Rational Canonical Form

The goal is to identify classes of similar matrices (matrices that differ by a change of basis).

A vector space $V$ over field $F$ with linear map $T : V \rightarrow V$ induces an $F[x]$-module on $V$. Multiplication in this module is defined by setting $x \cdot v = T(v)$, so that if $f(x) = a_n x^n + \ldots + a_1 x + a_0$, then $f(x) \cdot v = a_n T^n(v) + \ldots + a_1 T(v) + a_0 v$.

Since $F[x]$ is a principal ideal domain, the structure theorem applies to decompose $V$ as

$$V \cong (F[x]/(a_1)) \oplus \ldots \oplus (F[x]/(a_k))$$

Where $a_i | a_{i+1}$ for each $i$. If $r > 0$, then $V$ must be an infinite dimensional vector space, because $F[x]$ is an infinite dimensional vector space over $F$. So we can set $r = 0$ as long as we are dealing with finite dimensional vector spaces.

Recall that the annihilator of a module $V$ over $R$ is the set $r \in R$ such that $r \cdot v = 0$ for every $v \in V$. The annihilator $\text{Ann}(V)$ is an ideal of $R$. In the case where $R = F[x]$, suppose $\text{Ann}(V) = (m(x))$. Then $m(x)$ is the clearly the polynomial of smallest degree such that $m(T) = 0$. If we insist that $m$ is monic, then it is unique, and we call it the minimal polynomial.

**Theorem 1.** Given the decomposition

$$V \cong (F[x]/(a_1)) \oplus \ldots \oplus (F[x]/(a_k))$$

$a_k = m(x)$, the minimal polynomial. In other words, the minimal polynomial is the largest invariant factor.

**Proof.** Given any quotient ring $R/I$, we can make it into an $R$-module in the obvious way. Then $\text{Ann}(R/I) = I$.

By the divisibility condition, we have $(a_k) \subset \ldots \subset (a_1)$. So the annihilator of $V$ is the annihilator of $R/(a_k)$, which is $a_k$.

To translate this into the language of matrices, we have to choose a basis for $V$ such that the matrix of $T$ can be easily expressed. First, we will turn our attention to just one of the factors, $F[x]/(a)$. If $a$ is a polynomial of degree $k$, say $a(x) = x^k + \ldots + a_1 x + a_0$, then $R/(a)$ has basis of size $k$: $1, x(\text{ mod } a(x)), \ldots, x^{k-1}(\text{ mod } a(x))$. We are going to find a matrix for the module homomorphism sending $a \in V$, to $x \cdot a$. By the way that multiplication is defined, a matrix for this is a matrix for $T$ (since $x \cdot v = T(v)$). The map multiplication by $x$ on the basis is $1 \mapsto x$, $x \mapsto x^2, \ldots, x^{k-1} \mapsto -a_{k-1} x^{k-1} - \ldots - a_0$ all modulo $a(x)$. So the matrix can be easily expressed, and a matrix in this form is called a companion matrix.

$$
\begin{pmatrix}
0 & 0 & \ldots & -a_0 \\
1 & 0 & \ldots & -a_1 \\
0 & 1 & \ldots & -a_2 \\
\vdots & \vdots & \ddots & \vdots \\
0 & \ldots & \ldots & -a_{n-1}
\end{pmatrix}
$$
Now that we have a nice basis for each piece of the decomposition, we are just going to make a basis for all of $V$ by slapping together all of the bases.

**Lemma 2.** If $V = V_1 \oplus V_2$ and $e_1, \ldots, e_n$ is a basis for $V_1$ and $f_1, \ldots, f_m$ is a basis for $V_2$, then a basis for $V$ is $(e_1,0,\ldots,0), \ldots, (e_n,0,\ldots,0), (0,\ldots,0,f_1), \ldots, (0,\ldots,0,f_m)$.

**Proof.** For shorthand, just let $e_k$ denote the new element that is $e_k$ followed by $m$ zeroes. The list clearly spans. To check linear independence, suppose

$$a_1 e_1 + \ldots + a_n e_n + a_{n+1} f_1 + \ldots + a_{n+m} f_m = 0$$

Then $a_1 e_1 + \ldots + a_n e_n = 0$ and $a_{n+1} f_1 + \ldots + a_n + m f_m = 0$ since zero can be written in only way. Thus all the coefficients are zero because the $e_i$ and $f_i$ are a basis. \qed

With this, we can define **rational canonical form.** Given a matrix $A$, take the decomposition of its corresponding module and obtain invariant factors $a_1, \ldots, a_k$. Then the rational canonical form of $A$ is

$$
\begin{pmatrix}
C(a_1) \\
C(a_2) \\
\vdots \\
C(a_k)
\end{pmatrix}
$$

Where $C(a_i)$ denotes the companion matrix for $a_i$ and everything off the block diagonal is 0. This matrix describes the linear transformation in the special basis that we created above.

**Theorem 3.** Let $T$ and $S$ be linear transformations with the same rational canonical form. Then $T$ and $S$ are similar linear transformations and their matrices are similar too.

**Proof.** If $T$ and $S$ have the same matrix with respect to different bases, then they are similar because there is a change of basis $U$ such that $T = USU^{-1}$. \qed

A restatement of an important theorem in linear algebra will make finding rational canonical forms easier.

**Theorem 4 (Cayley-Hamilton).** The minimal polynomial for a matrix $A$ divides the characteristic polynomial of $A$.

**Proof.** Note that the usual form of Cayley-Hamilton is that if $c(x)$ is the characteristic polynomial of $A$, then $c(A) = 0$. Since the minimal polynomial, $m(x)$, is the smallest degree polynomial such that $m(A) = 0$, we immediately have that $m(x)$ divides $c(x)$. \qed