MATH 593 - Linear Algebra on a Ring

ARessegetes Stery

October 30, 2023

Contents

1 Linear Transformations on a Ring

Recall the two versions of Structural Theorem of finitely generated modules over PID:

Theorem 1.1 (Sturcture, v1). *Let M be a finitely generated R-module, with R a PID. Then there exists $a_1, \dots, a_m \in R \setminus \{0\}$ s.t. $a_1 \mid a_2 \mid \cdots \mid a_m$.*

Theorem 1.2 (Structure, v2). *Let M be a finitely generated R-module, with R a PID. Then there exists primes p_is and $n_i \in \mathbb{N}$ s.t. $M \simeq R^r \oplus R/(p_1^{n_1}) \oplus \cdots \oplus R/(p_r^{n_r})$.*

Example 1.1. Let $R = \mathbb{Z}$, with M an R-module. Since defining scalar multiplication on modules is equivalent to defining maps from R to endomorphisms on M, it is sufficient for M to be an abelian group. By Structural Theorem, there exists p_is and m_is s.t. $M \simeq \mathbb{Z}^r \oplus \mathbb{Z}/(p_1^{m_1}) \oplus \cdots \oplus \mathbb{Z}/(p_k^{m_k})$. M is finite (as a group) if and only if $r = 0$.

The direct sum allows describing it with a basis, which gives a generalization of linear algebra defined on ring (module) structure.

Parenthesis 1.1. Linear maps between elements in free modules can be represented as invertible matrices.

Proof. The reasoning is similar to that under the context of vector spaces. Fix R to be a commutative ring, with M a finitely generated R-module. Let $n = \operatorname{rank}(M)$. Then $M \simeq R^n$. Choose $B = (e_1, \dots, e_n)$ to be a basis of M.

For all $u \in M$, there exists a unique decomposition of u into the basis, i.e. there exists $a_1, \dots, a_n$ s.t. $u = \sum_{k=1}^n a_k e_k$. Denote $M_B(u) = (a_1, \dots, a_k)^T$.

Now consider change of basis. Suppose that $B' = (e'_1, \dots, e'_n)$ is another basis of M. There exists b_{ik}s s.t. $e_i = \sum_{k=1}^n b_{ik} e'_k$; and there exists c_{ik}s s.t. $e'_i = \sum_{k=1}^n b_{ik} e_k$. Apply the substitution twice gives

$$e_i = \sum_{j=1}^n b_{ij} e'_j = \sum_{j=1}^n b_{ij} \left(\sum_{k=1}^n c_{jk} e_k \right) = \sum_{k=1}^n \sum_{j=1}^n (b_{ij} c_{jk}) e_k \implies \left(\sum_{k=1}^n \sum_{j=1}^n (b_{ij} c_{jk}) e_k \right) - e_i = 0$$

Since e_is give a basis, this implies that $\sum_{j=1}^n (b_{ij} c_{jk}) = \delta_{ik}$. Let $V = (b_{ij}) \in M_n(R)$ to be the transition matrix from B to B', abd $U = (c_{ij}) \in M_n(R)$ the transition matrix from B' to B. Conducting this concurrently gives $UV = \operatorname{Id}_B$. Similarly $VU = \operatorname{Id}_{B'}$. □

Proposition 1.1. *The converse of the above also holds, i.e. If (c_{kl}) is invertible in $M_n(R)$, then for $e'_k = \sum_{l=1}^n c_{kl} e_l$, e'_ks also give a basis.*

Proof. It suffices to verify that e'_ks are R-linearly independent, and they span the whole module:

- If there exists λ_is that are not all zero, that $\sum_{i=1}^n \lambda_i e'_i = 0$, then $\sum_{i=1}^n \lambda_i \sum_{k=1}^n c_{ik} e_k = 0$ which implies that e_k are not R-linearly independent, which is a contradiction.
- Since (c_{kl}) is invertible, there exists some (b_{kl}) s.t. $e_k = \sum_{l=1}^n b_{kl} e_l$. Then, for all $u \in M$ with decomposition into the original basis $u = \sum_{i=1}^n u_i e_i$, there exists a decomposition into e'_ks: $u = \sum_{i=1}^n u_i \sum_{j=1}^n b_{ij} e_j$.

□

Remark 1.1. The transition matrix is compatible with representation of an element in the basis. Let $M \ni u = \sum_{i=1}^n u_i e_i$, with $U = (b_{ij})$ the transition matrix from $B = (e_i)$ to $B' = (e'_i)$. Then

$$u = \sum_{i=1}^n u_i e_i = \sum_{i=1}^n \left(u_i \sum_{j=1}^n b_{ij} e'_i \right) \implies M_{B'}(u) = U \cdot M_B(u)$$

Remark 1.2. Using such formalization the operations are represented in the identical way as that in vector spaces:

1. *Applying a linear map.* If $T : F \to G$ is not an endomorphism and T is specified via specifying the image of the basis $T(e_j) = \sum_{i=1}^n a_{ij} f_j$, where F and G are finitely generated free R-modules; and $B_F = (e_i), B_G = (f_i)$ give a basis in the corresponding module. Then the matrix representation of T under such bases is $M_{B_F B_G}(T) = (a_{ij})$. It acts in the same way as matrices acting on vectors, as for $M_{B_F}(u) = (b_1, \ldots, b_u)^T$

$$\begin{aligned} T(u) = T\left(\sum_{j=1}^n b_j e_j\right) &= \sum_{j=1}^n b_j T(e_j) = \sum_{j=1}^n b_j \left(\sum_{i=1}^n a_{ij} f_j\right) = \sum_{i=1}^n \sum_{j=1}^n (a_{ij} b_j) f_j \\ \implies M_{B_G}(T(u)) &= M_{B_F B_G}(T) \cdot M_{B_F}(u) \end{aligned}$$

2. *Composition of linear maps.* Consider $T : F \to G$ and $S : G \to H$ where $B_F = (e_i), B_G = (f_i)$ and $B_H = (g_i)$. To specify the linear maps, it suffices to specify where the elements of the basis is mapped to. Suppose that $T(e_i) = \sum_{j=1}^n a_{ji} f_j; S(f_i) = \sum_{j=1}^n b_{ji} h_j$. For $F \ni u = \sum_{i=1}^n u_i e_i$, considering $g \circ f$ gives

$$\begin{aligned} (S \circ T)(u) = (S \circ T)\left(\sum_{i=1}^n u_i e_i\right) &= S\left(\sum_{i=1}^n u_i \sum_{j=1}^n a_{ji} f_j\right) = \sum_{i=1}^n u_i \sum_{j=1}^n a_{ji} S(f_j) \\ &= \sum_{i=1}^n u_i \sum_{j=1}^n a_{ji} \sum_{k=1}^n b_{kj} h_j = \sum_{i=1}^n u_i \sum_{j=1}^n \left(\sum_{k=1}^n (a_{ji} b_{kj}) h_j\right) \\ \implies M_{B_F B_H}(S \circ T) &= B_{B_G B_H}(S) \cdot M_{B_F B_G}(T) \end{aligned}$$

   where the elements of $M_{B_F B_H}(S \circ T)$ is specified by $\sum_{j=1}^n \sum_{k=1}^n (a_{ji} b_{kj})$.

3. *Change of basis.* Now consider change of basis under the context of a linear transformation. Let $T : F \to G$ be an R-linear map, with $M_{B_F B_G}(T)$ the matrix representation of T under B_F and B_G. Now consider change of basis maps $U : B_F \to B'_F$ and $\tilde{U} : B_G \to B'_G$. We are interested in the corresponding map $\tilde{T}$ of T after applying the change of basis:

$$\begin{tikzcd} B'_F \arrow[r, "\tilde{T}"] & B'_G \\ B_F \arrow[u, "U"] \arrow[r, "T"] & B_G \arrow[u, "\tilde{U}"] \end{tikzcd}$$

   As proven above it is valid to express linear transformation and change of basis using matrices, and matrices corresponding to change of basis are invertible, we have for $u \in F$,

$$M_{B'_G}(T(u)) = M_{B_G B'_G}(\tilde{U}) M_{B_F B_G}(T) M_{B'_F B_F}(U) = M_{B_G B'_G}(\tilde{U}) M_{B_F B_G}(T) (M_{B_F B'_F}(U))^{-1}$$

4. *Change of basis on endomorphisms.* Then the equality above becomes

$$M_{B'_G}(T(u)) = M_{B_G B'_G}(U) M_{B_G}(T) M_{B'_G B_G}(U) = (M_{B'_G B_G}(U))^{-1} M_{B_G}(T) M_{B'_G B_G}(U)$$

which is exactly the conjugate of a matrix.

Definition 1.1. *Two matrices A and B in $M_n(R)$ are* ***similar*** *if there exists some invertible $U \in M_n(R)$ s.t. $A = U^{-1}BU$. Two R-linear maps T and $T' : F \to F'$ are* ***similar*** *if there exists some isomorphism φ s.t. $T' = \varphi^{-1}T\varphi$.*

Remark 1.3. Similarity is an equivalence relation, with $(A = U^{-1}BU) \wedge (B = V^{-1}CV) \implies A = (VU)^{-1}C(VU)$ for transitivity.

R-linear maps are similar to each other if and only if the corresponding matrix is similar, as on free modules linear maps can be represented by matrices.

Proposition 1.2. *There exists a canonical bijection between:*

$$\{R\text{-linear endomorphisms } F \to F\}/\text{similarity} \simeq M_n(R)/\text{similarity}$$

Proof. Choose B_F to be a basis of F. First verify that the map is bijective: as is formalized above since F is free, with a fixed basis linear transformations could be represented via matrices to indicate how the basis is transformed. Therefore, for any linear transformation there exists one matrix to represent it under B_F and vice versa. Further the choice of M_n is unique as matrices under different basis are conjugate w.r.t. the change of basis matrix. □

Remark 1.4. The bijection will still be valid without the quotient. However this will cease to be canonical as the map differs by the choice of basis on which the matrix conducts the representation.

2 Rational and Smith Normal Form

3 Minimal and Characteristic Polynomials

4 Jordan Normal Form