THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

DEPARTMENT OF MATHEMATICS

ANALOGIES IN LINEAR ALGEBRA AND GROUP THEORY

BEN TAYLOR
Spring 2013

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Mathematics
with honors in Mathematics.

Reviewed and approved* by the following:

Mihran Papikian
Assistant Professor of Mathematics
Thesis Supervisor

Sergei Tabachnikov
Professor of Mathematics
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

This thesis examines the relationship between the theory of finite abelian groups and the theory of linear operators over finite-dimensional vector spaces. We introduce the basic notions of module theory which allows us to generalize many facts about abelian groups and vector spaces. After stating several fundamental results from group theory, we proceed to prove that there exist analogous results in the study of finite-dimensional vector spaces. We also demonstrate that many of the fundamental objects of study in linear algebra, such as the minimal and characteristic polynomial, play the same role as some group-theoretic object.

TABLE OF CONTENTS

1 Introduction

The theory of modules plays a fundamental role in the study of algebraic structures. Modules allow us to generalize a lot of results about vector spaces and, as we will see, they also allow us to generalize many facts from group theory. We will examine the manner in which many important facts about vector spaces and abelian groups can be deduced by studying their module structures. This will allow us to show that there is a striking duality between linear algebra and group theory. In particular, many facts about linear operators on finite-dimensional vector spaces have group-theoretic analogs. Likewise, we will see that many of the fundamental objects of study in linear algebra, such as invariant subspaces and the minimal and characteristic polynomials of an operator, have group-theoretic counterparts.

2 Basic Notions

In the following, suppose R is a commutative ring and $a, b \in R$.

We say that a divides b, written $a \mid b$, if there exists $x \in R$ such that $b = ax$. If d divides both a and b and every common divisor of a and b divides d, then we say that d is a **greatest common divisor** of a and b, written $\gcd(a, b) = d$.

We call $x \in R$ **irreducible** if $x = ab$ implies a or b is a unit, i.e. has a multiplicative inverse. We say that $x \in R$ is **prime** if $x \mid ab$ implies $x \mid a$ or $x \mid b$. Note that these are a straightforward generalization of the prime elements in $\mathbb{Z}$.

We call the ring R an **integral domain** if the ring multiplication is commutative and for all $a, b \in R$: $ab = 0$ implies $a = 0$ or $b = 0$. Note that in an integral domain, every prime element is irreducible, but the converse is not true. One special type of integral domain in which the converse does hold is known as a **Unique Factorization Domain (UFD)**, which is an integral domain in which every non-zero element x can be written as a product $x = up_1p_2...p_n$ where u is a unit and $p_1, p_2, ..., p_n$ are irreducible. Moreover, if $x = wq_1q_2...q_m$ where w is a unit and $q_1, q_2, ..., q_m$ are irreducible, then we have $n = m$ and, after permutation of indices, $p_i = a_{ij}q_j$ for some unit a_{ij}.

If I is a subset of a commutative ring R, then we say I is an **ideal** if $ar \in I \ \forall a \in I, r \in R$ and $a + x \in I \ \forall a, x \in I$. An ideal generated by a single element,

$$I = (x) = \{ax : a \in R\}$$

is called **principal**.

UFDs in which every ideal is principal are known as **Principal Ideal Domains (PIDs)**. The ring of integers, $\mathbb{Z}$, is an example of a PID. We can see this by noting that $\mathbb{Z}$ is an infinite cyclic group so any ideal $I \subset \mathbb{Z}$ must be a cyclic subgroup and therefore generated by a single element. Two ideals $(a), (b)$ in a PID are called **comaximal** if $\gcd(a, b)$=1. For example, the ideals $2\mathbb{Z}$ and $3\mathbb{Z}$ are comaximal in $\mathbb{Z}$.

A commutative ring is called a **field** if it has a multiplicative identity $1 \neq 0$ and every non-zero element has a multiplicative inverse. Examples of fields include $\mathbb{R}, \mathbb{C}$, and $\mathbb{Z}_p$, the ring of integers modulo a prime number p. Given a ring R, we may define the **ring of polynomials over** R, denoted $R[x]$, to be the set of all polynomials with coefficients in R, equipped with the operations of addition and multiplication of polynomials. An important fact about polynomial rings is that there exists a polynomial division algorithm, similar to the usual division algorithm in $\mathbb{Z}$.

Lemma 2.1 *: Given $p(x), q(x) \in F[x]$ with $q(x) \not\equiv 0$, there exist $s(x), r(x) \in F[x]$ such that $p(x) = s(x)q(x) + r(x)$ with $deg(r(x)) < deg(q(x))$.*

Theorem 2.2 *: If F is a field, then $F[x]$ is a PID.*

Proof: It's clear that $F[x]$ is an integral domain. Suppose $I \subset F[x]$ is an ideal. If $I = (0)$, then I is principal. If $I \neq (0)$, then let $f(x)$ be a polynomial of minimal degree in I. It is clear that $(f(x)) \subset I$. Let $g(x) \in I$. By the polynomial division algorithm, there exist $s(x), r(x) \in F[x]$ such that $g(x) = f(x)s(x) + r(x)$ with $deg(r(x)) < deg(f(x))$. Thus, $r(x) = g(x) - f(x)s(x)$. Since I is an ideal, we get $r(x) \in I$ which implies $r(x) = 0$ since

otherwise $r(x)$ would be a polynomial in I of degree less than the degree of $f(x)$. Therefore $g(x) = f(x)s(x)$ so $g(x) \in (f(x))$. Hence $I = (f(x))$ so every ideal in $F[x]$ is principal. ■

Note that the irreducible elements in $F[x]$ are precisely the irreducible polynomials.

Our main focus here will be to demonstrate the interplay between finite dimensional vector spaces equipped with a linear operator and finite abelian groups. This will be accomplished by studying the underlying module structure of both vectors spaces and abelian groups. Given a commutative ring R, an **R-module** M is an abelian group $(M, +)$ along with an operation $R \times M \to M$, called scalar multiplication, such that for all $r, s \in R$ and $x, y \in M$:

i. $r(x + y) = rx + ry$
ii. $(r + s)x = rx + sx$
iii. $(rs)x = r(sx)$

For example, every ideal $I \subset R$ is an R-module, as is the Cartesian product R^n.

Given an R-module M, we say that the subset $N \subset M$ is an **R-submodule** if N is an additive subgroup of M and for all $n \in N, r \in R$, the product rn is in N. Given an R-module M and submodule N, the **quotient module** M/N is the quotient group M/N with addition and multiplication given by $[a]+[b] = [a+b]$ and $r \cdot [a] = [r \cdot a]$ for all $a, b \in M$ and $r \in R$.

We call an R-module M **finitely generated** if there exist $x_1, x_2, ..., x_n \in M$ such that for every $y \in M$, there exist $a_1, a_2, ..., a_n \in R$ with $y = a_1x_1 + a_2x_2 + ... + a_nx_n$. The Cartesian product R^n is clearly a finitely generated R-module, but not all modules are finitely generated. For instance, consider the ring $R[x]$ of polynomials over R, which is not finitely generated as an R-module.

Suppose M and N are R-modules. A map $\phi : M \to N$ is called an **R-module homomorphism** if for all $m, m' \in M$ and $r, s \in R$, we have $\phi(rm + sm') = r\phi(m) + s\phi(m')$. If ϕ is bijective, then it's called an **R-module isomorphism**.

The **image** of an R-module homomorphism $\phi : M \to N$ is the set

$$Im(\phi) := \{n \in N : n = \phi(m) \text{ for some } m \in M\}$$

and the **kernel** is the set of all elements that get mapped to the zero element in N, i.e.

$$ker(\phi) := \{m \in M : \phi(m) = 0_N\}.$$

The following theorem implies that ϕ is injective if and only if $ker(\phi) = \{0_M\}$.

Theorem 2.3 *: Suppose $\phi : M \to N$ is an R-module homomorphism. Then:*
1. $ker(\phi)$ is a submodule of M.
2. $Im(\phi)$ is a submodule of N.
3. $M/ker(\phi) \cong Im(\phi)$.

Let R be a commutative ring, M be an R-module, and S be a subset of M. We define the **annihilator** of S to be the set

$$Ann_R(S) := \{r \in R : rs = 0 \quad \text{for all } s \in S\}.$$

It is easy to see that $Ann_R(S)$ satisfies the conditions to be an ideal in R. In particular, if R is a PID, then $Ann_R(S)$ can be generated by a single element. If $Ann_R(S) = (z)$, then we call z a **minimal annihilator** of S, and it is unique up to multiplication by a unit.

Suppose G is a group in which every element has finite order, known as a **torsion group**. In particular, every finite group is a torsion group. We define the **exponent** of G to be the minimal $m \in \mathbb{N}$ such that $g^m = 0$ for all $g \in G$, i.e. the minimal annihilator of G as a $\mathbb{Z}$-module. Given a finite abelian group G, the fundamental theorem of finitely generated abelian groups (which we'll prove later) implies $G \cong \mathbb{Z}/a_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/a_t\mathbb{Z}$, from which it easily follows that the exponent of G is $lcm\{a_1, ..., a_t\}$ and the order of G is $a_1 \times ... \times a_t$. Another form of the fundamental theorem of finitely generated abelian groups implies that $G \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \oplus ... \oplus \mathbb{Z}/p_t^{k_t}\mathbb{Z}$ for some prime numbers $p_1, ..., p_t$.

We will now prove two statements about finite abelian groups, which we'll see correspond to similar statements about the minimal and characteristic polynomials of linear operators.

Theorem 2.4 *: A finite abelian group G is isomorphic to a direct sum of cyclic groups of prime orders if and only if its exponent is a product of distinct primes.*

Proof: If $G \cong \mathbb{Z}/p_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/p_t\mathbb{Z}$, where $p_1, ..., p_t$ are prime, then the exponent is $lcm\{p_1, ..., p_t\}$, which is the product of the distinct primes amongst $p_1, ..., p_t$.

Conversely, suppose $G \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \oplus ... \oplus \mathbb{Z}/p_t^{k_t}\mathbb{Z}$, where $p_1, ..., p_t$ are prime and some $k_i \geq 2$. Without loss of generality, suppose $k_1 = 2$. Then the exponent of G is $lcm\{p_1^2, p_2^{k_2} ..., p_t^{k_t}\}$ which implies that p_1^2 is a factor, so the exponent is not a product of distinct primes. ■

Another interesting fact about finite abelian groups is that for some small integer values, the order and exponent of a finite abelian group uniquely determine the group, up to isomorphism. For instance, the only group of order 4 and exponent 4 is $\mathbb{Z}/4\mathbb{Z}$, and the only group of order 4 and exponent 2 is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. On the other hand, if we consider the groups of order 16 with exponent 4, then we have both $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Theorem 2.5 *: Suppose G is a non-trivial finite group. Then G contains no proper, non-trivial subgroups if and only if G has prime order.*

Proof: Suppose G has prime order p and $H \subset G$ is a subgroup. By Lagrange's Theorem, $|H|$ divides p, so $|H| = 1$ or $|H| = p$. Therefore $H = \{e\}$ or $H = G$, so G has no proper, non-trivial subgroups.

Conversely, suppose G contains no proper, non-trivial subgroups. Since G is non-trivial, there exists $g \in G$ such that $g \neq e$. Therefore, $< g >= G$. Let $n = |g|$. If n is not prime, then $n = pq$ for some $p, q > 1$, but then $< g^p >$ is a proper subgroup of order q. Hence, n must be prime so G has prime order. ■

We call a finite abelian group **decomposable** if it can be written as the direct sum of two proper subgroups.

Theorem 2.6 *: Suppose G is a non-trivial finite abelian group. Then G is indecomposable if and only if G is cyclic and its order is a power of a prime.*

Proof: First recall that $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ if and only if $gcd(m,n) = 1$. Now suppose G is cyclic and has order p^k for some prime p and positive integer k, so $G \cong \mathbb{Z}/p^k\mathbb{Z}$. We can see that G is not isomorphic to a direct sum of two non-trivial subgroups by noting that, for any $l < k$, $\mathbb{Z}/p^k\mathbb{Z} \ncong \mathbb{Z}/p^l\mathbb{Z} \oplus \mathbb{Z}/p^{k-l}\mathbb{Z}$ since $gcd(p^l, p^{k-l}) \neq 1$. Hence G is indecomposable.

Now suppose the order of G is not a prime power, so $|G| = mn$ for some positive integers m, n such that $gcd(m,n) = 1$. Then $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ so G is decomposable. Likewise, if G is not cyclic then $G \ncong \mathbb{Z}/m\mathbb{Z}$ for any positive integer m and it follows that G must be isomorphic to a direct sum of non-trivial subgroups. ■

For finite abelian groups, the converse to Lagrange's Theorem also holds:

Theorem 2.7 *: Let G be a finite abelian group of order n and suppose $m \mid n$. Then there exists a subgroup of order m.*

Proof: Suppose $|G| = {p_1}^{n_1} \times {p_2}^{n_2} \times \cdots \times {p_k}^{n_k}$. Then we must have $m = {p_1}^{m_1} \times {p_2}^{m_2} \times \cdots \times {p_k}^{m_k}$ where $m_i \leq n_i$ for all i. It then follows from the fact that $\mathbb{Z}/{p_i}^{n_i}\mathbb{Z}$ has a subgroup of order $\mathbb{Z}/{p_i}^{m_i}\mathbb{Z}$ that we can find a subgroup of order m. For instance, if $|G| = 8$ and we wish to find a subgroup of order 4, then we have $G \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $G \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, or $G \cong \mathbb{Z}/8\mathbb{Z}$. In the first case, we can take $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \{0\}$. In the second case, we can take $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and in the final case we have $\mathbb{Z}/4\mathbb{Z}$. ■

3 General Theory of Modules

From this point on, we will always assume that R is a PID. Let M be an R-module. We call a subset $N \subset M$ a **spanning set** of M if for every $x \in M$, there exist $n_1, n_2, ..., n_k \in N$ and $r_1, r_2, ..., r_k \in R$ such that $x = r_1n_1 + r_2n_2 + ... + r_kn_k$.

Now suppose that $m_1, m_2, ..., m_k \in M$. If the only choice of scalars $r_1, r_2, ..., r_k \in R$ such that $r_1m_1 + r_2m_2 + ... + r_km_k = 0$ is the trivial combination $r_1 = r_2 = ... = r_k = 0$, then we say that the elements $m_1, m_2, ..., m_k$ are **linearly independent**. We call a linearly independent spanning set of M a **basis** of M.

We say that M is a **free R-module of rank n** if it has a basis consisting of n elements. Equivalently, M is a free R-module of rank n if it is isomorphic to $R^n = R \oplus R \oplus ... \oplus R$ (n-times).

We begin our discussion of module theory by proving an important structure theorem regarding modules over principal ideal domains.

Lemma 3.1 *: If M is a free R-module of rank n and $N \subset M$ is a submodule, then N is a free R-module of rank $m \leq n$ and there exists a basis $\{e_1, ..., e_n\}$ of M such that $\{a_1e_1, ..., a_me_m\}$ is a basis of N with $a_1 \mid a_2 \mid ... \mid a_m$.*

Theorem 3.2 *: If M is a finitely generated R-module, then $M \cong R^n \oplus R/(a_1) \oplus ... \oplus R/(a_m)$ with $n \geq 0$ and $a_1 \mid a_2 \mid ... \mid a_m$.*

Proof: Let $\{x_1, ..., x_n\}$ be a generating set for M and let $\{r_1, ..., r_n\}$ be a basis for R^n. Define $\phi : R^n \to M$ by $\phi(r_i) = x_i \ \forall 1 \leq i \leq n$. By Theorem 2.3, $R^n/ker(\phi) \cong Im(\phi) \cong M$ since $\{\phi(r_1), ..., \phi(r_n)\}$ spans M. By Lemma 3.1, there exists a basis $\{y_1, ..., y_n\}$ of R^n such that $\{a_1y_1, ..., a_my_m\}$ is a basis of $ker(\phi)$ with $a_1 \mid a_2 \mid ... \mid a_m$. Therefore $M \cong R^n/ker(\phi) \cong (Ry_1 \oplus ... \oplus Ry_n)/(Ra_1y_1 \oplus ... \oplus Ra_my_m)$.
Now consider the R-module homomorphism $\psi : Ry_1 \oplus ... \oplus Ry_n \to R/(a_1) \oplus ... \oplus R/(a_m) \oplus R^{n-m}$ given by $(b_1y_1, ..., b_ny_n) \mapsto (b_1 \ mod \ a_1, ..., b_m \ mod \ a_m, b_{m+1}, ..., b_n)$. We have $Im(\psi) = R/(a_1) \oplus ... \oplus R/(a_m) \oplus R^{n-m}$ and $ker(\psi) = Ra_1y_1 \oplus ... \oplus Ra_my_m$. Hence $M \cong R/(a_1) \oplus ... \oplus R/(a_m) \oplus R^{n-m}$ by Theorem 2.3. ■

The ring elements $a_1 \mid a_2 \mid ... \mid a_m$ in the proof of Theorem 3.2 are known as the **invariant factors** of the module M.

Two isomorphic modules have the same list of invariant factors. Rather than proving this rigorously, we will give an example to demonstrate the uniqueness of the invariant factors. This example will also illustrate how Theorem 3.2 will allow us to gain some insight into the study of finite abelian groups.

First, let $(G, +)$ be an abelian group and consider the action of $\mathbb{Z}$ on G given by:

$$nx = \begin{cases} x + x + ... + x \ \ (n \ \ times) & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -x - x - ... - x \ \ (n \ \ times) & \text{if } n < 0 \end{cases}$$

This action gives G a $\mathbb{Z}$-module structure. Since every module is an abelian group by definition, it follows that abelian groups and $\mathbb{Z}$-modules are the same thing.

Now consider the finite abelian groups $G = \mathbb{Z}_8 \oplus \mathbb{Z}_4$ and $H = \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Clearly these two groups have different invariant factors, and we see that they can not be isomorphic by observing that G and H have a different number of elements of order 2. This argument may be used to prove that any two isomorphic finite abelian groups must have the same list of invariant factors. A similar argument shows the uniqueness of the invariant factors for a general R-module.

We can now prove the following corollary to Theorem 3.2, known as the Fundamental Theorem of Finitely Generated Abelian Groups:

Corollary 3.3 *: Let G be a finitely generated abelian group. Then $G \cong \mathbb{Z}^n \oplus \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus ... \oplus \mathbb{Z}_{m_t}$ with $n \geq 0, m_i \geq 2$ $\forall i \in \{1, 2, ..., t\}$ and $m_i \mid m_{i+1}$ $\forall i \in \{1, 2, ..., t-1\}$, where $n, m_1, ..., m_t$ are unique.*

Proof: Since G is a finitely generated $\mathbb{Z}$-module, we can apply the structure theorem to get: $G \cong \mathbb{Z}^n \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/m_t\mathbb{Z}$ with $m_1 \mid m_2 \mid ... \mid m_t$. The uniqueness follows from the uniqueness of the invariant factors of a $\mathbb{Z}$-module. ■

Let's now return to module theory and prove an alternative form of Theorem 3.2. We'll make use of the following ring-theoretic fact, known as the Chinese Remainder Theorem:

Lemma 3.4 *: If $I_1, ..., I_k$ are pairwise comaximal ideals in R, then $R/(I_1 \cap ... \cap I_k) \cong R/I_1 \oplus ... \oplus R/I_k$.*

We say that an element $m \in M$ is a **torsion element** if there exists a non-zero $r \in R$ such that $rm = 0$. If every element in M is a torsion element, then we say M is a **torsion module**. Note that R is not a torsion module over itself since R is an integral domain, so $rx = 0$ implies $r = 0$ or $x = 0$. Thus, if M is a torsion module, then in the decomposition $M \cong R^n \oplus R/(a_1) \oplus ... \oplus R/(a_m)$, we must have $n = 0$. It should also be noted that a torsion abelian group is necessarily a torsion module, but the converse does not hold.

Theorem 3.5 *: If M is a finitely generated torsion R-module, then $M \cong R/(p_1^{\alpha_1}) \oplus ... \oplus R/(p_r^{\alpha_r})$ with $\alpha_i \geq 0$ $\forall 1 \leq i \leq r$ and $p_1, ..., p_r$ irreducible elements in R.*

Proof: Consider the invariant factors $a_1 \mid a_2 \mid ... \mid a_m$ of M. Since R is a PID, it is also a unique factorization domain so we can write $a_i = u_i p_{i_1}^{\alpha_{i_1}} p_{i_2}^{\alpha_{i_2}} ... p_{i_t}^{\alpha_{i_t}}$ $\forall 1 \leq i \leq m$ where u_i is a unit and $p_{i_1}, ..., p_{i_t}$ are irreducible and pairwise coprime. Since $gcd(p_{i_j}, p_{i_k}) = 1$ for $j \neq k$, we have that the ideals $(p_{i_1}^{\alpha_{i_1}}), ..., (p_{i_t}^{\alpha_{i_t}})$ are pairwise comaximal. It follows by the Chinese Remainder Theorem that:

$$R/(a_i) \cong R/(p_{i_1}^{\alpha_{i_1}}) \oplus ... \oplus R/(p_{i_t}^{\alpha_{i_t}}) \ \forall 1 \leq i \leq m.$$

Hence we have

$$M \cong R/(a_1) \oplus ... \oplus R/(a_m) \cong R/(p_1^{\alpha_1}) \oplus ... \oplus R/(p_r^{\alpha_r}).$$

■

The ring elements $p_1^{\alpha_1}, ..., p_r^{\alpha_r}$ are called the **elementary divisors** of M. (Note that the uniqueness of the elementary divisors follows from the uniqueness of the invariant factors.)

4 Linear Algebra

We now turn our attention to linear algebra and once again apply Theorem 3.2 to deduce a standard form for the object in question: this time canonical forms of a linear operator.

Now that we've seen some of the basics of module theory, we can easily define the fundamental notions of linear algebra, which is the study of abstract vector spaces and linear maps defined on them.

A **vector space** is an F-module where F is a field. We call F the **field of scalars**. Now suppose V and W are vector spaces. An F-module homomorphism $T : V \to W$ is called a **linear transformation**. A linear transformation from V to V is also called a **linear operator**. A subset $U \subseteq V$ is called a **subspace** if U is an F-submodule of V. If V has a basis consisting of n vectors, then we say that the **dimension** of V is n.

Let $T : V \to W$ be a linear transformation and let $U \subseteq V$. We say that U is **T-invariant** if $T(U) \subseteq U$, i.e. $T(u) \in U$ for all $u \in U$. We call the space $< v >:= span\{v, Tv, T^2v, ...\}$ the **cyclic subspace** generated by v. The fact that $< v >$ is T-invariant is clear from its definition.

Now let V be a vector space over a field F and let $T : V \to V$ be a linear operator. Define an action of $F[x]$ on V by $p(x)\cdot v = (a_nT^n+...+a_1T+a_0I)(v)$ where $p(x) = a_nx^n+...+a_1x+a_0$. This action gives V an $F[x]$-module structure. If V is finite dimensional, then V is a torsion $F[x]$-module. To see this, let V be an n-dimensional vector space over F and let $T : V \to V$ be a linear operator. Let v be an element of V and consider the set $\{v, Tv, ..., T^nv\}$. Since we have $n+1$ vectors in an n-dimensional space, there must exist $a_0, a_1, ..., a_n$, not all zero, such that $a_0v + a_1Tv + ... + a_nT^nv = 0$. Therefore $f(x) \cdot v = 0$ where $f(x) = a_0 + a_1x + ... + a_nx^n$.

As V is also finitely generated, Theorem 3.2 implies that V is isomorphic to a direct sum of **cyclic modules**, i.e. modules generated by a single element. Using the direct sum decompositions given by Theorems 3.2 and 3.5, we can find canonical forms for the operator T. If we use the invariant factors, we can obtain the rational canonical form of T. If we instead use the elementary divisors, we can obtain the Jordan canonical form of T

By Theorem 3.2, we know $V \cong F[x]/(a_1(x)) \oplus ... \oplus F[x]/(a_m(x))$ with $a_1(x) \mid ... \mid a_m(x)$. Consider the cylic module $F[x]/(a_i(x))$ and suppose $a_i(x) = x^{d_i} + a_{d_i-1}x^{d_i-1} + ... + a_1x + a_0$. As a cyclic module, $F[x]/(a_i(x))$ is generated by a single vector v, so that $F[x]/(a_i(x)) \cong span\{v, Tv, T^2v, ...\}$ but $T^{d_i}v = 0$ so actually $\{1, x, ..., x^{d_i-1}\}$ is linearly independent and forms a basis for $F[x]/(a_i(x))$. The action of T on this basis can easily be seen to give the matrix:

$$\begin{bmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & 0 & -a_{d_i-2} \\ 0 & 0 & 0 & \dots & 1 & -a_{d_i-1} \end{bmatrix}$$

We call this the **companion matrix** for the polynomial $x^{d_i} + a_{d_i-1}x^{d_i-1} + ... + a_1x + a_0$.

Since the action of T on the cyclic module $F[x]/(a_i(x))$ is given by the companion matrix above, it follows that the action of T on V is given by the direct sum of the companion matrices for the polynomials $a_1(x), ..., a_m(x)$, i.e.

$$M(T) = \begin{bmatrix} C_{a_1} & & & \\ & C_{a_2} & & \\ & & \ddots & \\ & & & C_{a_m} \end{bmatrix}$$

where C_{a_i} is the companion matrix for the polynomial $a_i(x)$ and there are zeros everywhere else. We call this matrix the direct sum of the matrices $C_{a_1}, C_{a_2}, ..., C_{a_m}$ and denote it $C_{a_1} \oplus ... \oplus C_{a_m}$.

Theorem 4.1 *: Let T be a linear operator on a finite-dimensional vector space V. Then there exists a unique list of polynomials $a_1(x), ..., a_m(x)$ with the property that there is a basis for V such that the matrix for T is given by $C_{a_1} \oplus ... \oplus C_{a_m}$, where C_{a_i} is the companion matrix for $a_i(x)$. We call this the* ***rational canonical form*** *of T.*

Now consider the decomposition given by Theorem 3.5: $V \cong F[x]/(p_1(x)^{r_1}) \oplus ... \oplus F[x]/(p_m(x)^{r_m})$ where $p_1(x), ..., p_m(x)$ are monic irreducible polynomials, namely the elementary divisors of T. Let's look at the action of T on the cyclic module $F[x]/(p(x)^r)$ where $deg(p(x)) = n$. It is easy to see that the minimal polynomial of this restriction is $p(x)^r$. We will show that the set

$$\{1, x, x^2, ..., x^{n-1}, p(x), xp(x), x^2p(x), ..., x^{n-1}p(x), ..., p(x)^{r-1}, xp(x)^{r-1}, ..., x^{n-1}p(x)^{r-1}\}$$

is a basis for this submodule. Suppose that there exist $b_0, b_1, ..., b_{nr-1}$ such that

$$b_0 + b_1x + b_2x^2 + ... + b_{nr-1}x^{n-1}p(x)^{r-1} = 0.$$

This gives us a polynomial of degree $nr-1$ that annihilates T, contradicting that the minimal polynomial $p(x)^r$ has degree nr. Therefore this set is linearly independent, and thus gives us a basis. With respect to this basis, the action of T is given by:

$1 \mapsto x$
$x \mapsto x^2$
$\vdots$
$x^{n-1} \mapsto p(x) - a_{n-1}x^{n-1} - \ldots - a_1x - a_0$
$p(x) \mapsto xp(x)$
$xp(x) \mapsto x^2p(x)$
$\vdots$
$x^{n-1}p(x) \mapsto p(x)^2 - a_{n-1}x^{n-1}p(x) - \ldots - a_1xp(x) - a_0p(x)$
$\vdots$
$p(x)^{r-1} \mapsto xp(x)^{r-1}$
$xp(x)^{r-1} \mapsto x^2p(x)^{r-1}$
$\vdots$
$x^{n-1}p(x)^{r-1} \mapsto -a_{n-1}x^{n-1}p(x)^{r-1} - \ldots - a_1xp(x)^{r-1} - a_0p(x)^{r-1}$

Hence T is given by the following $nr \times nr$ matrix, where C is the companion matrix for the polynomial $p(x)$ and B is the matrix with a 1 in the upper right entry and zeros everywhere else:

$$M(T) = \begin{bmatrix} C & & & & \\ B & C & & & \\ & B & \ddots & & \\ & & \ddots & \ddots & \\ & & & B & C \end{bmatrix}$$

It is easy to see that the action of T on $V \cong F[x]/(p_1(x)^{r_1}) \oplus ... \oplus F[x]/(p_m(x)^{r_m})$ is then the direct sum of the matrices of this form corresponding to each $p_i(x)$. We call the resulting matrix the **primary rational canonical form** or **generalized Jordan canonical form** of T.

Theorem 4.2 *: If T be a linear operator on a finite-dimensional vector space V, then there exists a basis for V such that T is in generalized Jordan canonical form.*

If F contains all of the eigenvalues of T so its characteristic polynomial splits over F, then the elementary divisors are all powers of linear polynomials and we have:

$$M_\beta(T|_{F[x]/(x-\lambda)^\alpha}) = \begin{bmatrix} \lambda & 0 & 0 & \dots & 0 & 0 \\ 1 & \lambda & & \dots & 0 & 0 \\ 0 & 1 & \lambda & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda & 0 \\ 0 & 0 & 0 & \dots & 1 & \lambda \end{bmatrix}$$

We call a matrix of this form a **Jordan block**. Since the matrix for T acting on $F[x]/(x-\lambda)^\alpha$ with respect to the basis β is the $\alpha \times \alpha$ Jordan block with eigenvalue λ we see that the matrix for T acting on $V \cong F[x]/(x-\lambda_1)^{\alpha_1} \oplus ... \oplus F[x]/(x-\lambda_m)^{\alpha_m}$ is the direct sum of the Jordan blocks corresponding to each of the elementary divisors of V, i.e.

$$M(T) = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_m \end{bmatrix}$$

where A_i is the $\alpha_i \times \alpha_i$ Jordan block with eigenvalue λ_i. We call this the **Jordan canonical form** of T. Since the elementary divisors are unique, as we already saw, it follows that the Jordan canonical form is unique up to permutation of the Jordan blocks (which corresponds to permutation of the cyclic modules in the direct sum decomposition of V).

We say that two linear transformations (matrices) A and B are **similar** if there exists an invertible linear transformation (matrix) C such that $A = CBC^{-1}$. Similar matrices share the same minimal and characteristic polynomials, among other properties.

Proposition: *Suppose $A : V \to V$ and $B : V \to V$ are similar $n \times n$ matrices. Then (V, A) and (V, B) are isomorphic $F[x]$-modules.*

Proof: Since A and B are similar, there exists an invertible matrix P such that $B = P^{-1}AP$. Further, x acts as the matrix A in (V, A) and as the matrix B in (V, B). Consider the map from (V, A) to (V, B) given by $\phi(v) = P^{-1}v$. This is clearly a bijection. Also, $\phi(x \cdot v) = \phi(Av) = P^{-1}Av = BP^{-1}v = B \cdot \phi(v) = x \cdot \phi(v)$, so this is an $F[x]$-module homomorphism. We conclude that (V, A) and (V, B) are isomorphic $F[x]$-modules. ■

Therein lies the importance of the Jordan canonical form: similarity defines an equivalence relation on the set of all matrices and the Jordan canonical form provides us with a canonical representative from each equivalence class.

Given a matrix A, we define the **characteristic polynomial** $p_A(x)$ to be the determinant of the matrix $xI - A$ and the **minimal polynomial** $m_A(x)$ to be the monic minimal annihilator of (V, A) in $F[x]$. Therefore $m_A(x)$ is the polynomial $f(x)$ of minimal degree such that $f(A) = 0$. Likewise, if $v \in V$, we let $m_v(x)$ denote the minimal annihilator of the vector v in $F[x]$.

Let's take a look now at what interesting properties of T we can deduce simply by examining its Jordan canonical form. In particular, let's use this form to find the minimal polynomial and characteristic polynomial of T. In order to do this, we'll utilize a simple fact from linear algebra which will also serve as an excellent example of a statement about linear operators which is analogous to a statement about finite abelian groups. More specifically, considering that the characteristic polynomial plays the same role as the order of a finite abelian group, we can consider the following proposition to be a sort of Lagrange's Theorem for linear operators.

Lemma 4.3 *: If $U \subset V$ is T-invariant, then $p_{T|_U}(x) \mid p_T(x)$.*

Proof: Let $\{u_1, u_2, ..., u_k\}$ be a basis for U and extend it to a basis $\beta := \{u_1, ..., u_k, v_1, ..., v_{n-k}\}$ for V. Then the matrix of T with respect to this basis is:

$T = \begin{bmatrix} T|_U & B \\ 0 & C \end{bmatrix}$. Therefore $p_T(x) = det(x - T|_U) \times det(x - C) = p_{T|_U}(x) \times det(x - C)$. ■

Corollary 4.4 *: $m_v(x) \mid p_T(x)$ for all $v \in V$.*

Proof: Let $v \in V$ and consider the cyclic subspace generated by v: $< v >= span\{v, Tv, ...\}$. It's clear that $< v >$ is T-invariant and its minimal polynomial is $m_v(x)$. It follows by the previous theorem that $m_v(x) \mid p_T(x)$. ■

Using the invariant factors of V, we have $V \cong F[x]/(a_1(x)) \oplus ... \oplus F[x]/(a_m(x))$. Since every vector in $F[x]/(a_i(x))$ is annihilated by $a_i(x)$, it follows that the minimal polynomial of T is the least common multiple of $\{a_1(x), ..., a_m(x)\}$, which is $a_m(x)$. Furthermore, it follows from the fact that the characteristic polynomial of $T|_{F[x]/(a_1(x))}$ is $a_i(x)$ that the characteristic polynomial of T is $a_1(x) \times ... \times a_m(x)$. (Note the similarity between this and the fact that the exponent of the finite group $\mathbb{Z}/a_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/a_t\mathbb{Z}$ is $lcm\{a_1, ..., a_t\}$ and the order is $a_1 \times ... \times a_t$.)

We call a linear operator $T : V \to V$ **diagonalizable** if there exists a basis such that the matrix is diagonal with respect to this basis, i.e.

$$M(T) = diag(\lambda_1, \lambda_2, ..., \lambda_m) = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_m \end{bmatrix}.$$

Theorem 4.5 *: A linear operator $T : V \to V$ is diagonalizable if and only if its minimal polynomial $m(x)$ splits as a product of distinct linear factors.*

Proof: Suppose $T : V \to V$ is diagonalizable. Since similar matrices have the same minimal polynomial, we may find $m(x)$ using a basis such that T is diagonal. In this case, it's clear that the minimal polynomial is $(x - \lambda_1) \times (x - \lambda_2) \times ... \times (x - \lambda_k)$, where $\lambda_1, ..., \lambda_k$ are the distinct eigenvalues on the main diagonal.

Conversely, suppose $m(x) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_k)$ where $\lambda_1, \lambda_2, ..., \lambda_k$ are distinct. Then the elementary divisors are all linear polynomials. It follows that the Jordan canonical form of T is a diagonal matrix. ■

Corollary 4.6 *(Cayley-Hamilton): If $T : V \to V$ is a linear operator with characteristic polynomial $p_T(x)$, then $p_T(T) = 0$.*

Proof: Follows immediately from the fact that the minimal polynomial $m(x) = lcm\{a_1(x), ..., a_m(x)\}$ and the characteristic polynomial $p_T(T) = a_1(x) \times ... \times a_m(x)$, so $m(x) \mid p_T(x)$. ■

Our next result will show the correspondence between subgroups of a finite abelian group and invariant subspaces of a vector space. Using this correspondence, we can then show that a certain existence theorem for subgroups also holds for invariant subspaces.

Theorem 4.7 *: Suppose $T : V \to V$ is a linear operator. Then V contains no proper, non-trivial T-invariant subspaces if and only if $p_T(x)$ is irreducible.*

Proof: Suppose $p_T(x)$ is irreducible and let $U \neq \{0\}$ be T-invariant. Since $p_{T|_U}(x)$ divides $p_T(x)$ and $p_T(x)$ is irreducible, we must have $p_{T|_U}(x) = p_T(x)$ which imples $\dim(U) = \dim(V)$. Hence $U = V$.

Conversely, suppose V contains no proper, non-trivial T-invariant subspaces. Let v be a non-zero vector in V and consider the cyclic subspace $< v >:= span\{v, Tv, ..., T^n v, ...\}$. $< v >$ is T-invariant and non-empty so we must have $< v >= V$. Therefore $p_T(x)$ equals the minimal polynomial $m(x)$. Now, assume $p_T(x)$ is reducible. Then $p_T(x) = f(x)g(x)$ for some $f(x), g(x) \in F[x]$ with $1 \leq deg(f(x)), deg(g(x)) \leq deg(p_T(x))$. By the Cayley-Hamilton Theorem, we have $f(T)g(T)w = p_T(T)w = 0$ for all $w \in V$ so either $f(T)$ or $g(T)$ is not injective. Suppose $f(T)$ is not injective. $v \in ker(f(T)) \implies f(T)v = 0 \implies f(T)Tv = T(f(T)v) = T(0) = 0$ so $ker(f(T))$ is a non-trivial T-invariant subspace of V and therefore $ker(f(T)) = V$. Thus $f(T)v = 0 \ \forall v \in V$. However, since the minimal polynomial $m(x) = p_T(x)$ divides every annihilating polynomial of V, we must have $p_T(x) \mid f(x)$, which

is a contradiction since $deg(f(x)) < deg(p_T(x))$. ■

We'll now prove an analog of Theorem 2.7 for invariant subspaces:

Theorem 4.8 *: Let $T : V \to V$ be a linear operator and suppose $q(x) \mid p_T(x)$. Then there exists an invariant subspace $U \subset V$ such that $p_{T|_U}(x) = q(x)$.*

Proof: Suppose $p_T(x) = p_1(x)^{r_1} \times p_2(x)^{r_2} \times ... \times p_k(x)^{r_k}$ is the irreducible factor decomposition of $p_T(x)$. Then, since $q(x) \mid p_T(x)$, we must have $q(x) = p_1(x)^{s_1} \times p_2(x)^{s_2} \times ... \times p_k(x)^{s_k}$ where $0 \leq s_i \leq r_i$.

By the elementary divisor form of the structure theorem, we have $V \cong F[x]/(p_1(x)^{r_1}) \oplus ... \oplus F[x]/(p_k(x)^{r_k})$. We know from the proof of the generalized Jordan canonical form that $F[x]/(p(x)^r)$ is isomorphic to:

$$span\{v, Tv, ..., T^{n-1}v, p(T)v, ..., T^{n-1}p(T)v, ..., p(T)^{r-1}v, Tp(T)^{r-1}v, ..., T^{n-1}p(T)^{r-1}v\}$$

We can see that $p(T)^{r-s}v$ spans a subspace isomorphic to $F[x]/(p(x)^s)$. Thus we can find subspaces isomorphic to $F[x]/(p_1(x)^{s_1}), ..., F[x]/(p_k(x)^{s_k})$ so the direct sum of these subspaces gives us a subspace $F[x]/(p_1(x)^{s_1}) \oplus ... \oplus F[x]/(p_k(x)^{s_k})$ and clearly the characteristic polynomial of T restricted to this subspace is $q(x)$. ■

Suppose V is a vector space and $T : V \to V$ is a linear operator. We call the pair (V, T) decomposable if there exist non-trivial invariant subspaces V_1 and V_2 such that $V \cong V_1 \oplus V_2$. We can now prove an analog of Theorem 2.6 for linear operators:

Theorem 4.9 *: Let $T : V \to V$ be a linear operator. Then (V, T) is indecomposable if and only if $V \cong F[x]/(p(x)^n)$ with $p(x)$ irreducible.*

Proof: Suppose $V \ncong F[x]/(p(x)^n)$ with $p(x)$ irreducible. Then, without loss of generality, we may assume $V \cong F[x]/(p_1(x)^{n_1}) \oplus F[x]/(p_2(x)^{n_2})$. It follows immediately that V is decomposable.

Now suppose $V \cong F[x]/(p(x)^n)$ with $p(x)$ irreducible. It follows immediately from the generalized Jordan canonical form that $F[x]/(p(x)^n) \ncong F[x]/(p(x)^l) \oplus F[x]/(p(x)^{n-l})$ for any $l < n$. Hence V is indecomposable. ■

5 Some Examples

In order to better understand our canonical forms, let's look at some examples to see how we can find the elementary divisors:

Consider the matrix $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$. We can find the elementary divisors of the $F[x]$-module (F^2, A) by putting the matrix $xI - A$ into **Smith normal form**. This is achieved by using elementary row and column operations to obtain a matrix of the form $\begin{bmatrix} a_1(x) & 0 \\ 0 & a_2(x) \end{bmatrix}$ where $a_1(x) \times a_2(x) = p_T(x)$. In this case, we get:

$xI - A = \begin{bmatrix} x-1 & 2 \\ 0 & x-1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 0 & (x-1)^2 \end{bmatrix}$ so the elementary divisors are 1 and $(x-1)^2$.

This implies that (F^2, A) may be written as $(F^2, A) \cong F[x]/(x-1)^2$.

It turns out that there is an algorithm which will always produce the elementary divisors. Suppose

$$xI - A = \begin{bmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & & \vdots \\ f_{n1} & \cdots & f_{nn} \end{bmatrix}.$$

Choose the non-zero entry of lowest degree, say $f_{ij}(x)$. By elementary row and column operations, we can replace each entry in the i^{th} row and j^{th} column by its residue modulo $f_{ij}(x)$. Now consider the following two cases:

Case 1: $f_{ij}(x)$ divides every entry in its row and column, so every residue is 0. We can then switch the 1^{st} and i^{th} rows as well as the 1^{st} and j^{th} columns to get the following matrix:

$$\begin{bmatrix} f_{ij}(x) & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \cdots & * \end{bmatrix}.$$

Case 2: $f_{ij}(x)$ does not divide every entry in its row and column, so there is some non-zero residue. Since every residue modulo $f_{ij}(x)$ has a degree strictly less than $deg(f_{ij}(x))$, we now have a matrix with a non-zero entry of minimal degree less than the minimal degree of our original matrix. We can take this new non-zero entry of minimal degree and repeat the same procedure. Since each step results in a matrix with a lower minimal degree than the previous one, this process must terminate, i.e. it must eventually happen that our non-zero entry of minimal degree divides every entry in its row and column, so we can proceed as in the first case.

Thus, in both cases we reduce our original matrix to one of the form:

$$\begin{bmatrix} f(x) & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \cdots & * \end{bmatrix}.$$

We then apply the same algorithm to the $(n-1) \times (n-1)$ matrix formed by removing the first row and column, and continue in this manner until we have obtained our diagonal matrix.

Now consider the matrix

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & -1 & -1 & -1 & -1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

We find the elementary divisors as follows:

$$xI - A = \begin{bmatrix} x-1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 0 & x & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & x & 0 & 0 & 0 & 0 & 1 \\ 0 & -1 & -1 & x & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 & x-1 & 0 & 0 & 0 \\ 0 & -1 & -1 & -1 & -1 & x-1 & 0 & -1 \\ 0 & 1 & 1 & 1 & 1 & 0 & x-1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & x \end{bmatrix}. \rightarrow$$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 1-x & x+1 & 1 & 1 & 1 & 1 & 1 & -1 \\ x-1 & -1 & x-1 & -1 & -1 & -1 & -1 & 1 \\ 1-x & 0 & 0 & x+1 & 1 & 1 & 1 & -1 \\ 0 & 0 & 0 & -1 & x-1 & 0 & 0 & 0 \\ 1-x & 0 & 0 & 0 & 0 & x & 1 & -1 \\ x-1 & 0 & 0 & 0 & 0 & -1 & x-2 & 1 \\ x(x-1) & -x & -x & -x & -x & -x & -x & x \end{bmatrix}. \rightarrow$$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1-x & x+1 & 1 & 1 & 1 & 1 & 1 & 0 \\ x-1 & -1 & x-1 & -1 & -1 & -1 & -1 & 0 \\ 1-x & 0 & 0 & x+1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & -1 & x-1 & 0 & 0 & 0 \\ 1-x & 0 & 0 & 0 & 0 & x & 1 & 0 \\ x-1 & 0 & 0 & 0 & 0 & -1 & x-2 & 0 \\ x(x-1) & -x & -x & -x & -x & -x & -x & 0 \end{bmatrix} \rightarrow \quad \cdots\cdots$$

$$\cdots\cdots \quad \rightarrow \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & (x-1)^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & x^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -x^2 & 2x-1 \\ 0 & 0 & 0 & 0 & 0 & 0 & x^2 & -x^2 \end{bmatrix} \rightarrow$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & (x-1)^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & x^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -x^2 & -(x-1)^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & x^2 & 0 \end{bmatrix} \rightarrow$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & (x-1)^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & x^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & (x-1)^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^2 \end{bmatrix} \rightarrow$$

We see that the elementary divisors are $x^2, x^2, (x-1)^2, (x-1)^2$. From this, we deduce that $(F^8, A) \cong F[x]/x^2 \oplus F[x]/x^2 \oplus F[x]/(x-1)^2 \oplus F[x]/(x-1)^2$

Now let's look at a few examples to see what we can learn from the minimal and characteristic polynomials of an operator:

Consider the operator on F^3 given by $T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Since $m_T(x) = (x-1)$ and $p_T(x) = (x-1)^3$, we have that $(F^3, T) \cong F[x]/(x-1) \oplus F[x]/(x-1) \oplus F[x]/(x-1)$.

Likewise, if we take the operator $S = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ on F^3, we see that $m_S(x) = (x-1)^2$ and $p_S(x) = (x-1)^3$, so $(F^3, S) \cong F[x]/(x-1) \oplus F[x]/(x-1)^2$.}

Just as we showed that some small values of the exponent and order of a finite abelian group uniquely determine the group, it is also true that we can determine the Jordan canonical form of some operators just by knowing the characteristic polynomial and minimal polynomial.

For instance, say we know that the characteristic polynomial of an operator T is $p(x) = (x-1)^2(x-2)^2$ and the minimal polynomial is $m(x) = (x-1)(x-2)^2$. The characteristic polynomial tells us that the Jordan canonical form must be:

$$\begin{bmatrix} 2 & a & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ where } a, b \in \{0, 1\}.$$

The minimal polynomial tells us we must have $a = 1$ and $b = 0$, since $a = 0$ would imply $(T - I)(T - 2I) = 0$ and $b = 1$ would imply that $(T - I)(T - 2I)^2 \neq 0$, both contradicting the fact that $m(x) = (x - 1)(x - 2)^2$.

Now suppose $m(x) = p(x) = (x - 1)^2(x - 2)^2$. In this case, we must have $a = b = 1$, since $a = 0$ would imply $(T - I)^2(T - 2I) = 0$ and $b = 0$ would imply $(T - I)(T - 2I)^2 = 0$, contradicting the fact that $m(x) = (x - 1)^2(x - 2)^2$.

References

[1] Dummit, D.; Foote, R. *Abstract Algebra: 3rd edition.* John Wiley & Sons, Inc.: 2003.
[2] MacLane, S.; Birkhoff, G. *Algebra: 3rd edition.* Chelsea Publishing Co.: 1988.

ACADEMIC VITA

Benjamin Taylor
806 Logandale Drive
Altoona, PA 16601
benter_07@hotmail.com

Education:

The Pennsylvania State University, Spring 2013
B.S. in Mathematics
Honors in Mathematics
Thesis Title: Analogies in Linear Algebra and Group Theory
Thesis Supervisor: Mihran Papikian

Activities and Honors:

Member, Phi Beta Kappa Honors Society, 2011 - Present
Participant, Penn State University MASS Program, Fall 2011
Recipient, The President Sparks Award, 2010
Recipient, Diehl Endowed Science Scholarship, 2010
Recipient, Keiter Science Honors Scholarship, 2010
Recipient, Society of Distinguished Alumni Trustee Matching Scholarship, 2012