A CHARACTERIZATION OF FINITELY GENERATED MODULES

by:

Karl Earl Schwede

A thesis submitted in partial fulfillment
for graduation with Honors in Mathematics

Whitman College
1999

Certificate of Approval

This is to certify that the accompanying thesis by Karl Earl Schwede has been accepted in partial fulfillment of the requirements for graduation with Honors in Mathematics.

Patrick Keef

Whitman College
May1999

CONTENTS

A CHARACTERIZATION OF FINITELY GENERATED MODULES

Part 1: Introduction

The purpose of this thesis is to characterize finitely generated modules. A standard result in undergraduate abstract algebra is that every finite Abelian group is isomorphic to a unique direct product of cyclic groups of prime power order. A similar statement can be made about finitely generated groups, except in this case there are also infinite cyclic summands. This result can be generalized further to R-modules where R is a Euclidean domain. This is the main result of this thesis. There are also some other statements about other more generalized domains as well. This thesis will conclude with an application to $F[x]$ modules.

Let us define an Abelian group and a ring as normally done (Gallian 41, 225). We will call the identity element 0. Let us define an R-module as follows:

DEFINITION 1.1 An R-module is an Abelian group under addition, with scalar multiplication from a commutative unitary ring R, and for any $a, b \in A$ and $r, s \in R$ we have that $r(a+b) = ra + rb$, $(r+s)a = ra + sa$, $(rs)a = r(sa)$, and $1a = a$. ■

Notice that this also implies that $0a = 0$ since $0 + 0a = 0a = (0+0)a = 0a + 0a$, so by cancellation, $0 = 0a$, and similarly this implies that for any $r \in R$, $r0 = 0$. We will be looking in particular at what happens when the ring is a Euclidean Domain. A Euclidean domain (Gallian 317) D is an integral domain where there is a function d from the nonzero elements of D to the non-negative integers such that for all non-zero $a, b \in D$, $d(a) \leq d(ab)$, and for all $a, b \in D$ where b

is non-zero, there exist elements q and r in D such that $a = bq + r$, where $r = 0$ or $d(r) < d(b)$. $\mathbb{Z}$ is a Euclidean domain with $d(x) = |x|$ and so is $F[x]$ where F is a field and $d(f(x)) = deg(f(x))$. A Euclidean domain is a principal ideal domain and also thus a unique factorization domain (Gallian 319).

DEFINITION 1.2 We call a non-empty subset of an R-module M a submodule if it is a subgroup under addition and also is closed under multiplication from the ring R. $\blacksquare$

Notice that we can think of Abelian groups as $\mathbb{Z}$-modules. That is to say for any $a \in A$, and some integer m, ma just means $a + a + \cdots + a$, m times, with $0a$ being the identity element in A. It is clear that multiplication from the integers is distributive if and only if A is Abelian. For suppose multiplication is distributive, then $(a + b) + (a + b) = 2(a + b) = 2a + 2b$ so $b + a = a + b$. For the converse suppose that our group is Abelian, then $n(a + b) = (a + b) + \cdots + (a + b) = na + nb$.

DEFINITION 1.3 Let M be an R-module and let $a_1, a_2, \ldots, a_k$ be elements of M. We will define $\langle a_1, \ldots, a_k \rangle = Span\{a_1, \ldots, a_k\} = \{0 + r_1a_1 + \cdots + r_ka_k | r_1, \ldots, r_k \in R\}$. $\blacksquare$

Note that $Span(\emptyset) = \{0\}$.

THEOREM 1.1 $\langle a_1, \ldots, a_k \rangle$ is a submodule of M. **Proof:** Suppose R is a ring, that M is an R module, and that $\{a_1, \ldots, a_k\}$ are elements of M. Now $\langle a_1, \ldots, a_k \rangle$ is non-empty since $0 + 1a_1 + \cdots + 1a_k = a_1 + \cdots + a_k \in \langle a_1, \ldots, a_k \rangle$. Then take any $a, b \in \langle a_1, \ldots, a_k \rangle$, by the definition of $\langle a_1, \ldots, a_k \rangle$ we know that $a = r_1a_1 + \cdots + r_ka_k$ and $b = s_1a_1 + \cdots + s_ka_k$, where r_i and s_i are ring elements, for $i = 1, \ldots, k$. Then $a - b = (r_1 - s_1)a_1 + \cdots + (r_k - s_k)a_k \in A$ and also $r(a) = (rr_1)a_1 + \cdots + (rr_k)a_k \in \langle a_1, \ldots, a_k \rangle$. Thus $\langle a_1, \ldots, a_k \rangle$ is a submodule of M. $\blacksquare$

DEFINITION 1.4 We call an R-module, M, *finitely generated* if M has a finite subset $\{a_1, \ldots, a_k\}$ such that $\langle a_1, \ldots, a_k \rangle = M$. $\blacksquare$

In this case we say that $\{a_1, \ldots, a_k\}$ generates, spans, or is a spanning set for M. We say that M is cyclic if there exists a single element $a \in M$ such that $\langle a \rangle = M$. Notice that if we consider a unitary ring as a module over itself, the module is finitely generated, and even cyclic since $\langle 1 \rangle = R$. If we consider $R \oplus R$ as a R module it too is finitely generated with a generating set $\{(1, 0), (0, 1)\}$.

Furthermore, if we let R be a module over itself, the submodules of R are exactly the ideals of R, since the ideals are the subgroups of R that are closed under multiplication by all elements of R.

We can also consider some examples finitely generated groups and modules.

Example 1.1 Any finite module is finitely generated. Simply take the generating set to be everything in the module.

Example 1.2 Any cyclic module (and also cyclic group) is finitely generated with the generator of the cyclic module being the spanning set for the module.

Example 1.3 The rational numbers are not a finitely generated $\mathbb{Z}$-module under the operation $+$; in other words they are not a finitely generated group. Assume that the set $\{p_1/q_1, \ldots, p_k/q_k\}$ is a generating set for $\mathbb{Q}$. Let q be the least common multiple of the denominators of our generating set, that is let $q = lcm(q_1, \ldots, q_k)$. Of course q must be nonzero. Notice that any linear combination of the elements in the generating set, say x/y, will have a denominator that divides q as long as x and y are relatively prime. But this is not a problem since every non-zero rational can be written in that form. Then, consider the rational number $1/(q+1)$. Since $q+1$ does not divide q, $1/(q+1) \notin \langle p_1/q_1, \ldots, p_k/q_k \rangle$ and therefore, the rational numbers are not finitely generated.

We can define a homomorphism between two R-modules as follows.

DEFINITION 1.5 Let M be a module over a ring R and let K be a module over R also, then we call a mapping $\phi: M \to K$ a homomorphism if for any m and n in M and for any r in R, $\phi(m+n) = \phi(m) + \phi(n)$ and $\phi(rm) = r\phi(m)$. ■

Notice that when R is a unitary ring, ϕ is a homomorphism if and only if $\phi(rm + rn) = r\phi(m) + r\phi(n)$.

DEFINITION 1.6 We call a bijective homomorphism an isomorphism. ■

THEOREM 1.2 A homomorphism whose domain is a finitely generated module is completely determined by its behavior on the generating set. **Proof:** Suppose that we have a homomorphism ϕ between two R-modules M and N, where M is finitely generated with generating set $\{a_1, \ldots, a_k\}$. Then take any $a \in M$ so $a = r_1a_1 + \cdots + r_ka_k$ for some $r_1, \ldots, r_k \in R$, thus

$\phi(a) = \phi(r_1 a_1 + \cdots + r_k a_k) = r_1\phi(a_1) + \cdots + r_k\phi(a_k)$. So, for any $a \in M$, $\phi(a)$ is completely determined by the image of the generating set. ■

Many of the familiar properties of homomorphisms hold. For example,

THEOREM 1.3 Suppose that ϕ is an R-module homomorphism between the two R-modules M and K, and that L is a submodule of K. Further suppose that ψ is a R-module homomorphism between K and N.

(a) $\phi(M)$ is a submodule of K **Proof:** For any $\phi(m), \phi(n) \in \phi(M)$, we have that $\phi(m) - \phi(n) = \phi(m - n) \in \phi(M)$, and also for any $r \in R$, $r\phi(m) = \phi(rm) \in \phi(M)$. Therefore $\phi(M)$ is closed under multiplication from R. ■

(b) $\phi^{-1}(L)$ is a submodule of M **Proof:** The fact that $\phi^{-1}(L)$ is non-empty and closed under group operations falls immediately from the fact that $\phi^{-1}(L)$ is a subgroup of M. Now consider multiplication from the ring R. Let $m \in \phi^{-1}(L)$ and $r \in R$. Then by the definition of ϕ^{-1}, $\phi(m) \in L$, so then $r\phi(m) \in L$ since L is a submodule of another R module. Thus $\phi(rm) \in L$ and $rm \in \phi^{-1}(L)$ which completes the proof. ■

(c) The composition of two homomorphism is a homomorphism. **Proof:** We will show that ϕ composed with ψ is an R-module homomorphism between M and N. For take any $r \in R$ and $x, y \in M$, then $\phi(\psi(r(x + y)) = \phi(r\psi(x) + r\psi(y)) = r\phi(\psi(x)) + r(\phi(\psi(x))$. ■

(d) The inverse function of an isomorphism is a isomorphism. **Proof:** This is easy to see for suppose ϕ is an isomorphism between two R-modules, M and K, then ϕ^{-1} is a bijection between K and M. To prove that it is an additive homomorphism consider $\phi^{-1}(x + y)$ where $x, y \in N$. Notice that $\phi(\phi^{-1}(x + y)) = x + y = \phi(\phi^{-1}(x)) + \phi(\phi^{-1}(y)) = \phi(\phi^{-1}(x) + \phi^{-1}(y))$. Thus $\phi^{-1}(x + y) = \phi^{-1}(x) + \phi^{-1}$ since ϕ is one-to-one. Now to prove that $\phi^{-1}(rx) = r\phi^{-1}(x)$. Note that $\phi(\phi^{-1}(rx)) = rx = r\phi(\phi^{-1}(x)) = \phi(r\phi^{-1}(x))$. So again $\phi^{-1}(rx) = r\phi^{-1}(x)$ which proves that the inverse function of an isomorphism is an isomorphism. ■

(e) The kernel of a homomorphism is a submodule. **Proof:** This is easy since clearly $\{0\}$ is a submodule of K. Notice that $Ker\phi = \phi^{-1}(\{0\})$ so then since $\phi^{-1}(\{0\})$ is a submodule of M, we are done. ■

We will now present some familiar results about modules and submodules. In particular we are interested in factor modules.

THEOREM 1.4 M/N forms an R-module. **Proof:** Let M be an R-module and let N be any submodule. Let us define the set $M/N = \{m + N | m \in M\}$. We claim that M/N is also an R-module where $(m_1 + N) + (m_2 + N) = (m_1 + m_2 + N)$ and $r(m_1 + N) = rm_1 + N$. Since the group is Abelian, N is normal and the first operation is well defined and forms a group (Gallian 173). Now consider the second operation. We want to prove that multiplication from the ring is well defined. Suppose that $m_1 + N = m_2 + N$, thus $m_1 = m_2 + n$ for some $n \in N$. Then $rm_1 = rm_2 + n'$ for some $n' \in N$ since N is closed under multiplication from the ring. Thus $rm_1 - rm_2 = n' \in N$ and therefore $rm_1 + N = rm_2 + N$. The rest of the properties follow directly from the fact that M is an R-module, because for any $a, b \in M$ and $r, s \in R$ we have that $r((a+N)+(b+N)) = r(a+b+N) = ra+rb+N = (ra+N)+(rb+N) = r(a+N)+r(b+N)$, and that $(r+s)(a+N) = (r+s)a+N = (ra+N)+(sa+N)$, and also that $(rs)(a+N) = rsa+N = r(sa+N)$ and finally, $1(a + N) = 1a + N = a + N$. So M/N is itself an R-module. ■

THEOREM 1.5 If M and N are modules over a ring R and ϕ is any surjective homomorphism from M onto N then if M is finitely generated, so is N. **Proof:** Let R be a ring and let M and N be R-modules, and also suppose that M is finitely generated with a generating set $\{a_1, \ldots, a_k\}$. We will show that the set $\{\phi(a_1), \ldots, \phi(a_k)\}$ generates N. For take any $n \in N$, since ϕ is surjective, there exists $m \in M$ such that $\phi(m) = n$. However, since M is finitely generated, $m = r_1a_1+\cdots+r_ka_k$ for some elements $r_1, \ldots, r_k \in R$. Thus $n = \phi(m) = \phi(r_1a_1)+\cdots+\phi(r_ka_k) = r_1\phi(a_1)+\cdots+r_k\phi(a_k)$ which completes the proof. Therefore $\langle\phi(a_1), \ldots, \phi(a_k)\rangle = N$. ■

This also shows the useful result that if A is a finitely generated module over a ring R, and B is any submodule of A, then the factor module A/B is finitely generated. The appropriate surjective homomorphism is $\phi(a) = a + B$.

We will now expand a familiar and very useful theorem to modules, what often called the first isomorphism theorem.

THEOREM 1.5 Let M and N be modules over a ring R and let ϕ be any homomorphism from M to N. Then $M/Ker\phi$ is isomorphic to $\phi(M)$. **Proof:** The obvious mapping, ψ, where $\psi(m + Ker\phi) = \phi(m)$ actually turns out to be the correct one. The fact that ψ is well defined and that it is an isomorphism at least up to the operation of $+$ is proved in exactly the same way as is done for groups so it will be omitted (Gallian 199). To show that $\psi(rx) = r\psi(x)$, notice that for any $m + Ker\phi \in M/Ker\phi$, we have that $\psi(r(m + Ker\phi)) = \psi(rm + Ker\phi) = \phi(rm) = r\phi(m) = r(\psi(m + Ker\phi))$. This completes the proof. ■

In the next section we will examine some properties of finitely generated modules.

Part 2: Submodules of Finitely Generated Modules

In this section we will prove the important theorem that every submodule of a finitely generated R-module is finitely generated, so long as R is a principal ideal domain. We will also explore the nature of a generating set; for example, whether it is linearly dependent. What follows is a sufficient condition for a module to be finitely generated.

THEOREM 2.1 Let A be a module and let B be a submodule of A. If both B and A/B are finitely generated then A is finitely generated. **Proof:** Since B and A/B are finitely generated modules, they both have generating sets, say $\{b_1, \ldots, b_i\}$ and $\{a_1 + B, \ldots, a_j + B\}$. We want to show that $\{a_1, \ldots, a_j, b_1, \ldots, b_i\}$ is a generating set for A. Clearly, $\langle a_1, \ldots, a_j, b_1, \ldots, b_i\rangle \subseteq A$. Take any $a \in A$, then because A/B is finitely generated, there exist ring elements $r_1, \ldots, r_j$ such that $a+B = r_1(a_1+B)+\cdots+r_j(a_j+B) = (r_1a_1+\cdots+r_ja_j)+B$. Clearly $a \in a+B$, so there exists some $b \in B$ such that $a = r_1a_1+\cdots+r_ja_j+b$. B however, is finitely generated also, so $b = s_1b_1+\cdots+s_ib_i$ for some $s_1, \ldots, s_i \in R$. Then $a = r_1a_1 + \cdots + r_ja_j + s_1b_1 + \cdots + s_ib_i \in \langle a_1, \ldots, a_j, b_1, \ldots, b_i\rangle$. ■

Just as done in linear algebra we can discuss linearly dependent and linearly independent subsets of modules.

DEFINITION 2.1 We call a finite subset of a module M, such as $\{a_1, \ldots, a_k\}$, linearly dependent if there exist ring elements $r_1, \ldots, r_k$, not all zero, such that $r_1a_1 + \cdots + r_ka_k = 0$, where 0 is the identity element of A. We call a subset of a module linearly independent if it is not linearly dependent. As in linear algebra we call a subset of a module M a basis for M if the subset generates A and if the subset is linearly independent. ■

Below are some results regarding bases.

THEOREM 2.2 A generating set $\{a_1, \ldots, a_k\}$ for an R-module M is linearly independent if and only if every element in M can be represented as a unique linear combination of the elements in the generating set. **Proof:** First let us assume that the generating set is linearly independent. Then assume that for some $a \in A, a = r_1a_1+\cdots+r_ka_k$ and $a = s_1a_1+\cdots+s_ka_k$ where $r_1, \ldots, r_k, s_1, \ldots, s_k$

are elements of R. Then $0 = a - a = (r_1 - s_1)a_1 + \cdots + (r_k - s_k)a_k$, but since our generating set is linearly independent, $r_i - s_i = 0$ so $r_i = s_i$ for all $i = 1, \ldots, k$. To prove the converse assume that $\{a_1, \ldots, a_k\}$ is linearly dependent. Then there exists elements of the ring $r_1, \ldots, r_k$, not all zero, such that $r_1a_1 + \cdots + r_ka_k = 0a_1 + 0a_2 + \cdots + 0a_k$. Thus 0 has two distinct representations. ■

Next we have an interesting lemma that proves many simple results for R-modules where R is an integral domain.

THEOREM 2.3 If R is an integral domain and M is an R-module with a generating set $\{a_1, \ldots, a_k\}$, and if $B = \{b_1, \ldots, b_l\}$ is any subset of M where $l > k$, then B is a linearly dependent set. **Proof:** Notice that $b_i \in M$ for all $i = 1, \ldots, l$. Thus we have elements $n_{xy} \in R$, where $x = 1, \ldots, l$ and $y = 1, \ldots, k$ such that

$$\begin{aligned} &b_1 = n_{11}a_1 + \cdots + n_{1k}a_k \\ &b_2 = n_{21}a_1 + \cdots + n_{2k}a_k \\ &\ldots \\ &b_l = n_{l1}a_1 + \cdots + n_{lk}a_k \end{aligned}$$

Notice, that we want to show that there exist ring elements m_1 to m_l, not all zero, such that $m_1b_1 + \cdots + m_lb_l = 0$, which would prove that $\{b_1, \ldots, b_l\}$ is linearly dependent. Now consider the following system of equations.

$$\begin{aligned} &m_1n_{11} + \cdots + m_ln_{l1} = 0 \\ &\ldots \\ &m_1n_{1k} + \cdots + m_ln_{lk} = 0 \end{aligned}$$

If this system of equations has a non-trivial solution in R, then those values of m_1 to m_l also make $m_1b_1 + \cdots + m_lb_l = 0$. Let F be the field of quotients for R (Gallian 273). Then there are elements $m_1, \ldots, m_l \in F$ not all zero that solve the system since $l > k$ because we can reduce this system over F, or in other words the number of columns is greater than the number of rows in the corresponding augmented matrix. But we can multiply through by the product of the denominators of the m_i's (over 1) to get solutions that are in R. Therefore the set $\{b_1, \ldots, b_l\}$ is linearly dependent.

■

There are two important immediate corollaries to this lemma. The first is that for any integral domain R, every basis of any R-module has the same size, since if one basis were smaller, then the larger basis would be linearly dependent. The second is that a basis is a smallest possible generating set for a module. It should be noted that a linearly independent set of maximal size is not necessarily a generating set. For example, in the finitely generated $\mathbb{Z}$-module (and also Abelian group) $\mathbb{Z}$, $\{2\}$ is a linearly independent set of maximal size in $\mathbb{Z}$ but it does not generate $\mathbb{Z}$. Also a minimal generating set is not always a basis, for example, $\{(1,0),(0,1)\}$ is a minimal generating set for the Abelian group $\mathbb{Z} \oplus \mathbb{Z}_3$, although it is not linearly independent since $3(0,1) = (0,0) = 0$.

Let M be a finitely generated R module with a generating set of size k. There is a natural surjective homomorphism from the R-module $R^k = R \oplus R \oplus \cdots \oplus R$ onto M. Suppose that M's generating set is $\{a_1, \ldots, a_k\}$. The function we want takes $(r_1, \ldots, r_k)$ to $r_1a_1 + \cdots + r_ka_k$. Notice that if our generating set is linearly independent, and thus a basis, this mapping is one-to-one and thus an isomorphism.

We will now prove that for a principal ideal domain R (Gallian 286), every submodule of a finitely generated R-module is finitely generated. First, however, we will prove the following lemma, that every submodule of R^k is finitely generated by a set of size k.

THEOREM 2.4 When R is a principal ideal domain, every submodule of the R module R^k is finitely generated and has a generating set of size k. **Proof:** We will use induction on k. For the base case of $k = 1$, we are looking at the submodules of R over R itself, which as we already noted are the ideals of R. Since R is a principal ideal domain every ideal and thus every submodule is of the form $\langle r \rangle$, where r is just an element of R, and thus every submodule of R has a finite generating set. Now let us assume that for some integer k, every submodule of R^k is finitely generated. Consider the homomorphism ϕ onto the first k-summands from R^{k+1} to R^k, in other words the mapping $\phi(m_1, \ldots, m_k, m_{k+1}) = (m_1, \ldots, m_k)$. The kernel of this homomorphism is clearly the subgroup $\{(m_1, \ldots, m_k, m_{k+1}) \in R^{k+1} | m_i = 0, i = 1, \ldots, k\}$ which is isomorphic to R, and thus finitely generated (with a single generator). Now let H be any submodule of R^{k+1}. Then $\phi(H)$ is a submodule of R^k, and thus by the induction hypothesis finitely generated with a generating set of size k. Let K be the kernel of that mapping from H to $\phi(H)$, so K is isomorphic to a submodule of R and is generated by a single element, since R is a principal ideal domain. By the first isomorphism theorem for modules, $\phi(H)$ is isomorphic to H/K. Thus H/K is finitely generated with a generating set of size k. Therefore by theorem 2.1, since both K and H/K are finitely generated, H is a finitely generated R-module with a generating set of size $k+1$, (of course it might have a smaller generating set). ■

This result and the next one can easily and obviously be extended to the case when we have a ring R with the property that every ideal is finitely generated. However, since what we will be dealing with in the next section are Euclidean domains which are principal ideal domains, looking at this restricted case is sufficient. In the general case where every ideal of R is finitely generated, some submodule of R^k might have a minimum generating set of size larger than k. Just as a side note, this property that every ideal is finitely generated is equivalent to the condition that every strictly increasing chain of ideals is finite in length (Gallian 322), or in other words that R is a Noetherian domain. We will now prove the main result of this section, that every submodule of a finitely generated R-module is finitely generated, so long as R is a principal ideal domain.

THEOREM 2.5 Let R be a principal ideal domain, then every submodule of a finitely R-module is finitely generated. **Proof:** Let M be a finitely generated R-module and let N be any submodule of M. Now M has a finite generating set say $S = \{a_1, a_2, \ldots, a_k\}$. Consider the natural surjective homomorphism, $\phi\colon R^k \to M$ defined by $\phi(r_1, \ldots, r_k) = r_1a_1 + r_2a_2 + \cdots + r_ka_k$. We know that $\phi^{-1}(N) = \{x \in R^k | \phi(x) \in N\}$ is a submodule of R^k. Therefore by theorem 2.4, $\phi^{-1}(N)$ is finitely generated. Now since ϕ is a surjective homomorphism onto N when its domain is restricted to $\phi^{-1}(N)$, by 1.5, N is finitely generated. ■

We now have a nice biconditional statement about finitely generated modules and their submodules.

THEOREM 2.6 If R is a principal ideal domain, M is an R-module and N is any submodule of M, then M is finitely generated if and only if N is finitely generated and M/N is finitely generated. **Proof:** This of course follows immediately from theorems 1.5, 2.1 and 2.5. ■

Part 3: A Factorization of Finitely Generated Modules

We will now prove our major result which is that every finitely generated R-module, where R is a Euclidean Domain, is isomorphic to the direct product of R-modules of the form $R/\langle a\rangle$, where a is an element of R. But first, we need a few more theorems. Let us consider any homomorphism $\phi\colon R^m \to R^n$. We will show that ϕ is a matrix transformation.

THEOREM 3.1 Let M be an $n \times m$ matrix over a ring R. Then there is a homomorphism $\phi\colon R^m \to R^n$ such that $\phi(x) = Mx$. **Proof:** Consider the $n \times m$ matrix M, and the mapping $\phi\colon R^m \to R^n$, where $\phi(x) = Mx$. Let x and y be in R^m and let r be in R, so we have $\phi(x+y) = M(x+y) = Mx + My = \phi(x) + \phi(y)$ and $\phi(rx) = M(rx) = (Mr)x = rMx = r\phi(x)$. Thus ϕ is a homomorphism. Therefore for every $n \times m$ matrix M with elements in R there is a homomorphism $\phi\colon R^m \to R^n$ such that $\phi(x) = Mx$. ■

Now we will prove the converse of the above statement.

THEOREM 3.2 Let R be a commutative ring. Then every homomorphism between the R-modules R^m and R^n is a matrix transformation. **Proof:** Let $\phi\colon R^m \to R^n$ be a homomorphism. Without loss of generality we can think of the elements of R^m as column vectors. Let us define e_i as the i'th column on the $m \times m$ identity matrix. Notice that ϕ is completely determined by how the different e_i's are mapped, since any homomorphism is completely determined by its behavior on the generating set. If we define the $n \times m$ matrix M so that i'th column is just $\phi(e_i)$, then $\phi(x) = Mx$. Thus every homomorphism $\phi\colon R^m \to R^n$ is a matrix transformation. ■

We have just established a correspondence between matrices and homomorphisms which will be vital in our proof shortly. But first there are a couple of interesting and probably expected points which can be made about the nature of the matrix M and its related homomorphism. If the columns of M are linearly independent, then the homomorphism is an injection. This is easy to see since only the zero vector is mapped to zero or in other words $|Ker(\phi)| = 1$. Also, if the columns of M span R^n then our homomorphism is a surjection. For take any $x \in R^n$ then, since the columns of

M are a spanning set, we can write $x = r_1v_1 + \cdots + r_mv_m$ where r_1 through r_m are elements of R and v_1 through v_m are the columns of M. Thus $\phi((r_1, \ldots, r_m)) = x$.

We will now prove that if R is a Euclidean domain, (and thus a principal ideal domain and also a unique factorization domain (Gallian 319)), then every finitely generated R-module is isomorphic to an R-module of the form $R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_k\rangle$, the direct product of cyclic R-modules. First we will present a small lemma.

Lemma: If R is a Euclidean domain, and if $r \in R$ and r is a unit, then $d(r) \leq d(x)$ for all non-zero $x \in R$. This is easy to prove; just note that by the definition of Euclidean domain $d(r) \leq d(rr^{-1}) = d(1) \leq d(1x) = d(x)$. Also it is easy to see that if $d(x) = d(1)$, then x is a unit. By the definition of a Euclidean Domain there exist elements q and r in R such that $1 = qx + r$ where $r = 0$ or $d(r) < d(x)$. But $d(r) < d(x)$ is a contradiction since $d(x) = d(1)$ and 1 is a unit. Thus $1 = qx + 0 = qx$ and x is a unit. ■

THEOREM 3.3 If R is a Euclidean domain, then every finitely generated R-module is isomorphic to an R module of the form $R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_k\rangle$ where $a_1, \ldots, a_k \in R$. **Proof:** Let R be a Euclidean domain and let M be a finitely generated R-module with a generating set $\{a_1, \ldots, a_k\}$. Consider the natural surjective homomorphism, $\phi\colon R^k \to M$ where $\phi(x_1, \ldots, x_k) = x_1a_1 + \cdots + x_ka_k$. Let us call the kernel of this homomorphism K. Since K is a submodule of R^k we know that it is finitely generated, and has a generating set of size k, say $\{b_1, \ldots, b_k\}$. Consider the homomorphism $\psi\colon R^k \to K$ where $\psi((x_1, \ldots, x_k) = x_1b_1 + \cdots + x_kb_k$. But then ψ is just a matrix transformation $\psi(v) = Cv$ where the columns of the matrix C are the elements of the generating set $\{b_1, \ldots, b_k\}$. So for every finitely generated module there is a $k \times k$ matrix C and its corresponding homomorphism ψ such that M is isomorphic to $R^k/\psi(R^k)$ by the first isomorphism theorem.

Now consider what happens if C is a diagonal matrix with entries $c_1, \ldots, c_k$ along the diagonal. Then $K = \langle c_1\rangle \oplus \langle c_2\rangle \oplus \cdots \oplus \langle c_k\rangle$. Notice that if $c_i = 0$, then $\langle c_i\rangle = \{0\}$ and if $\langle c_i\rangle$ is a unit, then $\langle c_i\rangle = R$. Now look at the quotient module $R^k/(\langle c_1\rangle \oplus \cdots \oplus \langle c_k\rangle)$. This module is isomorphic to the R-module $R/\langle c_1\rangle \oplus R/\langle c_2\rangle \oplus \cdots \oplus \mathbb{R}/\langle c_k\rangle$ with the obvious mapping. Notice that $R/\langle 0\rangle$ is just R

and $R/\langle u\rangle$ is isomorphic to $\{0\}$ whenever u is a unit. We can essentially throw away or forget about the the factors of the form $R/\langle u\rangle$, as they add nothing to the module.

We will now look at what happens if C is not a diagonal matrix. We will show how to reduce C to C', and that R/K is isomorphic to R/K', where K' is the image of the homomorphism corresponding to the reduced matrix C'. We will first show that the following row and column operations on C (which of course could change the homomorphism ψ) do not change the module R/K up to isomorphism. We will use ideas of elementary matrices to prove some of these results.

a.) Column Replacement: This is adding a scalar multiple of one column to another. Clearly this does not change the module $K = \psi(R^k)$. Since K has a generating set $\{b_1, \ldots, b_k\}$ and the matrix C consists of merely the elements of that set as columns, adding some scalar multiple of column i to column j is really just changing the generating set to $\{b_1, \ldots, b_i, \ldots, rb_i + b_j, \ldots, b_k\}$ for some ring element r, but of course that really changes nothing since b_j is still generated by the new generating set, namely by adding $-rb_i$ to $rb_i + b_j$.

b.) Column Scaling (by a unit in R): This is multiplying a column in C by a unit r which is equivalent to transforming the generating set of K from $\{b_1, \ldots, b_i, \ldots, b_k\}$ to $\{b_1, \ldots, rb_i, \ldots, b_k\}$ which of course both generate the same thing since $r^{-1}(rb_i) = b_i$.

c.) Column Interchange: This is just switching two columns in the matrix M. In terms of our basis $\{b_1, \ldots, b_i, \ldots, b_j, \ldots, b_k\}$, we are just switching b_i and b_j, which of course does not change K.

We will handle all these three row operations at once in the next paragraph.

d.) Row Replacement

e.) Row Scaling (by a unit in R)

f.) Row Interchange

Row operations are a bit more complicated; they change every element in the basis, and can change what elements are actually in K. However, what we will show is that $R^k/\psi_C(R^k)$ is isomorphic to $R^k/\psi_{EC}(R^k)$, where E is the elementary matrix corresponding to the appropriate row operation that was performed on C. Consider the mapping between these two modules defined by

$\theta(x) = Ex$. Since E is an elementary matrix it is easy to see it has an inverse. If E was created by performing a row replacement on the identity matrix, we can create E^{-1} by performing the same row replacement but by using the negative of the original scalar. If E was created by scaling a row by r then E^{-1} is created by scaling the same row by r^{-1}. If E was made by switching two of the columns of the identity matrix, then $E = E^{-1}$. Now consider $\theta(K)$, since E is a matrix, θ is a homomorphism, and in fact, since E has an inverse, θ has an inverse function $\theta^{-1}(x) = E^{-1}x$. Thus θ must be an injection, but it is also a surjection onto R^k since the columns of the identity matrix I span R^k, and so do the columns of an elementary matrix E, since one column operation can change I to any E. Therefore $\theta(K)$ is isomorphic to K. Thus the three row operations on M take K to an isomorphic R-module, K'.

Now we need to show that R^k/K is isomorphic to R^k/K' after performing a row operation (remember column operations change nothing). The mapping that takes $x+K$ to $\theta(x)+K' = Ex+K'$ works. We must show that the mapping is well defined. Suppose that $x+K = y+K$. Then $x-y = k$ for some $k \in K$, now $Ex - Ey = Ek \in \theta(K) = K'$. It is a homomorphism since it is a matrix transformation, it is an injection since E has an inverse, and it is a surjection since θ is a surjection onto R^k. Now we know that performing a finite number of row and column operations on C does not change R^k/K up to isomorphism.

We will show that given a $k \times k$ matrix C, we can reduce C, using the above operations, to a diagonal matrix, and thus not alter the corresponding module, at least up to isomorphism.

The Algorithm for Reducing our Matrix:

1. Take $m_{i,j}$ to be any non-zero element, (if there is no such element the matrix is diagonal) of the $n \times n$ matrix C where $d(m_{i,j}) \leq d(c)$ for any non-zero entry c in our matrix C. That is $m_{i,j}$ is smallest entry of the matrix up to the function d.

If $m_{i,j}$ divides every element in its row and column, then use column replacement and row replacement to make that row and column zero (except for $m_{i,j}$). We have effectively reduced the dimension of the matrix by 1 row and 1 column. Go to step 1 with our new $n-1 \times n-1$ matrix, unless our matrix has only one element, in that case proceed to step 2.

Otherwise $m_{i,j}$ doesn't divide some element of its row or column, say it doesn't divide m_t, then by the division algorithm for a Euclidean Domain, there exists non-zero elements r and p such that $m_t = pm_{i,j} + r$, where $d(r) < d(m_{i,j})$. Then add $-p$ times the row (column) containing $m_{i,j}$ to the row (column) containing m_t. Then the entry at m_t becomes r. The smallest element (up to the function d) is now at least no bigger than r, and we can restart step 1.

This first process cannot continue indefinitely since the matrix has finite dimension and since at each step in the second case $d(r)$ gets smaller, so eventually $d(r) = d(1)$ (in which case r would be a unit and it would divide everything in its row and column).

In many ways this procedure is similar to the Euclidean Algorithm, except that we are not necessarily performing operations on two elements.

2. We now have some permutation of a diagonal matrix. Use column interchange to construct a diagonal matrix.

This proves that when R is a Euclidean domain, every finitely generated R-module can be expressed as the direct product of cyclic R-modules, which also proves that every finitely generated group can be expressed as the direct product of cyclic groups. ■

Example 3.1 We will now show this theorem in use on a finitely generated Abelian group (a $\mathbb{Z}$-module). Let the generating set for K be $\left\{ \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix} \begin{pmatrix} -1 \\ 0 \\ 4 \end{pmatrix} \begin{pmatrix} 4 \\ -2 \\ -3 \end{pmatrix} \right\}$ so or matrix is $A = \begin{pmatrix} 2 & -1 & 4 \\ 3 & 0 & -2 \\ 1 & 4 & -3 \end{pmatrix}$. If we use $d(x) = |x|$, the smallest element of the matrix, up to d, is (-1) on row one column two, (the 1 on row three column one would work also). -1 divides everything in its row and column since it is a unit, thus we have $A = \begin{pmatrix} 2 & -1 & 4 \\ 3 & 0 & -2 \\ 9 & 0 & 13 \end{pmatrix}$ after performing the appropriate row replacement on row three. Making the rest of row one zero is achieved by performing two column replacement operations so $A = \begin{pmatrix} 0 & -1 & 0 \\ 3 & 0 & -2 \\ 9 & 0 & 13 \end{pmatrix}$. Now effectively we can forget about row one and column two of the matrix, leaving us with $A' = \begin{pmatrix} 3 & -2 \\ 9 & 13 \end{pmatrix}$. But for the sake of visual simplicity let us leave that row and column in, although we won't consider them for any operations. Thus the new smallest element of A is (-2) on row two column three. We can then use column replacement on column one to get the new $A = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & -2 \\ 22 & 0 & 13 \end{pmatrix}$, and then perform column replacement back on column three to get $A = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 22 & 0 & 57 \end{pmatrix}$, and then performing row replacement again to get $A = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 57 \end{pmatrix}$. We now only have to use column interchange and we have $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 57 \end{pmatrix}$. Thus our finitely generated group is isomorphic to $\mathbb{Z}/\langle 1 \rangle \oplus \mathbb{Z}/\langle -1 \rangle \oplus \mathbb{Z}/\langle 57 \rangle$ which is just $\mathbb{Z}_{57}$.

Part 4: The Factorization of Finitely Generated Modules is Unique

Now that we have shown that we can factor any R-module into a direct product of cyclic R-modules, we will show that this factorization is unique when written in a certain form. We will show that every finitely generated R-module, where R is an Euclidean domain, can be written uniquely (not counting the order in which they are written) as a direct product of R's, and of R-modules of the form $R/\langle a^k \rangle$ where a is irreducible. First we will show that the number of factors of the form R is unique.

THEOREM 4.1 In the above factorization, the number of factors of the form $R/\{0\} = R$ is unique. **Proof:** Suppose R is a Euclidean domain and that M is a finitely generated R-module, then by theorem 3.3, M is isomorphic to $R^k \oplus R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_t \rangle$, where a_i is non-zero, non-unit. Also suppose that M is isomorphic to $R^l \oplus R/\langle b_1 \rangle \oplus \cdots \oplus R/\langle b_s \rangle$ where b_i is non-zero, non-unit. Therefore $R^k \oplus R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_t \rangle$ is isomorphic to $R^l \oplus R/\langle b_1 \rangle \oplus \cdots \oplus R/\langle b_s \rangle$. Now since R is also an integral domain, $R^k \oplus R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_t \rangle$ has a linearly independent subset of size k, namely the first k columns (or rows) of the $k+t$ identity matrix, $e_1, \ldots, e_k$. This set is linearly independent since R has no zero divisors. What we will now show is that any larger subset is not linearly independent. Suppose that $v_1, \ldots, v_{k+1}$ is a linearly independent subset of $R^k \oplus R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_t \rangle$, then let $a = a_1 a_2 \cdots a_t$, and consider the set $av_1, \ldots, av_{k+1}$. Clearly this set must also be linearly independent, but it also must be a subset of the module generated by $e_1, \ldots, e_k$, since the last t summands must all be zero. Therefore, by theorem 2.3, $v_1, \ldots, v_{k+1}$ is linearly dependent, which is a contradiction, Thus, the largest linearly dependent subset of $R^k \oplus R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_t \rangle$ has size k. Similarly, $R^l \oplus R/\langle b_1 \rangle \oplus \cdots \oplus R/\langle b_s \rangle$ has a linearly independent subset of size l, and every larger subset is linearly dependent. Since the two modules are isomorphic, it is easy to see that $R^k \oplus R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_t \rangle$ has a linearly independent subset of size l and that $R^l \oplus R/\langle b_1 \rangle \oplus \cdots \oplus R/\langle b_s \rangle$ has a linearly independent subset of size k. Thus $k = l$. ■

We will also prove that when $R^k \oplus R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_t \rangle$ is isomorphic to $R^k \oplus R/\langle b_1 \rangle \oplus \cdots \oplus R/\langle b_s \rangle$, that $R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_t\rangle$ is isomorphic to $R/\langle b_1\rangle \oplus \cdots \oplus R/\langle b_s\rangle$

THEOREM 4.2 If R is an Euclidean domain and the R-module, $M = R^k \oplus R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_t\rangle$ is isomorphic to $N = R^k \oplus R/\langle b_1\rangle \oplus \cdots \oplus R/\langle b_s\rangle$ then $R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_t\rangle$ is isomorphic to $R/\langle b_1\rangle \oplus \cdots \oplus R/\langle b_s\rangle$. **Proof:** Since the two are isomorphic there exists an isomorphism between them, let us call it ψ. Now consider $G = \{(x_1, x_2, \ldots, x_{k+t} \in M | x_1 = \cdots = x_k = 0\}$, notice that G is a submodule of M. And consider what happens when you restrict ψ to G. We will call this mapping that takes G to $\psi(G)$, ϕ. Notice that ϕ is still an injection. We will show that $\phi(G) = H = \{(y_1, y_2, \ldots, y_{k+s} \in N | y_1 = \cdots = y_k = 0\}$. It is easy to see that $\phi(G)$ is contained in H, for suppose that for some $x \in G$, we have that $\phi(x) = (l_1, \ldots, l_j, \ldots, l_k, y_{k+1}, \ldots, y_{k+s})$, where l_j is not equal to zero. Then let $a = a_1 a_2 \cdots a_t$, so $0 = \phi(0) = \phi(ax) = a\phi(x) = (al_1, \ldots, al_j, \ldots)$ which is not equal to zero since al_j is not equal to zero because R is an integral domain. But we can also show that ϕ maps G onto H. First, let us define $b = b_1 b_2 \cdots b_s$. Now if we take any $y \in H$, then there exists $x \in M$ such that $\psi(x) = y$. Now suppose that $x \notin G$, then some entry of x, say x_i, is not equal to 0, where $1 \leq i \leq k$. Thus bx is not equal to 0. So $\psi(bx) = b\psi(x) = by = 0 = \psi(0)$, which is a contradiction since ψ is one-to-one. Thus the mapping $\phi\colon G \to H$ is an isomorphism, which completes the proof. ■

Now we will prove that any R-module of the form $R/\langle a\rangle$ is isomorphic to an R-module of the form $R/\langle {a_1}^{p_1}\rangle \oplus \cdots \oplus R/\langle {a_k}^{p_k}\rangle$, where a_i is an irreducible element of R. First we will prove two small lemmas.

Lemma 1: Let R be a principal ideal domain and let $x, y \in R$. Suppose x and y have no common non-trivial factors; we will prove that there exist s and t in R such that $sx + ty = 1$. Consider $\langle x\rangle$ and $\langle y\rangle$; since R is a principal ideal domain, we know that $\langle a\rangle = \langle x, y\rangle = \langle x\rangle + \langle y\rangle$. Then, since $x, y \in \langle x, y\rangle$, we have that $x = ma$ and $y = na$ for some $m, n \in R$, so a is a factor of both x and y, thus a is a unit. Therefore $\langle x, y\rangle = R$, and since $1 \in R$, there exist $s, t \in R$ such that $sx + ty = 1$. ■

This next lemma is reminiscent of the Chinese Remainder Theorem.

Lemma 2: Let R be a principal ideal domain and let a_1, a_2 be non-zero non-unit elements of R and also suppose that a_1 and a_2 have no common non-trivial factors. We will prove that for any $a, b \in R$, there exists $x \in R$ such that $x + \langle a_1 \rangle = a + \langle a_1 \rangle$ and $x + \langle a_2 \rangle = b + \langle a_2 \rangle$. By the previous lemma there exists $s_a, s_b, t_a, t_b \in R$ such that $s_a a_1 + t_a a_2 = a$ and $s_b a_1 + t_b a_2 = b$. Then let $x = s_b a_1 + t_a a_2$. Clearly this is a solution to the system. ■

THEOREM 4.3 If R is a Euclidean domain, then any R-module of the form $R/\langle a \rangle$, where a is a non-zero non-unit element of R, is isomorphic to $R/\langle a_1 \rangle \oplus R/\langle a_2 \rangle$ where $a = a_1 a_2$ and a_1 and a_2 have no common factors. **Proof:** Let R be a Euclidean domain and let us consider the homomorphism $\phi: R \to R/\langle a_1 \rangle \oplus R/\langle a_2 \rangle$, where a_1 and a_2 are non-zero non-unit elements that have no common factors and $\phi(x) = (x + \langle a_1 \rangle, x + \langle a_2 \rangle)$. Clearly this mapping satisfies all the homomorphism properties. We need to prove that ϕ is surjective. If take any $(a + \langle a_1 \rangle, b + \langle a_2 \rangle) \in R/\langle a_1 \rangle \oplus R/\langle a_2 \rangle$, by the second lemma there exists $x \in R$ such that $x + \langle a_1 \rangle = a + \langle a_1 \rangle$ and $x + \langle a_2 \rangle = b + \langle a_2 \rangle$, thus $\phi(x) = (a + \langle a_1 \rangle, b + \langle a_2 \rangle)$. We are going to use the first isomorphism theorem. Let $a_1 a_2 = a$. We need to prove that $Ker\phi = \langle a \rangle$. Suppose that $\phi(x) = (0 + \langle a_1 \rangle, 0 + \langle a_2 \rangle)$. Then x is in $\langle a_1 \rangle$ and thus a multiple of a_1. Similarly x is a multiple of a_2. Since R is a unique factorization domain and since a_1 and a_2 have no common factors, $a|x$, $Ker\phi$ is contained in $\langle a \rangle$. Now take $x \in \langle a \rangle$, thus $x = ya = ya_1a_2$. Then $\phi(x) = (ya_2a_1 + \langle a_1 \rangle, ya_1a_2 + \langle a_2 \rangle) = 0$. Thus by the first isomorphism theorem for modules, $R/\langle a_1 \rangle \oplus R/\langle a_2 \rangle$ is isomorphic to $R/\langle a \rangle$. ■

We can now change the factorization that we found in theorem 3.3 into a factorization of the form $R/{p_1}^{m_1} \oplus \cdots \oplus R/{p_k}^{m_k}$ where p_i is irreducible, and $m_i > 0$. We will now show that for any finitely generated module there is only one factorization of this form up to isomorphism and reordering the factors.

THEOREM 4.4 If R is a commutative unitary ring and M is an R-module and M is isomorphic to $H_1 \oplus \cdots \oplus H_k$ where H_1 through H_k are also R-modules, then the submodule of M, $rM = \{rx | x \in G\}$ (p is an element of R) is isomorphic to $rH_1 \oplus \cdots \oplus rH_k$. **Proof:** First we must show that rM is really a submodule of M; clearly it is non-empty since $r0 = 0$. Then take any $ra, rb \in rM$.

Thus $ra - rb = r(a-b) \in rM$, and for any $s \in R$, $sra = r(sa) \in M$. Thus rM is a submodule of M. Now to actually prove the lemma. Take any $ra \in rM$ (where a is just an arbitrary element of M so $a = (h_1, \ldots, h_k)$), then $ra = r(h_1, \ldots, h_k) = (rh_1, \ldots, rh_k) \in pH_1 \oplus \cdots \oplus pH_k$. Similarly, take any $(rh_1, \ldots, rh_k) \in rH_1 \oplus \cdots \oplus rH_k$, then $(rh_1, \ldots, rh_k)$ is isomorphic to $r(h_1, \ldots, h_k) = ra \in rM$. Therefore $rM = rH_1 \oplus \cdots \oplus rH_k$. ■

We will now show how we can reduce the problem to showing that there is only one way to write $R/\langle p^{m_1}\rangle \oplus \cdots \oplus R/\langle p^{m_k}\rangle$ (where p is irreducible), by showing that if q has no common factors with p then $qR/\langle p^m\rangle$ is isomorphic to $R/\langle p^m\rangle$.

THEOREM 4.5 If R is a Euclidean domain and $p, q \in R$ have no common factors then the R-module $qR/\langle p\rangle$ is isomorphic to $R/\langle p\rangle$. **Proof:** Let R be a Euclidean domain and suppose $p, q \in R$ have no common factors. Now consider the mapping $\phi\colon R \to qR/\langle p\rangle$ defined by $\phi(x) = qx + \langle p\rangle$. Clearly this mapping is well defined. The fact that ϕ is onto and satisfies the homomorphism properties is trivial and will be omitted. Consider the kernel of this homomorphism. Notice that $0 + \langle p\rangle = \phi(x) = qx + \langle p\rangle$ if and only if $p|qx$. Then since R is a unique factorization domain and p and q have no common factors, $p|x$. Therefore the kernel of ϕ is $\langle p\rangle$. So by the first isomorphism theorem $R/\langle p\rangle$ is isomorphic to $qR/\langle p\rangle$. ■

We will now that the the size of the minimum generating set of the R-module, $R/\langle p^{m_1}\rangle \oplus \cdots \oplus R/\langle p^{m_k}\rangle$ is k (where p is an irreducible element of R).

THEOREM 4.6 If R is an Euclidean domain and p is an irreducible element of R, then the size of the minimum generating set of the R-module, $M = R/\langle p^{m_1}\rangle \oplus \cdots \oplus R/\langle p^{m_k}\rangle$ is k. **Proof:** Suppose that R is a Euclidean domain and that p is an irreducible element of R. Also suppose that the minimum generating set for the R-module, $M = R/\langle p^{m_1}\rangle \oplus \cdots \oplus R/\langle p^{m_k}\rangle$, (where $m_i > 0$), is smaller than k. We can even suppose it is size $k-1$ since we can always add elements to a generating set. Of course there already exists a generating set of size k: the columns (or rows) of the $k \times k$ identity matrix. Consider the mapping $\phi\colon M \to (R/\langle p\rangle)^k$, where $(R/\langle p\rangle)^k = (R/\langle p\rangle) \oplus \cdots \oplus (R/\langle p\rangle)$ (k times). We define $\phi((x_1 + \langle p^{m_1}\rangle, x_2 + \langle p^{m_2}\rangle, \ldots, x_k + \langle p^{m_k}\rangle)) = (x_1 + \langle p\rangle, x_2 + \langle p\rangle, \ldots, x_k + \langle p\rangle))$.

This mapping is well defined, for if $x + \langle p^{m_i} \rangle = y + \langle p^{m_i} \rangle$ then $x - y = np^{m_i}$ for some $n \in R$, thus $x - y = (np^{m_i - 1})p \in \langle p \rangle$, thus $x + \langle p \rangle = y + \langle p \rangle$. The fact that it is an onto homomorphism is obvious so the proof will be omitted. Now consider $R/\langle p \rangle \oplus \cdots \oplus R/\langle p \rangle$. Since p is irreducible and since a Euclidean domain is a principal ideal domain, $\langle p \rangle$ is maximal. Thus $R/\langle p \rangle$ is a field (when you multiply from elements of $R/\langle p \rangle$); let us call it F. Now since $R/\langle p^{m_1} \rangle \oplus \cdots \oplus R/\langle p^{m_k} \rangle$ has a generating set of size $k-1$, so does F^k as an R-module since ϕ is an onto homomorphism. Suppose we call this generating set $B = \{b_1, \ldots, b_{k-1}\}$. Since B is a generating set it generates $e_1, \ldots, e_k$, the natural generating set for F^k, or in other words the columns of the $k \times k$ identity matrix. That is for each e_i there exist $r_{1,i}, \ldots, r_{k-1,i} \in R$ such that $r_{1,i}b_1 + \cdots + r_{k-1,i}b_{k-1} = e_i$. Remember both these elements, the b_i's and the e_i's, are all cosets of $\langle p \rangle$. Since $r_{j,i} \in R$ for $j = 1, .., k-1$ and $i = 1, \ldots, k$, thus $r_{j,i} + \langle p \rangle \in R/\langle p \rangle$ for $j = 1, .., k-1$ and $i = 1, \ldots, k$. Then in the $F = R/\langle p \rangle$ vector space F^k we have that $(r_{1,i} + \langle p \rangle)b_1 + \cdots + (r_{k-1,i} + \langle p \rangle)b_{k-1} = e_i$ and thus we have a generating set for F^k smaller than the basis $\{e_1, \ldots, e_k\}$, a contradiction. Thus the smallest generating set is of size k. ■

The above theorem is vitally important for the proof that the factorization is unique. We have only more thing to show before we can prove our main theorem. We will now show that $R/\langle p^n \rangle$ is isomorphic to $p^k R/\langle p^{n+k} \rangle$.

THEOREM 4.7 If R is an integral domain and p is an element of R then the R-module $R/\langle p^n \rangle$ is isomorphic to the R-module $p^k R/\langle p^{n+k} \rangle$. **Proof:** Let R be a Euclidean domain and let p be an element of R. Consider the natural homomorphism from R onto $p^k R/\langle p^{n+k} \rangle$, where $\phi(x) = p^k x + \langle p^{n+k} \rangle$. Consider the kernel of this mapping and notice that $\phi(x) = 0$ if and only if $p^{n+k} | p^k x$. Thus since R is a unique factorization domain, $p^{n+k} | p^n x$ if and only if $p^n | x$, so the kernel of ϕ is $\langle p^n \rangle$. Therefore by the first homomorphism theorem, the R-module $R/\langle p^n \rangle$ is isomorphic to the R-module $p^k R/\langle p^{n+k} \rangle$. ■

We can now prove that the factorization is unique.

THEOREM 4.8 Let R be a Euclidean domain, and let $p_1, \ldots, p_k, q_1, \ldots, q_l$ be irreducible elements of R. Then if $M = R/\langle {p_1}^{m_1} \rangle \oplus \cdots \oplus R/\langle {p_k}^{m_k} \rangle$ is isomorphic to $N = R/\langle {q_1}^{n_1} \rangle \oplus \cdots \oplus R/\langle {q_l}^{n_l} \rangle$, and if $R/\langle {p_i}^{m_i}\rangle$ is a factor of M, then it is one of the factors of N, or in other words there exists a j such that $p_i = q_j$ and $m_i = n_j$. **Proof:** Let R be a Euclidean domain, let $p_1, \ldots, p_k, q_1, \ldots, q_l$ be irreducible elements of R and suppose that the R-module $M = R/\langle {p_1}^{m_1}\rangle \oplus \cdots \oplus R/\langle {p_k}^{m_k}\rangle$ is isomorphic to the R-module $N = R/\langle {q_1}^{n_1}\rangle \oplus \cdots \oplus R/\langle {q_l}^{n_l}\rangle$. Now suppose that we group all the factors where $p_i = p_j$ together. We want to be able to consider one irreducible at a time and show that both sides have that common factor. Without loss of generality, let us consider just one of the p_i's, say p_1. Let $p = \prod\limits_{p_i \neq p_1} {p_i}^{m_i}$, and let $q = \prod\limits_{q_i \neq p_1} {q_i}^{n_i}$. Of course pqM is still isomorphic to pqN. By theorems 4.4 and 4.5, and since R is a unique factorization domain, pqM is isomorphic to $R/\langle {p_1}^{s_1}\rangle \oplus \cdots \oplus R/\langle {p_1}^{s_m}\rangle$ and pqN is isomorphic to $R/\langle {p_1}^{t_1}\rangle \oplus \cdots \oplus R/\langle {p_1}^{t_m}\rangle$ where every said factor of pqM is a factor of M and every factor of pqN is a factor of N, and also every factor of M of the form $R/\langle {p_1}^{k}\rangle$ is a factor of pqM and every factor of N of that form is also a factor of pqN. Or in other words we wiped out all of the factors of the form $R/\langle a\rangle$ where $a \neq p_1$ because in that case $a|pq$. The number of factors in pqM and pqN must be the same by theorem 4.6. We shall also assume that $s_m \leq \cdots \leq s_1$ and $t_m \leq \cdots \leq t_1$. We want to show that $t_i = s_i$. Remember we know that $R/\langle {p_1}^{s_1}\rangle \oplus \cdots \oplus R/\langle {p_1}^{s_m}\rangle$ is isomorphic to $R/\langle {p_1}^{t_1}\rangle \oplus \cdots \oplus R/\langle {p_1}^{t_m}\rangle$. Suppose that $t_i > s_i$; notice of course that ${p_1}^{s_i}R/\langle {p_1}^{s_1}\rangle \oplus \cdots \oplus {p_1}^{s_i}R/\langle {p_1}^{s_m}\rangle$ is still isomorphic to ${p_1}^{s_i}R/\langle {p_1}^{t_1}\rangle \oplus \cdots \oplus {p_1}^{s_i}R/\langle {p_1}^{t_m}\rangle$. But the first factorization clearly has a larger minimum generating set because multiplying by ${p_1}^{s_i}$ wipes out all of the factors generated by ${p_1}^{s_j}$ where $s_j \leq s_i$ because of theorem 4.7 and the fact that $s_m \leq \cdots \leq s_1$ and $t_m \leq \cdots \leq t_1$. But that is a contradiction. We arrive at the same contradiction if we suppose that $s_i > t_i$. Therefore $t_i = s_i$. This proves that all the factors of M are factors of N.

But we can also prove that every factor of N is a factor of M in exactly the same way. Thus, there is only one way to express a finitely generated R-module as a direct product of elements of the form $R^t \oplus R/\langle {p_1}^{m_1}\rangle \oplus \cdots \oplus R/\langle {p_k}^{m_k}\rangle$. ■

Now since we also have theorems 4.1 and 4.2, we have proved that we can write a finitely generated R module in a unique form. This form is completely analogous to what we have already done in finite Abelian groups. Notice that since a finitely generated $\mathbb{Z}$ module is also an Abelian group we have proved that every finitely generated Abelian group is isomorphic to direct product $\mathbb{Z}^k \oplus \mathbb{Z}_{{p_1}^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{{p_k}^{m_k}}$, where p_i is prime, and this is the only such product that the finitely generated Abelian group is isomorphic to. This completes the proof of our main theorem. We will now go on to consider some special cases of Euclidean domains, particularly polynomials, where we can apply our results.

Part 5: An Application to Polynomials

Let F be a field. Remember that $F[x]$ is a Euclidean domain with $d(f(x)) = degree f(x)$ for any $f(x) \in F[x]$. Consider the Abelian group F^n, where n is a natural number. Normally we multiply elements of F^n by elements of F to give us an n dimensional vector space. However, we can also multiply by polynomials from $F[x]$ so long as we carefully define what we mean. Let L be an $n \times n$ matrix with entries from the field F. Suppose that $f(x) = a_k x^k + \cdots + a_0$; then let us define $f(L) = a_k L^k + a_{k-1} L^{k-1} + \cdots + a_0 I$ where I is the identity matrix. Notice that for polynomials $f, g \in F[x]$, $(f+g)(L) = f(L) + g(L)$ and $(fg)(L) = f(L)g(L)$, since when adding or multiplying polynomials in x we collect like terms and we can perform the same procedure on polynomials of matrices. Let us define how multiplication from $F[x]$ works. Take any $v \in F^n$ and any $f(x) \in F[x]$ and let us define $f(x)v = f(L)v$. Since $(f+g)(L) = f(L) + g(L)$ and $(fg)(L) = f(L)g(L)$, this satisfies the properties needed to be a module.

Definition 5.1 We denote the module F^n with scalar multiplication from $F[x]$ where $f(x)v = f(L)v$ for $f(x) \in F[x]$, $v \in F^n$, and some fixed $n \times n$ matrix L, as $(F^n)_L$. ■

Let us remind ourselves that two $n \times n$ matrices, L_1 and L_2, are called similar if there exists some invertible matrix P such that $PL_1P^{-1} = L_2$. Also recall that similar matrices have the same characteristic polynomial and thus the same eigenvalues (Lay 309). We say that a matrix is diagonalizable if it is similar to a diagonal matrix. Notice that if $L_1 = PL_2P^{-1}$ then ${L_1}^n = P{L_2}^nP^{-1}$. This is easy since ${L_1}^n = (PL_2P^{-1})(PL_2P^{-1})(PL_2P^{-1}) \cdots (PL_2P^{-1}) = PL_2(P^{-1}P)L_2(P^{-1}P) \cdots (P^{-1}P)L_2P^{-1} = PL_2^nP^{-1}$.

Lemma: If $L_1 = PL_2P^{-1}$ for matrices L_1, L_2, and P (P invertible), then for any $f(x) \in F[x]$, $f(L_1) = Pf(L_2)P^{-1}$. This is easy to see, for if $f(x) = a_n x^n + \cdots + a_1 x + a_0$, then $f(L_1) = a_n(L_1)^n + \cdots + a_1(L_1) + a_0 I = a_n(PL_2P^{-1})^n + \cdots + a_1(PL_2P^{-1}) + a_0(PIP^{-1}) = Pa_n{L_2}^nP^{-1} + \cdots + Pa_0IP^{-1} = P(f(L_2))P^{-1}$, which completes the proof. ■

We will now prove an interesting theorem relating these modules to the problem of similarity of matrices.

THEOREM 5.1 Suppose that L_1 and L_2 are $n \times n$ matrices with entries from a field F. Then $(F^n)_{L_1}$ is isomorphic to $(F^n)_{L_2}$ if and only if L_1 and L_2 are similar. **Proof:** Suppose that L_1 and L_2 are similar matrices, that means that $PL_1P^{-1} = L_2$ for some invertible matrix P. Define $\phi\colon (F^n)_{L_1} \to (F^n)_{L_2}$ by $\phi(v) = P^{-1}v$ for any $v \in F^n$. This mapping clearly satisfies the additive homomorphism properties, and since P is invertible, it is a bijection as well. All is that is left to show is that $\phi(f(x)v) = f(x)\phi(v)$. For any $v \in (F^n)_{L_1}$ and $f(x) \in F[x]$ we have that $\phi(f(x)v) = P^{-1}(f(L_1)v) = P^{-1}(Pf(L_2)P^{-1}v) = f(L_2)(P^{-1}v) = f(x)\phi(v)$, which completes the first direction. Now to prove the converse, suppose that $(F^n)_{L_1}$ and $(F^n)_{L_2}$ are isomorphic as R-modules. Let ϕ be any isomorphism between them, Remember that ϕ is completely determined by its action on a generating set. The most obvious generating set is $\{e_1, \ldots, e_n\}$, the columns of the $n \times n$ identity matrix. Now ϕ must also map these elements to a generating set, say $\{a_1, \ldots, a_n\}$. Since $\{e_1, \ldots, e_n\}$ can generate all elements of $(F^n)_{L_1}$ using only polynomials of degree 0 (which is just multiplication by elements of F), so can $\{a_1, \ldots, a_n\}$. Thus ϕ is a matrix transformation that takes v to Av, where the columns of A are a_1 through a_n. Notice that since the columns of A span F^n as an F-module, A is invertible. Consider the inverse isomorphism ϕ^{-1}, since inverse matrices are unique, $\phi^{-1}(v) = A^{-1}v$. Therefore for $i = 1, \ldots, n$, $AL_1e_i = \phi(L_1e_i) = \phi(xe_i) = x\phi(e_i) = L_2Ae_i$. Thus, since $AL_1e_i = L_2Ae_i$ for all e_i, we know $AL_1 = L_2A$, and therefore $AL_1A^{-1} = L_2$ so L_1 and L_2 are similar, which completes the proof. ■

We can use the theorems we developed in sections 3 and 4 to examine the nature of these modules for particular matrices. We will first consider what happens when L is a diagonal matrix.

THEOREM 5.2 If F is a field and L is a diagonal matrix with entries from F then the $F[x]$ module F^n where $f(x)v = f(L)v$ for $f(x) \in F[x]$ and $v \in F^n$, is isomorphic to $F[x]/\langle x - b_1\rangle \oplus \cdots \oplus F[x]/\langle x - b_n\rangle$ where $b_1, \ldots, b_n$ are the entries along the diagonal of L. **Proof:** It is sufficient to prove that the kernel of the natural surjective homomorphism ϕ that takes $(F[x])^n$ to the $F[x]$ module $(F^n)_L$ using the generating set $\{e_1, \ldots, e_n\}$, (the columns of the $n \times n$ identity matrix), is $\langle x-b_1\rangle \oplus \cdots \oplus \langle x-b_n\rangle$. Now $\phi((f_1(x),\ldots,f_n(x))) = f_1(x)e_1+\cdots+f_n(x)e_n$. Notice that since L is diagonal L^k is diagonal with entries along the diagonal of ${b_1}^k,\ldots,{b_n}^k$. Thus if $f(x) = a_kx^k+a_{k-1}x^{k-1}+\cdots+a_1x+a_0$, then $f(L) = a_kL^k+\cdots+a_1L+a_0I = \begin{pmatrix} f(b_1) & 0 & \ldots & 0 \\ 0 & f(b_2) & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & f(b_n) \end{pmatrix}$. Suppose that $\phi((f_1(x),\ldots,f_n(x))) = 0$, then $f_1(L)e_1+\cdots+f_n(L)e_n = 0$. Therefore $f_1(b_1) = 0$, $f_2(b_2) = 0$ and so on all the way through $f_n(b_n) = 0$. Thus $x-b_i$ divides $f_i(x)$, so therefore $Ker\phi \subseteq (\langle x-b_1\rangle,\ldots,\langle x-b_n\rangle)$. But clearly from the above logic, $(\langle x-b_1\rangle,\ldots,\langle x-b_n\rangle) \subseteq Ker\phi$ as well, which completes the proof. ■

Notice that this result extends to all diagonalizable matrices as well, since if L is diagonalizable it is similar to a diagonal matrix D, and thus $(F^n)_L$ is isomorphic to $(F^n)_D$. Then since the eigenvalues of D are simply the entries along the diagonal and since similar matrices have the same eigenvalues, $(F^n)_L$ is isomorphic to $F[x]/\langle x-b_1\rangle \oplus \cdots \oplus F[x]/\langle x-b_n\rangle$, where $b_1,\ldots,b_n$ are the eigenvalues of L. Notice that the product of the $(x-a_i)$'s is the characteristic polynomial for L. In later theorems, we will extend this result to non-diagonalizable matrices.

Suppose we are given a particular polynomial $p(x)$ and we want to construct an $F[x]$ module, $(F^n)_L$ isomorphic to $F[x]/p(x)$. What matrix should we use? We will first show how to construct a matrix with a given characteristic polynomial.

THEOREM 5.3 The the characteristic polynomial of the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ 0 & 0 & 1 & \ldots & 0 & -a_3 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}$$

is $p(x) = (-1)^n(\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0)$. **Proof:** We will use induction on n. Our base case is $n = 2$. Note that the determinant of the matrix $\begin{pmatrix} -\lambda & -a_0 \\ 1 & -a_1-\lambda \end{pmatrix}$ is $\lambda^n + a_1\lambda + a_0$. Now assume that the statement is true up to $n-1$, and consider the $n \times n$ matrix A minus the identity matrix multiplied by λ.

$$A - \lambda I_n = \begin{pmatrix} -\lambda & 0 & ... & 0 & -a_0 \\ 1 & -\lambda & ... & 0 & -a_1 \\ 0 & 1 & ... & 0 & -a_2 \\ ... & ... & ... & ... & ... \\ 0 & 0 & ... & 1 & -a_{n-1} - \lambda \end{pmatrix}.$$

We will use cofactor expansion along the first row to calculate the determinant. Notice the only columns we need to concern ourselves with are the first and the last. Thus our characteristic polynomial is

$$-\lambda det \begin{pmatrix} -\lambda & 0 & ... & 0 & -a_1 \\ 1 & -\lambda & ... & 0 & -a_2 \\ 0 & 1 & ... & 0 & -a_3 \\ ... & ... & ... & ... & ... \\ 0 & 0 & ... & 1 & -a_{n-1} - \lambda \end{pmatrix} + (-1)^{n-1}(-a_0) det \begin{pmatrix} 1 & -\lambda & 0 & ... & 0 \\ 0 & 1 & -\lambda & ... & 0 \\ ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & 1 \end{pmatrix}.$$

By the induction, hypothesis the determinant of the first matrix is $(-1)^{n-1}(\lambda^{n-1} + a_{n-1}\lambda^{n-2} + \cdots + a_2\lambda + a_1)$, and clearly the determinant of the second matrix is 1. Thus the characteristic polynomial of A is $-\lambda(-1)^{n-1}(\lambda^{n-1} + a_{n-1}\lambda^{n-2} + \cdots + a_2\lambda + a_1) + (-1)^{n-1}(-a_0) = (-1)^n(\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_2\lambda^2 + a_1\lambda) + (-1)^n a_0 = (-1)^n(\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_2\lambda^2 + a_1\lambda + a_0)$ which completes the proof. ■

We will denote the matrix created in the above theorem for the specific polynomial $p(x)$ as $A_{p(x)}$. Suppose using the theorems from the previous sections for a particular matrix L we end up with a module isomorphic to $F[x]/\langle p(x) \rangle$ where $p(x)$ is not necessarily irreducible. We can assume without loss of generality that $p(x)$ is of the form $(-1)^n(x^n + a_{n-1}x^{n-1} + \cdots + a_0)$. By the previous there exists a matrix $A_{p(x)}$ whose characteristic polynomial is $p(x)$. We will now show that $F[x]/\langle p(x) \rangle$ is isomorphic to the $F[x]$ module $(F^n)_{A_{p(x)}}$.

THEOREM 5.4 Suppose that $p(x) \in F[x]$ and the degree of $p(x)$ is n, then $F[x]/\langle p(x) \rangle$ is isomorphic to $(F^n)_{A_{p(x)}}$. **Proof:** We can assume without loss of generality that $p(x)$ is of the form $(-1)^n(x^n + a_{n-1}x^{n-1} + \cdots + a_0)$ because $\langle p(x) \rangle = \langle q(x) \rangle$ for some monic polynomial, $q(x)$. Suppose that $p(x) = (-1)^n(x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)$. Notice that $\{1, x, x^2, \ldots, x^{n-1}\}$ forms a generating set of size n for $F[x]/\langle p(x) \rangle$ as an F module and thus as an $F[x]$ module as well.

Also note that $\{e_1, \ldots, e_n\}$ forms a generating set for F^n as an F-module, and thus again as an $F[x]$ module. Notice that for any $f(x) + \langle p(x)\rangle \in F[x]/\langle p(x)\rangle$, $f(x) + \langle p(x)\rangle = (b_{n-1}x^{n-1} + \cdots + b_1x + b_0) + \langle p(x)\rangle$ for some $b_{n-1}, \ldots, b_0 \in F$. Define a mapping $\phi\colon F^n \to F[x]/\langle p(x)\rangle$, where for any $a \in F^n$, $\phi(a) = \phi(a_1e_1 + \cdots + a_ne_n) = (a_nx^{n-1} + \cdots + a_2x + a_1) + \langle p(x)\rangle$ where a_i is the i'th entry of a. Clearly this mapping is well defined since there is no ambiguity in the domain of the function. This mapping is also surjective since every element in $F[x]/\langle p(x)\rangle$ can be written in the form $a_{n-1}x^{n-1} + \cdots + a_1x + a_0 + \langle p(x)\rangle$. This mapping is an additive homomorphism, since $\phi(v + w) = \phi((v_1 + w_1)e_1 + \cdots + (v_n + w_n)e_n) = ((v_n + w_n)x^{n-1} + \cdots + (v_1 + w_1)) + \langle p(x)\rangle = ((v_nx^{n-1} + \cdots + v_1) + \langle p(x)\rangle) + ((w_nx^{n-1} + \cdots + w_1) + \langle p(x)\rangle) = \phi(v) + \phi(w)$. We also must show that this mapping is an injection. For convenience, for any $v \in F^n$ we will denote $f_v(x) = v_nx^{n-1} + \cdots + v_1$ where $v_1, \ldots, v_n$ are the entries of v. Now suppose that $\phi(v) = \phi(w)$, then $f_v(x) + \langle p(x)\rangle = f_w(x) + \langle p(x)\rangle$, so $f_v(x) - f_w(x) \in \langle p(x)\rangle$. Since both $f_v(x)$ and $f_w(x)$ have degree less than n, so does their difference. Thus since the degree of $p(x)$ is n, $f_v(x) - f_w(x) = 0$, so $f_v(x) = f_w(x)$ and $v = w$. Thus the mapping is one-to-one. To complete the proof that ϕ is an isomorphism it is enough to show that $\phi(xe_i) = x\phi(e_i)$ and that $\phi(te_i) = t\phi(e_i)$ for any $t \in F$, because we can construct any polynomial out of x's and elements of F. For example, if these conditions hold, note that $\phi((x^2 + x)v) = \phi(x^2v) + \phi(xv) = x\phi(xv) + x\phi(v) = (x^2 + x)\phi(v)$. Notice that $\phi(xe_i) = \phi(A_{p(x)}e_i) = \phi(A_i)$, where A_i is the i'th column of $A_{p(x)}$. Suppose that $i \in \{1, \ldots, n-1\}$, then clearly, $\phi(A_i) = \phi(e_{i+1}) = x^i + \langle p(x)\rangle = x(x^{i-1} + \langle p(x)\rangle) = x\phi(e_i)$. Now for $i = n$, $\phi(xe_i) = \phi(xe_n) = \phi(A_{p(x)}e_n) = (-a_{n-1}x^{n-1} + -a_{n-2}x^{n-2} + \cdots + -a_1x + -a_0) + \langle p(x)\rangle$. Remember that $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, thus $x^n + \langle p(x)\rangle = (-a_{n-1}x^{n-1} + -a_{n-2}x^{n-2} + \cdots + -a_1x + -a_0) + \langle p(x)\rangle$, so now we have that $\phi(xe_n) = x^n + \langle p(x)\rangle = x(x^{n-1} + \langle p(x)\rangle) = x\phi(e_n)$. Therefore $\phi(xe_i) = x\phi(e_i)$. But also clearly $\phi(te_i) = tx^{i-1} + \langle p(x)\rangle = t(x^{i-1} + \langle p(x)\rangle) = t\phi(e_i)$. Therefore ϕ is an $F[x]$ module isomorphism, which completes the proof. ■

We will now show how to paste these matrices together to get arbitrary $F[x]$ modules of the form $F[x]/\langle p_1(x)\rangle \oplus \cdots \oplus F[x]/\langle p_k(x)\rangle$.

THEOREM 5.5 If F is a field then the $F[x]$ module of the form $F[x]/\langle p_1(x)\rangle \oplus \cdots \oplus F[x]/\langle p_k(x)\rangle$ is isomorphic to the $F[x]$ module F^n generated by the $n \times n$ block matrix

$$A = \begin{pmatrix} A_{p_1(x)} & 0 & \dots & 0 \\ 0 & A_{p_2(x)} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & A_{p_k(x)} \end{pmatrix},$$

where n is the sum of the degrees of the polynomials $p_1(x)$ through $p_k(x)$ and $A_{p_i(x)}$ is the matrix from theorem 5.3 with characteristic polynomial $p_i(x)$. **Proof:** First let us define d_i to be the degree of the polynomial $p_i(x)$. To prove this theorem, we will use induction on k. Result 5.4 provides a base case, so suppose that the statement is true up to $k-1$. Consider $F[x]$ modules $F[x]/\langle p_1(x)\rangle \oplus \cdots \oplus F[x]/\langle p_k(x)\rangle$ and $(F^n)_A$, (where A is defined as above). By the induction hypothesis $F[x]/\langle p_1(x)\rangle \oplus \cdots \oplus F[x]/\langle p_{k-1}(x)\rangle$ is isomorphic to the $F[x]$ module F^{n-d_k}, generated by the block matrix

$$A' = \begin{pmatrix} A_{p_1(x)} & 0 & \dots & 0 \\ 0 & A_{p_2(x)} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & A_{p_{k-1}(x)} \end{pmatrix}.$$

So there exists an $F[x]$ module isomorphism, call it ψ that takes $(F^{n-d_k})_{A'}$ onto $F[x]/\langle p_1(x)\rangle \oplus \cdots \oplus F[x]/\langle p_{k-1}(x)\rangle$. Also by theorem 5.4, there exists an isomorphism θ that takes $(F^{d_k})_{A_{p_k(x)}}$ onto $F[x]/\langle p_k(x)\rangle$. Now then we want to show that $(F^n)_A$ is isomorphic to $(F^{n-d_k})_{A'} \oplus (F^{d_k})_{A_{p_k(x)}}$. To see this take any $v \in (F^n)_A$, and define v_1 to be the first $(n-d_k)$ entries of v and v_2 the last d_k entries of v. Now consider the mapping $\phi\colon (F^n)_A \to (F^{n-d_k})_{A'} \oplus (F^{d_k})_{A_{p_k(x)}}$, where $\phi(v) = (v_1, v_2)$. It is obvious that this mapping is an additive isomorphism, so all that we need to check is that it preserves multiplication by polynomials. Again it is enough to check that it preserves multiplication by x and elements from F. Note that $\phi(xv) = \phi(Av) = ((Av)_1, (Av)_2)$. Now since the entries of the first $(n-d_k)$ columns of the last d_k rows of A are all zero, and the last d_k columns of the first $(n-d_k)$ rows are also zero, $(Av)_1 = A'v_1$ and $(Av)_2 = A_{p_k(x)}v_2$. Also, for any $t \in F$, clearly $\phi(tv) = t\phi(v)$. Thus ϕ is an $F[x]$ isomorphism. Therefore $(F^n)_A$ is isomorphic to $(F^{n-d_k})_{A'} \oplus (F^{d_k})_{A_{p_k(x)}}$ which is isomorphic to $F[x]/\langle p_1(x)\rangle \oplus \cdots \oplus F[x]/\langle p_{k-1}(x)\rangle \oplus F[x]/\langle p_k(x)\rangle$ which completes the proof. ■

We need one more theorem before we can write down some interesting corollaries. We need to show that the characteristic polynomial of A, from the above theorem, is the product of the $p_i(x)$'s.

THEOREM 5.6 Let F be a field and let us take any polynomials $p_1(x), \dots, p_k(x) \in F[x]$ of the form $(-1)^n(x^n + a_{n-1}x^{n-1} + \cdots + a_0)$. Then define $A_{p_1(x)}$ through $A_{p_k(x)}$ as was done in theorem 5.3. Then the $n \times n$ matrix

$$A = \begin{pmatrix} A_{p_1(x)} & 0 & \dots & 0 \\ 0 & A_{p_2(x)} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & A_{p_k(x)} \end{pmatrix}$$

has characteristic polynomial of $p_1(x)p_2(x)\cdots p_k(x)r$ where r is an element of F. **Proof:** Again let d_i be the degree of the polynomial $p_i(x)$. One method to find determinants is to reduce the matrix to echelon form and then multiply the elements along the diagonal together (multiplying by any scalars you may have used to reduce the matrix and also multiplying by -1 for every time you interchanged two rows). Suppose we let $B = A - \lambda I$, where I is the $n \times n$ identity matrix. When calculating the determinant of this matrix in this fashion we can effectively do each block of the matrix $(A_{p_i(x)} - \lambda I)$ separately. Then it is clear that the determinant of $A - \lambda I_n$ is just the determinant of $A_{p_1(x)} - \lambda I_{d_1}$ multiplied by the determinant of $A_{p_2(x)} - \lambda I_{d_2}$ and so on. Thus the characteristic polynomial of A is plus or minus $p_1(x)p_2(x)\cdots p_k(x)$ since the characteristic polynomial of $A_{p_i(x)}$ is just $(-1)^{d_i}p_i(x)$. This completes the proof. ■

We can further characterize the polynomials $p_1(x)$ through $p_k(x)$.

THEOREM 5.7 If the $F[x]$ module $(F^n)_L$ is isomorphic to $F[x]/\langle p_1(x)\rangle \oplus \cdots \oplus F[x]/\langle p_k(x)\rangle$, then the characteristic polynomial of L is some element in F multiplied by the product of the polynomials $p_1(x)$ through $p_k(x)$. **Proof:** Any $F[x]$ module $(F^n)_L$, where L is an $n \times n$ matrix over F, is isomorphic to $F[x]/\langle p_1(x)\rangle \oplus \cdots \oplus F[x]/\langle p_k(x)\rangle$, for some polynomials $p_1(x)$ through $p_k(x)$ by theorem 3.3. By our previous theorems, it is easy to see that the product $p(x) = \prod_{i=1}^{k} p_i(x)$ must be unique for any such factorization (up to multiplying by an element from the field, which is of course a unit), since to get to our unique factorization we factored the $p_i(x)$'s into relatively prime parts. Now this module is itself isomorphic to $(F^n)_A$ where A is the block diagonal matrix described in 5.5 and 5.6 with submatrices $A_{p_i(x)}$. Therefore, $(F^n)_A$ is isomorphic to $(F^n)_L$, which means A and

L are similar by theorem 5.1. Furthermore, as we noted earlier, they have the same characteristic polynomial. Thus, since the characteristic polynomial of A is the product of the $p_i(x)$'s and some field element, we have that $\prod_{i=1}^{k} p_i(x)$ multiplied by some field element is the characteristic polynomial of L. This completes the proof. ■

Note this also proves that the degree of the product of the $p_i(x)$'s is n. We can now prove a very interesting theorem about the characteristic polynomial.

THEOREM 5.8 Suppose that $p(x)$ is the characteristic polynomial of L, which is some $n \times n$ matrix over a field F. Then $p(L)$ is the zero matrix. **Proof:** Let F be a field, L be an $n \times n$ matrix over a field. Using theorem 3.3 the $F[x]$ module $(F^n)_L$ is isomorphic to $F[x]/\langle p_1(x)\rangle \oplus \cdots \oplus F[x]/\langle p_k(x)\rangle$ for some $p_1(x), \ldots, p_k(x) \in F[x]$. Thus there exists an isomorphism between them whose domain is the $F[x]$ module $(F^n)_L$; let us call this isomorphism ϕ. By 5.7, $\prod p_i(x) = rp(x)$ for some element $r \in F$. Notice that for any element $v \in F[x]/\langle p_1(x)\rangle \oplus \cdots \oplus F[x]/\langle p_k(x)\rangle$, $p(x)v = 0$. Thus $0 = \phi(0) = \phi(p(x)v) = p(x)\phi(v) = p(L)\phi(v)$. Since this holds for all $v \in F[x]/\langle p_1(x)\rangle \oplus \cdots \oplus F[x]/\langle p_k(x)\rangle$ and since ϕ is surjective, $p(L)e_i = 0$. Thus every column of $p(L)$ is zero, and therefore $p(L)$ is the zero matrix. ■

Let us conclude this section by comparing the $F[x]$ module $(F^n)_L$ to a finite Abelian group, a $\mathbb{Z}$ module. Notice that the above theorem essentially states that the characteristic polynomial of a matrix is the *order* of the $(F^n)_L$ module in the same way as the order of a finite Abelian group $\mathbb{Z}_{{p_1}^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{{p_k}^{n_k}}$ is ${p_1}^{n_1}{p_2}^{n_2} \cdots {p_k}^{n_k}$. Notice that for every finite Abelian group we have associated with it, a unique unordered sequence of prime integers raised to powers that completely determines the structure of the group. Furthermore, every two finite Abelian groups that have this sequence of integers are isomorphic. For the $F[x]$ module $(F^n)_L$ we have the same situation except that we have a unique unordered sequence irreducible polynomials raised to powers that completely determines the structure of the module. Since two $F[x]$ modules, $(F^n)_{L_1}$ and $(F^n)_{L_2}$ are isomorphic if and only if L_1 and L_2 a similar, it is easy to see that for every matrix there is a unique sequence of powers of irreducible polynomials associated with it such that two matrices are similar if and only if they have the same sequence of polynomials. Finally notice that a matrix is diagonalizable if all these polynomials have degree 1.

In summary, we have proved that when R is a principal ideal domain, every submodule of a finitely generated R-module is finitely generated. We have proved that when R is a Euclidean domain we can factor any finitely generated module uniquely as a module of the form $R/\langle {p_1}^{n_1}\rangle \oplus \cdots \oplus R/\langle {p_k}^{n_k}$ where the p_i's are irreducible. We have also proved that when $p(x)$ is the characteristic polynomial of a matrix L, that $p(L)$ is the zero matrix.

Bibliography

Gallian, Joseph A. Contemporary Abstract Algebra. 4th ed. New York: Houghton Mifflin Company, 1998.

Lay, David C. Linear Algebra and its Apllications. 2nd ed. Reading Massachusetts: Addison-Wesley, 1997.