Problem 5, Lang, p. 546.

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

We can assume that $m$ was chosen to be the smallest non-negative integer such that $T^m = 0$. In case $m = 0$, we get $\text{id}_E = T^0 = 0$. Then $E = \{0\}$ and $T = \text{id}_E : \{0\} \rightarrow \{0\}$. The only basis of $E$ is $B = \emptyset$. Then $M_B(T)$ doesn't have any meaning! Thus we consider only the case $m > 1$.

If $m = 1$ then $T = 0$. Then $M_B(T) = 0$ for any choice of basis $B$. The zero matrix is strictly upper triangular. Now we consider the case $m > 2$.

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

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

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 $T^l = \ker T^l$. Thus $T^l = 0$. Thus $u \in \ker T$. Thus $\ker T^{l+1} \subset \ker T^l$. Applying this result again and again, we get...
\[
\ker T^{l-1} = \ker T^l = \ker T^{l+1} = \ldots = \ker T^m = E. \quad \text{This is a contradiction because } m \text{ was chosen such that } m \text{ is minimal nonnegative integer satisfying } T^m = 0. \text{ Therefore } \ker T^{l+1} \neq \ker T^l \text{ for all } 1 \leq l \leq m. \quad \text{Because } E \text{ is a vector space, each } \ker T^{l-1} \text{ has a direct summand in } \ker T^l. \quad \text{We put }
\]
\[
V_0 = \ker T, \quad \ker T = V_0,
\]
\[
\ker T^2 = \ker T \oplus V_1,
\]
\[
\ker T^3 = \ker T^2 \oplus V_2,
\]
\[
\vdots
\]
\[
\ker T^m = \ker T^{m-1} \oplus V_{m-1}.
\]

Then \(V_0, V_1, \ldots, V_{m-1} \neq \{0\}^3\) and \(E = V_0 \oplus V_1 \oplus \ldots \oplus V_{m-2}\). Let
\[
\{e_i \mid 0 \leq i < k_1\} \text{ be a basis of } V_0,
\]
\[
\{e_i \mid k_1 \leq i < k_2\} \text{ be a basis of } V_1,
\]
\[
\{e_i \mid k_{m-1} < i \leq k_m = n\} \text{ be a basis of } V_{m-1}.
\]

Then \(B = \{e_1, e_2, \ldots, e_n\}\) is a basis of \(E\). We'll show that \(M_{gs}(T)\) is strictly upper triangular. For each \(i = 1, 2, \ldots, n\), there is \(j_i\) is an index \(j\) such that \(k_j < i \leq k_{j+1}\). Then \(e_i \in V_j \subset \ker T^{j+1}\). Then \(T^{j+1}(e_i) = 0\). Then
\[
T e_i \in \ker T^j = V_0 \oplus \ldots \oplus V_{j-1}.
\]

If \(j = 0\) then \(T e_i = 0\).

If \(j > 1\) then \(T e_i\) is a linear combination of \(e_s \mid 0 < s \leq k_j\). Thus the column vector \([T e_i]_B\) has the following form.
Thus if we put the matrix \( M = (m_{ij})_{1 \leq i,j \leq n} = M_b(T) = ([Te_1]_b \ldots [Te_n]_b) \) then \( m_{ri} = 0 \) for every \( r > k_i \). Since \( i > k_j \), we get \( m_{ri} = 0 \) for every \( r > i \).

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 \( m > 1 \)). We'll show that \( I_n + N \) is invertible. We have \( N^{2m} = 0 \). Thus

\[
I_n = I_n - N^{2m} = (I_n - N) (I_n + N^2 + \ldots + N^{2m-2}) = (I_n - N) (I_n + N) (I_n + N^2 + \ldots + N^{2m-2})
\]
Thus $I + N$ is invertible and its inverse is $(I - N)(I + N + N^2 + \ldots + N^{2m-2})$.

3) Problem 12, Lang, p. 546.

Let $k$ be a field and $G$ be the subset of $\text{GL}(n, k)$ 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 non-zero and hence a unit). We'll show that $G$ is a subgroup of $\text{GL}(n, k)$ with respect to the matrix multiplication.

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

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

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 $k = 1, \ldots, n$.

Thus $C_{ij} = 0$ for $i > j$. Thus $C$ is upper triangular. Since $G$ is

det$(C) = \det(A)\det(B) \neq 0$, every diagonal element of $C$ is non-zero.

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 $A^* = (P_{ij})$ with

$$P_{ij} = (-1)^{i+j} \det(A_{ij})$$

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 $P_{ij} = 0$. Thus,
$A^*$ is lower triangular. We have $A^{-1} = \frac{1}{\det(A)} A^*$. 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 $A, B \in H$, $a_{ii} = b_{ii} = 1 \neq 0$. Thus $C_{ii} = 1 \neq 0$. Thus $CEH$. Now for $A \in H$ and $B = A^{-1}$, we have $(In)_{ij} = a_{ij} b_{ji}$. Thus $1 = 1$. $b_{ii} = b_{ii}$. 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 $C = B^T A B \in G$. 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 non-zero diagonal elements. Then $K$ is a subgroup of $G$ and $K \approx \mathbb{K}^n$ in as multiplicative groups. We see that $HK \geq \mathbb{K}^n$. 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 $a_{ij} = c_{ij} c_{ij}^{-1}$ for all $1 \leq i, j \leq n$. 


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

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

$$= c_{ij} c_{ij}^{-1} b_{ij}$$

$$= c_{ij}$$

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

Then we have a canonical group isomorphism $HK/H \cong K/(KH) \cong K$. Thus $G/H \cong K \cong (k\langle \theta_3 \rangle)^n$.

④ Problem 13, Lang, p. 568.

Let $E$ be an $n$-dimensional vector space over a field $k$, and let $S \in End_k(E)$.

Consider the following $k$-algebra homomorphism $\sigma : k[t] \to End_k(E)$,

$$t \mapsto S.$$ Then $\sigma$ 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 $B = \{ e_1, \ldots, e_3 \}$ of $E$ such that $M_B(S)$ is diagonal. After exchanging rows and columns, we can assume that $M_B(S)$ is of the form:
Then we have \( S\epsilon_i = \lambda_i \epsilon_i \) for \( n_0 < i \leq n_1 \),
\( S\epsilon_i = \lambda_2 \epsilon_i \) for \( n_1 < i \leq n_2 \),
\( S\epsilon_i = \lambda_m \epsilon_i \) for \( n_m-1 < i \leq n_m = n \).

For each \( i = 1, \ldots, m \), 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)v = S(S-\lambda_i)v \quad \text{(because \( E \) is a \( k[t] \)-module, and \( k[t] \) is commutative)}
\]
\[
= S(0) = 0
\]

Thus \( S \in F_i \). Therefore \( F_i \) is \( S \)-invariant, i.e. \( F_i \) is a \( k[t] \)-submodule of \( E \).

We have \( \epsilon_i \in F_i \) for \( n_{i-1} < i \leq n_i \). We'll show that these \( \epsilon_i \)'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 \( v = q_1 \epsilon_1 + \ldots + q_n \epsilon_n \) with \( q_1, \ldots, q_n \in k \). Then

where \( \lambda_{i-1}, \lambda_m \) are distinct.
\[ 0 = (S - \lambda_1)v = (S - \lambda_1)(c_1e_1 + \cdots + c_ne_n) \]
\[ = \sum_{k=1}^{n} (c_kS_k - \lambda_1c_ke_k) \]
\[ = \sum_{k=n+1}^{n_1} \left( c_kS_k - \lambda_1c_ke_k \right) + \sum_{k=n_1+1}^{n_2} \left( c_kS_k - \lambda_2c_ke_k \right) + \cdots + \sum_{k=n_m+1}^{n} \left( c_kS_k - \lambda_mc_ke_k \right) \]
\[ = \sum_{k=n+1}^{n_1} c_k(\lambda_1 - \lambda_1)e_k + \cdots + \sum_{k=n_m+1}^{n} c_k(\lambda_m - \lambda_m)e_k \]

Since \( \{e_1, \ldots, e_n\} \) is \( k \)-linearly independent, \( c_k(\lambda_k - \lambda_1) = 0 \) for \( n_1 < k \leq n_m \).

Thus \( \{e_1, \ldots, e_n\} \) is a \( k \)-basis for \( F_k \).

Since \( \lambda_1 \neq \lambda_2 \), \( c_k = 0 \) for all \( k > n_2 \). Thus \( 0 \) is just a linear combination of \( e_1, \ldots, e_{n_1} \). Thus \( \{e_1, \ldots, e_{n_1}\} \) is a \( k \)-basis for \( F_k \).

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 \( k[t] \)-module of \( E \). Then \( E = F_1 + \cdots + F_m \) as \( k[t] \)-modules because \( k \subseteq k[t] \). We'll show that this sum is also a direct sum as \( k[t] \)-modules. By the definition of \( F_i \), we have

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

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 \( 2 \leq i \leq m \), \( (t - \lambda_i)v = (t - \lambda_2)v + (\lambda_2 - \lambda_i)v \). Thus \( v \notin F_i \). Thus \( F_1, \ldots, F_m \) are all distinct. Thus we have the direct sum \( E = F_1 \oplus \cdots \oplus F_m \) as \( k[t] \)-modules.
Then \( E \cong k[t]/(t-\lambda_1) \oplus \cdots \oplus k[t]/(t-\lambda_m) \)
\[ = k[t]/q(t) \quad \text{by Chinese's Remainder Theorem, where} \]
\[ q(t) = (t-\lambda_1) \cdots (t-\lambda_m). \]

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

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 \( k \subseteq k[t] \), each \( F_i \) is also a \( k \)-submodule of \( E \). By the same 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 \( r_1(t), \ldots, r_m(t) \in k[t] \) such that
\[ v = r_1(t)f_1 + \cdots + r_m(t)f_m \]
for some \( f_1, \ldots, f_m \in E \). 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 \( \{ e_i \mid \eta_0 < \eta_1 < \cdots < \eta_j \} \) be a \( k \)-basis of \( F_1 \),
\[ \{ e_i \mid \eta_1 < \eta_2 < \cdots < \eta_k \} \) be a \( k \)-basis of \( F_2 \),
\[ \vdots \]
\[ \{ e_i \mid \eta_{j-1} < \eta_j = 0 \} \) be a \( k \)-basis of \( F_{j-1} \).

Then \( B = \{ e_1, \ldots, e_n \} \) is a basis of \( E \). We have \( Se_i = \lambda_i e_i \) where \( \eta_{j-1} < \eta_j \).

Therefore, the matrix representing \( S \) in basis \( B \) is diagonal, which has \( \lambda_i \)'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 \( F \) 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 \( \lambda_1, \ldots, \lambda_m \) are distinct. Moreover, we showed in part (a) by using Structure Theorem for finitely-generated torsion module over \( k[t] \) that
\[ E = k[t]/q(t) \] as \( k[t] \)-modules. Because \( F \) is a \( k[t] \)-submodule of \( E \),
\[ F = U/q(t) \] where \( U \) is an ideal of \( k[t] \) containing \( q(t) \). Since \( k[t] \) is a PID, \( U = (q(t)) \) for some polynomial \( q(t) \). Because \( q(t) \in (q(t)), q(t) \mid q(t) \).

Thus there is a polynomial \( r(t) \) such that \( q(t) = q(t) r(t) \). Then \( r(t) \) is also
of the form \( (t-\beta_1) \cdots (t-\beta_k) \) with \( \beta_1, \ldots, \beta_k \) distinct.
(5) Let $E$ be an $n$-dimensional vector space over $k$, which is an algebraically closed field. Let $A \in \text{End}_k(E)$. We'll show that $A$ can be written as $A = S+N$ where

\[
\begin{align*}
S & \text{ is diagonalizable, } \\
N & \text{ is nilpotent, } \\
S \circ N & = N \circ S,
\end{align*}
\]

$S$ and $N$ are polynomials of $A$.

As usual, we consider the representation of $k[t]$ in $E$, namely a $k$-algebra homomorphism $\phi : k[t] \rightarrow \text{End}_k(E)$,

\[t \mapsto A.\]

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 $\lambda_1, \ldots, \lambda_m$ are distinct and $k_1, \ldots, k_m \geq 1$. Note that the case $q(t) \equiv 1$ implies $E = 1.E = q(t)E = 0$. Then $A$ is the zero endomorphism. Then $S$ and $N$ can be chosen as trivial endomorphisms.

Because $t-\lambda_1, \ldots, t-\lambda_m$ are distinct primes of $k[t]$, we got the prime power factorization of $q(t)$ in $k[t]$. 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, $T(F_i) \subseteq F_i$. 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 $(\ast)$, each $F_i$ is an $(n_i - n_{i-1})$-dimensional vector space over $k$.

Then there exists a $k$-basis $B_i = (e_{i+1}, \ldots, e_{n_i})$ of $F_i$ such that $M_{B_i}(T|_{F_i})$ is diagonal. Then we obtain a basis $B$ of $E$ by concatenating $B_1, B_2, \ldots, B_n$.

The representation matrix of $T$ of this basis is of the form

$$
M_B(T) = \begin{pmatrix}
M_{B_1}(T|_{F_1}) & & \\
& M_{B_2}(T|_{F_2}) & \\
& & \ddots \\
& & & M_{B_m}(T|_{F_m})
\end{pmatrix}
$$

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

Therefore, $M_B(S)$ is exactly of the form $(\ast)$. Therefore, both $M_B(S)$ and $M_B(T)$ are diagonal.
Because \( k < k[\mathcal{E}] \), each \( F_i \) is also a \( k \)-module. Thus we get 
\[
E = F_1 \oplus \cdots \oplus F_m \text{ as } k\text{-modules. Let } (n_i - n_{i-1}) \text{ be the dimension of } F_i \text{ as a vector space over } k, \text{ with } n_0 = 0 \text{ and } n_m = n. \text{ For any basis } \mathcal{B} \text{ of } E \text{ obtained by concatenating the bases of } F_1, F_2, \ldots, F_m, \text{ the matrix } M_{\mathcal{B}}(A) \text{ has in blocks along its diagonal.}
\]
\[
\begin{pmatrix}
F_1 & & \\
& F_2 & \\
& & \ddots \\
& & & F_m
\end{pmatrix}
\]

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 \( (e_{i+1}, \ldots, e_i) \) of \( F_i \) such that the representation matrix of \( T_i \) on this \( B_i \) is strictly upper triangular. Because \( A = T_i + \lambda_i I \) on \( F_i \),

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

Let \( B = (e_1, e_2, \ldots, e_n) \). Then
\[ E = E(t - \lambda_1) \oplus E(t - \lambda_2) \oplus \ldots \oplus E(t - \lambda_m), \]

where \( E(t - \lambda_i) \) is the \((t - \lambda_i)\)-submodule of \( E \). For each \( i = 1, \ldots, m \), we put \[ F_i = \{ \nu \in E \mid (A - \lambda_i I)^{k_i} \nu = 0 \}. \]

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 \( \nu \in F_1 \), we have \((t - \lambda_1)^{k_1} \nu = 0\). Thus \( \nu \in E(t - \lambda_1) \). Thus \( F_1 \subseteq E(t - \lambda_1) \). Conversely, for every \( \nu \in E(t - \lambda_1) \), there exists \( x \in \mathbb{N} \) such that \((t - \lambda_1)^x \nu = 0\). If \( x \leq k_1 \), then \((t - \lambda_1)^{k_1} \nu = 0\) then \( \nu \in F_1 \). If \( x > k_1 \), we put \( u = (t - \lambda_1)^{k_1} \nu \) and \( \beta = x - k_1 > 0 \). Then \((t - \lambda_1)^\beta u = 0\). Moreover, since \( q(t) \) annihilates \( E \) as \( k[t] \)-module, we have \( q(t) \nu = 0 \). Thus \((t - \lambda_1)^{k_1} \ldots (t - \lambda_m)^{k_m} u = 0 \). Because \( k[t] \) is a PID, we get \[ \gcd \left( (t - \lambda_1)^{k_1}, (t - \lambda_2)^{k_2}, \ldots, (t - \lambda_m)^{k_m} \right) u = 0 \]

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

We have showed that
\[
E = \ker [(A - \lambda_i I)^{k_i}] \oplus \ldots \oplus \ker [(A - \lambda_m I)^{k_m}]
\]
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, $M_\beta(N) = M_\beta(A) - M_\beta(S)$ is strictly upper triangular. Thus this matrix is nilpotent, i.e. there is $k \in \mathbb{N}$ with $M_\beta(N)^k = 0$. Thus $M_\beta(N^k) = 0$. Thus $N^k = 0$. Thus $N$ is a nilpotent endomorphism of $E$.

However, the fact that $g : k[t] \to \text{End}_E(E)$ is a $k[t]$-module homomorphism, we have $N = g(A) \circ (A - g(A)) = g(g(t)) \circ (t - g(t)) = g(g(t)(t - g(t))) = g((t - g(t))g(t)) = (A - g(A)) \circ g(A) = N \circ S$.

6. Problem 16, Lang, p. 569

Let $\Gamma$ be a free abelian group of rank $n \geq 1$, and $\Gamma'$ a subgroup of $\Gamma$. Let $\{v_1, \ldots, v_n\}$ be a basis of $\Gamma$, and $\{w_1, \ldots, w_n\}$ be a basis of $\Gamma'$. 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 $\Gamma$ as a free module over $\mathbb{Z}$ of rank $n$. Since $\Gamma'$ is a
We know that \((t-\lambda_1)^{k_1}, \ldots, (t-\lambda_m)^{k_m}\) are pairwise relatively prime. Thus, by Chinese's Remainder Theorem, there exists \(g(t) \in \mathbb{K}[t]\) such that

\[ g(t) \equiv \lambda_i \pmod{(t-\lambda_i)^{k_i}} \quad \forall i = 1, \ldots, m \]

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

\[ S_v = g(A)_v = (\lambda_i + r_i(t) (t-\lambda_i)^{k_i})_v = \lambda_i \cdot v \]

Thus,

\[ M_{Bc}(S|_{F_i}) = \begin{pmatrix} \lambda_i & 0 \\ 0 & \lambda_i \end{pmatrix} \]

Thus

\[ M_B(S) = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix} \]
\begin{align*}
\begin{pmatrix}
\vdots \\
\varepsilon_1 \\
\vdots \\
\varepsilon_n \\
\end{pmatrix}
&= B
\begin{pmatrix}
\vdots \\
\varphi_1 \\
\vdots \\
\varphi_n \\
\end{pmatrix},
\begin{pmatrix}
\vdots \\
\varphi_1 \\
\vdots \\
\varphi_n \\
\end{pmatrix}
= C
\begin{pmatrix}
\vdots \\
\varepsilon_1 \\
\vdots \\
\varepsilon_n \\
\end{pmatrix}.
\end{align*}

Then \( I_n = BC \) and \( \det B \) \( \det C \in \mathbb{R} \). Then we have
\begin{align*}
\begin{pmatrix}
\varphi_1 \\
\vdots \\
\varphi_n \\
\end{pmatrix}
&= C'
\begin{pmatrix}
\vdots \\
\varphi_1 \\
\vdots \\
\varphi_n \\
\end{pmatrix}
= C'
\begin{pmatrix}
\begin{pmatrix}
\delta_1 & 0 \\
0 & d_n \\
\end{pmatrix}
\varepsilon_1 \\
\vdots \\
\varepsilon_n \\
\end{pmatrix} =
C'
\begin{pmatrix}
\begin{pmatrix}
\delta_1 & \cdots & d_n \\
0 & \cdots & 0 \\
\end{pmatrix}
\varepsilon_1 \\
\vdots \\
\varepsilon_n \\
\end{pmatrix} B
\begin{pmatrix}
\vdots \\
\varphi_1 \\
\vdots \\
\varphi_n \\
\end{pmatrix}.
\end{align*}

Thus \( A = C'egin{pmatrix}
\delta_1 & \cdots & d_n \\
0 & \cdots & 0 \\
\end{pmatrix} B \).

Thus \( \det A = \frac{\det C'}{\pm 1} \frac{\det \begin{pmatrix}
\delta_1 & \cdots & d_n \\
0 & \cdots & 0 \\
\end{pmatrix}}{\pm 1} \).

Thus \( d = | \det A | = \delta_1 \cdots d_n \).

Next we'll show that \( (\Gamma : \Gamma') = d \). Consider the following map
\begin{align*}
\varphi: \Gamma / \Gamma' &\rightarrow (\mathbb{Z}/d_1) \oplus \cdots \oplus (\mathbb{Z}/d_n) \\
v + \Gamma' &\mapsto (c_1 + d_1 \mathbb{Z}, \ldots, c_n + d_n \mathbb{Z}),
\end{align*}
where \( v = c_1 \varepsilon_1 + \cdots + c_n \varepsilon_n \), with \( c_i \in \mathbb{Z} \).

\( \text{Check if } \varphi \text{ is well-defined}. \)

Suppose \( v' = c'_1 \varepsilon_1 + \cdots + c'_n \varepsilon_n \) \( \varphi(v) = c_1 \varepsilon_1 + \cdots + c_n \varepsilon_n \). Then we seek that \( v' - v \in \Gamma' \). Then \( (c'_1 - c_1) \varepsilon_1 + \cdots + (c'_n - c_n) \varepsilon_n \in \Gamma' \). Since \( \{ \varepsilon_1, \ldots, \varepsilon_n \} \) is a basis of \( \Gamma' \), there are \( r_1, \ldots, r_n \in \mathbb{Z} \) such that
submodule of \( M' \) of rank \( n \), there exists a basis \( \{e_1, \ldots, e_n\} \) of \( M' \) such that \( \{d_1 e_1, \ldots, d_n e_n\} \) is a basis of \( M' \), for some \( d_1, \ldots, d_n \in \mathbb{Z} \). As a consequence, each \( d_i \neq 0 \). Put \( f_i = d_i e_i \). We get

\[
\begin{pmatrix}
f_1 \\
\vdots \\
f_n
\end{pmatrix} = 
\begin{pmatrix}
d_1 & 0 & \cdots & 0 \\
0 & d_2 & \ddots & \vdots \\
\vdots & \ddots & \ddots & 0 \\
0 & \cdots & 0 & d_n
\end{pmatrix}
\begin{pmatrix}
e_1 \\
\vdots \\
e_n
\end{pmatrix}
\]

We can assume that \( d_1 \) was chosen to be all positive. We'll show that \( d_1 \cdots d_n = d \). Since \( \{w_1, \ldots, w_n\} \) is a basis of \( M' \), each \( f_i \) is a linear combination of \( w_1, \ldots, w_n \). 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 \( \{f_1, \ldots, f_n\} \) is a basis of \( M' \), each \( w_i \) is a linear combination of \( f_1, \ldots, f_n \). Thus there is a matrix \( C \) with coefficients 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 \( \det(I_n) = \det(C') \det(B') \). Then

\[
\det(I_n) \in \mathbb{Z}, \quad \det(C') \in \mathbb{Z}, \quad \det(B') \in \mathbb{Z}
\]

Thus \( \det(C'), \det(B') \in \{-1, 1\} \). Similarly, we have two matrices \( B, C \) with coefficients in \( \mathbb{Z} \) such that
\[(t^2+1)v = (A^2+c)\bar{v} = 0 \text{ for all } v \in V.\]

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

\[V \cong \left(\frac{R[t]}{(t^2+1)}\right) \oplus \left(\frac{R[t]}{(t^2+1)}\right) \oplus \ldots \oplus \left(\frac{R[t]}{(t^2+1)}\right).\]

Thus \(V = V_1 \oplus V_2 \oplus \ldots \oplus V_m\) as \(R[t]\)-modules such that \(\phi_i \cong \frac{R[t]}{(t^2+1)}\).

We know that \(R \subseteq R[t]\). Thus \(\phi_i\) is also an \(R\)-linear map. Put

\[\phi[t] = 1 + (t^2+1)R[t], \quad \phi[t] = t + (t^2+1)R[t].\]

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

\[f(t) = g(t)(t^2+1) + (at+b), \quad a, b \in R.\]

Then \([f(t)] = [at+b] = a\phi[t] + b\phi[t].\) Thus \([1], [t]\) generates \(R[t]/(t^2+1)\) as an \(R\)-module. Moreover, if \(a\phi[t] + b\phi[t] = 0\) then \(at + b = g(t)(t^2+1)\)

for some \(g(t) \in R[t]\). By equating the degrees both sides, we must have \(a = b = 0\).

Thus \(R[t]/(t^2+1)\) has an \(R\)-basis \(\{1, t\}\). Put \(e_i = \phi_i^{-1}(1)\) and \(e^i = \phi_i^{-1}(t)\). Then \(\{e_i, e^i\}\) is a basis of \(V_i\) as an \(R\)-module. Since \(\phi_i\) is an \(R[t]\)-module, we have \(e^i = \phi_i^{-1}(1) = \phi^{-1}(t\phi_i(1)) = t\phi_i^{-1}(1) = te^i.\)

Thus \(e^i = Ae^i\). We have \(Ae_i = e^i, \quad Ae^i = A^2e_i = -e_i.\)
\((c'_1 - c_i) e_1 + \cdots + (c'_n - c_n) e_n = r_1 f_1 + \cdots + r_n f_n\)

\[= r_1 d_1 e_1 + \cdots + r_n d_n e_n.\]

Thus \(c'_1 - c_i = r_i d_i \in d_i \mathbb{Z}\). Thus \(c'_1 + d_i \mathbb{Z} = c_i + d_i \mathbb{Z}\). Thus \(\varphi(u') = \varphi(u)\).

By the definition of \(\varphi\), 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 \(c_i = d_i r_i\). Then \(v = c_1 e_1 + \cdots + c_n e_n\)

\[= r_1 d_1 e_1 + \cdots + r_n d_n e_n\]

\[= r_1 f_1 + \cdots + r_n f_n \in \Gamma'.\]

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

In particular, \((\Gamma : \Gamma') = |\Z/d_1 \Z \oplus \cdots \oplus \Z/d_n \Z|\)

\[= |\Z/d_1 \Z| \cdot \left| \Z/d_2 \Z \right| \cdots \left| \Z/d_n \Z \right|\]

\[= d_1 d_2 \cdots d_n\]

\[= d.\]

\(\Box\) Problem 22, Lang, p. 540.

Let \(V\) be a vector space over \(\mathbb{R}\) of dimension \(n < \omega\). Let \(A : V \to V\) be an \(\mathbb{R}\)-linear map such that \(A^2 = -\text{id}\). Then \(A \in \text{End}_{\mathbb{R}}(V)\). Consider an \(\mathbb{R}\)-algebra homomorphism \(S : \mathbb{R}[t] \to \text{End}_{\mathbb{R}}(V), t \mapsto A\). This allows us to think of \(V\) as an \(\mathbb{R}[t]\)-module. Because \(A^2 + \text{id} = 0\), we have
Thus, as an endomorphism of $V_i$, $A$ has the representation matrix in basis $(e_i, e'_i)$ as follows: $M_{(e_i, e'_i)}(A) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Since $V = V_1 \oplus \ldots \oplus V_m$ as $R(R)$-modules, $V = V_1 \oplus \ldots \oplus V_m$ as $R$-modules. Thus $B = (e_1, e'_1, e_2, e'_2, \ldots, e_m, e'_m)$ is a basis as an $R$-basis of $V$. The matrix representing $A$ in this basis has the form:

$$M_B(A) = \begin{pmatrix} 0 & -1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \end{pmatrix}$$

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