Module Theory

Boran Erol

March 20, 2024

Here's the basic problem in module theory:

Given a ring with certain nice properties, classify all modules over that ring.

This problem turns out to be extremely difficult. Therefore, we restrict to certain types of modules and try classifying those modules.

Modules are the representation objects for rings. They are, by definition, algebraic objects on which rings act.

1 Definitions and Basic Properties

1.1 Definition and Characterization using the Endomorphism Ring

Definition 1. Let R be a ring and M be an Abelian group. M is said to be a left R-module if

1. $(M, +)$ is an additive Abelian group.
2. $\forall x \in M : 1 \cdot x = x$
3. $\forall a, b \in R : \forall x \in M : a \cdot (b \cdot x) = (ab) \cdot x$
4. $\forall a \in R : \forall x, y \in M : a(x + y) = ax + ay$
5. $\forall a, b \in R : \forall x \in M : (a + b)x = ax + bx$

Let M be a left R-module. Fix $a \in R$. Notice that using Axiom 4, the map $f_a : M \to M$ defined by $f_a(x) = ax$ is a group homomorphism. Now, consider $\phi : R \to \text{End}(M)$ defined by $\phi(a) = f_a$.

Lemma 1.1. ϕ is a ring homomorphism.

Proof.

$$\phi(a + b)(x) = f_{a+b}(x) = (a + b)x = ax + bx = f_a(x) + f_b(x) = \phi(a)(x) + \phi(b)(x)$$

$$\phi(ab)(x) = f_{ab}(x) = (ab)x = a(bx) = f_a(bx) = f_a(f_b(x)) = \phi(a)\phi(b)(x)$$

□

Similarly, given $\phi : R \to End(M)$ a ring homomorphism, we can give M a module structure.

1.2 Exercises

Lemma 1.2. Let F be a field and $R = M_n(F)$. An element $A \in R$ is a zero divisor if and only if it's singular.

The units of $M_n(F)$ form the **general linear group** $GL_n(F)$.

2 Isomorphism Theorems for Modules

Theorem 2.1. Let $\phi : M \to N$ be a module homomorphism. Then,

$$M/\ker(\phi) \cong N$$

Theorem 2.2. Let M be a module and N, K be submodules. Then,

$$N/(N \cap K) \cong (N + K)/K$$

Proof. Consider $\phi : N \to (N + K)/K$ defined by $\phi(n) = n + K$. $\ker(\phi) = N \cap K$, so we conclude the proof by the first isomorphism theorem. □

Theorem 2.3 (Correspondence Theorem)**.** Let M, N be R-modules and $f : M \to N$ be a surjective module homomorphism. Then,

$$\Phi : \{\text{submodules of M containing } \ker(f)\} \to \{\text{submodules of N}\}$$

is a bijection given by $\Phi(K) = f(K)$.

In particular, considering $M = R$ as a module over itself and $N = I$ for some ideal I, this reproduces the correspondence theorem for ideals.

3 Endomorphism Rings of Modules

Let R be a ring and M, N be R-modules. We'll examine $Hom_R(M, N)$.

This is an additive Abelian group using pointwise addition.

It's an R-module where the R-action is defined to be $r \cdot f(x) = rf(x)$.

Notice that you can't really endow it with a natural ring structure if $M \neq N$ since function composition doesn't work. If $M = N$, though, this natural ring structure works and is called the **endomorphism ring of the module** M.

Lemma 3.1. Let R be a ring and M, N be modules. If $M \cong N$ as modules, $End(M) \cong End(N)$ as rings.

In general, the converse is not true.

4 Direct Sums of Modules

Blablabla.

5 Free Modules

Every vector space has a basis. This is not free for modules.

Free modules are a generalization of vector spaces. They're modules that have a basis.

Definition 2. A module M is said to be **free** if there's a subset $S \subseteq M$ such that S is a basis for M.

Definition 3. Let R be a ring and M be a module over R. M is said to be **cyclic** if M is generated by a single element.

Definition 4. A free module of rank 1 over R is called **infinite cyclic**.

Lemma 5.1. Let R be a ring and M be an R-module generated by n elements. Then, every quotient module of M can be generated by n elements.

Proof. □

Corollary 5.1.1. Let M be a cyclic module. Then, every quotient module of M is also cyclic.

Lemma 5.2. Let M be a cyclic module generated by x. Then,

$$M \cong R/\operatorname{Ann}_R(x)$$

Proof. Consider the surjective homomorphism from R to M given by $r \mapsto rx$. □

Lemma 5.3. Let R be a domain and let M be a free-module of rank n. Then, any $n+1$ elements of M are linearly dependent, i.e. for any $y_1, ..., y_{n+1} \in M$ we have $r_1, ..., r_{n+1} \in R$ such that some r_i is non-zero and

$$r_1 y_1 + ... + r_{n+1} y_{n+1} = 0$$

Proof. If M is a free-module of rank n, $M \cong R^n$. Consider the field of fractions of R (call it F). Then, M is an n-dimensional vector space. Then, there are $a_1, ..., a_{n+1} \in F$ such that at least one a_i is non-zero and

$$a_1 y_1 + ... + a_{n+1} y_{n+1} = 0$$

Clearing out the denominators of the a_i's we can get r_i's such that the linear combination is still 0. We thus conclude the proof. □

5.1 Exercises

Lemma 5.4. Let R be a commutative ring and $I \subsetneq R$ be an ideal. If I is a free R-module, I is principal.

Proof. Let β be a finite basis for I. Assume by contradiction that β has at least two elements. Let $s_1, s_2 \in \beta$. Then, $s_2 s_1 - s_1 s_2 = 0$, which contradicts the linear independence of β. We thus conclude the proof. □

Lemma 5.5. Let R be a ring. If every module over R is free, R is either the zero ring or a field.

Proof. We prove the contrapositive. In other words, we prove that every ring with a non-zero non-unit ideal has a module over it that is not free. Let R be a non-zero ring and I be a proper ideal of R. Then, consider R/I as an R-module. R/I is not the zero ring, so it's not generated by the empty set. Moreover, any non-empty set $S \subseteq R/I$ is not R-linearly independent since multiplying by an element in the ideal maps all elements in R/I to 0. Thus, R/I is not free over R. □

Lemma 5.6. Let R be a commutative ring and consider $M = Rx + Ry$ where x, y are indeterminates. M is not a free $R[x, y]$-module.

Proof. Notice that M corresponds to the ideal in $R[x, y]$ generated by x and y. Therefore, to show that M is not free, it suffices to show that the ideal (x, y) in $R[x, y]$ is not principal by Lemma 5.4. To see this, notice that x and y are non-associate irreducibles in $R[x, y]$, so their greatest common divisor is 1. □

6 Torsion Modules

Lemma 6.1. Let R be a ring with zero divisors. Then, every non-zero R-module has non-zero torsion elements.

Proof. Let M be a non-zero R-module and r be a zero divisor in R and let $s \in R : sr = 0$. Let x be a non-zero element of M. If $rx = 0$, we're done. Otherwise, $rx \in Tor(M)$ since $s \cdot (rx) = 0$. □

Lemma 6.2. Let R be a ring and M, N be R-modules. Let $f : M \to N$ be a module homomorphism. Then, $f(Tor(M)) \subseteq Tor(N)$.

Proof. Let $x \in Tor(M)$. Then, there's some non-zero r in R such that $r \cdot x = 0$. Then, $r \cdot f(x) = f(rc\dot{x}) = f(0) = 0$, so $f(x) \in Tor(N)$. □

Definition 5. A module M is said to be a **torsion module** if $\mathrm{Tor}(M) = M$.

Definition 6. A module M is said to be **torsion-free** if $\mathrm{Tor}(M) = \{0\}$.

Lemma 6.3. Every finite Abelian group is a torsion $\mathbb{Z}$-module.

Proof. Let A be an Abelian group of order n. Considering A as a $\mathbb{Z}$-module, $\forall a \in A : na = 0$. Therefore, $\forall a \in A : a \in Tor(M)$. □

$\mathbb{Z}/n\mathbb{Z}[x]$ is an infinite Abelian group that's also a torsion module.

Lemma 6.4. Let R be an integral domain. Every finitely generated torsion module has a non-zero annihilator.

Proof. Let M be a finitely generated module. By the structure theorem, □

Here's an example that demonstrates that the finitely generated condition in the above lemma is necessary. Let M be the direct product of $\mathbb{Z}/p\mathbb{Z}$ for all primes p. M is a torsion module, but the annihilator of M is the zero ideal.

Lemma 6.5. Let M be a module over a domain R. Then, $\mathrm{Tor}(M)$ has rank 0.

Proof. Notice that $\forall x \in M : \{x\}$ is linearly dependent since there's some non-zero $r \in R$ such that $rx = 0$. *I don't understand how to finish this.* □

Lemma 6.6. Let M be a module over a domain R. If M is free, M is torsion free.

Proof. Let B be a basis for M. By contradiction, assume there's some non-zero torsion element x of M and $r \in R : rx = 0$. Since B is a basis, there's some $r_1, ..., r_n$ in R and $b_1, ..., b_n$ in B such that

$$x = \sum_{i=1}^{n} r_i b_i$$

Then,

$$rx = \sum_{i=1}^{n} r r_i b_i$$

Since R is a domain, rr_i is non-zero. We have thus reached a contradiction, since we have a non-zero R-linear combination of B that's zero, contradicting the R-linear independence of B. □

Lemma 6.7. Let M be a module over a domain R. Then, $M/\mathrm{Tor}(M)$ is torsion free.

Proof. Let $x \in M$ and assume $rx \in \mathrm{Tor}(M)$ for some $r \in R$. Then, $\exists s \in R : srx = 0 \implies (sr)x = 0 \implies x \in \mathrm{Tor}(M)$. □

Lemma 6.8. Let R be a domain. Then, every ideal of R (considered as a submodule) is torsion-free.

Proof. □

7 Simple Modules

Definition 7. A module M is said to be **simple** if M is not the zero module and the only submodules of M are 0 and M.

Lemma 7.1. *M is simple if and only if M is a cyclic module generated by any nonzero element.*

Proof. Let M be an simple module. Let x be a non-zero element in M. Then, the submodule generated by x has to be M.

Conversely, let M be a cyclic module generated by any nonzero element. Let N be a nonzero submodule of M. Since any nonzero element is a generator, $N = M$. □

Example 7.2. Let's now try to classify all simple $\mathbb{Z}$-modules. Let M be an simple $\mathbb{Z}$-module. Notice that the morphism from $\mathbb{Z}$ to M defined by $x \mapsto xm$ is surjective since the image is a non-zero submodule of M, so it has to be M. Moreover, the kernel is not zero since M can't be $\mathbb{Z}$, as $\mathbb{Z}$ is not simple. Then, $M \cong \mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$. Then, n has to be prime since otherwise we can consider Sylow subgroups and contradict irreducibility.

Lemma 7.3. *Let R be a commutative ring. An R-module M is simple if and only if M is isomorphic (as an R-module) to R/I where I is a maximal ideal of R.*

Proof. □

Lemma 7.4. *Let M_1, M_2 be simple R-modules. Then, any non-zero homomorphism $f : M_1 \to M_2$ is an isomorphism.*

Proof. This follows immediately from the fact that $Ker(f)$ and $Im(f)$ are submodules. □

Corollary 7.4.1. *Assume M is an simple R-module. Then, $End_R(M)$ is a division ring.*

7.1 Exercises

Lemma 7.5. Let F be a field, $R = M_n(F)$ and $V = F^n$. V is a simple module over R.

Proof. We'll use Lemma 7.1. Let $0 \neq v \in V$. Notice that $\forall w \in V : \exists AinR : Aw = v$ simply by mapping the basis elements accordingly (which we can do because inverses exist). We thus conclude the proof. □

8 Finitely Generated Modules

Lemma 8.1. Let M be an R-module. M is finitely generated if and only if there's some $n \in \mathbb{N}$ and $\phi : R^n \to M$ such that ϕ is surjective.

Lemma 8.2. Let M be a (left) R-module and N be a submodule of M. If N and M/N are finitely generated, M is finitely generated.

Proof. Let $\{a_1, a_2, ..., a_n\}$ be a generating set for N and $\{b_1, b_2, ..., b_n\}$ be a generating set for M/N. Let f be the canonical surjective module homomorphism from M to M/N. Since f is surjective, for every non-zero $\hat{x} \in M/N$, there exists $x \in M$ such that $f(x) = \hat{x}$. For every b_i, pick some c_i such that $f(c_i) = b_i$. We'll prove that $\{a_1, a_2, ..., a_n, c_1, c_2, ..., c_m\}$ is a generating set for M. Let $x \in M$. We have the following two cases:

Case 1: $x \in N$. Then, $x = r_1a_1 + r_2a_2 + ... + r_na_n$ for some $r_1, r_2, ..., r_n$ in R.

Case 2: $x \in M - N$. Then, $\hat{x}$ is non-zero in M/N, so there are $r_{n+1}, r_{n+2}, ..., r_{m+n}$ such that $\hat{x} = r_{n+1}b_1 + ..., +r_{m+n}b_m$. Pulling back using f, we have that $x = r_{n+1}c_1 + ... + r_{n+m}c_m$. □

9 Noetherian Modules

These are analogous to Noetherian rings.

Lemma 9.1. Let M be a Noetherian R-module and f be a surjective endomorphism of M. Then, f is an isomorphism.

Proof. Let $M_n = \ker(f^n)$. Notice that $M_{n+1} \subseteq M_n$ and $\forall n \in \mathbb{N} : M_n$ is a submodule of M. Since M is Noetherian, $\exists n \in \mathbb{N} : \forall k \geq 0 : M_n = Mn + k$. □

10 Modules over PIDs

Modules over fields (vector spaces) are always free and we can classify finite dimensional vector spaces easily. How much can we generalize this? It turns out, not much further than PIDs. In this scenario, the nice ideal structure of PIDs is reflected in the modules.

Here's some intuition for why we're considering PIDs. Let R be a domain. Recall that R is a module over itself. Then, every ideal of R is a submodule. Recall that if I is a free submodule, I is principal. Then, if every submodule of R is free, R is a PID.

Theorem 10.1. Let M be a module over a PID R. If M is free, every submodule of M is free.

Proof. □

This result doesn't hold when R is not a PID. In fact, any non-principal ideal can be used to construct a counterexample. Let R be a ring and I be a non-principal ideal in R. Then, I is not free over R since every I that is free over R is principal by Lemma 5.4.

Lemma 10.2. Every finitely generated R-module M is isomorphic to $R^n/Im(g)$ for some $g : R^m \to R^n$.

Proof. Let M be an R-module generated by n elements. Then, there's a surjective homomorphism $f : R^n \to M$. Since $\ker(f)$ is a submodule of R^n, $\ker(f) \cong R^m$ for some $m \leq n$. Let ϕ be the isomorphism. Then, let g be the map defined by applying ϕ and injecting $\ker(f)$ into R^n. Notice that $Im(g) = \ker(f)$, so $M \cong R^n/Im(g)$. □

Definition 8. A **presentation of M** is a homomorphism $g : R^m \to R^n$ and an isomorphism $M \cong R^n/Im(g)$.

Notice that using Lemma 10.2, we can ensure that g is injective. However, this isn't necessary.

Let $A \in M_{nxm}(R)$ such that $Ax = g(x)$. Such an A exists since g is a homomorphism of free modules. We can thus represent any finitely generated module M using a matrix. This presentation is not unique. We can analyze the matrix representation of finitely generated modules in order to learn more about the module itself.

10.1 Structure Theorem of Finitely Generated Modules over PIDs

Corollary 10.2.1. Let M be a finitely generated module over a PID R. M is free if and only if M is torsion free.

Proof. You have to generate the torsion element, but you can't generate it without being linearly dependent. □

Lemma 10.3. Let M be a finitely generated torsion module over a PID R. Then, M is a simple module if and only if $M = \langle x \rangle$ and $Ann(x) = (p)$ for some prime p.

Proof. Applying the structure theorem for finitely generated modules, we get that $M \cong R/I$ for some ideal I of R. Then, using Lemma 7.3 , I has to be a maximal ideal. Since prime ideals are maximal ideals in PIDs, we conclude the proof. □

11 Modules over Euclidean Domains

There's an algorithmic version of the theorems we've proven for PIDs. They're presented here.

Theorem 11.1 (Existence of Invariant Factor Form)**.**

Proof. Let M be a module and let $g : R^m \to R^n$ such that $M \cong R^n/Im(g)$. We proved that there's invertible $h : R^m \to R^m$ and $f : R^n \to R^n$ such that $M \cong R^n/Im(fgh)$. Since the matrix corresponding to fgh is in normal form, $Im(fgh) = R^s \bigoplus d_1R \bigoplus d_2R ... \bigoplus d_kR$. We therefore conclude the proof. □

Corollary 11.1.1. Let R be a PID. Every torsion free finitely generated R-module is free.

The elementary divisors of a finitely generated module M are just the invariant factors of the primary components of $\text{Tor}(M)$.

Theorem 11.2 (Existence of Elementary Divisor Form)**.**

Proof. □

Lemma 11.3. Let R be a PID and M be an R-module. M is cyclic if and only if $M \cong R/(a)$ for some $a \in R$.

Proof. Assume M is cyclic. Then, there's some $x \in M$ such that x generates M. Consider the module homomorphism $\phi_x : R \to M$ given by $\phi(r) = rx$. Since x generates M, ϕ is surjective. Since R is a PID, $ker(\phi_x) = (a)$ for some $a \in R$.

Then, by the first isomorphism theorem for modules, $M \cong R/(a)$.

For the converse, notice that a is a generator for the module $R/(a)$. □

Proof. One can also consider Lemma 5.2. The fact that R is a PID immediately gives us the desired result. □

Corollary 11.3.1. Let R be a PID and M be a cyclic R-module. Then, every submodule of M is also cyclic.

Proof. Let M be a cyclic module over a PID R. Then, $M \cong R/aR$ for some $a \in R$. Let N be a submodule of M. Then, N is an ideal of R/aR. Recall that every ideal in the ring R/aR corresponds to an ideal in the ring R that contains aR. Since R is a PID, every ideal in R/aR is also principal. Then, there's a single element that generates N. □

Lemma 11.4. Let M be a finitely generated torsion module over a PID R and let $n = |IF(M)|$. M can be generated by n elements and can't be generated by less than n elements.

Proof. Let M be a finitely generated torsion module over a PID R and let $n = |IF(M)|$. Then,

$$M \cong R/d_1R \oplus ...R/d_nR$$

for some $d_i \in R$ such that $d_i \mid d_{i+1}$. Notice that the set $\{e_1, ..., e_n\}$ generates the right hand side.

We'll now prove that M can't be generated by $n - 1$ elements. Assume by contradiction that M can be generated using $m < n$ elements. Then, $M \cong R^m/N$ where N is a submodule of R^m. However, this immediately implies that M has at most m invariant factors, which is a contradiction. □

12 Finitely Generated Abelian Groups

Recall that there's a one-to-one correspondence between Abelian groups and $\mathbb{Z}$-modules.

Also recall that we can identify every ideal of $\mathbb{Z}$ with a unique positive integer d.

12.1 Module of Fractions, Limited Construction

Let R be a domain and F be its field of fractions.

We'll put an equivalence relation on $M \times R$ by letting $(m, a) \sim (m', a')$ if and only if $am' = a'm$.

We'll denote by FM the set of equivalence classes.

Lemma 12.1. *FM is a vector space over F.*

Proof. □

Notice that we've defined ϕ that goes from R-modules to F-modules. ϕ is called a functor and also acts on module homomorphisms. More formally, if $g : M \to N$, $Fg : FM \to FN$ where $\phi(g) = Fg$.

12.2 Determination of rank by using reductions to linear algebra

Let R be a PID and M be a finitely generated R-module. Recall that $M \cong Tor(M) \oplus R^s$ where $s = rank(M)$.

12.3 Exercises

If M is a finite Abelian group, M is naturally a $\mathbb{Z}$-module. Can this action be extended to make M into a $\mathbb{Q}$-module?

13 Modules over F[x]

Sherstov: It is hard to factor integers. However, it is really easy to factor polynomials over fields into irreducibles, because polynomials have a rich algebraic structure.

Let F be a field and $R = F[x]$. Recall that R is a Euclidean Domain. In particular, R is a PID. Recall that we can identify every ideal of R with a unique monic polynomial in $F[x]$.

Also recall that F is a subring of R corresponding to constant polynomials. This is useful because every R-module M can be made into a vector space over F by considering the module structure given by the pullback. Equivalently, this can be thought of as restricting the scalars.

Let $0 \neq g \in R$ be a non-constant polynomial. Our goal is now to understand R/gR better. R/gR is a module over R, so we can use the trick in mentioned in the previous paragraph and find $\dim_F(R/gR)$.

We'll think of F as being contained in R/gR. More formally, here's how we injectively map F into R/gR as a ring. Consider the canonical ring homomorphism from $R \to R/gR$ defined by $g \mapsto \bar{g}$. Then, consider the map $F \hookrightarrow R \to R/gR$. This is a composition of ring homomorphisms, so it's a ring homomorphism. Since the domain is a field, it has to be injective. We'll just denoted $\hat{a} \in R/gR$ by a and assume F is contained in R/gR for notational ease.

Proposition 13.1. $\dim_F(R/gR) = n = deg(g)$

Proof. Let $g = a_0 + a_1 x + ... + x^n$. Notice that g is monic since we're identifying R/gR with its unique monic polynomial.

We'll now show that $\{\bar{1}, \bar{x}, ..., \bar{x}^{n-1}\}$ generate R.

Let $h \in R$. Then, $h = g \cdot q + r$ for some unique $q, r \in R$ such that $r = 0$ or $deg(r) < n$. Notice that $\bar{h} = barr$. If $r = 0$, $\bar{h} = 0$. Otherwise, $\bar{h}$ is an F-linear combination of $\{\bar{1}, \bar{x}, ..., \bar{x}^{n-1}\}$ since r is a linear combination of $\{1, x, ..., x^{n-1}\}$. We have thus proven that $\{\bar{1}, \bar{x}, ..., \bar{x}^{n-1}\}$ is a generating set. We'll now prove that it's independent.

Assume that $\sum_{i=0}^{n-1} a_i \bar{x}^i = 0$ in R/gR. Then, $f = \sum_{i=0}^{n-1} a_i x^i \in gR$. Then, f is a polynomial of degree less than n divisible by a polynomial of degree n, so $f = 0$. We thus conclude the proof. □

Now, let R be a polynomial ring over a field M be a finitely generated R-module. Then, by the invariant form for finitely generated modules, we have that

$$M \cong R/f_1R \oplus R/f_2R \oplus ... \oplus R/f_rR \oplus R^s$$

Then, by the proposition,

$$\text{M is torsion} \iff s = 0 \iff \dim_F(M) \text{ is finite}$$

In mathematics, there are sometimes different languages to describe the same phenomenon. In this case, we'll have 3 different languages to describe the same phenomenon.

14 Indecomposable Modules

Definition 9. A module is called **indecomposable** if it can't be expressed as a direct sum of its submodules.

15 Canonical Forms using IF and ED Form

Canonical forms are useful since they give us a method to test if two linear operators are identical. In other words, it let's us check whether two matrices are similar.

This is another case where we use the structure of the space being acted upon is used to obtain information on the algebraic objects which are acting.

15.1 The Characteristic and Minimal Polynomial

Definition 10. The polynomial $\det(xI - T)$ is called the **characteristic polynomial of** T and is denoted $c_T(x)$.

Definition 11. The unique monic polynomial which generates $Ann(V)$ in $F[x]$ is called the **minimal polynomial of** T and is denoted $m_T(x)$.

Notice that the definition also implies that $m_T(x)$ divides any polynomial f with $f(T) = 0$.

Proposition 15.1. The minimal polynomial $m_T(x)$ is the largest invariant factor of V. All the invariant factors divide $m_T(x)$.

Proof. $F[x]$ is a PID and the last invariant factor generates the annihilator since all the other IFs divide it and it annihilates the last cyclic module. □

Theorem 15.2 (Cayley-Hamilton)**.** The minimal polynomial for T divides the characteristic polynomial of T.

Proof. Since the characteristic polynomial is the product of all invariant factors, this is immediate. □

Lemma 15.3. Let $A \in M_n(F)$. The minimal polynomial of A has the same irreducible divisors as the characteristic polynomial of A.

Proof. Since the minimal polynomial divides the characteristic polynomial, it suffices to show that every irreducible divisor of the characteristic polynomial divides the minimal polynomial.

Let f be an irreducible polynomial that divides the characteristic polynomial. Then, f is also prime since $F[x]$ is a Euclidean domain. Then, f divides one of the invariant factors by a simple inductive argument on the number of invariant factors. Since the minimal polynomial is the greatest invariant factor, f also divides the minimal polynomial. □

Corollary 15.3.1. The characteristic polynomial divides a power of the minimal polynomial.

15.2 Rational Canonical Form

The rational canonical form doesn't concern itself with finding a nice representation of the matrix. It just finds a **canonical** representation, however ugly it is.

Let V be a finite dimensional vector space over F with dimension n.

Any nonzero free $F[x]$-module (being isomorphic to a direct sum of copies of $F[x]$) is an infinite dimensional vector space over F. Since V is finite dimensional, V is a torsion $F[x]$-module.

Lemma 15.4. Let $a(x) \in F[x]$. The characteristic polynomial of the companion matrix of $a(x)$ is $a(x)$.

Theorem 15.5 (Rational Canonical Form)**.** Let $A \in M_n(F)$. Then, A is conjugate (similar) to

for unique monic polynomials $f_1 \mid f_2 \mid ... \mid f_r$.

Corollary 15.5.1. A, B in $M_n(F)$ are similar if and only if $RFC(A) = RFC(B)$.

We found representatives of conjugacy classes in order to check similarity.

Theorem 15.6 (Rational Canonical Form for Linear Operators)**.** Let A be a linear operator in a finite dimenasional vector space over F. Then, there's a basis such that [A] is in rational canonical form.

The rational canonical form of a linear operator stays the same in the K if F is a subfield of K.

15.3 Jordan Canonical Form

We'll assume that F contains all eigenvalues of T. In other words, we assume that the characteristic polynomial of T splits over F.

Proposition 15.7. The following conditions are equivalent:

1.

Corollary 15.7.1. T is diagonalizable if and only if $m_T(x)$ doesn't have repeated roots.

Proof. □

Jordan forms are not useful numerically.

15.4 Exercises

Lemma 15.8. Let $A \in M_n(R)$ such that $A = A^2$. Then, A is diagonalizable with 0s and 1s on the diagonal.

Proof. Notice that the minimal polynomial of A divides $x^2 - x = x(x-1)$. Then, all the invariant factors are $x(x-1), x, (x-1)$. Then, the characteristic polynomial splits and 0 and 1 are the only roots of the characteristic polynomial. □

16 Exact Sequences: Projective, Injective and Flat Modules

Given two modules A, C, how many possible ways are there for us to extend C to B such that $B/A \cong C$? Is this always possible?

Let A, C be R-modules. Then, letting $B := C \oplus A$, $B/A \cong C$. Therefore, $1 \to A \to C \oplus A \to C \to 1$ is a short exact sequence.

Notice that if A, C are groups, this means that B is the semidirect product of A and C. This is another way of seeing that semidirect products are direct sums for Abelian groups.

Definition 12. Let $0 \to A \xrightarrow{\psi} B \xrightarrow{\phi} C \to 0$ be a short exact sequence of R-modules. The sequence is said to be **split** if there's a map $\alpha : C \to B$ such that $\phi \circ \alpha$ is the identity map on C.

16.1 Exercises

Lemma 16.1. Let R be a ring. Prove that every R-module is injective if and only if every R-module is projective.

Proof. □