Elementary Divisors, Invariant Factors, and Canonical Forms

Let R be a PID and let M be a finitely generated R-module. Then we have the following two decompositions of M into cyclic modules:

$$M \simeq R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_n), \tag{IF}$$

where the $a_i \in R$ are nonzero, nonunits and $a_1 \mid a_2 \mid \cdots \mid a_n$, and

$$M \simeq R^r \oplus R/(p_1^{e_1}) \oplus \cdots R/(p_r^{e_r}), \tag{ED}$$

where the $p_i \in R$ are not necessarily distinct primes and $e_i > 0$.

We call $a_1, \ldots, a_n$ the list of invariant factors, and $p_1^{e_1}, \ldots, p_r^{e_r}$ the elementary divisors, and these lists uniquely determine M. Actually, in class we only showed that the elementary divisors are unique, but here we will show how to go between the elementary divisors and the invariant factors.

To go from a list of invariant factors to a list of elementary divisors is simply the Chinese Remainder Theorem. We know that each cyclic module $R/(a_i)$ decomposes into a direct sum of cyclic modules whose annihilators are prime powers, and we combine the lists for each cyclic module to get the list of elementary divisors.

To go from the elementary divisors to the invariant factors is slightly more difficult to explain, but is not actually much more complicated. Suppose you have a list $p_1^{e_1}, \ldots, p_r^{e_r}$ of elementary divisors. Comparing annihilators, we see that a_n is the product of the largest of the prime powers among these elementary divisors. In other words, if $p_i^{e_i}$ and $p_j^{e_j}$ are two elementary divisors and $p_i = p_j$, then we include the one which has the larger (if they're equal pick either one) exponent in our factorization of a_n. This gives us our largest invariant factor, a_n, but we still need the rest. To get a_{n-1}, we throw out the prime powers appearing in a_n and repeat the algorithm.

To see how this works in practice, let's do an example over $\mathbb{Z}$ and an example over $F[t]$.

Example 1. Let M be a finitely generated abelian group with elementary divisors $2^2, 2^5, 3, 3^3, 5^2, 5^2$. What are the invariant factors?

Applying the algorithm above we get that the largest invariant factor is $2^5 \cdot 3^3 \cdot 5^2$. Throwing these out, the remaining invariant factors are $2^2, 3, 5^2$, and their product must be the remaining invariant factor. So the two invariant factors are $a_1 = 2^2 \cdot 3 \cdot 5^2$ and $a_2 = 2^5 \cdot 3^3 \cdot 5^2$. There is no other way that we could have gotten the condition $a_1 \mid a_2$!

Example 2. Let M be a finitely generated $\mathbb{R}[t]$ module. Recall that the prime elements of $\mathbb{R}[t]$ are irreducible polynomials. Suppose the elementary divisors of M are $t+1, t+1, (t+1)^2, (t^2+1)$. Then the list of invariant factors is

$$t+1,\ t+1,\ (t+1)^2(t^2+1).$$

For this last example, let's put the corresponding linear operator we get on M (as a vector space) into rational canonical form!

Recall that the companion matrix for each invariant factor $f(t)$ has dimension $n \times n$, where $n = \deg f$, so for a linear polynomial it's simply a 1×1 matrix. The matrix consists of 1's below the diagonal, the negatives of the coefficients $a_0, \ldots, a_{n-1}$ of f in the last column, and zeros everywhere else. For $f(t) = t+1$ we get the matrix $\begin{pmatrix} -1 \end{pmatrix}$, and for the minimal polynomial

$(t+1)^2(t^2+1) = t^4 + 2t^3 + 2t^2 + 2t + 1$ we get the 4×4 matrix

$$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & -2 \end{pmatrix}$$

Putting the three blocks together we get the 6×6 matrix

$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & -2 \\ 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix}$$

To go back to the example in class, suppose that you are given a matrix and want to put it into rational canonical form by determining its invariant factors. For 2×2 matrices and 3×3 matrices, it is sufficient to know the minimal polynomial and the characteristic polynomial, but for larger matrices more information is necessary in general. You will only be responsible for cases where there is no ambiguity.

Example 3. Find the rational canonical form (over $\mathbb{R}$) for the matrix

$$A = \begin{pmatrix} 2 & -2 & 14 \\ 0 & 3 & -7 \\ 0 & 0 & 2 \end{pmatrix}$$

given that its characteristic polynomial is $(t-2)^2(t-3)$ and its minimal polynomial is $(t-2)(t-3)$.

The minimal polynomial is exactly the largest invariant factor, so the only remaining term we have to work with is $(t-2)$, which must be the final invariant factor.

So there are two invariant factors, namely $(t-2)$ and $(t-2)(t-3) = t^2 - 5t + 6$. This gives a 1×1 block and a 2×2 block, which yields the matrix

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -6 \\ 0 & 1 & 5 \end{pmatrix}$$

For the exam, you do not need to know Jordan canonical form, but I want to clarify my comments in class so there is no confusion.

If your field contains the eigenvalues of the linear operator T, which are the roots of the characteristic polynomial, then you can put the corresponding matrix into Jordan canonical form. In this case, all of the prime elements of $F[t]$ which appear in the elementary factor decomposition will be linear polynomials. So rather than working with the invariant factor decomposition, we will work with the elementary divisor decomposition. In this case, each cyclic module looks like $F[t]/(t-\alpha)^n$, and the corresponding block is an $n \times n$ matrix of the form

$$\begin{pmatrix} \alpha & 1 & 0 & \cdots & 0 \\ 0 & \alpha & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \alpha & 1 \\ 0 & 0 & \cdots & 0 & \alpha \end{pmatrix}.$$

So, if you know the invariant factors, you can get the elementary divisors, and from there you can obtain the Jordan canonical form. (Note: in this case, there is no ordering on the blocks).

In the previous example, $\mathbb{R}$ contains the eigenvalues $2, 3$, so we can put it into Jordan canonical form. The invariant factors are $(t-2)$ and $(t-2)(t-3)$, so the elementary divisors are $(t-2)$, $(t-2)$, and $(t-3)$ (all the primes to all the powers that they appear with in the factorizations of the invariant factors). So each Jordan block is just a 1×1 matrix consisting of the root of that polynomial. Hence the Jordan form is actually diagonal and is exactly

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

To conclude, here's an exercise:

Exercise: Suppose that $T\colon V \to V$ has elementary divisors

$$(t+2), (t+2)^2, (t-1), (t-1).$$

What is the corresponding matrix for T in Rational Canonical Form? Jordan Canonical Form?