7.4. Computations of Invariant factors

- Let A be nxn matrix with entries in F[x].
- Goal: Find a method to compute the invariant factors $p_1,\ldots,p_r$.
- Suppose A is the companion matrix of a monic polynomial $p=x^n+c_{n-1}x^{n-1}+\ldots+c_1x+c_0$.

$$xI-A=\begin{bmatrix} x & 0 & 0 & \ldots & 0 & c_0 \\ -1 & x & 0 & \ldots & 0 & c_1 \\ 0 & -1 & x & \ldots & 0 & c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & x & c_{n-2} \\ 0 & 0 & 0 & \ldots & -1 & x+c_{n-1} \end{bmatrix}$$

$$\begin{bmatrix} x & 0 & 0 & \dots & 0 & c_0 \\ -1 & x & 0 & \dots & 0 & c_1 \\ 0 & -1 & x & \dots & 0 & c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & x^2 + c_{n-1}x + c_{n-2} \\ 0 & 0 & 0 & \dots & -1 & x + c_{n-1} \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & x^n + \dots + c_1 x + c_0 \\ -1 & 0 & 0 & \dots & 0 & x^{n-1} + \dots + c_2 x + c_1 \\ 0 & -1 & 0 & \dots & 0 & x^{n-2} + \dots + c_3 x + c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & x^2 + c_{n-1}x + c_{n-2} \\ 0 & 0 & 0 & \dots & -1 & x + c_{n-1} \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & 0 & \dots & 0 & p = x^n + \dots + c_1 x + c_0 \\ -1 & 0 & 0 & \dots & 0 & 0 \\ 0 & -1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & -1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & p = x^n + \dots + c_1 x + c_0 \\ -1 & 0 & 0 & \dots & 0 & 0 \\ 0 & -1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & -1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} p & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix}$$

- Thus det(xI-A)=p.
- Elementary row operations in $F[x]^{nxn}$.

1. Multiplication of one row of M by a nonzero scalar in F.
2. Replacement of row r by row r plus f times row s. ($r \neq s$)
3. Interchange of two rows in M.

- nxn-elementrary matrix is one obtained from Identity marix by a single row operation.
- Given an elementary operation e.
  - e(M)=e(I)M.
  - $M=M_0$->M_1->….->M_k=N row equivalences N=PM where $P=E_1 \ldots E_k$.
  - P is invertible and $P^{-1}=E^{-1}{}_k \ldots . E^{-1}{}_1$ where the inverse of an elementary matrix is elementary and in $F[x]^{nxn}$.

- Lemma. M in $F[x]^{mxn}$.
  - A nonzero entry in its first column.
  - Let p=g.c.d(column 1 entries).
  - Then M is row-equivalent to N with (p,0,…,0) as the first column.
- Proof: omit. Use Euclidean algorithms.
- Theorem 6. P in $F[x]^{mxm}$. TFAE
  1. P is invertible.
  2. det P is a nonzero scalar in F.
  3. P is row equivalent to mxm identity matrix.
  4. P is a product of elementary matrix.

- Proof: 1->2 done. 2->1 also done.
- We show 1->2->3->4->1.
- 3->4,4->1 clear.
- (2->3) Let $p_1,..,p_m$ be the entries of the first column of P.
  - Then $\gcd(p_1,..,p_m)=1$ since any common divisor of them also divides det P. (By determinant formula).
  - Now use the lemma to put 1 on the (1,1)-position and (i,1)-entries are all zero for i>1.

- Take (m-1)x(m-1)-matrix M(1|1).
- Make the (1,1)-entry of M(1|1) equal to 1 and make (i,1)-entry be 0 for i > 1.
- By induction, we obtain an upper triangular matrix R with diagonal entries equal to 1.
- R is equivalent to I by row-operations--clear.

- Corollary: M,N in $F[x]^{nxn}$. N is row-equivalent to M <-> N=PM for invertible P.

- Definition: N is equivalent to M if N can be obtained from M by a series of elementary row-operations or elementary column-operations.

- Theorem 7. N=PMQ, P, Q invertible <-> M, N are equivalent.
- Proof: omit.

- Theorem 8. A nxn-matrix with entry in F. p_1, …,p_r invariant factors of A. Then matrix xI-A is equivalent to nxn-diagonal matrix with entries p_1,..,p_r,1,…,1.
- Proof: There is invertible P with entries in F s.t. PAP^{-1} is in rational form with companion matrices A_1,..,A_r in block-diagonals.
  - $P(xI-A)P^{-1}$ is a matrix with block diagonals $xI-A_1$, …,$xI-A_r$.
  - $xI-A_i$ is equivalent to a diagonal matrix with entries p_i,1,…,1.
  - Rearrange to get the desired diagonal matrix.

- This is not algorithmic. We need an algorithm. We do it by obtaining Smith normal form and showing that it is unique.
- Definition: N in $F[x]^{mxn}$. N is in Smith normal form if

1. Every entry off diagonal is 0.
2. Diaonal entries are $f_1,\ldots,f_l$ s.t. f_k divides f_{k+1} for k=1,..,l-1 where l is min{m,n}.

- Theorem 9. M in $F[x]^{mxn}$. Then M is equivalent to a matrix in normal form.
- Proof: If M=0, done. We show that if M is not zero, then M is equivalent to M' of form:

$$\begin{bmatrix} f_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & R & \\ 0 & & & \end{bmatrix}$$

- where f_1 divides every entries of R.
- This will prove our theorem.

- Steps: (1) Find the nonzero entry with lowest degree. Move to the first column.
- (2) Make the first column of form (p,0,..,0).
- (3) The first row is of form (p,a,…,b).
- (3') If p divides a,..,b, then we can make the first row (p,0,…,0) and be done.
- (4) Do column operations to make the first row into (g,0,…,0) where g is the gcd(p,a, …,b). Now deg g < deg p.
- (5) Now go to (1)->(4). deg of M strictly decreases. Thus, the process stops and ends at (3') at some point.

- If g divide every entry of S, then done.
- If not, we find the first column with an entry not divisible by g. Then add that column to the first column.
- Do the process all over again. Deg of M strictly decreases.
- So finally, the steps stop and we have the desired matrix.

- The uniqueness of the Smith normal form. *(To be sure we found the invariant factors.)*
- Define $\delta_k(M)$ = g.c.d.{det of all kxk-submatrices of M}.
- Theorem 10. M,N in $F[x]^{mxn}$. If M,N are equivalent, then $\delta_k(M)= \delta_k(N)$.
- Proof: elementary row or column operations do not change δ_k.

- Corollary. Each matrix M in $F[x]^{mxn}$ is equivalent to precisely one matrix N which is in normal form.
- The polynomials $f_1,\ldots,f_k$ occuring in the normal form are
- $$f_k = \frac{\delta_k(M)}{\delta_{k-1}(M)}, 1 \le k \le \min\{m,n\}$$

  where $\delta_0(M):=1$.
- Proof: $\delta_k(N) = f_1 f_2 \ldots f_k$ if N is in normal form and by the invariance.