CANONICAL FORMS FOR LINEAR TRANSFORMATIONS AND MATRICES

The purpose of these notes is to present the rational canonical form and Jordan canonical form theorems for my Math 790 class. Fix an n-dimensional vector space V over the field F. Write $\mathcal{L}(V,V)$ for the vector space of linear transformations from V to itself and recall that $\mathcal{L}(V,V)$ is isomorphic as a vector space (and as a ring) to $M_n(F)$, the set of $n \times n$ matrices with entries in F. The impetus for our work is provided by the following question. Given $T \in \mathcal{L}(V,V)$, can we represent T by a matrix having a "canonical" (i.e., "natural") form? It turns out that the form of the matrix we obtain depends heavily on the factorization of the minimal polynomial of T over F. For example, writing $\mu_T(x)$ for the minimal polynomial of T, if $\mu_T(x)$ has all of its roots in F, it turns out that T is triangularizable. In other words, there exists a basis $\mathcal{B}$ such that the matrix for T with respect to $\mathcal{B}$ is lower (or upper) triangular. In fact, we will be able to do much better, in that we will be able to put T into its so-called *Jordan canonical form* whenever $\mu_T(x)$ splits over F. The Jordan form will still be triangular, but most of its off diagonal entries will be zero. When $\mu_T(x)$ does not necessarily have its roots in F, the situation is more complicated. Nevertheless, the *rational canonical form* will still be a desirable form in that, while not upper triangular, it will be "zero-heavy".

Before embarking on the statements and proofs, we recall a few definitions from class. Fix once and for all $T \in \mathcal{L}(V,V)$ and $\mu_T(x)$, the minimal polynomial of T over F. Recall that a subspace $W \subseteq V$ is *T-invariant* if $T(w) \in W$ for all $w \in W$. T-invariant subspaces play a central role in what follows; they provide the proper vehicle for proofs by induction and are an integral part of the decomposition of V leading to the canonical forms. Here is an easy way to get a T-invariant subspace. Fix $v \in V$ and let W denote the subspace spanned by the vectors $\{v, T(v), T^2(v), \dots\}$. Then W is a T-invariant subspace, since T takes a typical vector $\alpha_0 v + \cdots + \alpha_r T^r(v)$ in W to $\alpha_0 T(v) + \cdots + \alpha_r T^{r+1}(v)$, which is again in W. Note that $W = \{f(T)(v) \mid f(x) \in F[x]\}$. We call W the *cyclic subspace generated by v* and denote it by $\langle T, v\rangle$. Our first proposition details some basic facts about cyclic subspaces.

Proposition A. *Let $v \in V$, set $W := \langle T, v\rangle$ and suppose $r = \deg \mu_T(x)$.*

- *(i) W is spanned by the vectors $\{v, T(v), \dots, T^{r-1}(v)\}$.*
- *(ii) If $f(x) \in F[x]$ satisfies $f(T)(v) = 0$, then $f(T)(w) = 0$, for all $w \in W$. Thus, $f(T|_W) = 0$. In particular, $f(T|_W) = 0$ if and only if $f(T)(v) = 0$.*
- *(iii) Let $\mu_{T|_W}(x)$ denote the minimal polynomial of $T|_W$ and let c be the degree of $\mu_{T|_W}(x)$. Then $\mathcal{B} = \{v, T(v), \dots, T^{c-1}(v)\}$ is a basis of W. In particular, $\dim W = \deg \mu_{T|_W}(x)$.*
- *(iv) The matrix of $T|_W$ with respect to the basis $\mathcal{B}$ is the companion matrix of $\mu_{T|_W}(x)$, $C(\mu_{T|_W}(x))$.*

Proof. (i) follows, since if $w \in W$, $w = f(T)(v)$, for some $f(X) \in F[x]$. Write $f(X) = \mu_T(x)h(x) + r(x)$, where $r(x)$ has degree less than r. Then $f(T)(v) = r(T)(v)$, since $\mu_T(T) = 0$. Thus, $f(T)(v) = r(T)(v)$ belongs to the span of $\{v, T(v), \dots, T^{r-1}(v)\}$.

For (ii), if $w \in W$, then $w = g(T)(v)$, for some $g(x) \in F[x]$. Therefore,

$$f(T)(w) = f(T)g(T)(v) = g(T)f(T)(v) = g(T)(0) = 0.$$

For (iii), the same proof in (i) shows that W is spanned by $\{v, T(v), \dots, T^{c-1}(v)\}$. On the other hand, a non-trivial dependence relation on these vectors would give rise to a polynomial $g(x)$ of degree less that c such that $g(T)(v) = 0$. By (ii), this would mean $g(T|_W) = 0$, contradicting that $\mu_{T|_W}(x)$ is the minimal polynomial of $T|_W$. Thus, $\{v, T(v), \dots, T^{c-1}(v)\}$ is a basis for W, so $\dim W = \deg \mu_{T|_W}(x)$.

For (iv), suppose $\mu_{T|_W}(x) = x^c + a_{c-1}x^{c-1} + \cdots + a_0$. Then

$$T(v) = 1 \cdot T(v), T(T(v)) = 1 \cdot T^2(v), \dots, T(T^{c-2}(v)) = 1 \cdot T^{c-1},$$

which shows that the matrix consisting of the first $c-1$ columns of the matrix of $T|_W$ with respect to $\mathcal{B}$ equals $\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$. To compute the last column of the matrix, apply T to $T^{c-1}(v)$, to get:

$$T(T^{c-1}(v)) = T^c(v) = -a_0 \cdot 1 + (-a_1) \cdot T(v) + \cdots + (-a_{c-1}) \cdot T^{c-1}(v),$$

since $\mu_{T|_W}(T)(v) = 0$. Thus, the full matrix of T with respect to $\mathcal{B}$ equals

$$C = \begin{pmatrix} 0 & 0 & 0 & \cdots & -a_0 \\ 1 & 0 & 0 & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -a_{c-1} \end{pmatrix},$$

the companion matrix of $\mu_{T|_W}(x)$.

It is not difficult to show the converse to part (iv) above, namely, that if W is a T invariant subspace of dimension c, and there exists a basis $\mathcal{B} = \{w_1, w_2, \ldots, w_c\} \subseteq W$ such that the matrix of $T|_W$ with respect to $\mathcal{B}$ equals C as above, then for $2 \leq i \leq c$, $w_i = T^{i-1}(w_1)$ and $W = \langle T, w_1 \rangle$. Moreover, one has $\mu_{T|_W}(x) = x^c + a_{c-1}x^{c-1} + \cdots + a_0$.

In what follows, we will rely heavily on Proposition A above. Now suppose that W is an arbitrary T-invariant subspace. Then T induces a linear transformation $T|_W : W \to W$. The basic strategy for finding the canonical forms for T is roughly the following. Proceed by induction on the dimension of V. Find a T-invariant subspace $U \subseteq V$ satisfying $V = W \oplus U$. By induction there is a basis for W bringing $T|_W$ to the desired form and a basis for U bringing $T|_U$ to the desired form. Putting these bases together brings T to the desired form. In fact, we will see that $W = \langle T, v \rangle$ for a suitably chosen $v \in V$. The challenge will then be to find a T-invariant complement U, since not every T-invariant subspace of V admits a T-invariant complement. Ultimately, it will follow that V is the direct sum of finitely many subspaces of the form $\langle T, v \rangle$.

The next proposition shows that if V is the direct sum of T-invariant subspaces, then there exists a basis for V for which the corresponding matrix of T takes a "block diagonal" form. This is the first significant step along our lengthy path.

Proposition B. *Let $W_1, \ldots, W_k$ be T-invariant subspaces such that $V = W_1 \oplus \cdots \oplus W_k$. For each $1 \leq i \leq k$, let $\mathcal{B}_i := \{w_{i1}, \ldots, w_{in_i}\}$ be a basis for W_i and set $\mathcal{B} := \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$, which is a basis for V. Let A denote the matrix of T with respect to $\mathcal{B}$ and A_i denote the matrix of $T|_{W_i}$ with respect to $\mathcal{B}_i$. Furthermore, write $\mu_T(x)$ for the minimal polynomial of T. Finally, for $1 \leq i \leq k$, let $\mu_{T_i}(x)$ be the minimal polynomial of $T|_{W_i}$. Then:*

(i) The matrix for T with respect to B has the (block diagonal) form

$$A = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_k \end{pmatrix}.$$

(ii) $\mu_T(x) = LCM(\mu_{T_1}(x), \ldots, \mu_{T_k}(x))$.

Proof. Part (i) is basically clear. When we apply T to the basis vectors in $\mathcal{B}_i$, the resulting vectors belong to W_i and are expressible in terms of the vectors in $\mathcal{B}_i$. It follows that the column in A corresponding to $T(w_{ij})$ is zero in all entries save possibly the entries belonging to rows $n_1 + \cdots + n_{i-1} + 1$ through $n_1 + \cdots + n_i$ (for all $1 \leq j \leq n_i$). Thus A takes the required from. For part (ii), set $h(X) := LCM(\mu_{T_1}(X), \ldots, \mu_{T_k}(X))$. Let $1 \leq i \leq k$, take $w_i \in W_i$ and write $h(X) = a_i(X)\mu_{T_i}(X)$. Then $h(T)(w_i) = a_i(T)(\mu_{T_i}(T)(w_i)) = 0$. Since $V = W_1 + \cdots + W_k$, it follows that $h(T)(v) = 0$, for all $v \in V$. Thus, $h(T) = 0$, so $\mu_T(x)$ divides $h(X)$. On the other hand, $\mu_T(T) = 0$, so $\mu_T(T|_{W_i}) = 0$, for each i. Thus, $\mu_{T_i}(X)$ divides $\mu_T(x)$ for all i, so $h(X)$ divides $\mu_T(x)$, by the definition of LCM. Since $h(X)$ and $\mu_T(x)$ are monic polynomials, $h(X) = \mu_T(x)$. $\square$

Now that we know that a matrix decomposition follows from a decomposition of V into a direct sum of T-invariant subspaces, we need to know when we can achieve such a decomposition. For any given V, there are many ways to do this. The next proposition shows one possible approach, namely, that we can decompose V according to how we factor $\mu_T(x)$, the minimal polynomial of T, into a product of irreducible polynomials over F. As we will see below, factorization over F plays a crucial role in the decomposition of V into T invariant subspaces of the required type.

Proposition C. *Suppose we factor $\mu_T(x) = p_1(x)^{e_1} \cdots p_k(x)^{e_k}$, with each $p_i(x)$ irreducible over F. Then there exist subspaces $W_1, \ldots, W_k \subseteq V$ satisfying the following conditions.*

(i) $W_1, \ldots, W_k$ are T-invariant.
(ii) $V = W_1 \oplus \cdots \oplus W_k$.
(iii) $p_i(x)^{e_i}$ is the minimal polynomial of $T|_{W_i}$, for $1 \leq i \leq k$.

Proof. For each $1 \leq i \leq k$, set $W_i := \ker(p_i(T)^{e_i})$. Then each W_i is T-invariant. Indeed, $w_i \in W_i$ implies $p_i(T)^{e_i}(w_i) = 0$, so $0 = T(p_i(T)^{e_i}(w_i)) = p_i(T)^{e_i}(T(w_i))$, so $T(w_i) \in W_i$. This gives (i). For part (ii), set $f_i(x) := \prod_{j \neq i} p_j(x)^{e_j}$. Then $f_1(x), \ldots, f_k(x)$ have no common divisor, so there exist $a_1(x), \ldots, a_k(x) \in F[x]$ such that
$a_1(x)f_1(x) + \cdots + a_k(x)f_k(x) = 1$. Thus, for all $v \in V$,

$$v = a_1(T)f_1(T)(v) + \cdots + a_k(T)f_k(T)(v).$$

However, for each $1 \leq i \leq k$,

$$p_i(T)^{e_i}(a_i(T)f_i(T)(v)) = a_i(T)(\mu_T(T)(v)) = 0.$$

Thus, each $a_i(T)f_i(T)(v) \in W_i$ and $V = W_1 + \cdots + W_k$. To show that the sum is direct, fix an i between 1 and k and take $c_i(x), d_i(x) \in F[x]$ satisfying $c_i(x)p_i(x)^{e_i} + d_i(x)f_i(x) = 1$. Suppose that $w_i = w_1 + \cdots + w_{i-1} + w_{i+1} + \cdots + w_k$, with $w_j \in W_j$, for all j. Then

$$w_i = (1 - c_i(T)p_i(T)^{e_i})(w_i) =$$

$$d_i(T)f_i(T)(w_1) + \cdots + d_i(T)f_i(T)(w_{i-1}) + d_i(T)f_i(T)(w_{i+1}) + \cdots + d_i(T)f_i(T)(w_k) = 0,$$

since $f_i(T)(w_j) = 0$, for all $j \neq i$. Thus, $W_i \cap (W_1 + \cdots W_{i-1} + W_{i+1} + \cdots + W_k) = 0$, and the sum is direct. This gives part (ii).

To prove part (iii), let $\mu_{T_i}(x)$ denote the minimal polynomial of $T|_{W_i}$, for $1 \leq i \leq k$. Then $\mu_{T_i}(x)$ divides $p_i(x)^{e_i}$, for all i, since $p_i(T|_{W_i})^{e_i} = 0$, by definition of W_i. Thus, $\mu_{T_i}(x) = p_i(x)^{e_i'}$, $e_i' \leq e_i$, since $p_i(x)$ is irreducible. On the other hand, by Proposition C,

$$p_1(x)^{e_1} \cdots p_k(x)^{e_k} = \mu_T(x) = LCM(\mu_{T_1}(x), \ldots, \mu_{T_k}(x)) = p_1(x)^{e_1'} \cdots p_k(x)^{e_k'}.$$

It follows at once that each $e_i' = e_i$ and thus, $\mu_{T_i}(x) = p_i(x)^{e_i}$, for all i, which is what we want. □

Now, let's summarize what we've done by putting together Propositions B and C. Factor the minimal polynomial $\mu_T(x) = p_1(x)^{e_1} \cdots p_k(x)^{e_k}$, with each $p_i(x)$ irreducible over F. By Proposition C, we can can decompose V as a direct sum of the T-invariant subspaces $W_i := \ker(p_i(T)^{e_i})$. We will refer to the W_i as the *primary components* of V. By Proposition B, if we take a basis $\mathcal{B}$ for V comprised of bases from $W_1, \ldots, W_k$, the matrix of T with respect to $\mathcal{B}$ is block diagonal, where the ith block diagonal entry is the matrix of $T|_{W_i}$ with respect to the selected basis from W_i. We will refer to these blocks as *primary blocks* associated to T. As things now stand, the primary blocks have no particular form. The next and most difficult phase of our journey requires an analysis at the primary block level. In other words, we assume that $\mu_T(x)$ is a power of an irreducible polynomial and push on from there.

Remark D. In the best of worlds, each primary component W_i in our general discussion would be cyclic with respect to some $w_i \in W_i$ so that the matrix of $T|_{W_i}$ with respect to a cyclic basis was a companion matrix. Alas this is not so; but we will see that each primary component can be decomposed into a direct sum of such spaces, so that the matrix of $T|_{W_i}$ will be block diagonal, with companion matrices as blocks. Putting all of the bases together for all of the summands, it will then follow that there is a basis for V for which the corresponding matrix of T consists of finitely many blocks, each of which is a companion matrix.

Before proceeding further, we need the concept of a maximal vector.

Definition-Remark E. A vector u in the finite dimensional vector space U is said to be a *maximal vector* for $T \in \mathcal{L}(U,U)$ if $\dim\langle T,u\rangle$ is the largest possible, i.e., $\dim\langle T,u\rangle$ equals the degree (say r) of $\mu_T(x)$. In this case, we have:

(i) The vectors $\{v, T(v), \ldots, T^{r-1}(v)\}$ are a basis for $U' := \langle T, v\rangle$. This follows since, by Proposition A, these vectors span U', and thus for a basis, since $\dim U' = r$.

(ii) $\mu_T(x)$ is the minimal polynomial for $T|_{U'}$. This follows, since $\deg \mu_{T|_{U'}}(x) = r = \deg \mu_T(x)$, and $\mu_{T|_{U'}}(x)$ divides $\mu_T(x)$.

(iii) By Proposition A, the matrix of $T|_{U'}$ with respect to the basis $\{u, T(u), \ldots, T^{r-1}(u)\}$ is $C(\mu_T(x))$.

The following proposition shows that a maximal vector always exists when $\mu_T(x)$ is a power of an irreducible polynomial.

Proposition F. *Let W be a finite dimensional vector space and T a linear operator on W. Suppose that the minimal polynomial of T is $p(x)^e$, with $p(x)$ an irreducible polynomial over F. Then T admits a maximal vector w.*

Proof. By Proposition A, since for any $u \in W$, $\langle T, u\rangle$ is spanned by the set $\{u, T(u), \ldots, T^{r-1}(u)\}$, if $u, T(u), \ldots, T^{r-1}(u)$ are linearly independent, then they form a basis for $\langle T, u\rangle$. This in turn implies that $\dim\langle T,u\rangle = \deg \mu_T(x)$, which implies that u is a maximal vector for T. Thus, we seek $w \in W$ such that $\{w, T(w), \ldots, T^{r-1}(w)\}$ is a linearly independent set of vectors.

Now, suppose the proposition is false. Let $w_1, \ldots, w_d \in W$ be a basis for W and let W_i be the cyclic subspace generated by w_i, for $1 \le i \le d$. Let $f_i(x)$ denote the minimal polynomial of $T|_{W_i}$. Since, by assumption, $w_i, T(w_i), \ldots, T^{r-1}(w_i)$ are linearly dependent, there exists a non-trivial dependence relation on this set, for each $1 \le i \le d$. Any dependence relation gives rise to a non-zero polynomial $h_i(x) \in F[x]$ of degree $r-1$ or less such that $h_i(T)(w_i) = 0$. By Proposition A, this means $h_i(T|_{W'}) = 0$, so $f_i(x)$ divides $h_i(x)$. In particular, $f_i(x)$ has degree less than or equal to $r-1$. On the other hand, since $p(T)^e = 0$, $p(T|_{W_i})^e = 0$, so $f_i(x)$ divides $p(x)^e$. Since $p(x)$ is irreducible, this forces $f_i(x)$ to be a power of $p(x)$, and since $f_i(x)$ has degree less than r, $f_i(x) = p(x)^{e_i}$, for some $e_i \le e-1$. Thus, each $f_i(x)$ divides $p(x)^{e-1}$. Writing $p(x)^{e-1} = p(x)^{c_i} f_i(x)$, for some c_i, it follows that $p(T)^{e-1}(w_i) = p(T)^{c_i} f_i(T)(w_i) = 0$, for all i. Since the w_i form a basis for W, $p(T)^{e-1}(w) = 0$, for all $w \in W$, so $p(T)^{e-1} = 0$. But this contradicts the fact that $p(x)^e$ is the minimal polynomial of T. Thus, there must be a basis element $w_i i$ such that $w_i, T(w_i), \ldots, T^{r-1}(w_i)$ are linearly independent, so that w_i is a maximal vector for T. □

Now if we think of W in Proposition F as one of the primary components of V, then we have the start of the decomposition alluded to in Remark D. Suppose $w \in W$ is a maximal vector for $T|_W$ and we could find a T-invariant subspace U such that $W = \langle T, w\rangle \oplus U$. Then we could either repeat the construction of Proposition F on U, or simply apply induction to write U as a direct sum of T-invariant *cyclic* subspaces. Thus, W is then decomposed into a sum of cyclic subspaces with bases so that that the matrix of the restriction of T with respect to any of these bases is a companion matrix. Thus T restricted to W can then be represented as a block diagonal matrix with companion matrices for blocks. Doing this for each primary block would yield the result we seek. Thus, we must find U, a T-invariant complement of a cyclic subspace generated by a maximal vector. This is the most difficult part of the proof of our canonical form theorems.

The conductor. Let B be finite dimensional vector space, $T \in \mathcal{L}(B,B)$ and $A \subseteq B$ a T-invariant subspace. Fix a vector $v \in B \backslash A$. Then there is a unique monic polynomial $g(x)$ of least degree, called the *conductor of v into A*, such that :

(i) $g(T)(v) \in A$.

(ii) Whenever $f(x)$ is a polynomial with $f(T)(v) \in A$, then $g(x)$ divides $f(x)$.

The existence of $g(x)$ should be standard by now. Take $g(x)$ to be the monic polynomial of least degree such that $g(T)(v) \in A$. Note that $\mu_T(T)(v) = 0 \in B$, so the set of monic polynomials $h(x)$ satisfying $h(T)(v) \in A$ is not just the zero polynomial, so $g(x)$ exists. Now, if $f(x)$ is a polynomial such that $f(T)(v) \in A$, then the division algorithm applied by dividing $f(x)$ by $g(x)$ gives a remainder $r(x)$ of degree less than the degree of $g(x)$. An easy calculation shows $r(T)(v) \in A$, so by definition of $g(x)$, $r(x) = 0$, i.e., $g(x)$ divides $f(x)$. It follows from this that if the minimal polynomial of T is $p(x)^e$, with $p(x)$ irreducible over F, then the conductor of v into A is $p(x)^{e'}$ for some $e' \le e$, and in fact, e' is the least positive integer such that $p(T)^{e'}(v) \in A$.

We will see below that the conductor plays a key role in finding a T-invariant complement.

Admissible subspaces. Given a vector space U and $T \in \mathcal{L}(U,U)$, a subspace $W \subseteq U$ is said to be *T-admissible* if T-invariant, and whenever $f(x) \in F[x]$ and $u \in U$, $f(T)(u) \in W$ implies there exists $w \in W$ such that $f(T)(u) = f(T)(w)$.

Here is an easy, but significant proposition.

Proposition G. *Suppose $W \subseteq U$ is a T-invariant subspace and W admits a T-invariant complement, i.e., there exists a T-invariant subspace $W' \subseteq U$ such that $U = W \oplus W'$. Then W is a T-admissible subspace.*

Proof. Take $u \in U$ and suppose $f(T)(u) \in W$, for some $f(x) \in F[x]$. Write $u = w + w'$, for $w \in W$ and $w' \in W'$. Then $f(T)(u) = f(T)(w) + f(T)(w')$, and thus $f(T)(u) - f(T)(w) = f(T)(w')$. Since W and W' are T-invariant, the left hand side of this equation belongs to W and the right hand side belongs to W'. Thus, $f(T)(w') \in W \cap W' = 0$. Therefore, $f(T)(u) = f(T)(w)$, as required. □

The following proposition is the crucial component to finding T-invariant complements - and is the most difficult step leading to the canonical forms.

Proposition H. *Let W be a finite dimensional vector space over F and $T \in \mathcal{L}(W,W)$. Suppose that $\mu_T(x) = p(x)^e$, for $p(x)$ irreducible over F. Let $W_0 \subseteq W$ be a T-admissible subspace and e_0 be the least positive integer such that $p(T)^{e_0}(u) \in W_0$ for all $u \in W$. Then, there exists $v \in W$ such that:*

(i) The conductor of v into W_0 is $p(x)^{e_0}$.
(ii) $W_0 \cap \langle T, v\rangle = 0$.
(iii) $W_0 + \langle T, v\rangle$ is T-admissible.

Proof. Let $v_1, \ldots, v_s$ be that part of a basis for W obtained by extending a basis for W_0 to a basis for W. For each $1 \leq i \leq s$, let $p(x)^{e_i}$ be the conductor of v_i into W_0. Take e_0 to be the maximum of the e_i, and without loss of generality, assume $e_0 = e_1$, so that $p(x)^{e_0}$ is the conductor of v_1 into W_0. Then $p(T)^{e_0}(v_j) \in W_0$, for all v_j, and hence $p(T)^{e_0}(u) \in W_0$, for all $u \in W$. Note that no value smaller than e_0 works, since $p(x)^{e_0}$ is the conductor of v_1 into W_0.

Now, $p(T)^{e_0}(v_1) \in W_0$, and since W_0 is T-admissible, $p(T)(v_1) = p(T)(w_0)$, for some $w_0 \in W_0$. Set $v := v_1 - w_0$. This is the v we seek.

To see that $p(x)^{e_0}$ is the conductor of v into W_0, note that $f(T)(v) = f(T)(v_1) - f(T)(w_0)$, for all $f(x) \in F[x]$. Since $f(T)(w_0) \in W_0$, it follows that $f(T)(v) \in W_0$ if and only if $f(T)(v_1) \in W_0$. Since this holds for all $f(x) \in F[x]$, it follows that the conductor of v into W_0 equals the conductor of v_1 into W_0, which is $p(x)^{e_0}$. This gives (i).

For (ii), Suppose $u = W_0 \cap \langle T, v\rangle$. If we write $u = d(T)(v)$, for some $d(x) \in F[x]$, then $p(x)^{e_0}$ divides $d(x)$, by since part (i), $p(x)^{e_0}$ is the conductor of v into W_0. We may write $d(x) = d_0(x)p(x)^{e_0}(x)$. Thus,

$$u = d(T)(v) = d_0(T)p(T)^{e_0}(v) = d_0(T)(p(T)^{e_0}(v_1) - p(T)^{e_0}(w_0)) = d_0(T)(0) = 0,$$

which is what we want.

For (iii), suppose $u \in W$ and $f(T)(u) \in W_0 + \langle T, v\rangle$, for some $f(x) \in F[x]$. We wish to show that $f(T)(u) = f(T)(z)$, for some $z \in W_0 + \langle T, v\rangle$. We can write $f(x) = p(x)^{e'} f_0(x)$, where $p(x)$ does not divide $f_0(x)$. We consider two cases.

For the first case, suppose $e' \geq e_0$. Then $p(T)^{e'}(u) \in W_0$ (by the choice of e_0), so $f(T)(u) \in W_0$. Since W_0 is T-admissible, we have $f(T)(u) = f(T)(z)$, for some $z \in W_0$ which gives what we want, since $W_0 \subseteq W_0 + \langle T, v\rangle$.

Suppose $e' < e_0$. Write $f(T)(u) = w_0' + h(T)(v)$, for $w_0' \in W_0$ and $h(x) \in F[x]$. We can also write $1 = a(x)f_0(x) + b(x)p(x)^e$, for $a(x), b(x) \in F[x]$. Note that for all $u' \in W$, $u' = a(T)f_0(T)(u')$, since $u' = a(T)f_0(T)(u') + b(T)p(T)^e(u')$, and $b(T)p(T)^e(u') = 0$. Now we apply $p(T)^{e_0 - e'}$ to the equation $f(T)(u) = w_0 + h(T)(v)$. This yields:

$$p(T)^{e_0} f_0(T)(u) = p(T)^{e_0 - e'}(w_0') + p(T)^{e_0 - e'} h(T)(v).$$

Therefore,

$$p(T)^{e_0} f_0(T)(u) - p(T)^{e_0 - e'}(w_0') = p(T)^{e_0 - e'} h(T)(v),$$

which shows that $p(T)^{e_0-e'}(T)h(T)(v)$ belongs to W_0. Thus, $p(x)^{e_0-e'}(x)h(x)$ is divisible by $p(x)^{e_0}$, the conductor of v into W_0. Since $p(x)$ is irreducible, we may write $h(x) = h_0(x)p(x)^{e'}$. Returning to the original equation $f(T) = w_0' + h(T)(v)$, this becomes

$$p(T)^{e'}f_0(T)(u) = w_0' + p(T)^{e'}h_0(T)(v),$$

which yields

$$p(T)^{e'}(f_0(T)(u) - h_0(T)(v)) = w_0'.$$

Since W_0 is T-admissible, $w_0' = p(T)^{e'}(w_2)$, for some $w_2 \in W_0$. Substituting this into the first displayed equation on this page, we get

$$p(T)^{e'}f_0(T)(u) = p(T)^{e'}(w_2) + p(T)^{e'}h_0(T)(v).$$

As noted above, $w_2 = f_0(T)a(T)(w_2)$ and $h_0(T)(v) = f_0(T)a(T)h_0(T)(v)$. Substituting this into the latest displayed equation yields,

$$p(T)^{e'}f_0(T)(u) = p(T)^{e'}f_0(T)a(T)(w_2) + p(T)^{e'}f_0(T)a(T)h_0(T)(v).$$

Finally, since $f(x) = p(x)^{e'}a(x)$, we have

$$f(T)(u) = f(T)a(T)(w_2) + f(T)a(T)h_0(T)(v) = f(T)(a(T)(w_2) + a(T)h_0(T)(v)).$$

Since $a(T)(w_2) \in W_0$ and $a(T)h_0(T)(v) \in \langle T, v\rangle$, $z := a(T)(w_2) + a(T)h_0(T)(v)$ belongs to $W_0 + \langle T, v\rangle$, and $f(T)(u) = f(T)(z)$, which gives what we want. □

As a corollary to Proposition H we see that when $\mu_T(x)$ is a power of an irreducible polynomial, a T-invariant subspace has a T-invariant complement if and only if it is T-admissible.

Corollary I. *Let W be a finite dimensional vector space and suppose $T \in \mathcal{L}(W, W)$ has the property that $\mu_T(x) = p(x)^e$, with $p(x)$ irreducible over F. For a T-invariant subspace $W_0 \subseteq W$, W_0 has a T-invariant complement if and only if W_0 is T-admissible. In particular, if $w \in W$ is a maximal vector for T, then $\langle T, w\rangle$ admits a T-invariant complement.*

Proof. If W_0 is T-admissible, then W_0 has a T-invariant complement, by Proposition G. Conversely, suppose that W_0 is T-admissible. Let W' be a subspace maximal with respect to the properties that $W' \cap W_0 = 0$ and $W_0 + W'$ is T-admissible. Note W is finite dimensional, so there is no need for anything like Zorn's Lemma. If $W_0 + W' \neq W$, then we can apply Proposition H to the admissible subspace $W_0 + W'$ to find a (cyclic) subspace W'' such that $(W_0 + W') \cap W'' = 0$ and $(W_0 + W') + W'$ is T-admissible. But then $W_0 \cap (W' + W'') = 0$ (check this!) and $(W' + W'')$ is a larger subspace with $W_0 + (W' + W'')$ admissible, a contradiction. Thus, $W_0 + W' = W$ and therefore $W = W_0 \oplus W'$, as required. □

Our first Theorem provides the final step before the rational canonical form theorem. that follow.

Theorem J. *Let T be a linear operator on the n-dimensional vector space W. Let $p(x)^e$ denote the minimal polynomial of T, where $p(x)$ is irreducible over F and set $r := \deg(p(x)^e)$. Then there exist cyclic subspaces $W_1, \ldots, W_t$ of W such that*

(i) $W = W_1 \oplus \cdots \oplus W_t$.
(ii) For each i, the minimal polynomial of $T|_{W_i}$ is $p(x)^{e_i}$, for some $e_i \leq e$.
(iii) Each W_i has a basis of the form $\mathcal{B}_i := \{w_i, T(w_i), \ldots, T^{r_i-1}(w_i)\}$, where $r_i = \deg p(x)^{e_i}$.
(iv) The matrix of T with respect to the basis $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_t$ is

$$A = \begin{pmatrix} C(p(x)^{e_1}) & 0 & \cdots & 0 \\ 0 & C(p(x)^{e_2}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & C(p(x)^{e_t}) \end{pmatrix}$$

Moreover, we can arrange the ordering so that $e = e_1 \geq e_2 \geq \cdots \geq e_t$.

Proof. The first statement follows by induction on $\dim W$. If we take $W_0 = 0$ in Proposition H, then for v as in the conclusion of Proposition H, $W_1 := \langle T, v\rangle$ is a T-admissible subspace. By Corollary I, there is a T-invariant subspace W' such that $W = W_1 \oplus W'$. By induction, we can write $W' = W_2 \oplus \cdots \oplus W_t$, where each W_i is a cyclic subspace of W', and hence a cyclic subspace of W. Thus, $W = W_1 \oplus \cdots \oplus W_t$. Let us change notation and set $v = w_1$ and write each $W_i = \langle T, w_i\rangle$.

Note, that in the special case of Proposition H with $W_0 = 0$, the least positive integer e_0 with $p(T)^{e_0}(u) = 0$ for all $u \in W$, is $e = e_0$. Since $p(x)^e$ is the conductor of $w_1 = v$ into 0, it follows that $p(x)^e$ is the minimal polynomial of $T|_{W_1}$ (by Proposition A) and thus w_1 is a maximal vector. It also follows from Proposition A that $\mathcal{B}_1 := \{w_1, T(w_1), \ldots, T^{r_1-1}(w_1)\}$ is a basis for W_1, where $r_1 = r = \deg p(x)^{e_1}$. In addition, Proposition A yields that the matrix of $T|_{W_1}$ is $C(p(x)^{e_1})$. Applying induction to $T|_{W'}$, together with Proposition B, completes the proof of (i)-(iv). For the final statement, the induction hypothesis implies we can arrange to have $e_2 \geq \cdot \geq e_t$, where $p(x)^{e_2}$ is the minimal polynomial of $T_{W'}$. Since this latter polynomial must divide $\mu_T(x) = p(x)^{e_1}$, we have $e_1 \geq e_2$, and thus $e = e_1 \geq \cdots \geq e_t$. □

We are now ready for the main result of these notes.

Theorem K. *(Rational Canonical Form via elementary divisors) Factor $\mu_T(x) = p_1(x)^{e_1} \cdots p_k(x)^{e_k}$, with each $p_i(x)$ irreducible over F. Then there exists a basis $\mathcal{B}$ for V such that A, the matrix of T with respect to $\mathcal{B}$, has the the block diagonal form*

$$A = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_k \end{pmatrix},$$

where $A_1, \ldots, A_k$ are primary blocks corresponding to $p_1(x)^{e_1}, \ldots, p_k(x)^{e_k}$, and for each $1 \leq i \leq k$,

$$A_i = \begin{pmatrix} C(p_i(x)^{e_{i,1}}) & 0 & \cdots & 0 \\ 0 & C(p_i(x)^{e_{i,2}}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & C(p_i(x)^{e_{i,t_i}}) \end{pmatrix}$$

for integers $e_i = e_{i,1} \geq e_{i,2} \geq \cdots \geq e_{i,t_i}$.

Proof. By Proposition C, we may decompose $V = W_1 \oplus \cdots \oplus W_k$, where for each $1 \leq i \leq k$, W_i is T-invariant and the minimal polynomial of $T|_{W_i}$ is $p_i(x)^{e_i}$. By Theorem J, we may decompose each $W_i = W_{i,1} \oplus \cdots \oplus W_{i,t_i}$ so that for each $1 \leq j \leq t_i$, $W_{i,j}$ has a basis of the form $\mathcal{B}_{i,j} = \{w_{i,j}, T(w_{i,j}), \ldots T^{r_{i,j}-1}(w_{i,j})\}$ and the minimal polynomial of $T|_{W_{i,j}}$ is $p_i(x)^{e_{i,j}}$ with $e_i = e_{i,1} \geq \cdots \geq e_{i,t_i}$ and $deg(p_i(x)^{e_{i,j}}) = r_{i,j}$. The matrix of $T|_{W_{i,j}}$ with respect to the given basis is $C(p_i(x)^{e_{i,j}})$. Since

$$V = W_{1,1} \oplus \cdots \oplus W_{1,t_1} \oplus \cdots \oplus W_{k,1} \oplus \cdots \oplus W_{k,t_k},$$

if we take $\mathcal{B} := \mathcal{B}_{1,1} \cup \cdots \cup \mathcal{B}_{1,t_1} \cup \cdots \cup \mathcal{B}_{k,1} \cup \cdots \cup \mathcal{B}_{k,t_k}$, then the matrix of T with respect to $\mathcal{B}$ has the required form (by Proposition B). □

Remarks L. (i) The process leading to the rational canonical form is algorithmic. In other words, starting with a particular T, we can follow the path just traversed to construct the basis $\mathcal{B}$ in Theorem K. Of course, the process needn't be the most efficient or even doable in any reasonable amount of time – with or without the aid of a computer. To summarize, first find the minimal polynomial $\mu_T(x)$. This can be calculated since it divides the characteristic polynomial of T and we can calculate the characteristic polynomial using determinants. Then factor $\mu_T(x) = p_1(x)^{e_1} \cdots p_k(x)^{e_k}$, with each $q_i(x)$ irreducible over F. Again, factoring efficiently may be hard. Next calculate $ker(p_i(T)^{e_i})$ for each $1 \leq i \leq k$. This is equivalent to solving a homogenous system of equations, so Gaussian elimination applies. As in the proof of Theorem K, restricting T to each $ker(p_i(T)^{e_i})$ then reduces the problem to the case where the minimal polynomial of T is $p(x)^e$, with $p(x)$ irreducible. Now, as in the proof of Theorem J, set $r := deg(p(x)^e)$ and consider the set $\{v, T(v), \ldots, T^{r-1}(v)\}$ as v ranges through the standard basis (say) for V. Since one of these basis vectors must be a maximal vector for T, one of these collections must be linearly independent, a condition that can be checked with Gaussian elimination. Calling the v that works w_1 and using W_1 to denote the

corresponding cyclic subspace generated by w_1, use the proof of Proposition H to construct a second vector w_2 such that $W_2 := \langle T, w_2\rangle$ has the property that $W_1 \cap W_2 = 0$. It's important to note that, as in the porrof of Proposition H, w_2 can be found by applying powers of the irreducible polynomial evaluated at T to a finite set of vectors. Finally repeat the process described in Proposition H finitely many times until W is written as a direct sum of cyclic subspaces.

(ii) Let the collection of integers $\{e_{i,j}\}$ be given as in Theorem K. The polynomials $\{p_i(x)^{e_{i,j}}\}$ are called the elementary divisors of T and uniquely determine the rational canonical form of T. We'll see below, that the elementary divisors of T are unique. In other words, up to a possible permutation of primary blocks along the diagonal, the rational canonical form of T is unique. If we just want the rational canonical form of T and not the basis giving it, there is a constructive procedure leading to the calculation of the elementary divisors of T. The procedure is easy to describe, but the proof that the procedure works is a bit beyond the scope of this course.

(iii) Of course, the rational canonical form theorem has a version for matrices. Take C in $M_n(F)$. Let T_C be the linear transformation $T_C : F^n \to F^n$ defined by $T_C(v) = C \cdot v$. Then C is the matrix of T with respect to the standard basis of F^n. If $\mathcal{B}$ is the basis for which the matrix $A := [T_C]_{\mathcal{B}}$ is rational canonical form (as in Theorem K), then $P^{-1}CP = A$, for P the change of basis matrix whose columns are the vectors in $\mathcal{B}$. We call A the rational canonical form of C.

(iv) While the rational canonical form for a transformation or matrix is unique, different rational canonical forms could have the same minimal polynomial. Thus, the minimal polynomial alone does not determine a unique rational canonical form. However, for a fixed n and a fixed polynomial $f(X)$ of degree less than or equal to n, there are only finitely many $n \times n$ matrices in rational canonical form having minimal polynomial $f(X)$. We illustrate this in the Examples below.

(v) There is a second form of the rational canonical form theorem, in which one starts with the cyclic subspace generated by a maximal vector, say v, for the entire vector space V. One then finds a T invariant complement of $\langle T, v\rangle$ and the proof then proceeds by induction as before. Fortunately, all of the hard work has already been done, and the second version of the rational canonical form theorem follows fairly painlessly from the version given above, as we will see in the next two propositions.

Proposition M. *Factor the minimal polynomial of T as $\mu_T(x) = p_1(x)^{e_1} \cdots p_k(x)^{e_k}$, with each $p_i(x)$ irreducible over F and write r for the degree of $\mu_T(x)$. Let $V = W_1 \oplus \cdots \oplus W_k$ be the corresponding primary decomposition and for each $1 \le i \le k$, let $w_i \in W_i$ be a maximal vector for $T|_{W_i}$. Then $v = w_1 + \cdots + w_k$ is a maximal vector for T if and only each w_i is a maximal vector for $T|_{W_i}$. In particular, a maximal vector for T exists, since each W_i has a maximal vector for $T|_{W_i}$, by Proposition F.*

Proof. Suppose each w_i is a maximal vector for $T|_{W_i}$. We induct on k. If $k = 1$, there is nothing to prove. Suppose $k \ge 3$, and we have proven the case $k = 2$. We can write $V = W_1 \oplus U$, where $U = W_2 \oplus \cdots \oplus W_k$, and $\mu_{T|_U(x)} = p_2(x)^{e_2} \cdots p_k^{e_k}(x)$ (by Proposition B). By induction, $w_2 + \cdots + w_k$ is a maximal vector for U and by the case $k = 2$, it follows that $w_1 + (w_2 + \cdots + w_k)$ is a maximal vector for V. Therefore, we just have to prove the case $k = 2$.

Write $v = w_1 + w_2$. We wish to show that $v, T(v), \ldots, T^{r-1}(v)$ are linearly independent, where $r = \deg \mu_T(x)$. Suppose they are not. Then there exists $h(x) \in F[x]$ with $\deg h(x) \le r-1$ and $h(T)(v) = h(T)(w_1 + w_2) = 0$. Then $h(T)(w_1) = -h(T)(w_2)$. Since $h(T)(w_1) \in W_1$, $h(T)(w_2) \in W_2$, and $W_1 \cap W_2 = 0$, it follows that $h(T)(w_1) = 0 = h(T)(w_2)$. By Proposition A (ii), $h(T)|_{W_i} = 0$, for $i = 1, 2$. But then $p_1(x)^{e_1}$ and $p_2(x)^{e_2}$ divide $h(x)$. Since these are powers of distinct irreducible polynomials, $\mu_T(x) = p_1(x)^{e_1} p_2(x)^{e_2}$ divides $h(x)$. This is a contradiction, since $\deg h(x) < \deg \mu_T(x)$. Thus, $v, T(v), \ldots, T^{r-1}(v)$ are linearly independent, and hence, v is a maximal vector for T. □

For the converse, suppose that v is a maximal vector for V. If we set $V_1 = \langle T, v\rangle$, then $\dim V_1 = \deg \mu_T(x)$, and by Proposition A, $\mu_T(x)$ is the minimal polynomial for $T|_{V_1}$. It also follows by Proposition A, that if we show that $p_i(x)^{e_i}$ is the minimal polynomial for $T|_{\langle T, w_i\rangle}$, then w_i is a maximal vector for $T|_{W_i}$. Suppose that for some i, say $i = 1$, $p_1(x)^{e_1}$ is not the minimal polynomial for $T|_{\langle T, w_1\rangle}$. Since $p_1(x)$ is irreducible, the minimal polynomial for $T|_{\langle T, w_1\rangle}$ must be of the form $p_1(x)^{e'}$, with $e' < e_1$. If we now set $f(x) := p_1(x)^{e'} p_2(x)^{e_2} \cdots p_k(x)^{e_k}$, it follows that $f(T)(w_i) = 0$, for all i and thus $f(T)(v) = 0$. But then

$f(T)(u) = 0$, for all $u \in V_1$, by Proposition A. Thus, $f(T|_{V_1}) = 0$, a contradiction, since $f(x)$ has degree less than the degree of $\mu_T(x)$ and $\mu_T(x)$ is the minimal polynomial of $T|_{V_1}$. Therefore, each w_i is a maximal vector for $T|_{W_i}$, and the proof is complete. □

Proposition N. *Suppose $v \in V$ is a maximal vector and set $V_1 := \langle T, v\rangle$. Then there exists a T-invariant subspace $U \subseteq V$ such that $V = V_1 \oplus U$. In fact, $V = V_1 \oplus \cdots \oplus V_d$, where each V_i is a cyclic subspace of V.*

Proof. Write $V = W_1 \oplus \cdots \oplus W_k$, the primary decomposition of V. By the elementary divisor form of the Rational Canonical Form Theorem, we may write each $W_i = W_{i,1} \oplus \cdots \oplus W_{i,t_i}$, where each $W_{i,j}$ is a cyclic subspace, and $W_{i,1}$ is the cyclic subspace of W_i generated by a maximal vector w_i for $T|_{W_i}$. By the previous proposition, $v = w_1 + \cdots + w_k$ is a maximal vector for T. We claim $\langle T, v\rangle = W_{1,1} \oplus \cdots \oplus W_{k,1}$. Suppose this were the case. If we set

$$U = (W_{1,2} \oplus \cdots \oplus W_{1,t_1}) \oplus \cdots \oplus (W_{k,2} \oplus \cdots \oplus W_{k,t_k}),$$

then U is a T-invariant subspace and $V = V_1 \oplus U$, as required. To prove the claim, we first note that $v \in S := W_{1,1} + \cdots + W_{k,1}$, since each $w_i \in W_{i,1}$. Moreover, S is T-invariant, so $T^c(v) \in S$, for all c which shows $\langle T, v\rangle \subseteq S$. To show $S \subseteq \langle T, v\rangle$, it suffices to shows each $W_{j,1} \subseteq \langle T, v\rangle$. Fix j and set $h(x) := \Pi_{i\neq j} p_i(x)^{e_i}$. Then $h(T)(w_i) = 0$, for all $i \neq j$. Since $h(x)$ and $p_j(x)^{e_j}$ are relatively prime, we can write $1 = a(x)h(x) + b(x)p_j(x)^{e_j}$, for some $a(x), b(x) \in F[x]$. Then

$$\begin{aligned} w_j &= a(T)h(T)(w_j) + b(T)p_j(T)^{e_j}(w_j) = a(T)h(T)(w_j) + 0 \\ &= a(T)h(T)(w_j) + a(T)h(T)(w_1) + \cdots + \hat{j} + \cdots + a(T)h(T)(w_k) \\ &= a(T)h(T)(w_1 + \cdots + w_k) \\ &= a(T)h(T)(v), \end{aligned}$$

which shows that $w_j \in \langle T, v\rangle$. Since $\langle T, v\rangle$ is T invariant, it follows that $W_{j,1} = \langle T, w_j\rangle \subseteq \langle T, v\rangle$, which proves $S \subseteq \langle T, v\rangle$. Thus, $\langle T, v\rangle = S = W_{1,1} + \cdots + W_{k,1}$. This latter sum is direct, since each $W_{j,1} \subseteq W_j$, which finishes the proof of the claim.

The second statement follows by induction in $\dim V$. By Proposition M, there exists a maximal vector $v \in V$. If we set $V_1 := \langle T, v\rangle$, then by what we have just shown, there exists a T-invariant subspace $U \subseteq V$ such that $V = V_1 \oplus U$. Applying the induction hypothesis to U complete the proof.

Theorem O. *(Rational Canonical Form Theorem via invariant factors) There exists a basis $\mathcal{B}$ of V and monic polynomials $f_1(x), \ldots, f_d(x)$ in $F[x]$ with the following properties:*

(i) $f_1(x) = \mu_T(x)$.

(ii) $f_d(x)|f_{d-1}(x)|\cdots|f_1(x)$.

(iii) The matrix of T with respect to $\mathcal{B}$ is

$$\begin{pmatrix} C(f_1(x)) & 0 & \cdots & 0 \\ 0 & C(f_2(x)) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & C(f_d(x)) \end{pmatrix}.$$

Proof. Let $v \in V$ be a maximal vector for T and set $V_1 := \langle T, v\rangle$. If $V = \langle T, v\rangle$, then we are done by Definition-Remark F. Otherwise, by Proposition N, there exists a T-invariant subspace U such that $V = V_1 \oplus U$. If r denotes the degree of $\mu_T(x)$, note that the matrix of $T|_{V_1}$ with respect to the basis $\mathcal{B}_1 := \{v, T(v), \ldots, T^{r-1}(v)\}$ is $C(\mu_T(x))$, so we take $f_1(x) = \mu_T(x)$. Moreover, since $\mu_T(T|_U) = 0$, the minimal polynomial of $T|_U$ divides $f_1(x) = \mu_T(x)$. Now, by induction on the dimension of V, the conclusions of the theorem hold for $T|_U$. Thus, if $f_2(x), \ldots, f_d(x)$ are the resulting polynomials and $\mathcal{B}_2$ is the resulting basis of U, then $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ and $f_1(x), \ldots, f_d(x)$ satisfy the conclusions of the theorem for V. □

Definition P. The polynomials $f_1(x), \ldots, f_d(x)$ in Theorem O are called the *invariant factors* of T. They are uniquely determined by T.

We now consider the case where our linear transformation T has the property that its minimal polynomial has all of its roots in F. We'll see below that the Jordan canonical form for T is lower triangular. In fact, aside from possibly having 1's below the main diagonal, the rest of its entries will be zero.

The first step towards the Jordan canonical form is a consideration of the case where all of the roots of $\mu_T(x)$ are zero. In this case $\mu_T(x) = x^e$, for some e, so $T^e = 0$. Such a transformation is said to be *nilpotent*. Similarly, a matrix B is said to be nilpotent if $B^e = 0$ for some e. The archetypal nilpotent matrix is a lower (or upper) triangular matrix with zero's down the diagonal. More explicitly, for each $s \geq 1$ let M_s denote the following $s \times s$ matrix

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

Then M_s satisfies $M_s^s = 0$ and $M_s^{s-1} \neq 0$. In other words, the minimal polynomial for M_s is x^s. We now show that any nilpotent transformation (or nilpotent matrix) can brought to block diagonal form with matrices M_s down the diagonal.

Theorem Q. *(Nilpotent Form) Assume that T is a nilpotent linear transformation with minimal polynomial x^e. Then there exists a basis $\mathcal{B}$ for V and integers $e = e_1 \geq \ldots \geq e_t$ such that A, the matrix of T with respect to $\mathcal{B}$, has the block diagonal form*

$$A = \begin{pmatrix} M_{e_1} & 0 & \cdots & 0 \\ 0 & M_{e_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M_{e_t} \end{pmatrix}.$$

Proof. We just use Theorem K to find a basis $\mathcal{B}$ such that A, the matrix of T with respect to $\mathcal{B}$ is in rational canonical form. Since the minimal polynomial of T is x^e, A has just one primary block, A itself. The primary block in turn has the block diagonal form

$$A = \begin{pmatrix} C(x^{e_1}) & 0 & \cdots & 0 \\ 0 & C(x^{e_2}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & C(x^{e_t}) \end{pmatrix},$$

with $e = e_1 \geq \cdots \geq e_t$. But a quick check reveals that $C(x^{e_i}) = M_{e_i}$, for all i, which gives what we want.

We now use Theorem Q to give us the Jordan canonical form theorem. The proof is based upon the following observation. If the minimal polynomial of T has the form $(x - \lambda)^e$, then the transformation $S := T - \lambda$ is nilpotent and can therefore be brought to nilpotent form. Interpreting this in terms of T allows us to put λ's above the 1's appearing in the nilpotent form. In fact, for $s \geq 1$ and $\lambda \in F$, we define the $s \times s$ *Jordan block associated to* λ to be the $s \times s$ matrix

$$J(s, \lambda) := \begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 \\ 1 & \lambda & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \cdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & \lambda \end{pmatrix}.$$

Theorem R. *(Jordan Canonical Form) Let $\mu_T(x)$ be the minimal polynomial of T and suppose that $\mu_T(x)$ has all of its roots in F. Write $\mu_T(x) = (x - \lambda_1)^{e_1} \cdots (x - \lambda_k)^{e_k}$. Then there exists a basis $\mathcal{B}$ for V such that A, the matrix of T with rsapect to $\mathcal{B}$, has the block diagonal form*

$$A = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_k \end{pmatrix},$$

where $A_1, \ldots, A_k$ are primary blocks corresponding to $(x - \lambda_1)^{e_1}, \ldots, (x - \lambda_k)^{e_k}$, and for each $1 \leq i \leq k$,

$$A_i = \begin{pmatrix} J(e_{i,1},\lambda_i) & 0 & \cdots & 0 \\ 0 & J(e_{i,2},\lambda_i) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J(e_{i,t_i},\lambda_i) \end{pmatrix}$$

for integers $e_i = e_{i,1} \geq e_{i,2} \geq \cdots \geq e_{i,t_i}$. We call $\{(x-\lambda_i)^{e_{i,j}}\}$, the Jordan elementary divisors of T.

Proof. By Proposition C, we may find T-invariant subspaces $W_1, \ldots, W_k \subseteq V$ such that for each $1 \leq i \leq k$, the minimal polynomial of $T|_{W_i}$ is $(x-\lambda_i)^{e_i}$. Set $S_i := (T-\lambda_i)|_{W_i}$. S_i is nilpotent, so there exists a basis $\mathcal{B}_i$ of W_i such that the matrix of S_i with respect to $\mathcal{B}_i$ equals

$$\begin{pmatrix} M_{e_{i,1}} & 0 & \cdots & 0 \\ 0 & M_{e_{i,2}} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M_{e_{i,t_i}} \end{pmatrix},$$

For $e_i = e_{i,1} \geq \cdots \geq e_{i,t_i}$. Now $T|_{W_i} = S_i + \lambda_i \cdot I_{W_i}$. Therefore, the matrix A_i of $T|_{W_i}$ with respect to $\mathcal{B}_i$ is the matrix of S_i with respect to $\mathcal{B}_i$ plus λ_i times the corresponding identity matrix, i.e.,

$$A_i = \begin{pmatrix} J(e_{i,1},\lambda_i) & 0 & \cdots & 0 \\ 0 & J(e_{i,2},\lambda_i) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J(e_{i,t_i},\lambda_i) \end{pmatrix},$$

as required. Putting together the bases $\mathcal{B}_i$ yields the required basis $\mathcal{B}$. □

Examples S. (i) Let $F = \mathbb{Q}$ and set $q(x) = (x-2)^3(x^2+1)^2$. We want to find the elementary divisor version of the rational canonical forms for all 11×11 matrices in $M_{11}(\mathbb{Q})$ having minimal polynomial $q(x)$. Since $q(x)$ has two irreducible factors, the matrices we seek have two primary blocks, each of which are to be decomposed into blocks of companion matrices associated either to a power of $x-2$ less than or equal to 3 or a power of x^2+1 less than or equal to 2. Each primary block is strictly determined by its elementary divisors, so in fact it suffices to list all possible sets of elementary divisors for 11×11 matrices having minimal polynomial $q(X)$. It turns out that there are eight possible rational canonical forms. Call these matrices $B_1, \ldots, B_8$. We assign each of these the following elementary divisors :
(a) $B_1 : (x-2)^3, (x-2)^3, (x-2), (x^2+1)^2$.
(b) $B_2 : (x-2)^3, (x-2)^2, (x-2)^2, (x^2+1)^2$.
(c) $B_3 : (x-2)^3, (x-2)^2, (x-2), (x-2), (x^2+1)^2$.
(d) $B_4 : (x-2)^3, (x-2), (x-2), (x-2), (x-2), (x^2+1)^2$.
(e) $B_5 : (x-2)^3, (x-2)^2, (x^2+1)^2, (x^2+1)$.
(f) $B_6 : (x-2)^3, (x-2), (x-2), (x^2+1)^2, (x^2+1)$.
(g) $B_7 : (x-2)^3, (x^2+1)^2, (x^2+1)^2$.
(h) $B_8 : (x-2)^3, (x^2+1)^2, (x^2+1), (x^2+1)$.
Each B_i therefore is block diagonal, with companion matrices corresponding to the listed elementary divisors down the diagonal. For example

$$B_1 = \begin{pmatrix} 0 & 0 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & -12 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 8 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -12 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

where the block diagonal entries are $C((x-2)^3)$, $C((x-2)^3)$, $C(x-2)$ and $C((x^2+1)^2)$.

(ii) The invariant factors for all 9×9 matrices having minimal polynomial $q(x)$ are:
(a) $C_1 : (x-2)^3(x^2+1), (x-2)^3, (x-2)$.
(b) $C_2 : (x-2)^3(x^2+1)^2, (x-2)^2, (x-2)^2$.
(c) $C_3 : (x-2)^3(x^2+1)^2, (x-2)^2, (x-2)(x-2)$.
(d) $C_4 : (x-2)^3(x^2+1)^2, (x-2), (x-2), (x-2)(x-2)$.
(e) $C_5 : (x-2)^3(x^2+1)^2, (x^2+1)^2$.
(f) $C_6 : (x-2)^3(x^2+1)^2, (x^2+1)(x-2)^2$.
(g) $C_7 : (x-2)^3(x^2+1)^2, (x^2+1)(x-2), (x-2)$.
(h) $C_8 : (x-2)^3(x^2+1)^2, (x^2+1), (x^2+1)$.

(iii) Set $F = \mathbb{Q}(i)$ and $q(x) = (x-2)^3(x^2+1)^2 = (x-2)^3(x+i)^2(x-i)^2$. We seek Jordan canonical forms for all 9×9 matrices having minimal polynomial $q(x)$. As before, the primary blocks are determined by their elementary divisors, though the Jordan block associated to a Jordan elementary divisor is *not* the companion matrix of the elementary divisor. For example, if the elementary divisors are $(x-2)^3, (x-2)^2, (x+i)^2, (x-i)^2$, the corresponding Jordan form has block diagonal entries $J(3,2), J(2,2), J(2,-i), J(2,i)$. Here, the first two Jordan blocks make up the primary block corresponding to $(x-2)^3$ and the second and third Jordan blocks are the primary blocks associated to $(x-i)^2$ and $(x+i)^2$. The complete list of possible Jordan elementary divisors for this example is :
(a) $C_1 : (x-2)^3, (x-2)^2, (x+i)^2, (x-i)^2$.
(b) $C_2 : (x-2)^3, (x-2), (x-2), (x+i)^2, (x-i)^2$.
(c) $C_3 : (x-2)^3, (x-2), (x+i)^2, (x+i), (x-i)^2$.
(d) $C_4 : (x-2)^3, (x-2), (x+i)^2, (x-i)^2, (x-i)$.
(e) $C_5 : (x-2)^3, (x+i)^2, (x+i)^2, (x-i)^2$.
(f) $C_6 : (x-2)^3, (x+i)^2, (x+i), (x+i), (x-i)^2$.
(g) $C_7 : (x-2)^3, (x+i)^2, (x+i), (x-i)^2, (x-i)$.
(h) $C_8 : (x-2)^3, (x+i)^2, (x-i)^2, (x-i)^2$.
(i) $C_9 : (x-2)^3, (x+i)^2, (x-i)^2, (x-i), (x-i)$.
Thus, for example,

$$C_5 = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -i & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -i & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & i & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & i \end{pmatrix}.$$

The last issue we want to discuss concerns uniqueness of the canonical forms. As before, let us factor $\mu_T(x) = p_1(x)^{e_1} \cdots p_k(x)^{e_k}$, with each $p_i(x)$ irreducible over F. Suppose that $\mathcal{B}$ and $\mathcal{B}'$ are bases such that A and A', the matrices of T with respect to $\mathcal{B}$ and $\mathcal{B}'$, are in the rational canonical form given by Theorem K. We wish to show that as long as we fix the order of the irreducible factors of $\mu_T(x)$ (equivalently, fix the order of the primary blocks associated to T), $A = A'$. Otherwise, A can be obtained from A' by permuting its primary blocks. After all, the primary blocks are defined to be matrices of T restricted to $\ker(p_i(T)^{e_i})$, for all $1 \leq i \leq k$, and are therefore uniquely determined by the factors $p_i(x)^{e_i}$. So, we fix the given order of factors in $\mu_T(x)$. Clearly, within any primary block, the structure of A and A' are uniquely determined by the corresponding elementary divisors. Thus, $A = A'$ if we prove the following Theorem.

Theorem T. *Let W be a finite dimensional vector space with linear operator T. Let $p(x)^e$ be the minimal polynomial of T. Assume that $p(x)$ is irreducible over F and $deg(p(x)^e) = r$. Suppose that $W_1, \ldots, W_t$ are T-invariant subspaces satisfying the conclusions of Theorem I. For each $1 \leq i \leq t$, let $\mathcal{B}_i$ denote the corresponding basis and $p(x)^{e_i}$ the corresponding elementary divisor (so $e = e_1 \geq \cdots \geq e_t$). Suppose, in addition, that $U_1, \ldots, U_h$ are T-invariant subspaces satisfying the conclusions of Theorem I and that for*

each $1 \leq j \leq h$, $\mathcal{U}_j := \{u_j, T(u_j), \ldots, T^{s_j-1}(u_j)\}$ is the corresponding basis and $p(x)^{f_j}$ is the corresponding elementary divisor (so $e = f_1 \geq \cdots \geq f_h$). Then $t = h$ and $e_1 = f_1, \ldots, e_t = f_t$.

Proof. Let m be the smallest positive integer such that $e_m \neq f_m$. Without loss of generality, suppose $e_m > f_m$. We now make the following claim : For all $i \leq m$,

$$\dim(p(T)^{f_m}(U_i)) = s_i - s_m \qquad \text{and} \qquad \dim(p(T)^{f_m}(W_i)) = r_i - r_m.$$

Suppose the claim holds. Since $p(T)^{f_m}(U_i) = 0$ for all $i \geq m$, it follows that

$$p(T)^{f_m}(V) = p(T)^{f_m}(U_1) \oplus \cdots \oplus p(T)^{f_m}(U_{m-1}),$$

so $\dim(p(T)^{f_m}(V)) = (s_1 - s_m) + \cdots + (s_{m-1} - s_m)$. Similarly,

$$p(T)^{f_m}(V) = p(T)^{f_m}(V_1) \oplus \cdots \oplus p(T)^{f_m}(V_{m-1}) \oplus p(T)^{f_m}(V_m),$$

so $\dim(p(T)^{f_m}(V)) = (r_1 - s_m) + \cdots + (r_{m-1} - s_m) + (r_m - s_m)$. Therefore,

$$(s_1 - s_m) + \cdots + (s_{m-1} - s_m) = (r_1 - s_m) + \cdots + (r_{m-1} - s_m) + (r_m - s_m).$$

But, $s_j = f_j \cdot \deg(p(x))$ and $r_i = e_i \cdot \deg(p(x))$, for all i and j. By our choice of m, we get $r_m - s_m = 0$, a contradiction. Thus, $e_i = f_i$ for all i and $t = h$.

To verify the claim, it clearly suffices to prove the following statement. Let W be a T-invariant subspace with basis $\{w, T(w), \ldots, T^{r-1}(w)\}$. Suppose that $p(x)^a$ ($p(x)$ irreducible) is the minimal polynomial of $T|_W$ and $\deg(p(x)^a) = r$. Suppose $b \leq a$ and $\deg(p(x)^b) = d$. Then $\dim(p(T)^b(W)) = r - d$. To see this, set $W' := p(T)^b(W)$ and $w' := p(T)^b(w)$. We will show that $\mathcal{B}' := \{w', T(w'), \ldots, T^{r-d-1}(w')\}$ is a basis for W'. Now, $p(T)^{a-b}(w') = p(T)^a(w) = 0$. Since $\deg(p(x)^{a-b}) = d - r$, $T^j(w')$ can be expressed in terms of the vectors in $\mathcal{B}'$ for all $j \geq d - r$, so $\mathcal{B}'$ spans W'. This also shows that W' is T-invariant, so the minimal polynomial of $T|_{W'}$ must divide $p(x)^{a-b}$. Let $f(x)$ denote the minimal polynomial of $T|_{W'}$. Then, $0 = f(T)(w') = f(T)p(T)^b(w)$, so $f(T|_W)p(T|_W)^b = 0$. Thus, $p(x)^a$ divides $f(x)p(x)^b$, $p(x)^{a-b}$ divides $f(x)$. Therefore, $f(x) = p(x)^{a-b}$ and it follows that $\mathcal{B}'$ is linearly independent. Hence the claim has been verified and the proof of Theorem P is now complete. □

It follows from the previous theorem that if the minimal polynomial of T has its roots in F, then the Jordan canonical form for T is unique. As before, it suffices to show that the the form taken by any primary block is unique. But the ith primary block is determined by its Jordan elementary divisors, which in turn are the elementary divisors in the rational canonical form of the nilpotent transformation $T - \lambda_i$. These latter elementary divisors are unique, by Theorem T.

Department of Mathematics, The University of Kansas, Lawrence, KS, 66045