An Outline of Module Theory

S. Kumaresan
School of Math. and Stat.
University of Hyderabad
Hyderabad 500046
kumaresa@gmail.com

1 Basic Notions of Modules

1. Definition of a left R-module.

2. Examples

   (a) A vector space over a field.

   (b) R or more generally a left ideal of R as an R-module.

   (c) R^n as an R-module.

   (d) Any abelian group as a $\mathbb{Z}$-module.

   (e) Let $T\colon V \to V$ be a linear map of a vector space over F. Then V as an $F[x]$ module via T: $f(x)v := f(T)(v)$.

   (f) Let G be an abelian group. Let $R = \operatorname{End} G$. Then G is an R-module.

   (g) Let V be a vector space over R. Let $R := \operatorname{End} V$. Then V is an R-module.

   The last two examples are bi-modules(meaning?). We may consider $ngf := (ng)f$ which is the same as $n(gf)$ Similar remarks apply to αvf where $\alpha \in F$ and $f \in \operatorname{End} V$.

3. Submodules: Definition.

4. Examples of Submodules

   (a) Submodules of $\mathbb{Z}$-modules

   (b) Submodules of V as an $F[x]$ module via T.

   (c) Submodule $\langle S \rangle$ generated by a subset $S \subset M$.

   (d) Finitely generated (FG) and cyclic submodules

5. R-maps (or R-homomorphisms) between R-modules.

6. Image and kernel of an R-map.

7. Quotient module.

8. First fundamental theorem for an R-map.

9. Annihilator of an R-module $\mathrm{Ann}\,(M)$.

10. Let M be cyclic. Then $M \simeq R/\mathrm{Ann}\,(M)$.

11. Let M be finitely generated.

    (a) When do we say $\{x_1, \ldots, x_r\}$ freely generate M?

    (b) What do we mean by M is a (FG) free module? Equivalent formulations.

12. Direct sums of modules.

2 Structure Theorems for Finitely Generated Modules over a Euclidean Domain

1. Smith Normal Form over a Euclidean domain.

2. Theorem: *Let R be a Euclidean domain and M be a free module of rank m. Let $N \leq M$ be a submodule. Then there exist elements $x_1, \ldots, x_m$ of M, a natural number r and positive integers $d_1, \ldots, d_r$ such that*
   (i) *M is freely generated by $\{x_1, \ldots, x_m\}$;*
   (ii) *$d_1x_1, d_2x_2, \ldots, d_rx_r$ freely generate N;*
   (iii) *d_j divided d_{j+1} for $1 \leq j < r$.*

   Outline of Proof.
   Assume that N is finitely generated. If n is the rank of M, we assume that $M = R^n$ with the natural basis. Let $x_1, \ldots, x_m$ be generators of N. Each of these is an element of R^n and hence can be written as a row vector and hence we obtain an $m \times n$ matrix, say A, with entries in R.

   Let $\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$ be the Smith nomal form of A. Let D be the diagonal matrix with entries $d_1, \ldots, d_r$ with $d_i | d_{i+1}$. Let N' be the submodule generated by the row vectors of the normal form. We claim that $N = N'$.

   To establish the claim, we need only show that the (admissible) elementary row and column operations on A produce the same submodule.

   It is easy to see that any (admissible elementary) row operation results in a change of the generating set for N.

   It is again easy to see that any (admissible elementary) column operation results in a change of the standard basis of R^n to another basis of R^n.

   We now show that N is FG. The proof is by induction on n, the case $n = 0$ being obviously true.

   Consider

   $$J := \{r \in R : \exists\, r_2, \ldots, r_n \in R \text{ such that } (r_1, r_2, \ldots, r_n) \in N\}.$$

   Then J is a (necessarily principal) ideal, say $J = (a)$.

Since $a \in J$, there exist $b_2, \dots, b_n \in R$ such that $(a, b_2, \dots, b_n) \in N$. Let

$$N_1 := \{(r_1, \dots, r_n) \in N : r_1 = 0\}.$$

Then N_1 is a submodule. We claim that N_1 and $(a, b_2, \dots, b_n)$ generate N. For, if $(r_1, r_2, \dots, r_n) \in N$, then $r_1 = ra$, as $r_1 \in J = (a)$. We have

$$(r_1, r_2, \dots, r_n) - s(a, b_2, \dots, b_n) \in N_1.$$

Since N_1 is a submodule of R^{n-1}, by induction, it is FG. The result follows.

3. Theorem: *Let R be a Euclidean domain and M be a finitely generated R-module. Then there exist elements $d_1, \dots, d_n$ of R and an integer $r \in \mathbb{Z}_+$ such that*
   (i) *none of the d_i's are units;*
   (ii) *d_i divided d_{i+1} for $1 \leq i \leq r-1$;*
   (iii) *$d_i = 0$ for $i > r$;*
   (iv) *$M \simeq R/\langle d_1 \rangle \oplus \cdots \oplus R/\langle d_m \rangle$.*

   If d_i is a unit, it will appear in the beginning due the divisibility condition. In such a case, $R/\langle d_i \rangle = 0$ and so we can remove all the units from the sequence $d_1, \dots, d_m$.

   Let M be FG, say, by $x_1, \dots, x_n$. Consider the map

   $$f \colon R^n \to M \text{ defined by } f(r_1, \dots, r_n) := r_1 x_1 + \cdots + r_n x_n.$$

   We have $\operatorname{Im} f = M$ and the kernel N is FG. Let $e_1, \dots, e_n$ denote the standard basis for R^n. Then by the last item, there exist a basis $\{\$e_1, \dots, e_n\}$ of R^n and elements $d_i \in R$, $1 \leq i \leq r$ such that (i) $\{d_1 e_1, d_r e_r\}$ generate N and (ii) $d_i | d_{i+1}$, for $1 \leq i \leq r-1$. We claim that $M \simeq (f(e_1)) \oplus \cdots \oplus (f(e_n))$, a direct sum of the cyclic submodules $(f(e_i))$ and we have $\operatorname{Ann}(f(e_i)) = (d_i)$. In particular,

   $$M \simeq R/(d_1) \oplus \cdots \oplus R/(d_r).$$

4. Let R be a PID. Let M be an R-module with $\operatorname{Ann}(M) = (r)$ with $r \neq 0$. Assume that $r = pq$ with p and q coprime. Let $M_p := \{x \in M : px = 0\}$ and $M_q := \{x \in M : qx = 0\}$. Then $M \simeq M_p \oplus M_q$.

5. Theorem: *Let R be a PID and M an R-module. Let $Ann(M) = (r)$. Let $r = p_1^{m_1} \cdots p_n^{m_n}$ be the irreducible decomposition. Then*

   $$M = M_1 \oplus \cdots M_n \quad \textit{where} \quad M_i := \{x \in M : p_i^{m_i} x = 0\}.$$

6. Let M be a finitely generated torsion module over a Euclidean domain. Then M is isomorphic to a direct sum of cyclic submodules whose annihilators are (p^m) where p is an irreducible element of R.

   The generators p^m are called the elementary divisors of M. These are the factors arise when the invariant factors are factorized into irreducibles.

7. Uniqueness of elementary divisors.

   Assume that M is expressed in two different ways as a direct sum of cyclic submodules whose annihilators are powers of irreducibles. Then the annihilators are unique up to associates.

   Enough to prove this when $\operatorname{Ann}(M)$ is a prime power. If N is a cyclic submodule whose annihilator is (p^n), (p, a prime), then N is contained in the p-primary component which is uniquely determined.

   Assume $\operatorname{Ann}(M) = (p^n)$, p a prime. Let $M = M_1 \oplus \cdots \oplus M_k$ where M_i is a cyclic module whose annihilator is (p^{n_i}) where $1 \leq n_i \leq n$. Since (p) is a maximal ideal in R, the quotient $R/(p)$ is a field, say F. Consider the submodule pM. It is easy to see that M/pM is a vector space over F in an obvious manner. The cosets of x_i, a generator of M_i from a basis of M/pM and hence its dimension over F is k.

   Now, assume that $n_i > 1$ for $1 \leq i \leq k_1$ and $n_r = 1$ for $k_1 < r \leq k$. Then pM is the direct sum of cyclic submodules generated by $px_1, \ldots, px_{k_1}$. Note that since $px_r = 0$ for $r > n_1$, they generate the zero modules and hence may be ignored. Hence $\dim pM/p^2M = k_1$ as an F-vector space.

   In a similar fashion, we see that $\dim p^jM/p^{j+1}M$ is the number of elements $n_1, \ldots, n_k$ which are greater than j.

   The last observation we need is the following: if we are told how many of $n_1, \ldots, n_k$ are greater than j for each $j \geq 0$, we can recover n_i's.

   For example, if the dimensions of $p^jM/p^{j+1}M$ for $0 \leq j \leq 4$ are respectively 8,4,3,1,0, then there are eight n_i's and they are 1,1,1,1,2,4,4,5.

3 Finitely Generated Abelian Groups

1. Let G be a finitely generated abelian group. Then
$$G \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r} \oplus \mathbb{Z} \cdots \oplus \mathbb{Z},$$
where $d_i \in \mathbb{N}$ for $1 \leq i \leq r$ and $d_i | d_{i+1}$ for $1 \leq i \leq r-1$.

2. Let G be a finitely generated abelian group. Assume that G admits two decompositions as in the last item:
$$\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r} \oplus \mathbb{Z} \cdots \oplus \mathbb{Z} \simeq G \simeq \mathbb{Z}_{t_1} \oplus \cdots \oplus \mathbb{Z}_{t_s} \oplus \mathbb{Z} \cdots \oplus \mathbb{Z}$$
Then $r = s$ and the numbers of components isomorphic to $\mathbb{Z}$ in the both the decompositions are the same.

3. Let p be a prime. The number of non-isomorphic abelian groups of order p^m is $p(m)$, the number of partitions of m.

4. Let $n = p_1^{m_1} \cdots p_k^{m_k}$. Then the number of non-isomorphic abelian groups of order n is $p(m_1) \cdots p(m_k)$.

5. Examples. Let us classify all abelian groups of order 60 (up to isomorphim). We have $60 = 2^2 \times 3 \times 5$. For the prime 2, its exponent is 2 and $p(2) = 2$: $2 = 2, 1 + 1$. The exponents of the other primes are 1 and hence the number of non-isomorphic abelian groups of order is $p(2) \times p(2) \times p(1) = 2$. We do similar exercises for abelian groups of orders 38, 108, 144. We tabulate them below.

Ord.	**Elem.Div.**	**Prim.Decomp.**	**Inv.Factor Dec.**	**Inv. Factors**
60	$2^2, 3, 1$	$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	$\mathbb{Z}_{60}$	60
	$2, 2, 3, 1$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	$\mathbb{Z}_2 \times \mathbb{Z}_{30}$	$30, 2.$
36	$2^2, 3^2$	$\mathbb{Z}_4 \times \mathbb{Z}_9$	$\mathbb{Z}_{36}$	36
	$2^2, 3, 3$	$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_{12}$	$3, 12$
	$2, 2, 3^2$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$	$\mathbb{Z}_2 \times \mathbb{Z}_{18}$	$2, 18$
	$2, 2, 3, 3$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_6 \times \mathbb{Z}_6$	$6, 6$
108	$2^2, 3^3$	$\mathbb{Z}_4 \times \mathbb{Z}_{27}$	$\mathbb{Z}_{108}$	108
	$2^2, 3^2, 3$	$\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_{36}$	$3, 36$
	$2^2, 3, 3, 3$	$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{12}$	$3, 3, 12$
	$2, 2, 3^3$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27}$	$\mathbb{Z}_2 \times \mathbb{Z}_{54}$	$2, 54$
	$2, 2, 3^2, 3$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_3$	$\mathbb{Z}_6 \times \mathbb{Z}_{18}$	$6, 18$
	$2, 2, 3, 3, 3$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_6$	$3, 6, 6$
144	$2^4, 3^2$	$\mathbb{Z}_{16} \times \mathbb{Z}_9$	$\mathbb{Z}_{144}$	144
	$2^4, 3, 3$	$\mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_{48}$	$3, 48$
	$2^3, 2, 3^2$	$\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_9$	$Z_2 \times \mathbb{Z}_{72}$	$2, 72$
	$2^3, 2, 3, 3$	$\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_6 \times \mathbb{Z}_{24}$	$6, 24$
	$2^2, 2^2, 3^2$	$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_9$	$\mathbb{Z}_4 \times \mathbb{Z}_{36}$	$4, 36$
	$2^2, 2^2, 3, 3$	$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_{12} \times \mathbb{Z}_{12}$	$12, 12$
	$2^2, 2, 2, 3^2$	$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{36}$	$2, 2, 36$
	$2^2, 2, 2, 3, 3$	$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{12}$	$2, 6, 12$
	$2, 2, 2, 2, 3^2$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{18}$	$2, 2, 2, 18$
	$2, 2, 2, 2, 3, 3$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_6$	$2, 2, 6, 6$
180	$2^2, 3^2, 5$	$\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$	$\mathbb{Z}_{180}$	180
	$2^2, 3, 3, 5$	$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	$\mathbb{Z}_3 \times \mathbb{Z}_{180}$	$3, 60$
	$2, 2, 3^2, 5$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$	$\mathbb{Z}_2 \times \mathbb{Z}_{90}$	$2, 90$
	$2, 2, 3, 3, 5$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	$\mathbb{Z}_6 \times \mathbb{Z}_{30}$	$6, 30$
360	$2^3, 3^2, 5$	$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$	$\mathbb{Z}_{360}$	360
	$2^3, 3, 3, 5$	$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	$\mathbb{Z}_3 \times \mathbb{Z}_{120}$	$3, 120$
	$2^2, 2, 3^2, 5$	$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$	$\mathbb{Z}_2 \times \mathbb{Z}_{180}$	$2, 180$
	$2^2, 2, 3, 3, 5$	$Z_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	$\mathbb{Z}_6 \times \mathbb{Z}_{60}$	$6, 60$
	$2, 2, 2, 3^2, 5$	$Z_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{90}$	$2, 2, 90$
	$2, 2, 2, 3, 3, 5$	$Z_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	$\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{30}$	$2, 6, 30$

Exercise: Write down similar table for abelian groups of order 1008. Do you see how to read the last column (invariant factors) from the second column (elementary divisors) without writing the intermediate columns of groups?

6. Exercises

Ex. 1. What is the smallest $n \in \mathbb{N}$ such that there are exactly 3 non-isomorphic abelian groups of order n?

Ex. 2. Prove that any abelian group of order 45 has an element of order 15. Can you make a similar statement for 9 in place of 15?

Ex. 3. Let G be an abelian group. Assume that G has exactly three elements of order 2. Identify G.

Ex. 4. Let G be a finite abelian group whose order is square free. Prove that G is cyclic.

Ex. 5. Let G be a finite abelian group. Prove that G is cyclic iff for every prime divisor p of $|G|$, there exist exactly p elements of order p.

Ex. 6. Let G be a finite subgroup of the multiplicative group F^* of a field F. Prove that G is cyclic.

Ex. 7. Let G be an abelian group of order n. Prove that for any divisor d of n, there exists a subgroup of order n.

4 Normal Forms of Matrices

1. Let V be a cyclic $F[x]$-module via T, say, generated by v. Let $\dim V = n$. Then the elements $v, Tv, \dots T^{n_1}v$ form a basis of V. Let $T^n v = -(a_0 v + a_1 Tv + \cdots + T^{n-1}v)$ and $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$. The matrix A of T relative to this ordered basis is the companion matrix $C(f)$ of f:

$$C(f) := \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & -a_{n-2} \\ 0 & 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}$$

2. Let V be the $F[x]$ module via T. Assume that $\mathrm{Ann}\,(V) = (g^m)$. We now select a more suitable basis to simplify the matrix of T:

$$\begin{array}{lllll} v & Tv & T^2v & \dots & T^{m-1}v \\ g(T)v & g(T)Tv & g(T)T^2v & \dots & g(T)T^{m-1}v \\ \vdots & \vdots & \vdots & \vdots & \\ g(T)^{r-1}v & g(T)^{r-1}\circ Tv & g(T)^{r-1}\circ T^2v & \dots & g(T)^{r-1}\cdot T^{m-1}v. \end{array}$$

Thus, if we let $w_{ij} := g(T)^{j-1}T^{i-1}v$, the ordered basis is

$$w_{11}, w_{21}, \dots, w_{m1}, w_{12}, w_{22}, \dots, w_{m2}, \dots, w_{1r}, w_{2r}, \dots, w_{mr}.$$

The matrix of T relative to this basis is

$$C(m,g) := \begin{pmatrix} C(g) & & & & \\ A & C(g) & & & \\ & A & C(g) & & \\ & & \ddots & \ddots & \\ & & & A & C(g) \end{pmatrix},$$

where $C(g)$ is the companion $m \times m$ matrix of g and A is an $m \times m$ matrix whose $(1m)$-th entry is 1 and the rest are zero:

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Let $g(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + x^n$. Note that T maps each vector to the next element in the row except the last element of the row. To see where the last elements of the row go, observe that

$$\begin{aligned} T(T^{n-1}(v) &= T^n(v) = g(T)(v) - (c_0 v + c_1 Tv + \cdots + c_{n-1}T^{n-1}v) \\ T(g(T)^{r-j})(T^{n-1}(v)) &= (g(T)^{r-j}(T^n(v)) \\ &= T(g(T)^{r-j})\left(c_0 v + c_1 Tv + \cdots + c_{n-1}T^{n-1}v\right) \\ &= -c_0(g(T)^{r-j}(v) - \cdots - c_{n-1}(g(T)^{r-j})(T^{n-1}v) + g(T)^{r-j+1}(v). \end{aligned}$$

3. **Rational Canonical Form: Invariant Factors Version**
   Let $T\colon V \to V$ be a linear map. We consider it as an $F[x]$-module via T. Let $d_i(x)$, $1 \leq i \leq r$ be the invariant factors of the module. Then there exists an (ordered) basis of V relative to which the matrix of T is a block diagonal matrix with entries $C(d_i)$ and zeros elsewhere.

4. **Rational Canonical Form: Elementary Divisors Version**
   If the elementary divisors of the module are $g_1^{m_1}, \dots, g_k(x)^{m_k}$, then there is a basis of V relative to which the matrix of T is a block diagonal matrix with $C(m_1, g_1), \dots, C(m_k, g_k)$ as the diagonal entries and zeros elsewhere.

5. A very special case of the last item is when the field F is algebraically closed. The elementary divisors are irreducible polynomials and hence they are of the form $(x-a)^m$. The matrix $C(m, x-a)$ is the Jordan block of size $m \times m$:

$$J(m;a) := \begin{pmatrix} a & 0 & 0 & \dots & 0 \\ 1 & a & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & \dots & a & 0 \\ 0 & 0 & \dots & 1 & a \end{pmatrix}$$

Lemma 8. *Let $g(x) \in F[x]$. Then the characteristic polynomial of $C(g)$ is g.*

Proof. by induction on the degree of g. Use Laplace expansion. □

Theorem 9 (Cayley-Hamilton)**.**

Proposition 10. *Let $g(x) = (x-a)^m$. Then $C(g)$ is similar to $J(m, a)$.*

Proof. If we define $Tv := C(g)v$ where $v \in F^m$, then V is a cyclic $F[x]$ module via T with a basis $\{e_1, Te_1, \dots, T^{m-1}e_1\}$.

Let $B := \{u_1 := e_1, u_2 := (T-aI)u_1, \dots, u_m := (T-aI)^{m-1}e_1\}$. Since $T^ie_1 \in LS(\{u_1, \dots, u_i\})$, the set spans V and hence is a basis of V. What is the matrix of T relative to this basis? If $j \leq m$,

Check the suffixes.

$$\begin{aligned} Tu_j &= T(T-aI)^{j-1}e_1 \\ &= (T-aI)^{j-1}Te_1 \\ &= (T-aI)^{j-1}(aI + (T-aI))e_1 \\ &= a(T-aI)^{j-1}e_1 + (T-aI)^je_1. \end{aligned}$$

In particular, if $j < m$, we have $Tu_j = au_j + u_{j+1}$ and $Tu_m = au_m$. Thus the matrix of T relative to this basis is the Jordan block $J(m, a)$. Since $C(g)$ and $J(m, a)$ represent the same linear map T, the matrices are similar. □