# Structure Theorem of Modules over PID applied to RCF

August 2023
Tim Bates

Linear algebra is the study of vector spaces and homomorphisms (linear operators) between them. Operators between finite dimensional vector spaces may be represented by matrices with respect to some basis. A canonical form is simply a representation of the linear operator in a particularly natural basis. We will be using the structure theorem of finitely generated modules over a PID in order to produce two such canonical forms.

---

**Theorem 1.** *Let $R$ be a PID and let $M$ be a finitely generated $R$-module. There exists a unique decreasing sequence of proper ideals, $(d_1) \supseteq (d_2) \supseteq \cdots \supseteq (d_n)$ such that $M$ is isomorphic to the direct sum of cyclic modules:*

$$M \cong \bigoplus_{i=1}^{n} R/(d_i)$$

*Moreover, two such modules are isomorphic if and only if they admit the same decomposition into cyclic submodules.*

Recall that abelian groups can be identified as $\mathbb{Z}$-modules. We can see then that the structure theorem for finitely generated Abelian groups is a special case of theorem 1.

Another equivalent formulation for this theorem is the primary decomposition.

**Theorem 2.** *Let $R$ be a PID and let $M$ be a finitely generated $R$-module. There exists a sequence unique up to order of primary ideals $(p_1^{r_1}), \ldots, (p_m^{r_m})$ such that $M$ is isomorphic to the direct sum of cyclic modules;*

$$M \cong \bigoplus_{i=1}^{m} R/(p_i^{r_i})$$

*Two $R$-modules are equivalent if and only if they admit the same decomposition up to order of summation.*

---

A vector space $V$ is simply a module over a field $F$. A linear map $T : V \to V$ allows us to upgrade $V$ from an $F$-module to an $F[x]$-module in the following way. For $v \in V$, $x \cdot v = T(v)$. It is routine to verify that this satisfies the module axioms. Now we then have a pair $(V, T)$ which corresponds to a $F[x]$-module.

If $(V, T)$ is a $F[x]$-module, then any submodule $W$ must be a subspace which is invariant under the action of $T$. In otherwords, a $T$-invariant subspace. Theorem 1 and 2 now yields the following result.

**Theorem 3.** *If $T$ is a linear operator on a finite dimensional vector space $V$ over a field $F$, then*

$$V \cong W_1 \oplus \ldots W_m$$

*where each $W_i$ is a cyclic $T$-invariant subspace of $V$ such that $(f_i(t))$ annihilates $W_i$ where either $(f_1) \supseteq (f_2) \supseteq \cdots \supseteq (f_m)$ or $(f_i) = (g_i^{n_i})$ where $g_i$ is irreducible in $F[x]$.*

*Proof.* Again we view $V$ as an $F[x]$-module. Since $V$ is finite dimensional, there is a basis $\mathcal{B} = \{e_i\}_{i=1}^{n}$ such that every $v \in V$ is a linear combination of elements in $\mathcal{B}$. This basis also extends as a basis of $V$ as an $F[x]$ modules since $xe_i = T(e_i) = \sum_j \alpha_j e_j$. For any vector, there exists some polynomial $f(x) \in F[x]$ such that $f(x)v = 0$ which follows from the fact that $\{v, Tv, \ldots, T^n v\}$ is a lienarly dependent set, thus

$$a_0 v + a_1 Tv + \cdots + a_n T^n v = 0$$

admits a nontrivial solution. Thus $V$ is an $F[x]$-module with no free component, thus by the structure theorem of finitely generated modules over a PID, the result follows. □

Moreover in each cyclic subspace $W$, there is a vector $w$ such that $\{w, Tw, \dots, T^{k-1}w\}$ is a basis for $W$. If $T^k w = \sum_{i=0}^{k-1} a_i T^i v$, then $O_v$ is generated by $x^s - \sum_{i=0}^{k-1} a_i x^i$. Now we can present the transformation $T$ as a matrix with respect to this basis. When $i < k-1$, we see that $T(T^i v) = T^{i+1} v$, so there should be a one in the $(i+1, i)$th entry. Finally, $TT^{k-1} = T^k = \sum_{i=1}^{k-1} a_i T^i v$, thus the entries are the $a_i$ in the last column. This is called the companion matrix of the monic generator of the order of the cyclic subspace.

If $f(x) = a_0 + a_1 x + \dots a_{n-1} x^{n-1} + x^n$, then

$$C(f) = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & \dots & 0 & \vdots \\ & \dots & \dots & \dots & 0 & \vdots \\ 0 & 0 & \dots & \dots & 1 & -a_{m-1} \end{pmatrix}$$

is the companion matrix. Moreover, if $W = F[t]/(f)$, the companion matrix represents $T$.

**Theorem 4.** *Every $n \times n$ matrix $A$ over a field $F$ is similar to a direct sum of companion matrices $C(f_1), \dots, C(f_m)$ such that $f_1 | \dots | f_m$ or such that each $f_i = g_i^m$ for some irreducible polynomial $g_i$.*

*Proof.* With respect to the standard basis on $F^n$, the matrix $A$ represents a linear operator $T$. We then know that the pair $V$ and $T$ defines a $F[x]$-module which by Theorem 3 decomposes into a direct sum of cyclic $T$-invariant subspaces such that polynomials $f_1 | f_2 \dots | f_m$ or such that $f_i = g_i^n$ for some irreducibles $g_i$. Now in each cyclic $T$ invariant subspace $W_i$ we can choose a vector $w_i$ such that $\{w_i, Tw_i, \dots, T^s w_i\}$ forms a basis for that subspace. Since we can do this for each subspace, we can choose a basis for $V$:

$$\{w_1, Tw_1, \dots, w_2, Tw_2, \dots, T^{s_m} w_m\}$$

where the matrix presenting $T$ with respect to this matrix is the direct sum of the companion matrices for $f_i$. □

This matrix $B$ which we obtained in this manor with $f_1 | \dots | f_m$ is called the rational canonical for $A$ and the $f_i$ are called the ivariant factors. Notice by the structure theorem that the RCF is unique, thus we indeed refer to THE rational canonical form of a linear operator.