Name: Tuan Pham
ID: 4652218

Math 8202: General Algebra

Homework #2

10/10.

(1) Problem 9, Lang, p. 546.

Let E be an n-dimensional vector space over a field k. Suppose that $T: E \to E$ is a linear map with $T^m = 0$ for some number m. We'll show that there exists a basis $\mathcal{B}$ of E such that $M_{\mathcal{B}}(T)$ is strictly upper triangular.

We can assume that m was chosen to be the smallest nonnegative integer such that $T^m = 0$. In case $m = 0$, we get $id_E = T^0 = 0$. Then $E = \{0\}$ and $T = id_E : \{0\} \to \{0\}$. The only basis of E is $\mathcal{B} = \phi$. Then '$M_\phi(T)$' doesn't have any meaning! Thus we consider only the case $m \geq 1$. If $m = 1$ then $T \equiv 0$. Then $M_{\mathcal{B}}(T) = 0$ for any choice of basis $\mathcal{B}$. The zero matrix is strictly upper triangular. Now we consider the case $m \geq 2$.

By the observation that $Tu = 0$ implies $T^2 u = 0$, we have

$$0 \subset \ker T \subset \ker T^2 \subset \dots \subset \ker T^{m-1} \subset \ker T^m = E.$$

We'll show that $\ker T^{l-1} \neq \ker T^l$ for $1 \leq l \leq m$. Suppose by contradiction that $\ker T^{l-1} = \ker T^l$ for some $1 \leq l \leq m$. Then for every $u \in \ker T^{l+1}$, $T^{l+1}(u) = 0$. Thus $Tu \in \ker T^l = \ker T^{l-1}$. Thus $T^l u = 0$. Thus $u \in \ker T^l$. Thus $\ker T^{l+1} \subset \ker T^l$. Then $\ker T^l = \ker T^{l+1}$. Applying this result again and again, we get

2

$\ker T^{l-1} = \ker T^{l} = \ker T^{l+1} = \cdots = \ker T^{m} = E$. This is a contradiction because m was chosen such that m is minimal nonnegative integer satisfying $T^m = 0$. Therefore $\ker T^{l-1} \subsetneq \ker T^{l}$ for all $1 \le l \le m$. Because E is a vector space, each $\ker T^{l-1}$ has a direct summand in $\ker T^{l}$. We put

$$V_0 = \ker T, \quad \ker T = V_0,$$

$$\ker T^2 = \ker T \oplus V_1,$$

$$\ker T^3 = \ker T^2 \oplus V_2,$$

$$\vdots$$

$$\ker T^m = \ker T^{m-1} \oplus V_{m-1}.$$

Then $V_0, V_1 \cdots, V_{m-1} \neq \{0\}$ and $E = V_0 \oplus V_1 \oplus \cdots \oplus V_{m-1}$. Let

$\{e_i \mid 0 = k_0 < i \le k_1\}$ be a basis of V_0,

$\{e_i \mid k_1 < i \le k_2\}$ be a basis of V_1,

$\cdots$

$\{e_i \mid k_{m-1} < i \le k_m = n\}$ be a basis of V_{m-1}.

Then $\mathcal{B} = \{e_1, e_2 \cdots, e_n\}$ is a basis of E. We'll show that $M_{\mathcal{B}}(T)$ is strictly upper triangular. For each $i = 1, 2 \cdots, n$, there is an index j such that $k_j < i \le k_{j+1}$. Then $e_i \in V_j \subset \ker T^{j+1}$. Then $T^{j+1}(e_i) = 0$. Then

$$Te_i \in \ker T^{j} = V_0 \oplus \cdots \oplus V_{j-1}.$$

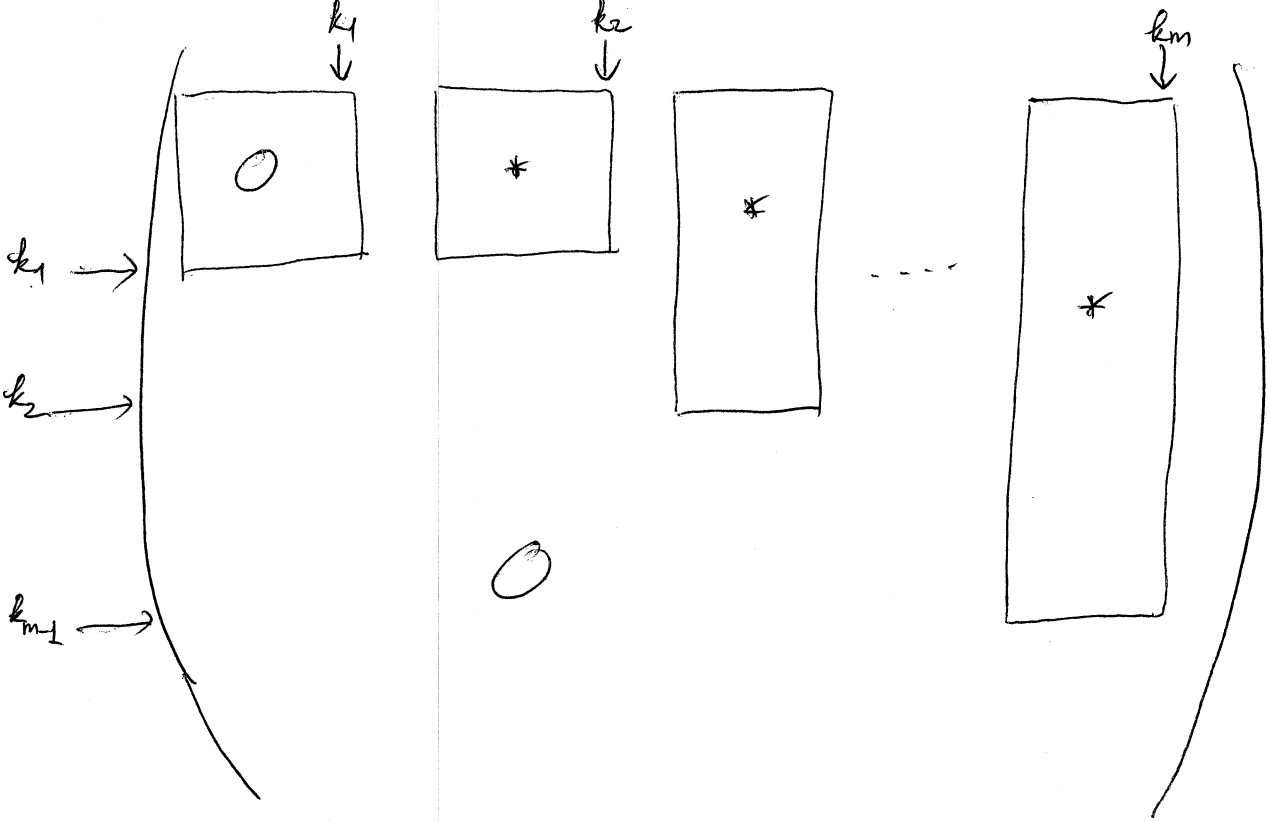
If $j = 0$ then $Te_i = 0$.

If $j \ge 1$ then Te_i is a linear combination of $\{e_s \mid 0 < s \le k_j\}$. Thus the column vector $[Te_i]_{\mathcal{B}}$ has the following form

$$[Te_i]_\beta = \begin{pmatrix} * \\ \vdots \\ * \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow k_j$$

Thus if we put the matrix $M = (m_{ij})_{1 \le i,j \le n} = M_\beta(T) = ([Te_1]_\beta \cdots [Te_n]_\beta)$ then $m_{ri} = 0$ for every $r > k_j$. Since $i > k_j$, we get $m_{ri} = 0$ for every $r \ge i$.

Thus M is strictly upper triangular.



② Problem 10, Lang, p. 546

Let N be a nilpotent $n \times n$ matrix, (say $N^m = 0$ for some $m \ge 1$). We'll show that $I_n + N$ is invertible. We have $N^{2m} = 0$. Thus

$$I_n = I_n - N^{2m} = (I_n - N^2)(I_n + N^2 + \cdots + N^{2m-2})$$
$$= (I_n - N)(I_n + N)(I_n + N^2 + \cdots + N^{2m-2})$$

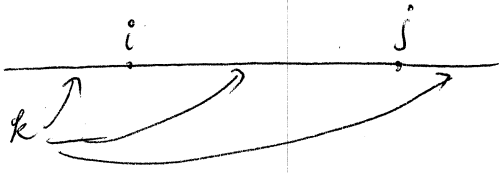
Thus I_n+N is invertible and its inverse is $(I_n-N)(I_n+N^2+\dots+N^{2m-2})$.

(3) Problem 12, Lang, p. 546.

Let k be a field and G be the subset of $GL(n,k)$ containing all upper triangular matrices with non-zero diagonal elements. (Every matrix in G is invertible because its determinant is the product of all elements on the diagonal, which is nonzero and hence a unit). We'll show that G is a subgroup of $GL(n,k)$ with respect to the matrix multiplication.

For $A, B \in G$, we put $C=AB$. Then for $1\le i,j\le n$,

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$



Since A and B are upper triangular, $a_{ik}=0$ if $i>k$, $b_{kj}=0$ if $k>j$. Thus if $i>j$ then $a_{ik}=0$ or $b_{kj}=0$ for all $k=1,\dots,n$.

thus $c_{ij}=0$ for $i>j$. Thus C is upper triangular. Since ~~C is~~ $\det(C)=\det(A)\det(B)\neq 0$, every diagonal element of C is nonzero. Thus $C\in G$. For $A\in G$, we'll show that $A^{-1}\in G$. It suffices to show that A^{-1} is upper triangular. The adjoint matrix of A is $A^* = (\Gamma_{ij})$ with $\Gamma_{ij} = (-1)^{i+j}\det(A_{ij})$ where A_{ij} is the matrix obtained by omitting the i'th row and the j'th column of A. For $i<j$, A_{ij} is upper triangular with one zero coefficient on the diagonal. Thus $\det(A_{ij})=0$ and $\Gamma_{ij}=0$. Thus,

A^* is lower triangular. We have $A^{-1} = \frac{1}{\det(A)} {}^tA^*$. Therefore A^{-1} is ~~lower~~ upper triangular. We've proved that G is a subgroup of $GL(n,k)$.

Let H be the subset of G containing all matrices with one's on the diagonal. We'll show that H is a subgroup of G. For $A, B \in G$ and $C = AB$ we know that $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$

Then $c_{ii} = \sum_{k=1}^{n} a_{ik} b_{ki} = a_{ii} b_{ii}$ (because A, B are upper triangular).

In case $A, B \in H$, $a_{ii} = b_{ii} = 1 \ \forall i$. Thus $c_{ii} = 1 \ \forall i$. Thus $C \in H$. Now for $A \in H$ and $B = A^{-1}$, we have $(I_n)_{ij} = a_{ii} b_{ii}$. Thus $1 = 1 \cdot b_{ii} = b_{ii}$. Thus $B \in H$. Therefore, H is a subgroup of G.

Next, we'll show that H is a normal subgroup of G. For $A \in H$, $B \in G$, we have $C = B^{-1}AB \in G$. On the diagonal, the multiplication is simply termwise. Thus $c_{ii} = b_{ii}^{-1} a_{ii} b_{ii} = a_{ii} = 1$. Thus $C \in H$. Thus H is normal in G. Put K to be the subset of G containing all diagonal matrices with nonzero diagonal elements. Then K is a subgroup of G and $K \simeq (k \setminus \{0\})^n$ as multiplicative groups. We see that $H \cap K = \{I_n\}$. We will show that $G = HK$. For $C = (c_{ij}) \in G$, we put $B = (b_{ij})$ with $b_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ c_{ii} & \text{if } i = j \end{cases}$.

We put the matrix $A = (a_{ij}) \in G$ with $a_{ij} = c_{ij} c_{jj}^{-1}$ for all $1 \leq i, j \leq n$.

Then $a_{ii} = c_{ii} c_{ii}^{-1} = 1$. Thus $A \in H$. We have

$$\sum_{k=1}^{n} a_{ik} b_{kj} = a_{ij} b_{jj} \quad (\text{because } b_{kj} = 0 \text{ if } k \neq j)$$

$$= c_{ij} \underbrace{c_{jj}^{-1} b_{jj}}_{1}$$

$$= c_{ij}$$

Thus $C = AB$. Therefore $G = HK$.

Good

Then we have a canonical group isomorphism $HK/H \simeq K/(K \cap H) \simeq K$.

Thus $G/H \simeq K \simeq (k \setminus \{0\})^n$.

④ Problem 13, Lang, p. 568.

Let E be an n-dimensional vector space over a field k, and let $S \in \mathrm{End}_k(E)$.

Consider the following k-algebra homomorphism $\varphi : k[t] \longrightarrow \mathrm{End}_k(E)$, $t \mapsto S$.

Then φ makes E a $k[t]$-module.

(a) Suppose that S is diagonalizable, we'll show that its minimal polynomial over k is of type $q(t) = \prod_{i=1}^{m} (t - \lambda_i)$, where $\lambda_1, \ldots, \lambda_m$ are distinct elements of k.

Because S is diagonalizable, there exists a basis $\mathcal{B} = \{e_1, \ldots, e_n\}$ of E such that $M_{\mathcal{B}}(S)$ is diagonal. After exchanging rows and columns, we can assume that $M_{\mathcal{B}}(S)$ is of the form:

$$M_{\mathcal{B}}(S) = \begin{pmatrix} \begin{matrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_1 \end{matrix} & & & 0 \\ & \begin{matrix} \lambda_2 & & 0 \\ & \ddots & \\ 0 & & \lambda_2 \end{matrix} & & \\ 0 & & \ddots & \\ & & & \begin{matrix} \lambda_m & & 0 \\ & \ddots & \\ 0 & & \lambda_m \end{matrix} \end{pmatrix}$$

where $\lambda_1, \dots, \lambda_m$ are distinct.

n_1, n_2, $n_m = n$

Then we have $Se_i = \lambda_1 e_i$ for $n_0 = 0 < i \leq n_1$,

$Se_i = \lambda_2 e_i$ for $n_1 < i \leq n_2$,

- - - -

$Se_i = \lambda_m e_i$ for $n_{m-1} < i \leq n_m = n$.

For each $i = 1, \dots, m$, we put $F_i = \{v \in E \mid (S - \lambda_i)v = 0\}$. Because $S - \lambda_i$ is a k-linear map, F_i is a vector space over k. Moreover, for each $v \in F_i$, we have

$$(S - \lambda_i)Sv = S(S - \lambda_i)v \quad \text{(because } E \text{ is a } k[t]\text{-module, and } k[t] \text{ is commutative)}$$

$$= S(0) = 0$$

Thus $Sv \in F_i$. Therefore F_i is S-invariant, i.e. F_i is a $k[t]$-submodule of E. We have $e_\ell \in F_i$ for $n_{i-1} < \ell \leq n_i$. We'll show that these e_ℓ's form a k-basis for F_i. It suffices to prove the claim for $i = 1$. The proof for other i's follows by the same argument. For each $v \in F_1$, we write $v = c_1 e_1 + \dots + c_n e_n$ with $c_1, \dots, c_n \in k$. Then

$$0=(S-\lambda_1)v=(S-\lambda_1)(c_1e_1+\cdots+c_ne_n)$$

$$=\sum_{k=1}^{n}(c_kSe_k-\lambda_1c_ke_k)$$

$$=\sum_{k=n_0+1}^{n_1}\underbrace{(c_kSe_k-\lambda_1c_ke_k)}_{0}+\sum_{k=n_1+1}^{n_2}(c_kSe_k-\lambda_1c_ke_k)+\cdots+\sum_{k=n_{m-1}+1}^{n_m}(c_kSe_k-\lambda_1c_ke_k)$$

$$=\sum_{k=n_1+1}^{n_2}c_k(\lambda_2-\lambda_1)e_k+\cdots+\sum_{k=n_{m-1}+1}^{n_m}c_k(\lambda_m-\lambda_1)e_k$$

Since $\{e_1,\dots,e_n\}$ is k-linearly independent, $c_k(\lambda_2-\lambda_1)=0$ for $n_1<k\le n_2$,

$\cdots\qquad\cdots$

$c_k(\lambda_m-\lambda_1)=0$ for $n_{m-1}<k\le n_m$.

Since $\lambda_2,\dots,\lambda_m\neq\lambda_1$, $c_k=0$ for all $k>n_1$. Thus v is just a linear combination of $e_1,\dots,e_{n_1}$. Thus $\{e_1,\dots,e_{n_1}\}$ is a k-basis for F_1.

What we've shown lead to $E=F_1\oplus\cdots\oplus F_m$ as k-modules. We know that each F_i is also a $k[t]$-submodule of E. Then $E=F_1+\cdots+F_m$ as $k[t]$-modules because $k\subset k[t]$. We'll show that this sum is also a direct sum as $k[t]$-modules. By the definition of F_i, we have

$$F_i=\{v\in E\mid(t-\lambda_i)v=0\}\simeq k[t]/(t-\lambda_i)$$

Since $(t-\lambda_i)$ is a maximal ideal of $k[t]$, F_i is a simple $k[t]$-module. Take $v\in F_1\setminus\{0\}$. Then $(t-\lambda_1)v=0$. For $2\le i\le m$, $(t-\lambda_i)v=\underbrace{(t-\lambda_1)v}_{0}+\underbrace{(\lambda_1-\lambda_i)v}_{\neq 0}\neq 0$.

Thus $v\notin F_i$. Thus $F_1,\dots,F_m$ are all distinct. Thus we have the direct sum $E=F_1\oplus\cdots\oplus F_m$ as $k[t]$-modules.

Then $E \simeq k[t]/(t-\lambda_1) \oplus \cdots \oplus k[t]/(t-\lambda_m)$

$\simeq k[t]/q(t)$ by Chinese's Remainder theorem, where

$q(t) = (t-\lambda_1)\cdots(t-\lambda_m)$.

Thus $q(t)$ is the (monic) minimal polynomial that annihilates E as a $k[t]$-module. Thus $q(t)$ is the minimal polynomial of the presentation (E, S).

(b) Now assuming that (E, S) has the minimal polynomial as above, where $\lambda_1, \ldots, \lambda_m$ are distinct. We'll show that S is diagonalizable.

Because $q(t) = (t-\lambda_1)\cdots(t-\lambda_m)$. is an exponent of E as a $k[t]$-module, by the structure theorem of finitely-generated torsion module over PID, we have

$$E \simeq k[t]/(t-\lambda_1) \oplus \cdots \oplus k[t]/(t-\lambda_m).$$

Thus there exist $k[t]$-submodules $F_1, \ldots, F_m$ of E such that $E = F_1 \oplus \cdots \oplus F_m$ as $k[t]$-modules. Since $k \subset k[t]$, each F_i is also a k-submodule of E. By the same ~~reason~~ reason, the sum $F_1 + \cdots + F_m$ is also direct as k-modules. We'll show that $E = F_1 + \cdots + F_m$ as k-modules. Because $E = F_1 + \cdots + F_m$ as $k[t]$-modules, for each $v \in E$, there are ~~$r_1(t), \ldots, r_m(t) \in k[t]$~~ $f_1, \ldots, f_m \in F$ such that

$$v = \cancel{r_1(t) f_1 + \cdots + r_\ell(t) f_\ell} \; f_1 + \cdots + f_m$$

~~for some $f_1, \ldots, f_\ell \in$~~ Thus $E = F_1 + \cdots + F_m$ as k-modules. Therefore we have $E = F_1 \oplus \cdots \oplus F_m$ as k-modules.

Let $\{e_i \mid n_0 = 0 < i \le n_1\}$ be a k-basis of F_1,

$\{e_i \mid n_1 < i \le n_2\}$ be a k-basis of F_2,

- - - -

$\{e_i \mid n_{m-1} < i \le n_m = n\}$ be a k-basis of F_m.

Then $\mathcal{B} = \{e_1, \dots, e_n\}$ is a basis of E. We have $S e_i = \lambda_j = e_i$ where $n_{j-1} < i \le n_j$. Therefore, the matrix representing S in basis $\mathcal{B}$ is diagonal, which has λ_j's on its diagonal. Thus S is diagonalizable.

(c) Let F be a subspace of E that is S-invariant. Suppose that S is diagonalizable as an endomorphism of E. We'll show that S is also diagonalizable as an endomorphism of F.

Because S is diagonalizable as an endomorphism of E, in part (a) we showed that (E, S) has the minimal polynomial $q(t) = (t-\lambda_1)\cdots(t-\lambda_m)$ where $\lambda_1, \dots, \lambda_m$ are distinct. Moreover, we showed in part (a) by using Structure Theorem for finitely-generated torsion module over $k[t]$ that $E \simeq k[t]/q(t)$ as $k[t]$-modules. Because F is a $k[t]$-submodule of E, $F \simeq U/q(t)$ where U is an ideal of $k[t]$ containing $q(t)$. Since $k[t]$ is a PID, $U = (\tilde{q}(t))$ for some polynomial $\tilde{q}(t)$. Because $q(t) \in (\tilde{q}(t))$, $\tilde{q}(t) \mid q(t)$. Thus there is a polynomial $r(t)$ such that $q(t) = \tilde{q}(t) r(t)$. Then $r(t)$ is also of the form $(t-\beta_1)\cdots(t-\beta_k)$ with $\beta_1, \dots, \beta_k$ distinct.

⑤ Let E be an n-dimensional vector space over k, which is an algebraically closed field. Let $A \in \mathrm{End}_k(E)$. We'll show that A can be written as $A = S+N$ where
$$\begin{cases} S \text{ is diagonalizable,} \\ N \text{ is nilpotent,} \\ S \circ N = N \circ S, \\ S \text{ and } N \text{ are polynomials of } A. \end{cases}$$

As usual, we consider the representation of $k[t]$ in E, namely a k-algebra homomorphism $\varphi : k[t] \longrightarrow \mathrm{End}_k(E)$,
$$t \longmapsto A.$$

This ring homomorphism allows us to consider E as a $k[t]$-module. Let $q(t)$ be the minimal polynomial of the presentation (E, A). Because k is algebraically closed, we can write $q(t) = (t-\lambda_1)^{k_1} \cdots (t-\lambda_m)^{k_m}$, where $\lambda_1, \dots, \lambda_m$ are distinct and $k_1, \dots, k_m \geq 1$. Note that the case $q(t) \equiv 1$ implies $E = 1 \cdot E = q(t)E = 0$. Then A is the zero endomorphism. Then S and N can be chosen as trivial endomorphisms.

Because $t-\lambda_1, \dots, t-\lambda_m$ are distinct primes of $k[t]$, we got the prime power factorization of $q(t)$ on $k[t]$. Because $q(t)$ is an exponent of E as a $k[t]$-module, we can apply the structure theorem for finitely-generated torsion module E over the PID $k[t]$. Then

Then F_i is a vector space over k due to the linearity of $(S-\lambda_i)$. For each $v \in F_i$, we have $S(Tv) = T(Sv) = T(\lambda_i v) = \lambda_i (Tv)$.

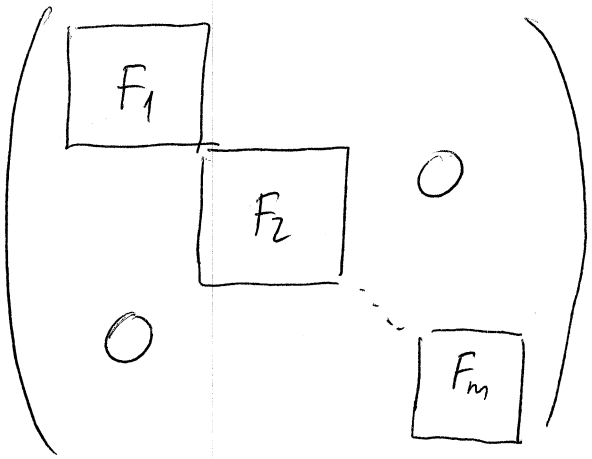
Thus $Tv \in F_i$. Therefore $T(F_i) \subset F_i$. This means each F_i is T-invariant. We know that T is diagonalizable as an endomorphism of E. By part (c), T is also diagonalizable as an endomorphism of F_i. By the definition of F_i and the matrix (*), each F_i is an $(n_i - n_{i-1})$-dimensional vectorspace over k. Then there exists a k-basis $\mathcal{B}_i = (e_{n_{i-1}+1}, \dots, e_{n_i})$ of F_i such that $M_{\mathcal{B}_i}(T|_{F_i})$ is diagonal. Then we obtain a basis $\mathcal{B}$ of E by concatenating $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_m$. The representation matrix of T of this basis is of the form

$$M_{\mathcal{B}}(T) = \begin{pmatrix} \boxed{M_{\mathcal{B}_1}(T|_{F_1})} & & & 0 \\ & \boxed{M_{\mathcal{B}_2}(T|_{F_2})} & & \\ & & \ddots & \\ 0 & & & \boxed{M_{\mathcal{B}_m}(T|_{F_m})} \end{pmatrix}$$

Since each block is diagonal, $M_{\mathcal{B}}(T)$ is also diagonal. On each F_i, $Sv = \lambda_i v$. Thus, $M_{\mathcal{B}_i}(S|_{F_i}) = \begin{pmatrix} \lambda_i & & 0 \\ & \ddots & \\ 0 & & \lambda_i \end{pmatrix}$.

Therefore, $M_{\mathcal{B}}(S)$ is exactly of the form (*). Therefore, both $M_{\mathcal{B}}(S)$ and $M_{\mathcal{B}}(T)$ are diagonal.

Because $k \subset k[t]$, each F_i is also a k-module. Thus we get $E = F_1 \oplus \cdots \oplus F_m$ as k-modules. Let $(n_i - n_{i-1})$ be the dimension of F_i as a vector space over k, with $n_0 = 0$ and $n_m = n$. For any basis $\mathcal{B}$ of E obtained by contatenating the bases of $F_1, F_2, \ldots, F_m$, the matrix $M_{\mathcal{B}}(A)$ has m blocks along its diagonal.



For each i, we have $F_i = \{v \in E : T_i^{k_i} v = 0\}$ where $T_i = A - \lambda_i I$. If we consider T_i as an endomorphism on F_i, we'll have $T_i^{k_i} = 0$, i.e. a nilpotent endomorphism of F_i. Then by Problem (1), there exists a basis $(e_{n_{i-1}+1}, \ldots, e_{n_i})$ of F_i such that the representation matrix of T_i on this $\mathcal{B}_i$ is strictly upper triagular. Because $A = T_i + \lambda_i I$ on F_i,

$$M_{\mathcal{B}_i}(A|_{F_i}) = \begin{pmatrix} \lambda_i & * \\ & \ddots \\ 0 & & \lambda_i \end{pmatrix} \Bigg\} n_i - n_{i-1}$$

Let $\mathcal{B} = (e_1, e_2, \ldots, e_n)$. Then

14

$$E = E(t-\lambda_1) \oplus E(t-\lambda_2) \oplus \dots \oplus E(t-\lambda_m),$$

where $E(t-\lambda_i)$ is the $(t-\lambda_i)$-submodules of E. For each $i = 1, \dots, m$, we put $F_i = \{v \in E \mid (A-\lambda_i I)^{k_i} v = 0\}$.

We'll show that $F_i = E(t-\lambda_i)$. By similarity, it suffices to show that $F_1 = E(t-\lambda_1)$. For every $v \in F_1$, we have $(t-\lambda_1)^{k_1} v = 0$. Thus, $v \in E(t-\lambda_1)$. Thus $F_1 \subset E(t-\lambda_1)$. Conversely, for every $v \in E(t-\lambda_1)$, there exists $\alpha \in \mathbb{N}$ such that $(t-\lambda_1)^{\alpha} v = 0$. If $\alpha \leq k_1$ then $(t-\lambda_1)^{k_1} v = 0$, then $v \in F_1$. If $\alpha > k_1$, we put $u = (t-\lambda_1)^{k_1} v$ and $\beta = \alpha - k_1 > 0$. Then $(t-\lambda_1)^{\beta} u = 0$. Moreover, since $q(t)$ annihilates E as $k[t]$-module, we have $q(t) v = 0$. Thus $(t-\lambda_2)^{k_2} \dots (t-\lambda_m)^{k_m} \underbrace{(t-\lambda_1)^{k_1} v}_{u} = 0$. Thus $(t-\lambda_2)^{k_2} \dots (t-\lambda_m)^{k_m} u = 0$. Because $k[t]$ is a PID, we get

$$\underbrace{\gcd\left((t-\lambda_1)^{\beta}, (t-\lambda_2)^{k_2} \dots (t-\lambda_m)^{k_m}\right)}_{1} u = 0$$

Thus $u = 0$. Thus $(t-\lambda_1)^{k_1} v = 0$. Thus $v \in F_1$. Therefore $F_1 = E(t-\lambda_1)$.

We have showed that

$$E = \underbrace{\ker\left[(A-\lambda_1 I)^{k_1}\right]}_{F_1} \oplus \dots \oplus \underbrace{\ker\left[(A-\lambda_m I)^{k_m}\right]}_{F_m}$$

as $k[t]$-modules.

Thus S is diagonalizable. Put $N = A - S = A - g(A)$. Then both S and N are polynomials of A. Also, $M_{\mathcal{B}}(N) = M_{\mathcal{B}}(A) - M_{\mathcal{B}}(S)$ is strictly upper triangular. Thus this matrix is nilpotent, i.e. there is $l \in \mathbb{N}$ with $M_{\mathcal{B}}(N)^l = 0$. Thus $M_{\mathcal{B}}(N^l) = 0$. Thus $N^l = 0$. Thus N is a nilpotent endomorphism of E.

Then, through that $\rho : k[t] \longrightarrow \mathrm{End}_k(E)$ is a ring homomorphism, we have

$$\begin{aligned} S \circ N = g(A) \circ (A - g(A)) &= \rho(g(t)) \circ \rho(t - g(t)) \\ &= \rho(g(t)(t - g(t))) = \rho((t - g(t))g(t)) \\ &= \rho(t - g(t)) \circ \rho(g(t)) = (A - g(A)) \circ g(A) \\ &= N \circ S \end{aligned}$$

⑥ Problem 16, Lang, p. 569

Let Γ be a free abelian group of rank $n \geq 1$, and Γ' a subgroup of

Let $\{v_1, \dots, v_n\}$ be a basis of Γ, and $\{w_1, \dots, w_n\}$ be a basis of Γ'. We put matrix $A = (a_{ij})_{1 \leq i,j \leq n}$ with coefficients in $\mathbb{Z}$ such that

$$\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = A \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

Also, put $d = |\det A|$. We'll show that $(\Gamma : \Gamma') = d$.

We view Γ as a free module over $\mathbb{Z}$ of rank n. Since Γ' is a

16

$$M_{\mathcal{B}}(A) = \begin{pmatrix} \begin{pmatrix} \lambda_1 & * \\ & \ddots \\ 0 & \lambda_1 \end{pmatrix} & & 0 \\ & \begin{pmatrix} \lambda_2 & * \\ & \ddots \\ 0 & \lambda_2 \end{pmatrix} & \\ 0 & & \ddots \\ & & & \begin{pmatrix} \lambda_m & * \\ & \ddots \\ 0 & \lambda_m \end{pmatrix} \end{pmatrix}$$

We know that $(t-\lambda_1)^{k_1}, \dots, (t-\lambda_m)^{k_m}$ are pairwise relatively prime. Thus, by Chinese's Remainder theorem, there exists $g(t) \in k[t]$ such that

$$g(t) \equiv \lambda_i \pmod{(t-\lambda_i)^{k_i}} \qquad \forall i = 1, \dots, m$$

Put $S = g(A) \in \mathrm{End}_k(E)$. For every $v \in F_i$, we have

$$Sv = g(A)v = \left(\lambda_i + r_i(t)(t-\lambda_i)^{k_i}\right)v = \lambda_i v$$

Thus, $M_{\mathcal{B}_i}(S|_{F_i}) = \begin{pmatrix} \lambda_i & & 0 \\ & \ddots & \\ 0 & & \lambda_i \end{pmatrix}$.

Thus

$$M_{\mathcal{B}}(S) = \begin{pmatrix} \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_1 \end{pmatrix} & & 0 \\ & \begin{pmatrix} \lambda_2 & & 0 \\ & \ddots & \\ 0 & & \lambda_2 \end{pmatrix} & \\ 0 & & \ddots \\ & & & \begin{pmatrix} \lambda_m & & 0 \\ & \ddots & \\ 0 & & \lambda_m \end{pmatrix} \end{pmatrix}$$

$$\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = B \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, \qquad \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = C \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}.$$

Then $I_n = BC$ and $\det B, \det C \in \{\pm 1\}$. Then we have

$$\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = C' \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = C' \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = C' \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix} B \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

Thus $$A = C' \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix} B.$$

Thus $$\det A = \underbrace{\det C'}_{\pm 1} \underbrace{\det \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}}_{d_1 \cdots d_n} \underbrace{\det B}_{\pm 1} = \pm d_1 \cdots d_n.$$

Thus $$d = |\det A| = d_1 \cdots d_n.$$

Next we'll show that $(\Gamma : \Gamma') = d$. Consider the following map

$$\varphi : \Gamma/\Gamma' \longrightarrow (\mathbb{Z}/d_1) \oplus \cdots \oplus (\mathbb{Z}/d_n)$$

$$v + \Gamma' \longmapsto (c_1 + d_1\mathbb{Z}, \cdots, c_n + d_n\mathbb{Z}),$$

where $v = c_1 e_1 + c_2 e_2 + \cdots + c_n e_n$, with $c_i \in \mathbb{Z}$.

• Check of φ is well-defined.

Suppose $v' = c_1' e_1 + \cdots + c_n' e_n$, $v = c_1 e_1 + \cdots + c_n e_n$. Then we check that $v' - v \in \Gamma'$. Then $(c_1' - c_1) e_1 + \cdots + (c_n' - c_n) e_n \in \Gamma'$. Since $\{f_1, \cdots, f_n\}$ is a basis of Γ', there are $r_1, \cdots, r_n \in \mathbb{Z}$ such that

Submodule of Γ of rank n, there exists a basis $\{e_1, \dots, e_n\}$ of Γ such that $\{d_1 e_1, \dots, d_n e_n\}$ is a basis of Γ', for some $d_1, \dots, d_n \in \mathbb{Z}$. As a consequence, each $d_i \neq 0$. Put $f_i = d_i e_i$. We get

$$\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

We can assume that d_i was chosen to be all positive. We'll show that $d_1 \cdots d_n = d$. Since $\{w_1, \dots, w_n\}$ is a basis of Γ', each f_i is a linear combination of $w_1, \dots, w_n$. Thus there is a matrix B with coefficients in $\mathbb{Z}$ such that

$$\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = B' \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$$

Conversely, since $\{f_1, \dots, f_n\}$ is a basis of Γ', each w_i is a linear combination of $f_1, \dots, f_n$. Thus there is a matrix C with coefficient in $\mathbb{Z}$ such that

$$\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = C' \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}$$

Thus $\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = C'B' \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$. Thus $I_n = C'B'$. Then $\underbrace{\det I_n}_{1} = \underbrace{\det C'}_{\in \mathbb{Z}} \underbrace{\det B'}_{\in \mathbb{Z}}$

Thus $\det C', \det B' \in \{-1, 1\}$. Similarly, we have two matrices B, C with coefficients in $\mathbb{Z}$ such that

$(t^2+1)v = (A^2+id)v = 0$ for all $v \in V$.

Thus (t^2+1) - annihilates V as an $\mathbb{R}[t]$-module. We know that (t^2+1) is a prime in $\mathbb{R}[t]$. Thus by Structure Theorem for finitely generated torsion module V over $\mathbb{R}[t]$, we have

$$V \simeq \left(\mathbb{R}[t]/(t^2+1)\right) \oplus \left(\mathbb{R}[t]/(t^2+1)\right) \oplus \cdots \oplus \left(\mathbb{R}[t]/(t^2+1)\right).$$

Thus $V = V_1 \oplus V_2 \oplus \cdots \oplus V_m$ as $\mathbb{R}[t]$-modules such that $V_i \overset{\varphi_i}{\simeq} \mathbb{R}[t]/(t^2+1)$.

We know that $\mathbb{R} \subset \mathbb{R}[t]$. Thus φ_i is also an $\mathbb{R}$-linear map. Put

$$[1] = 1+(t^2+1)\mathbb{R}[t], \quad [t] = t+(t^2+1)\mathbb{R}[t].$$

Then for each $[f(t)] = f(t)+(t^2+1)\mathbb{R}[t]$, we divide $f(t)$ by (t^2+1).

$$f(t) = g(t)(t^2+1)+(at+b), \quad a,b \in \mathbb{R}.$$

Then $[f(t)] = [at+b] = a[t]+b[1]$. Thus $\{[1],[t]\}$ generates $\mathbb{R}[t]/(t^2+1)$ as an $\mathbb{R}$-module. Moreover, if $a[t]+b[1]=0$ then $at+b = g(t)(t^2+1)$ for some $g(t) \in \mathbb{R}[t]$. By equating the degrees both sides, we must have $a=b=0$.

Thus $\mathbb{R}[t]/(t^2+1)$ has an $\mathbb{R}$-basis $\{[1],[t]\}$. Put $e_i = \varphi_i^{-1}([1])$ and $e_i' = \varphi_i^{-1}([t])$. Then $\{e_i, e_i'\}$ is a basis of V_i as an $\mathbb{R}$-module. Since φ_i^{-1} is an $\mathbb{R}[t]$-module, we have $e_i' = \varphi_i^{-1}([t]) = \varphi_i^{-1}(t[1]) = t\,\varphi_i^{-1}([1]) = te_i$.

Thus $e_i' = Ae_i$. We have $Ae_i = e_i'$, $Ae_i' = A^2e_i = -e_i$.

$$(c_1'-c_1)e_1+\cdots+(c_n'-c_n)e_n = r_1f_1+\cdots+r_nf_n$$
$$= r_1d_1e_1+\cdots+r_nd_ne_n.$$

Thus $c_i'-c_i = r_id_i \in d_i\mathbb{Z}$. Thus $c_i'+d_i\mathbb{Z} = c_i+d_i\mathbb{Z}$. Thus $\varphi(v')=\varphi(v)$.

- By the definition of φ, it is naturally a $\mathbb{Z}$-linear map and surjective.
- Suppose that $\varphi(v)=0$. Then $c_i+d_i\mathbb{Z}=0$. Then there exists $r_i\in\mathbb{Z}$ such that $c_i=d_ir_i$. Then $v = c_1e_1+\cdots+c_ne_n$
$$= d_1r_1e_1+\cdots+d_nr_ne_n$$
$$= r_1f_1+\cdots+r_nf_n \in \Gamma'$$

Thus $v+\Gamma'=0$. Thus φ is injective. Therefore, φ is a $\mathbb{Z}$-isomorphism.

In particular, $(\Gamma:\Gamma') = |\mathbb{Z}/d_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/d_n\mathbb{Z}|$
$$= |\mathbb{Z}/d_1\mathbb{Z}||\mathbb{Z}/d_2\mathbb{Z}|\cdots|\mathbb{Z}/d_n\mathbb{Z}|$$
$$= d_1d_2\cdots d_n$$
$$= d.$$

⑦ Problem 22, Lang, p. 540.

Let V be a vector space over $\mathbb{R}$ of dimension $n<\infty$. Let $A: V\to V$ be an $\mathbb{R}$-linear map such that $A^2=-id$. Then $A\in \mathrm{End}_{\mathbb{R}}(V)$. Consider an $\mathbb{R}$-algebra homomorphism $\varphi: \mathbb{R}[t]\to \mathrm{End}_{\mathbb{R}}(V)$, $t\mapsto A$. This allows us to think of V as an $\mathbb{R}[t]$-module. Because $A^2+id=0$, we have

Thus, as an endomorphism of V_i, A has the representation matrix in basis (e_i, e_i') as follow $M_{(e_i, e_i')}(A) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Since $V = V_1 \oplus \cdots \oplus V_m$ as $\mathbb{R}[t]$-modules, $V = V_1 \oplus \cdots \oplus V_m$ as $\mathbb{R}$-modules.

Thus $\mathcal{B} = (e_1, e_1', e_2, e_2', \ldots, e_m, e_m')$ is ~~a basis~~ an $\mathbb{R}$-basis of V. The matrix representing A in this basis has the form:

$$M_{\mathcal{B}}(A) = \begin{pmatrix} \boxed{\begin{matrix} 0 & -1 \\ 1 & 0 \end{matrix}} & & & 0 \\ & \boxed{\begin{matrix} 0 & -1 \\ 1 & 0 \end{matrix}} & & \\ & & \ddots & \\ 0 & & & \boxed{\begin{matrix} 0 & -1 \\ 1 & 0 \end{matrix}} \end{pmatrix}$$

The dimension of V is $|\mathcal{B}| = 2m$. Also, $V = V_1 \oplus \cdots \oplus V_m$ is a decomposition of V as a direct sum of m A-invariant subspaces.