20250525 MATH4302 Assignment 3

(1) Solution: For the following $\mathbb{F}_2[x]$-entry matrix:

$$A=\begin{pmatrix} x+1 & x & 1 \\ x & 0 & x \\ x & 1 & x^2 \end{pmatrix}$$

Step 1: All 1×1 minors of A are $x+1, x, 1, x, 0, x, x, 1, x^2$

Hence, the ideal $I_1(A)$ generated by them has a single generator:

$m_1(A) = \gcd(x+1, x, 1, 0, x^2) = 1$

Step 2: All 2×2 minors of A are:

$$\begin{vmatrix} x+1 & x \\ x & 0 \end{vmatrix} = -x^2 = x^2, \quad \begin{vmatrix} x+1 & 1 \\ x & x \end{vmatrix} = x^2, \quad \begin{vmatrix} x & 1 \\ 0 & x \end{vmatrix} = x^2$$

$$\begin{vmatrix} x+1 & x \\ x & 1 \end{vmatrix} = -x^2+x+1 = x^2+x+1, \quad \begin{vmatrix} x+1 & 1 \\ x & x^2 \end{vmatrix} = x^3+x^2-x = x^3+x^2+x, \quad \begin{vmatrix} x & 1 \\ 1 & x^2 \end{vmatrix} = x^3-1 = x^3+1$$

$$\begin{vmatrix} x & 0 \\ x & 1 \end{vmatrix} = x, \quad \begin{vmatrix} x & x \\ x & x^2 \end{vmatrix} = x^3-x^2 = x^3+x^2, \quad \begin{vmatrix} 0 & x \\ 1 & x^2 \end{vmatrix} = -x = x.$$

Hence, the ideal $I_2(A)$ generated by them has a single generator:

$m_2(A) = \gcd(x^2, \underline{x^2+x+1}, x^3+x^2+x, x^3+1, \underline{x}, x^3+x^2) = 1.$

irreducible in $\mathbb{F}_2[x]$. $-\infty < \mathrm{Deg}(x) < 2$

Step 3: All 3×3 minors of A are:

$$\begin{vmatrix} x+1 & x & 1 \\ x & 0 & x \\ x & 1 & x^2 \end{vmatrix} = 0 + x^3 + x - 0 - (x^2+x) - x^4 = -x^4+x^3-x^2 = x^4+x^3+x^2$$

Hence, the ideal $I_3(A)$ generated by them has a single generator:

$m_3(A) = \gcd(x^4+x^3+x^2) = x^4+x^3+x^2$

To conclude, the invariant factors of A are:

$$d_1 = m_1 = 1,\ d_2 = m_2/m_1 = 1/1 = 1,\ d_3 = m_3/m_2 = (x^4+x^3+x^2)/1 = x^4+x^3+x^2.$$

The Smith Normal Form of A is:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^4+x^3+x^2 \end{pmatrix}$$

Of course, we may also compute this by reduction.

$$A = \begin{pmatrix} x+1 & x & 1 \\ x & 0 & x \\ x & 1 & x^2 \end{pmatrix}$$

$$A_1 = AP_1 = \begin{pmatrix} x+1 & x & 1 \\ x & 0 & x \\ x & 1 & x^2 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & x & x+1 \\ x & 0 & x \\ x^2 & 1 & x \end{pmatrix}$$

$$A_2 = P_2A_1 = \begin{pmatrix} 1 & 0 & 0 \\ -x & 1 & 0 \\ -x^2 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x & x+1 \\ x & 0 & x \\ x^2 & 1 & x \end{pmatrix} = \begin{pmatrix} 1 & x & x+1 \\ 0 & x^2 & x^2 \\ 0 & x^3+1 & x^3+x^2+x \end{pmatrix}$$

$$A_3 = A_2P_3 = \begin{pmatrix} 1 & x & x+1 \\ 0 & x^2 & x^2 \\ 0 & x^3+1 & x^3+x^2+x \end{pmatrix}\begin{pmatrix} 1 & -x & -x-1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x^2 & x^2 \\ 0 & x^3+1 & x^3+x^2+x \end{pmatrix}$$

$$\gcd(x^2, x^3+1) = 1, \quad (-x)(x^2)+(1)(x^3+1) = 1$$

$$A_4 = A_3P_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x^2 & x^2 \\ 0 & x^3+1 & x^3+x^2+x \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x^2 & 0 \\ 0 & x^3+1 & x^2+x+1 \end{pmatrix}$$

$$A_5 = P_5A_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -x & 1 \\ 0 & -x^3-1 & x^2 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & x^2 & 0 \\ 0 & x^3+1 & x^2+x+1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & x^3+x+1 \\ 0 & 0 & x^4+x^3+x^2 \end{pmatrix}$$

$$A_6 = A_5P_6 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & x^3+x+1 \\ 0 & 0 & x^4+x^3+x^2 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -x^2-x-1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^4+x^3+x^2 \end{pmatrix}$$

$$A_6 = A_5P_6 = P_5A_4P_6 = P_5A_3P_4P_6 = P_5A_2P_3P_4P_6 = P_5P_2A_1P_3P_4P_6$$
$$= P_5P_2AP_1P_3P_4P_6 = PAQ.$$

$$P = P_5P_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -x & 1 \\ 0 & -x^3-1 & x^2 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ -x & 1 & 0 \\ -x^2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & x & 1 \\ x & x^3+1 & x^2 \end{pmatrix}$$

$$Q = P_1P_3P_4P_6 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & -x & -x-1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -x^2-x-1 \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & -x & -x-1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & x^2+x \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & x^2+x \\ 1 & x & x^3+1 \end{pmatrix}.$$

(2)

1) $\gcd(2,3)=1$, $(-1)\cdot(2)+(1)\cdot(3)=1$, $\overbrace{\begin{pmatrix} -1 & 1 \\ -3 & 2 \end{pmatrix}}^{\det=1}\begin{pmatrix} 2 \\ 3 \end{pmatrix}\overbrace{(1)}^{\det=1} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

2) $\gcd(2,2)=2$ $(1)\cdot(2)+(0)\cdot(2)=2$,
$\gcd(2,4)=2$, $(1)\cdot(2)+(0)\cdot(4)=2$ $\overbrace{\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}}^{\det=1}\begin{pmatrix} 2 & 4 \\ 2 & 2 \end{pmatrix}\overbrace{\begin{pmatrix} 1 & +2 \\ 0 & -1 \end{pmatrix}}^{\det=-1} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$

(3) Proof: Assume that R is a nonzero commutative ring with identity, such that every submodule of every free R-module is free.

Take an arbitrary ideal I of R. As $\{\vec 0\} = R\vec 0$ is principal, assume WLOG that $I \neq \{\vec 0\}$

Step 1: We prove that I has a basis $\mathcal{B}_I$.

R has a basis $\{\vec 1\}$ $\Rightarrow$ R is a free R-module
I is an ideal of R $\Rightarrow$ I is a submodule of R
$\Bigg\}\Rightarrow I$ has a basis $\mathcal{B}_I$.

Step 2: As $I \neq \{0\}$, $|\mathcal{B}_I| > 0$, it remains to prove that $|\mathcal{B}_I| < 2$. ($\neq 0$).

Assume to the contrary that I contains two R-linearly independent $\vec r_1, \vec r_2 \in \mathcal{B}_I$.

now R contains two R-linearly independent $\vec r_1, \vec r_2$, contradicting to $\underbrace{\vec r_2}_{\neq 0}\vec r_1 - \underbrace{\vec r_1}_{\neq 0}\vec r_2 = \vec 0$.

Hence, $|\mathcal{B}_I| = 1$, I is principal.

(4) Proof: Assume that $M=\langle\vec{m}\rangle$ is a cyclic R-module, and N is a submodule of M. As $\{\vec{0}\}=\langle\vec{0}\rangle$ is cyclic, assume WLOG that $N\neq\{\vec{0}\}$.

Define $Count=\{\overset{\substack{\mathbb{Z}\\ \rotatebox{90}{$\in$}}}{|c|}>0 : \overset{\substack{R\\ \rotatebox{90}{$\in$}}}{c}\overset{\substack{M\\ \rotatebox{90}{$\in$}}}{\vec{m}}\in N\}$. As $N\neq\{\vec{0}\}$, $Count\neq\emptyset$.

As $Count$ is bounded below by 1, $Count$ has a minimum, say, $\overset{\substack{\mathbb{Z}\\ \rotatebox{90}{$\in$}}}{n}$.

By minimality, $N=\langle\overset{\substack{R\\ \rotatebox{90}{$\in$}}}{n}\overset{\substack{M\\ \rotatebox{90}{$\in$}}}{\vec{m}}\rangle$ is cyclic. Here, we identify $\overset{\substack{\mathbb{Z}\\ \rotatebox{90}{$\in$}}}{n}=\overset{\substack{\mathbb{Z}\\ \rotatebox{90}{$\in$}}}{1}+\cdots+1$ with $\overset{\substack{R\\ \rotatebox{90}{$\in$}}}{n}=\overset{\substack{R\\ \rotatebox{90}{$\in$}}}{1}+\cdots+1$.

(5) Proof: As V is a vector space, it is an Abelian group:

$$(\vec{v}_1+\vec{v}_2)+\vec{v}_3=\vec{v}_1+(\vec{v}_2+\vec{v}_3)$$
$$\vec{v}_1+\vec{v}_2=\vec{v}_2+\vec{v}_1$$
$$\vec{0}+\vec{v}=\vec{v}$$
$$(-\vec{v})+\vec{v}=\vec{0}$$

As T is an endomorphism on V, there is a scalar multiplication:

$$\left(\sum_{i=0}^{m}\alpha_i x^i\sum_{j=0}^{n}\beta_j x^j\right)\vec{v}=\sum_{i,j=0,0}^{m,n}\alpha_i\beta_j x^{i+j}\vec{v}$$
$$=\sum_{i,j=0,0}^{m,n}\alpha_i\beta_j T^{i+j}\vec{v}=\sum_{i=0}^{m}\alpha_i T^i\left(\sum_{j=0}^{n}\beta_j T^j\vec{v}\right)=\sum_{i=0}^{m}\alpha_i x^i\left(\sum_{j=0}^{n}\beta_j x^j\vec{v}\right)$$

$$1\vec{v}=I\vec{v}=\vec{v}$$

$$\left(\sum_{i=0}^{m}\alpha_i x^i+\sum_{j=0}^{n}\beta_j x^j\right)\vec{v}=\sum_{k=0}^{\max\{m,n\}}(\alpha_k+\beta_k)x^k\vec{v}$$
$$=\sum_{k=0}^{\max\{m,n\}}(\alpha_k+\beta_k)T^k\vec{v}=\sum_{i=0}^{m}\alpha_i T^i\vec{v}+\sum_{j=0}^{n}\beta_j T^j\vec{v}=\sum_{i=0}^{m}\alpha_i x^i\vec{v}+\sum_{j=0}^{n}\beta_j x^j\vec{v}$$

$$\sum_{i=0}^{m}\alpha_i x^i(\vec{v}_1+\vec{v}_2)=\sum_{i=0}^{m}\alpha_i T^i(\vec{v}_1+\vec{v}_2)=\sum_{i=0}^{m}\alpha_i T^i\vec{v}_1+\sum_{i=0}^{m}\alpha_i T^i\vec{v}_2$$
$$=\sum_{i=0}^{m}\alpha_i x^i\vec{v}_1+\sum_{i=0}^{m}\alpha_i x^i\vec{v}_2$$

As V is finite-dimensional, it is a finite K-span, thus a finite $K[x]$-span.

As T is an endomorphism on a finite-dimensional space V, T has a minimal polynomial $f(x) \neq 0$, so every element $\vec{v}$ annihilates when acted by $f(x)$, it is torsioned.

(6). Proof: $\vec{0} \in N_1 \Rightarrow \vec{0} \in \bigcup_{i=1}^{+\infty} N_i$

$\vec{v}_i \in N_i$ and $\vec{v}_j \in N_j \Rightarrow \vec{v}_i + \vec{v}_j \in N_{\max\{i,j\}} \subseteq \bigcup_{i=1}^{+\infty} N_i$.

$\vec{v}_i \in N_i \Rightarrow -\vec{v}_i \in N_i \subseteq \bigcup_{i=1}^{+\infty} N_i$

Hence, $\bigcup_{i=1}^{+\infty} N_i = \{\vec{v} \in M : \vec{v} \text{ belongs to some } N_i\}$ is a sub-module of M.

(7) Proof: ϕ_n is a well-defined function $\Leftrightarrow \left(\forall m_1, m_2 \in \mathbb{Z}, \overset{\text{consider their difference}}{\overbrace{m_1 = m_2}} (\text{mod } n) \Rightarrow \phi_n(m_1) = \phi_n(m_2)\right)$

$\Leftrightarrow \left(\forall m \in \mathbb{Z}, m \equiv 0 (\text{mod } n) \Rightarrow \phi_n(m) = 0\right) \Leftrightarrow \underset{A}{\underset{\Psi}{n}}\,\underset{A}{\underset{\Psi}{a}} = \underset{A}{\underset{\Psi}{0}}$.

Here, we assumed that ϕ_n is a homomorphism iff it is well-defined function.

This is the case, because $\phi_n(k_1+k_2) = (k_1+k_2)a = k_1a + k_2a = \phi_n(k_1) + \phi_n(k_2)$.

Let's proceed to prove that the two $\mathbb{Z}$-modules $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$, A_n are isomorphic. To do so, construct a map: $\sigma: \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \to A_n, \psi_n \mapsto \psi_n(1)$.

This map is well-defined, because $n \cdot \psi_n(1) = \psi_n(n \cdot 1) = \psi_n(0) = 0$, $\psi_n(1) \in A_n$.

This map is a homomorphism, because $\sigma(\psi_n + \theta_n) = (\psi_n + \theta_n)(1) = \psi_n(1) + \theta_n(1) = \sigma(\psi_n) + \sigma(\theta_n)$

$\sigma(k\psi_n) = (k\psi_n)(1) = k\psi_n(1) = k\sigma(\psi_n)$.

This map is injective, because $\sigma(\psi_n) = 0 \Rightarrow \forall k \in \mathbb{Z}/n\mathbb{Z}, \psi_n(k) = k\psi_n(1) = k\sigma(\psi_n) = 0 \Rightarrow \psi_n = 0$

This map is surjective, because $\forall a \in A_n, \exists \phi_n \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A), \sigma(\phi_n) = a$

Hence, σ is an isomorphism.

(8) Proof: Define a function $\sigma : \mathbb{Z} \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}), \sigma(k) = \phi_k$.

Here, $\phi_k : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is defined by $\phi_k(l) = k \cdot \left[\frac{n}{(m,n)}\right] \cdot \left[\frac{m}{(m,n)}\right]^{-1} \cdot l$,

where $\left[\frac{m}{(m,n)}\right]^{-1}$ is an inverse of $\frac{m}{(m,n)}$ in $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

This map ϕ_k is well-defined, because $\frac{m}{(m,n)}, n$ are coprime, $\left[\frac{m}{(m,n)}\right]^{-1}$ exists, and:

$l_1 \equiv l_2 \pmod{m} \Rightarrow \phi(l_1) \equiv \phi(l_2) \pmod{n}$,

$\phi_k(l_1+l_2) = k\left[\frac{n}{(m,n)}\right]\left[\frac{m}{(m,n)}\right]^{-1}(l_1+l_2) = k\left[\frac{n}{(m,n)}\right]\left[\frac{m}{(m,n)}\right]^{-1} l_1 + k\left[\frac{n}{(m,n)}\right]\left[\frac{m}{(m,n)}\right]^{-1} l_2 = \phi_k(l_1) + \phi_k(l_2)$,

$\phi_k(\lambda l) = k\left[\frac{n}{(m,n)}\right]\left[\frac{m}{(m,n)}\right]^{-1}(\lambda l) = \lambda\left(k\left[\frac{n}{(m,n)}\right]\left[\frac{m}{(m,n)}\right]^{-1} l\right) = \lambda \phi_k(l)$, $\phi_k \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$

This map σ is a homomorphism, because:

$\phi_{k_1+k_2}(l) = (k_1+k_2)\left[\frac{n}{(m,n)}\right]\left[\frac{m}{(m,n)}\right]^{-1} l = k_1\left[\frac{n}{(m,n)}\right]\left[\frac{m}{(m,n)}\right]^{-1} l + k_2\left[\frac{n}{(m,n)}\right]\left[\frac{m}{(m,n)}\right]^{-1} l = \phi_{k_1}(l) + \phi_{k_2}(l)$

$\phi_{\lambda k}(l) = (\lambda k)\left[\frac{n}{(m,n)}\right]\left[\frac{m}{(m,n)}\right]^{-1} l = \lambda\left(k\left[\frac{n}{(m,n)}\right]\left[\frac{m}{(m,n)}\right]^{-1} l\right) = \lambda \phi_k(l)$,

This map σ has kernel $(m,n)\mathbb{Z}$, because:

$\phi_k = 0 \Leftrightarrow \phi_k(1) = k\left[\frac{n}{(m,n)}\right]\left[\frac{m}{(m,n)}\right]^{-1} = 0 \Leftrightarrow k$ is divisible by (m,n).

This map σ is surjective, because:

$\psi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \Rightarrow$ The order of $\psi(1)$ divides (m,n)

$\Rightarrow (m,n)\psi(1)$ is a multiple of $n \Rightarrow \psi = \phi_k$

Hence, it follows from the first isomorphism theorem that:

$$\mathbb{Z}/(m,n)\mathbb{Z} \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$$

When $m=30, n=21$, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/30\mathbb{Z}, \mathbb{Z}/21\mathbb{Z})$ has three elements:

$\phi_0 : l \mapsto 0 \cdot 7 \cdot 10^{-1} \cdot l = 0$, $\phi_1 : l \mapsto 1 \cdot 7 \cdot 10^{-1} \cdot l = 7l$, $\phi_2 : l \mapsto 2 \cdot 7 \cdot 10^{-1} \cdot l = 14l$.

(9). Solution: Recall that column space is invariant under column transformations.

$$\begin{pmatrix} -7 & 0 & -6 \\ 6 & 3 & 0 \\ 6 & 0 & 6 \end{pmatrix} \xrightarrow{\text{Column①+Column②}*(-2)} \begin{pmatrix} -7 & 0 & -6 \\ 0 & 3 & 0 \\ 6 & 0 & 6 \end{pmatrix} \xrightarrow{\text{Column①+Column③}*(-1)}$$

$$\begin{pmatrix} -1 & 0 & -6 \\ 0 & 3 & 0 \\ 0 & 0 & 6 \end{pmatrix} \xrightarrow{\text{Column①}*(-1)} \begin{pmatrix} 1 & 0 & -6 \\ 0 & 3 & 0 \\ 0 & 0 & 6 \end{pmatrix} \xrightarrow{\text{Column③+Column①}*(6)}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

. Hence, we not only computed the smith normal form of A, but also give an explicit characterization of $\mathrm{Col}(A) \cong \mathbb{Z} \times 3\mathbb{Z} \times 6\mathbb{Z}$.

Now $\mathbb{Z}^3/N = (\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z})/(\mathbb{Z}\times 3\mathbb{Z}\times 6\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$

(10) Proof:

N is finitely generated $\Rightarrow$ N has a spanning set $S = \{\vec{s}_1, \vec{s}_2, \cdots, \vec{s}_\mu\}$.

M/N is finitely generated $\Rightarrow$ M/N has a spanning set $T = \{\vec{t}_1 + N, \vec{t}_2 + N, \cdots, \vec{t}_\nu + N\}$.

Hence, M has a spanning set $\{\vec{s}_1, \vec{s}_2, \cdots, \vec{s}_\mu, \vec{t}_1, \vec{t}_2, \cdots, \vec{t}_\nu\}$, so M is finitely generated.