We have two big results (stated in **(Can2)** and **(Can3)**) concerning the behaviour of a single linear transformation T of a vector space V. In particular, we have seen that it is the so-called ELEMENTARY DIVISORS and INVARIANT FACTORS which completely determine the behaviour of T. However, for the most part, we have no idea how to actually find this data. In the previous lecture **(Ch)** we introduced the characteristic polynomial as a tool for finding the minimal polynomial. We now discuss other computational ideas which will enable us to determine the other information that we need.

Let us first recall the proof of **(Ch3)**(ii) where we showed that the characteristic polynomial of the companion matrix of any monic polynomial is, in fact, that polynomial. This just involved manipulating a determinant in order to make an inductive step. Much of what we will do in this lecture has a similar flavour; we will manipulate matrices (having polynomial entries) using row and column operations. Let us begin by defining precisely which operations we will need. Let $M \in \mathbb{M}_n(\mathbb{F}[x])$, and let r and s be rows of M. Then an ELEMENTARY ROW OPERATION (ERO) on M is one of the following:

(ERO1) replace r with αr for some nonzero scalar $\alpha \in \mathbb{F}$;

(ERO2) replace r with $r + f(x)s$ for some $f(x) \in \mathbb{F}[x]$; or

(ERO3) interchange r and s.

A matrix E is an ELEMENTARY MATRIX if it can be obtained from the identity matrix by means of a single ERO. Note that, if e denotes an ERO, then $e(M) = EM$, where $E = e(I)$; hence one can effect an ERO by premultiplying by a suitable elementary matrix. We will say that matrices M and N are ROW EQUIVALENT if there is a (finite) succession of EROs taking M to N:

$$M = M_0 \rightsquigarrow M_1 \rightsquigarrow M_2 \rightsquigarrow \ldots \rightsquigarrow M_k = N.$$

Note that, if M and N are row equivalent, then $N = PM$ for some invertible $P \in \mathbb{M}_n(\mathbb{F}[x])$.

One similarly defines ELEMENTARY COLUMN OPERATIONS (ECOs) and COLUMN EQUIVALENCE of matrices. We now define matrices M and N to be EQUIVALENT (denoted $M \sim N$) if there is a (finite) succession of operations, each of which is an ERO or an ECO, taking M to N. Again, note that if M and N are equivalent, then there exist invertible matrices P and Q such that $N = PMQ$. We begin with a rather technical result which will be of use in our algorithm.

(Inv1) Lemma. *Let $M \in \mathbb{M}_n(\mathbb{F}[x])$ have some nonzero entry in its first column, and let $p(x)$ be the*

GCD of the entries in the first column. Then M is row-equivalent to a matrix N having first column

$$\begin{pmatrix} p(x) \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{1}$$

Proof. In fact, we give an algorithm to produce such an N. Initialise $M^{(0)} := M$; we will produce a suitable N, having the property stated, following a finite sequence of approximations $M^{(i)}$. Let X denote a fixed approximation of N, let γ be the first column of X and let $f_1(x), \dots, f_n(x)$ denote the entries of γ. Set

$$l(X) := \min_{f_i \neq 0}\{\deg f_i\} \quad \text{and} \quad p(X) := \gcd(f_1, \dots, f_n).$$

Let j be the smallest index such that $\deg f_j = l(X)$. The next approximation is the matrix X' obtained after the following three steps have been performed:

1. For each $1 \leq i \neq j \leq n$, use the division algorithm to find $q_i(x)$ and $r_i(x)$ such that $f_i(x) = f_j(x)q_i(x) + r_i(x)$ and $\deg r_i < \deg f_j$. As in (ERO2), subtract $q_i(x)$ times row j from row i.

2. As in (ERO1), multiply row 1 by the reciprocal of the leading coefficient of $f_j(x)$.

3. As in (ERO3), interchange rows 1 and j.

It is clear that $X' \sim X$ and that X' has first column

$$\gamma' = \begin{pmatrix} \tilde{f}_j(x) \\ r_2(x) \\ \vdots \\ r_{j-1}(x) \\ r_1(x) \\ r_{j+1}(x) \\ \vdots \\ r_m(x) \end{pmatrix}$$

where $\tilde{f}_j$ is just $f_j(x)$ divided by its leading coefficient. Furthermore, we have:

(a) $p(X') = p(X)$.

(b) Exactly one of the following holds:

   i. $0 \leq l(X') < l(X)$; or

   ii. All entries of γ' other than the first are 0.

Consider the alternative in (b)ii. Here, in view of observation (a), we have $\tilde{f}_j = \gcd(f_1, \ldots, f_n)$. In this case the procedure terminates, returning X'. If alternative (b)i. occurs, then we iterate the above procedure with the new approximation X'.

Since successive instances of (b)i. give rise to strictly decreasing, nonnegative values of the function l, it follows that after finitely many iterations (t say) we will get alternative (b)ii. In particular, the procedure will eventually terminate.

To summarise, we get a sequence $M = M^{(0)}, M^{(1)}, \ldots, M^{(t)}$ of matrices with $M^{(i)} \sim M^{(i+1)}$, $p(M^{(i)}) = p(M^{(i+1)})$ and $M^{(t)}$ has first column of the form in equation (1) with $p(x) = p(M^{(0)}) = p(M^{(t)})$. The result now follows. □

An immediate theoretical application of the Lemma is to the following important generalisation of a well-known fact concerning elements of matrix rings over fields.

(Inv2) Theorem. *For $P \in \mathbb{M}_n(\mathbb{F}[x])$ the following are equivalent:*

(i) P is invertible.

(ii) The determinant of P is a nonzero constant polynomial.

(iii) P is row equivalent to the $n \times n$ identity matrix.

(iv) P is a product of elementary matrices.

Proof. *(i)* ⇒ *(ii)* follows from the fact that the determinant function is multiplicative and the units of $\mathbb{F}[x]$ are the nonzero scalar polynomials. *(iii)* ⇒ *(iv)* and *(iv)* ⇒ *(i)* are obvious so we need only prove *(ii)* ⇒ *(iii)*.

We proceed by induction on n. The case $n = 1$ being trivial, suppose that $n > 1$, $P \in \mathbb{M}_n(\mathbb{F}[x])$ with $\det(P)$ a nonzero constant polynomial, and that the result holds for smaller matrices. Observe first, using the column expansion of the determinant, that the GCD of the entries of the first column of P divides $\det(P)$. Since the latter is a nonzero constant polynomial, it follows that the former is a unit. In particular, by **(Inv1)**, P is row equivalent to

$$Q = \begin{pmatrix} 1 & a_2 & \ldots & a_n \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}$$

Since an ERO changes the determinant of a matrix by (at most) a scalar factor, it follows that

$$\det(Q) = \det(B) \text{ is a nonzero constant polynomial.}$$

By induction, B is row equivalent to the $(n-1)\times(n-1)$ identity matrix, and the result now follows easily. □

The following consequence of **(Inv2)** is immediate.

(Inv3) Corollary. *Matrices $M, N \in \mathbb{M}_n(\mathbb{F}[x])$ are equivalent if and only if $N = PMQ$ for some invertible matrices $P, Q \in \mathbb{M}_n(\mathbb{F}[x])$.* □

Let us quickly revisit the special case where the linear transformation T acts cyclically on the vector space V. We saw here that T is represented, relative to a suitable basis, by the companion matrix $C(m_T)$ (where $m_T(x)$ is the minimal polynomial of T). We used this fact to demonstrate that $c_T(x) = m_T(x)$ by showing that $c_{C(f)}(x) = f(x)$ for any monic polynomial. We proved the latter fact using induction but it can also be deduced as a scholium to the following useful fact.

(Inv4) Lemma. *Let $f(x) \in \mathbb{F}[x]$ be a monic polynomial of degree n. Then the matrix $X_f := xI_n - C(f)$ is equivalent to*

$$\mathrm{diag}(f(x), 1, \ldots, 1).$$

Proof. Let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$. Then

$$X_f = xI_n - C(f) = \begin{pmatrix} x & -1 & 0 & \ldots & 0 \\ 0 & x & -1 & \ldots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & x & -1 \\ a_0 & a_1 & \ldots & a_{n-2} & x + a_{n-1} \end{pmatrix}$$

As in (ERO3), successively swap rows n and $n-1$, then $n-1$ and $n-2$, and so on, to obtain the equivalent matrix

$$\begin{pmatrix} a_0 & a_1 & \ldots & a_{n-2} & x + a_{n-1} \\ x & -1 & 0 & \ldots & 0 \\ 0 & x & -1 & \ldots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & x & -1 \end{pmatrix}$$

Next (using the column analogue of (ERO2)), successively add x times column n to column $n-1$, then x times column $n-1$ to column $n-2$, and so on, to obtain the equivalent matrix

$$\begin{pmatrix} f(x) & g_1(x) & \dots & g_{n-2}(x) & g_{n-1}(x) \\ 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & -1 & \dots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix},$$

where $g_i(x) = x^{n-i} + a_{n-i-1}x^{n-i-1} + \ldots + a_{i+1}x + a_i$. Finally, as in (ERO3), add $g_i(x)$ times row i to row 1 and, as in (ERO1), multiply row i by -1 $(2 \leq i \leq n)$ to obtain an equivalent matrix to X_f of the desired form. □

The next observation provides the foundation for our proposed algorithm to compute invariant factors.

(Inv5) Theorem. *Let $A \in \mathbb{M}_n(\mathbb{F})$ have invariant factors $p_1(x), \ldots, p_m(x)$. Then*

$$xI_n - A \;\sim\; \operatorname{diag}(p_1(x), p_2(x), \ldots, p_m(x), 1, \ldots, 1).$$

Proof. By **(Can3)**, there exists invertible $P \in \mathbb{M}_n(\mathbb{F})$ such that $PAP^{-1} = \operatorname{diag}(C(p_1), C(p_2), \ldots, C(p_m))$. By **(Inv3)**,

$$P(xI_n - A)P^{-1} \;=\; xI_n - PAP^{-1} \;=\; \operatorname{diag}(xI_{n_1} - C(p_1), \ldots, xI_{n_m} - C(p_m))$$

is row equivalent to A. Finally, by **(Inv4)**, each $xI_{n_j} - C(p_j)$ is row equivalent to $\operatorname{diag}(p_j(x), 1, \ldots, 1)$. The result now follows easily. □

The theorem tells us that, in theory, we can manipulate the matrix $xI - A$ using EROs and ECOs to obtain the invariant factors. Unfortunately it doesn't tell us *how* to do this. Moreover, the proof uses the RCF of A which presupposes that we have the invariant factors at hand! What we need is a reliable method for computing the invariant factors of any given A.

First some terminology. We shall say that a matrix $M \in \mathbb{M}_n(\mathbb{F}[x])$ is in NORMAL FORM if

$$N = \operatorname{diag}(f_1(x), f_2(x), \ldots, f_n(x)),$$

where $f_i(x)|f_{i+1}(x)$ for each $1 \leq i < n$. Consider the following algorithm which, for any given matrix $M \in \mathbb{M}_n(\mathbb{F}[x])$, claims to return an equivalent matrix N which is in normal form.

ALGORITHM: `NormalForm(` M `)`

INPUT: A matrix $0 \neq M \in \mathbb{M}_n(\mathbb{F}[x])$.

OUTPUT: A matrix N in normal form which is equivalent to M.

Procedure: *If $n = 1$, return M. Otherwise perform each the following steps.*

> ***Step 0:*** *Set $l(M)$ to be the minimum of the degrees of the nonzero entries of M. Find the first column having an entry with degree $l(M)$ and interchange that column with the first.*
>
> ***Step 1:*** *Run the following subroutine.*
>
> *(a) Apply* **(Inv2)** *to M so that the first* ***column*** *has entries $p(x), 0, \ldots, 0$.*
>
> *(b) If the first* ***row*** *has entries $p(x), 0, \ldots, 0$ go to step 1(d). Otherwise apply an analogue of* **(Inv2)** *so that the first row has entries $q(x), 0, \ldots, 0$.*
>
> *(c) If step 1(b) disturbed the first column (i.e. if all entries of the first column other than the first are no longer 0), go back to step 1(a). Otherwise proceed to step 1(d).*
>
> *(d) Now we have a matrix*
>
> $$N = \begin{pmatrix} g(x) & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & X & \\ 0 & & & \end{pmatrix}. \tag{2}$$
>
> *If $g(x)$ divides every entry of X then go to step 2. Otherwise find the first column which has an entry not divisible by $g(x)$, add it to the first column, and return to step 1(a).*
>
> ***Step 2:*** *Now we have a matrix N of the form in equation (2) such that $g(x)$ divides every entry of X. Recursively compute $N :=$* `NormalForm(` X `)`*, and return* diag($g(x)$, N).

end;

(Inv6) Proposition. *The procedure* `NormalForm` *terminates with an output of the desired form.*

Proof. It should be clear that if the above procedure terminates, then the output has the stated properties. It suffices to show that it does indeed terminate.

First observe, in any fixed iteration of the procedure, step 1(d) will be reached. For, a disturbance of the first column in executing step 1(b) can only occur if $\deg(q) < \deg(p)$. Since the degree of the top left entry can only decrease finitely many times, we will eventually be able to perform step 1(b) without disturbing the first column, whence the procedure proceeds to step 1(d).

Next observe, in any fixed iteration, that step 2 will be reached. For, if we reach step 1(d) and $g(x)$ does not divide each entry of X, then we return to step 1(a) with a new matrix whose first column has an entry $h(x)$ which $g(x)$ does not divide. Hence the next time the procedure reaches step 1(e), the degree of $g(x)$ will have decreased. Once again, this can only occur finitely many times, so we will eventually arrive at step 1(d) with a $g(x)$ dividing every element of X, and the procedure will then progress to the recursive step 2.

That the entire procedure terminates now follows from the fact that the number of recursive calls is $n-1$. □

> **Remark:** One can show (although we will not) that each matrix $M \in \mathbb{M}_n(\mathbb{F}[x])$ has a unique normal form. Hence, in view **(Inv5)**, for any given $A \in \mathbb{M}_n(\mathbb{F})$, `NormalForm(` $xI - A$ `)` produces a diagonal matrix from which the invariant factors of A can easily be read off. Note also that if one has an algorithm for factoring polynomials, then one can also obtain the elementary divisors of A. Innocent though it sounds, however, the problem of factoring polynomials over fields is difficult one to solve efficiently.

Exercises.

1. Suppose that you compute `NormalForm(` $xI - A$ `)` for some matrix $A \in \mathbb{M}_n(\mathbb{F})$ and get a matrix $\operatorname{diag}(f_1(x), \ldots, f_n(x))$ for which $f_1(x)$ is non-constant. What can you say about $\deg(f_1)$ and what can you say about A?
2. Let T be the linear transformation of $\mathbb{R}^8$ which is represented in the elementray basis by the matrix

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & -1 & -1 & -1 & -1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Find the characteristic polynomial and invariant factors of T ... and have fun while you work.