generalization of a vector space. One may ask, why do we care?
Introduction

A module, in short is a generalization of a vector space. One may ask, why do we care?

1. In general, it is good to generalize mathematical structures.
Introduction

A module, in short is a generalization of a vector space. One may ask, why do we care?

1. In general, it is good to generalize mathematical structures.
2. The mathematics you will see here is typical of what might go on in an abstract algebra course.
Introduction

A module, in short is a generalization of a vector space. One may ask, why do we care?

1. In general, it is good to generalize mathematical structures.
2. The mathematics you will see here is typical of what might go on in an abstract algebra course.
3. You can apply them to generate canonical forms of matrices.
Introduction

A module, in short is a generalization of a vector space. One may ask, why do we care?

1. In general, it is good to generalize mathematical structures.
2. The mathematics you will see here is typical of what might go on in an abstract algebra course.
3. You can apply them to generate canonical forms of matrices.
4. They are cool.
# Table of Contents

1. **Introduction**
2. **Defining a Module**
3. **Module Properties**
4. **Modules Over Principle Ideal Domains**
5. **Conclusion**
6. **References**
Defining a Module

- A module is a generalization of a vector space. Instead of our scalers coming from a field, they come from a ring.
Defining a Module

- A module is a generalization of a vector space. Instead of our scalers coming from a field, they come from a ring.
- A field is just a ring with additional structure added. So similarly, a vector space is a “very structured” module.
Defining a Module

- A module is a generalization of a vector space. Instead of our scalers coming from a field, they come from a ring.
- A field is just a ring with additional structure added. So similarly, a vector space is a “very structured” module.
- Before we can define a module we need to introduce the concept of a ring and of a group.
What is a Field?

Let us work backwards from a familiar object, a field!

**Definition**

A field is a set $F$ along with two operations multiplication $(\cdot)$ and addition $(+)$ such that the following hold...

1. **Closure:** For all $a, b \in F$, $a + b$ and $a \cdot b$ are in $F$.
2. **Associativity:** For all $a, b, c \in F$, $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. **Commutativity:** For all $a, b \in F$, $a + b = b + a$ and $a \cdot b = b \cdot a$.
4. **Identities:** There are identity elements 0 and 1 in $F$, such that for all $f \in F$, $0 + f = f$ and $1 \cdot f = f$.
5. **Inverses:** For all $f \in F$, there exist elements $-f \in F$ and $f^{-1} \in F$ such that $f + (-f) = 0$ and $f \cdot f^{-1} = 1$.
6. **Distribution:** For all $a, b, c \in F$, $a \cdot (b + c) = a \cdot b + a \cdot c$.
What is a Field?

Let us work backwards from a familiar object, a field!

Definition

A field is a set $F$ along with two operations multiplication ($\cdot$) and addition (+) such that the following hold...

- **Closure**: For all $a, b \in F$, $a + b$ and $a \cdot b$ are in $F$. 
What is a Field?

Let us work backwards from a familiar object, a field!

**Definition**

A field is a set $F$ along with two operations multiplication ($\cdot$) and addition (+) such that the following hold...

- **Closure**: For all $a, b \in F$, $a + b$ and $a \cdot b$ are in $F$.
- **Associativity**: For all $a, b, c \in F$, $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
What is a Field?

Let us work backwards from a familiar object, a field!

**Definition**

A field is a set $F$ along with two operations multiplication ($\cdot$) and addition ($+$) such that the following hold...

- **Closure:** For all $a, b \in F$, $a + b$ and $a \cdot b$ are in $F$.
- **Associativity:** For all $a, b, c \in F$, $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- **Commutativity:** For all $a, b \in F$, $a + b = b + a$ and $a \cdot b = b \cdot a$. 
What is a Field?

Let us work backwards from a familiar object, a field!

Definition

A field is a set $F$ along with two operations multiplication ($\cdot$) and addition ($+$) such that the following hold...

- **Closure**: For all $a, b \in F$, $a + b$ and $a \cdot b$ are in $F$.
- **Associativity**: For all $a, b, c \in F$, $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- **Commutativity**: For all $a, b \in F$, $a + b = b + a$ and $a \cdot b = b \cdot a$.
- **Identities**: There are identity elements $0$ and $1$ in $F$, such that for all $f \in F$, $0 + f = f$ and $1 \cdot f = f$. 


What is a Field?

Let us work backwards from a familiar object, a field!

Definition

A field is a set $F$ along with two operations multiplication ($\cdot$) and addition ($+$) such that the following hold...

- Closure: For all $a, b \in F$, $a + b$ and $a \cdot b$ are in $F$.
- Associativity: For all $a, b, c \in F$, $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Commutativity: For all $a, b \in F$, $a + b = b + a$ and $a \cdot b = b \cdot a$.
- Identities: There are identity elements 0 and 1 in $F$, such that for all $f \in F$, $0 + f = f$ and $1 \cdot f = f$.
- Inverses: For all $f \in F$, there exist elements $-f \in F$ and $f^{-1} \in F$ such that $f + -f = 0$ and $f \cdot f^{-1} = 1$. 
What is a Field?

Let us work backwards from a familiar object, a field!

**Definition**

A field is a set $F$ along with two operations multiplication ($\cdot$) and addition ($+$) such that the following hold...

- **Closure:** For all $a, b \in F$, $a + b$ and $a \cdot b$ are in $F$.
- **Associativity:** For all $a, b, c \in F$, $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- **Commutativity:** For all $a, b \in F$, $a + b = b + a$ and $a \cdot b = b \cdot a$.
- **Identities:** There are identity elements 0 and 1 in $f$, such that for all $f \in F$, $0 + f = f$ and $1 \cdot f = f$.
- **Inverses:** For all $f \in F$, there exist elements $-f \in F$ and $f^{-1} \in F$ such that $f + -f = 0$ and $f \cdot f^{-1} = 1$.
- **Distribution:** For all $a, b, c \in F$, $a \cdot (b + c) = a \cdot b + a \cdot c$. 
What is a Ring?

A ring $R$, is very similar to a field. We still have two operations, but we abandon the following...
What is a Ring?

A ring $R$, is very similar to a field. We still have two operations, but we abandon the following...

(i) Multiplication does not need to commute.
What is a Ring?

A ring $R$, is very similar to a field. We still have two operations, but we abandon the following...

(i) Multiplication does not need to commute.
(ii) There does not need to be a multiplicative identity 1.
A ring $R$, is very similar to a field. We still have two operations, but we abandon the following...

(i) Multiplication does not need to commute.
(ii) There does not need to be a multiplicative identity $1$.
(iii) Given an element $r \in R$, there does not need to be a multiplicative inverse.
Examples

Example

$\mathbb{Z}$, with “regular” addition and multiplication.
Examples

Example
\( \mathbb{Z} \), with “regular” addition and multiplication.

Example
\( \mathbb{Z}_n \) with modular addition and multiplication.
Examples

Example
\( \mathbb{Z} \), with “regular” addition and multiplication.

Example
\( \mathbb{Z}_n \) with modular addition and multiplication.

Example
\( M_2(\mathbb{R}) \), the set of all 2 \( \times \) 2 matrices with real coefficients under matrix addition and multiplication.
What is a Group

A group $G$ is one of the simplest algebraic structures to define. It only has one operator, and it does not need to be commmunative. All that remains is...
A group $G$ is one of the simplest algebraic structures to define. It only has one operator, and it does not need to be commmumnative. All that remains is...

(i) Closure
A group $G$ is one of the simplest algebraic structures to define. It only has one operator, and it does not need to be commutative. All that remains is...

(i) Closure

(ii) Associativity
What is a Group

A group $G$ is one of the simplest algebraic structures to define. It only has one operator, and it does not need to be commmununative. All that remains is...

(i) Closure
(ii) Associativity
(iii) Identity
What is a Group

A group $G$ is one of the simplest algebraic structures to define. It only has one operator, and it does not need to be commmutative. All that remains is...

(i) Closure
(ii) Associativity
(iii) Identity
(iv) Inverses

Note, if a group has an operation that is commutative, we say that it is an abelian group.
Examples

Example

\( \mathbb{Z} \), under “regular” addition.
Examples

Example
\( \mathbb{Z} \), under “regular” addition.

Example
\( \mathbb{Z}_n \) with modular addition.
Examples

Example
\( \mathbb{Z} \), under “regular” addition.

Example
\( \mathbb{Z}_n \) with modular addition.

Example
\( M_2(\mathbb{R}) \) under matrix multiplication.
Examples

Example
\( \mathbb{Z} \), under “regular” addition.

Example
\( \mathbb{Z}_n \) with modular addition.

Example
\( M_2(\mathbb{R}) \) under matrix multiplication.

Example
The set of vectors in \( \mathbb{C}^n \) under vector addition.
What is a Module?

Definition

If $R$ is a commutative ring, then an $R$-module is an abelian group $M$ equipped with a scalar multiplication $R \times M \to M$, denoted by $(r, m) \to rm$, such that the following axioms hold for all $m, m' \in M$ and all $r, r', 1 \in R$:

1. $r(m + m') = rm + rm'$
2. $(r + r')m = rm + r'm$
3. $(rr')m = r(r'm)$
4. $1m = m$. 
Simple Example

Example
If we let $R = \mathbb{Z}$ and let our underlying group $G = \mathbb{Z}_6$, then we have a $\mathbb{Z}$-module, where scalar multiplication is defined as group exponentiation.
Simple Example

Example
If we let $R = \mathbb{Z}$ and let our underlying group $G = \mathbb{Z}_6$, then we have a $\mathbb{Z}$-module, where scalar multiplication is defined as group exponentiation.

Example (Calculation)

$$4(2 + 3) = 4(5) = 5^4 = 5 + 5 + 5 + 5 = 20 \equiv_6 2$$

Note: We could actually let $G$ be any abelian group, and we could still define a $\mathbb{Z}$-module with scalar multiplication defined as exponentiation.
Exotic Example

Here we give a more interesting example.
Exotic Example

Here we give a more interesting example.

- First note that if $k$ is a field, then $k[x]$, the set of polynomials with coefficients in $k$ is a commutative ring (this is a basic result from ring theory). We can now create a $k[x]$-module given a linear transformation $T : V \to V$ where $V$ is a finite dimensional vector space over $k$. 
Exotic Example

Here we give a more interesting example.

- First note that if $k$ is a field, then $k[x]$, the set of polynomials with coefficients in $k$ is a commutative ring (this is a basic result from ring theory). We can now create a $k[x]$-module given a linear transformation $T : V \rightarrow V$ where $V$ is a finite dimensional vector space over $k$.
- We now define scaler $k[x] \times V \rightarrow V$ multiplication as...
Given $f(x) = \sum_{i=0}^{m} c_i x^i \in k[x]$, then

$$f(x)v = \left( \sum_{i=0}^{m} c_i x^i \right) v = \sum_{i=0}^{m} c_i T^i(v)$$

where $T^0$ is the identity map $1_v$, and $T^i$ is the composite of $T$ with itself $i$ times if $i \geq 1$. We denote $V$ when viewed under a $k[x]$ module by $V^T$. 
Exotic Example

Given $f(x) = \sum_{i=0}^{m} c_i x^i \in k[x]$, then

$$f(x)v = \left( \sum_{i=0}^{m} c_i x^i \right) v = \sum_{i=0}^{m} c_i T^i(v)$$

where $T^0$ is the identity map $1_v$, and $T^i$ is the composite of $T$ with itself $i$ times if $i \geq 1$. We denote $V$ when viewed under a $k[x]$ module by $V^T$.

The module defined above is extremely important for deriving canonical forms.
Overview

Many of the structural concepts from vector spaces have analogous concepts in modules. Namely...
Overview

Many of the structural concepts from vector spaces have analogous concepts in modules. Namely...

- Instead of subspaces, we have submodules.
Overview

Many of the structural concepts from vector spaces have analogous concepts in modules. Namely...

- Instead of subspaces, we have submodules.
- Instead of linear transformations, we have $R$-maps.
Overview

Many of the structural concepts from vector spaces have analogous concepts in modules. Namely...

- Instead of subspaces, we have submodules.
- Instead of linear transformations, we have $R$-maps.
- Both have a kernel.
Overview

Many of the structural concepts from vector spaces have analogous concepts in modules. Namely...

- Instead of subspaces, we have submodules.
- Instead of linear transformations, we have $R$-maps.
- Both have a kernel.
- Both have a direct and internal direct sum.
Overview

Many of the structural concepts from vector spaces have analogous concepts in modules. Namely...

- Instead of subspaces, we have submodules.
- Instead of linear transformations, we have $R$-maps.
- Both have a kernel.
- Both have a direct and internal direct sum.
- Instead of having a finite bases, a module is finitely generated (this might be a stretch).
Cyclic Submodules

A submodule is exactly how you think it would be.

**Definition**

\( N \) is a submodule of \( R \)-module \( M \) if whenever \( n_1, n_2 \in N \), then \( n_1 + n_2 \in N \) and \( rn \in N \) for all \( r \in R \) and \( n \in N \).
Cyclic Submodules

A submodule is exactly how you think it would be.

**Definition**

$N$ is a submodule of $R$-module $M$ if whenever $n_1, n_2 \in N$, then $n_1 + n_2 \in N$ and $rn \in N$ for all $r \in R$ and $n \in N$.

**Definition**

If $M$ is an $R$-module and $m \in M$, then the **cyclic submodule** generated by $m$ is

$$\langle m \rangle = \{rm : r \in R\}.$$
Cyclic Submodules

A submodule is exactly how you think it would be.

**Definition**

\( N \) is a submodule of \( R \)-module \( M \) if whenever \( n_1, n_2 \in N \), then \( n_1 + n_2 \in N \) and \( rn \in N \) for all \( r \in R \) and \( n \in N \).

**Definition**

If \( M \) is an \( R \)-module and \( m \in M \), then the **cyclic submodule** generated by \( m \) is

\[
\langle m \rangle = \{ rm : r \in R \}.
\]

A module is cyclic if \( M = \langle m \rangle \) for some \( m \). This is “like” having a basis with dimension 1.
Cyclic Submodules

We can have more than one element generating a submodule as well.

**Definition**

A submodule generated by a set $X$ is

$$\langle X \rangle = \left\{ \sum_{\text{finite}} r_i x_i : r_i \in R \text{ and } x_i \in X \right\}.$$
Cyclic Submodules

We can have more than one element generating a submodule as well.

**Definition**

A submodule generated by a set \( X \) is

\[
\langle X \rangle = \left\{ \sum \text{finite} r_i x_i : r_i \in R \text{ and } x_i \in X \right\}.
\]

If \( X \) is a finite set and \( M = \langle X \rangle \), this is like a vector space having a finite basis. Note however, that a smaller set \( X \) could generate the same submodule, and so it is not completely analoguous.
Examples

Example

Our example before where $R = \mathbb{Z}$ and $G = \mathbb{Z}_6$ is cyclic, since 1 added with itself multiple times can generate everything in the group. If $G = \mathbb{Z}$, then 1 and $-1$ would each be generators.
Examples

Example
Our example before where $R = \mathbb{Z}$ and $G = \mathbb{Z}_6$ is cyclic, since 1 added with itself multiple times can generate everything in the group. If $G = \mathbb{Z}$, then 1 and $-1$ would each be generators.

Example
Remember that every vector space is actually a special type of module. In particular our good friend $\mathbb{C}^n$ is a module. But when $n \geq 2$, $\mathbb{C}^n$ is not cyclic, since its dimension is greater than 1.
# Table of Contents

1. Introduction
2. Defining a Module
3. Module Properties
4. Modules Over Principle Ideal Domains
5. Conclusion
6. References
Overview

We now start to restrict our attention to modules over principle ideal domains. A PID is basically a ring where quotient structures are easily expressed which forces nice factorization properties. By restricting our attention we hope to...
Overview

We now start to restrict our attention to modules over principle ideal domains. A PID is basically a ring where quotient structures are easily expressed which forces nice factorization properties. By restricting our attention we hope to...

- Generalize more group structures.
Overview

We now start to restrict our attention to modules over principle ideal domains. A PID is basically a ring where quotient structures are easily expressed which forces nice factorization properties. By restricting our attention we hope to...

- Generalize more group structures.
- Develop decompositions for modules.
Overview

We now start to restrict our attention to modules over principle ideal domains. A PID is basically a ring where quotient structures are easily expressed which forces nice factorization properties. By restricting our attention we hope to...

- Generalize more group structures.
- Develop decompositions for modules.
- Set the groundwork for the development of canonical forms.
The Annihilator

An element in a group has an order. Here we extend this notion to modules

Definition

If $M$ is $R$-module, and $m \in M$, then its annihilator is

$$\text{ann}(m) = \{r \in R : rm = 0\}.$$
The Annihilator

An element in a group has an **order**. Here we extend this notion to modules

**Definition**

If $M$ is $R$-module, and $m \in M$, then its **annihilator** is

$$\text{ann}(m) = \{ r \in R : rm = 0 \}.$$  

If $\text{ann}(m) \neq \{0\}$ then we say $m$ has a finite order, otherwise it has an infinite order. Note that the annihilator forms an ideal, and using the first isomorphism theorem with the $R$-map $f : R \to \langle m \rangle$ where $f(r) = rm$ we can derive $\langle m \rangle \cong R/\text{ann}(m)$. 
Torsion Submodules

Definition

If $M$ is an $R$-module, and $R$ is an integral domain, then its torsion submodule $tM$ is defined by

$$tM = \{ m \in M : m \text{ has finite order} \}$$
Torsion Submodules

**Definition**

If $M$ is an $R$-module, and $R$ is an integral domain, then its **torsion submodule** $tM$ is defined by

$$tM = \{m \in M : m \text{ has finite order}\}$$

**Definition**

A module is **torsion** if $tM = M$ and **torsion-free** if $tM = \{0\}$. 
Proposition

If $R$ is an integral domain (a commutative ring where if $ab = 0$, $a = 0$ or $b = 0$) and $M$ is an $R$-module, then $tM$ is a submodule of $M$. 

$tM$ is a Torsion Submodule over an Integral Domain
**Proposition**

*If* $R$ *is an integral domain* (a commutative ring where if* $ab = 0$, $a = 0$ *or* $b = 0$) *and* $M$ *is an* $R$-*module, then* $tM$ *is a submodule of* $M$.

**Proof.**

All we must show is that $tM$ is closed under both addition and scaler multiplication defined in $M$. Take $m, m' \in tM$, then there exists elements $r, r' \in R$ such that $rm = 0$ and $rm' = 0$. Now $rr'(m + m') = 0$. Since $rr' \neq 0$, $(m + m')$ has a nonzero annihilator. Now take $s \in R$ and $m \in tM$, then again there is an $R$ such that $rm = 0$. Now with some massaging

$$r(sm) = (rs)m = (sr)m = s(rm) = 0$$

so $sm \in tM$ as well.
$V^T$ is Torsion

Recall our example $V^T$ which formed a $k[x]$-module.

**Proposition**

*Given a finite dimensional vector space $V$ over a field $k$ and a linear transformation $T : V \to V$, the $k[x]$-module $V^T$ is torsion.*
Recall our example $V^T$ which formed a $k[x]$-module.

**Proposition**

*Given a finite dimensional vector space $V$ over a field $k$ and a linear transformation $T : V \rightarrow V$, the $k[x]$-module $V^T$ is torsion.*

**Proof.**

We want to show that for any element in $V^T$, there is an element in its annihilator. Let the dimension of $V = n$ and take $v \in V^T$, then the set $\{v, T(v), \ldots, T^n(v)\}$ must be linearly dependant. So there is a nontrivial solution using scalars $a_0, a_1, \ldots, a_n$ such that $\sum_{i=0}^{n} a_i T^i(v) = 0$. This implies the nonzero polynomial $p(x) = \sum_{i=0}^{n} a_i x^i \in \text{ann}(v)$.
Splitting the Free and Torsion Parts

Definition

An $R$-module $F$ is called a **free** $R$-module if $F$ is isomorphic to a direct sum of multiple $R$’s. More precisely, given an index set $I$

$$F = \sum_{i \in I} R_i$$

where $R_i = \langle b_i \rangle \cong R$ for all $i \in I$. 

Theorem (Separating Decomposition)

If $R$ is a PID, every finitely generated $R$-module $M$ is a direct sum $M = tM \oplus F$. 


Splitting the Free and Torsion Parts

**Definition**

An $R$-module $F$ is called a **free** $R$-module if $F$ is isomorphic to a direct sum of multiple $R$'s. More precisely, given an index set $I$

$$F = \sum_{i \in I} R_i$$

where $R_i = \langle b_i \rangle \cong R$ for all $i \in I$.

**Theorem (Separating Decomposition)**

*If $R$ is a PID, then every finitely generated $R$-module $M$ is a direct sum*

$$M = tM \oplus F.$$
Primary Decomposition of Modules

Definition

Let $R$ be a PID and $M$ be an $R$-module. If $P = \langle p \rangle$ is a non-zero prime ideal in $R$, then $M$ is $\langle p \rangle$-primary if for each $m \in M$, there is an $n \geq 1$ such that $p^n m = 0$. $M$’s $\langle p \rangle$-primary component is

$$M_P = \{ m \in M : p^n m = 0 \text{ for some } n \geq 1 \}.$$
## Primary Decomposition of Modules

### Definition

Let $R$ be a PID and $M$ be an $R$-module. If $P = \langle p \rangle$ is a non-zero prime ideal in $R$, then $M$ is \textit{\langle p \rangle-primary} if for each $m \in M$, there is an $n \geq 1$ such that $p^n m = 0$. $M$’s \textit{\langle p \rangle-primary component} is

\[ M_P = \{ m \in M : p^n m = 0 \text{ for some } n \geq 1 \}. \]

### Theorem (Primary Decomposition of Modules)

\textit{Every finitely generated torsion $R$ module $M$, where $R$ is a PID, is a direct sum of its $P$-primary components. Symbolically,}

\[ M = \sum_P M_P \]
Basis Theorem

Theorem

If $R$ is a PID, then every finitely generated $R$-module $M$ is a direct sum of cyclic modules in which each cyclic summand is isomorphic to $R$ or is primary.
Basis Theorem

Theorem

*If* $R$ *is a PID, then every finitely generated* $R$-*module* $M$ *is a direct sum of cyclic modules in which each cyclic summand is isomorphic to* $R$ *or is primary.*

Outline.

Given an $R$ module, $M$...

1. First use our Separating Theorem to write $M = tM \oplus F$. All that matters now is $tM$.
2. Use our Primary Decomposition Theorem to write $tM = \sum P M_P$.
3. Finish by showing each $M_P$ is cyclic.
Proposition

Two finitely generated torsion modules $M$ and $M'$ over a PID are isomorphic if and only if $M_P \cong M'_P$ for every nonzero prime ideal $P$. 
Isomorphic Modules have Isomorphic Components

Proposition

Two finitely generated torsion modules $M$ and $M'$ over a PID are isomorphic if and only if $M_P \cong M'_P$ for every nonzero prime ideal $P$.

Proof.

$(\Rightarrow)$ Let $f : M \to M'$ be an $R$-map. If we take $m \in M_P$ where $P = \langle p \rangle$, then $p^k m = 0$ for some $k \geq 1$. Now because $f$ is an $R$-map,

$$p^k f(m) = f(p^k m) = f(0) = 0$$

which implies $p^k f(m) \in M'_P$ and $f(M_P) \subseteq M'_P$. Similarly $f^{-1}(M'_P) \subseteq M_P$ which shows that $f$ restricted to $M_P$ maps onto $M'_P$. 

Proof Continued

Proof.

$(\Leftarrow)$ If we have $M_P = M'_P$ for all $P$, then we can define an isomorphism between $M$ and $M'$ using our Primary Decomposition Theorem. Let $\phi_P$ denote an isomorphism between $M_P$ and $M'_P$, then $\phi : M \rightarrow M'$ defined as

$$\phi(m) = \phi \left( \sum_P M_P \right) = \sum_P \phi_P(M_P)$$

is an isomorphism.
The Fundemental Theorem of Finitely Generated Abelian Groups

Theorem (Judson: Fundemental Theorem of Finitely Generated Abelian Groups)

Every finitely generated abelian group $G$ is isomorphic to a direct product of cyclic groups of the form

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$
The Fundamental Theorem of Finitely Generated Abelian Groups

Theorem (Judson: Fundamental Theorem of Finitely Generated Abelian Groups)

*Every finitely generated abelian group* $G$ *is isomorphic to a direct product of cyclic groups of the form*

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

*This theorem follows as a corollary from the Basis Theorem if we let our* $R$ *be* $\mathbb{Z}$ *and let our scaler multiplication be exponentiation.*
The End!
1 Advanced Modern Algebra by Joseph Rotman
2 Abstract Algebra theory and applications by Thomas Judson
3 Rational Canonical Form by Glenna Toomey