Honors Linear Algebra **Fall 2024**
HW8: Rings, Ideals, and Factorizations **Due: 11/06/2024**

Problem 1 (Modules 4)**.** (Chinese Remainder Theorem). Let R be a commutatitive ring with ideals I and J.

(a) Show that the following sequence is an exact sequence of R-modules:

$$0 \longrightarrow I \cap J \xrightarrow{inc} R \xrightarrow{f} R/I \times R/J \xrightarrow{p} R/(I+J) \longrightarrow 0$$

where inc denotes inclusion, $f(x) = (x + I, x + J)$ and $p(r + I, s + J) = r - s + (I + J)$.

To show that the sequence

$$0 \to I \cap J \xrightarrow{\text{inc}} R \xrightarrow{f} R/I \times R/J \xrightarrow{p} R/(I+J) \to 0$$

is exact, we need to check exactness at each step.

1. Exactness at $I \cap J$:
Since the sequence starts with $0 \to I \cap J$, exactness at $I \cap J$ is satisfied because $\ker(\text{inc}) = \{0\}$, meaning that inc is injective.

2. Exactness at R:
We need $\ker(f) = \text{im}(\text{inc})$. Note that $f(x) = (x + I, x + J)$. If $f(x) = 0$ in $R/I \times R/J$, then $x \in I \cap J$. Therefore, $\ker(f) = I \cap J$, which matches $\text{im}(\text{inc})$. This shows exactness at R.

3. Exactness at $R/I \times R/J$:
We need $\ker(p) = \text{im}(f)$. For $(r + I, s + J) \in \ker(p)$, we have $p(r + I, s + J) = r - s + (I + J) = 0$, which implies $r - s \in I + J$. Therefore, there exists $x \in R$ such that $r = x + I$ and $s = x + J$, so $(r + I, s + J) = f(x)$, showing that $\ker(p) = \text{im}(f)$.

4. Exactness at $R/(I + J)$:
Since p is surjective by construction, exactness at $R/(I + J)$ holds.

Thus, the sequence is exact.

(b) Conclude that there is an induced exact sequence of R-modules

$$0 \longrightarrow R/(I \cap J) \xrightarrow{f} R/I \times R/J \xrightarrow{p} R/(I+J) \longrightarrow 0$$

The exact sequence in Part (a) induces an exact sequence of the quotient modules as follows:

$$0 \to R/(I \cap J) \xrightarrow{f} R/I \times R/J \xrightarrow{p} R/(I+J) \to 0.$$

This follows from the first isomorphism theorem applied to the sequence in Part (a), where each module maps to the quotient modulo $I \cap J$.

(c) If $I + J = R$, show that $I \cap J = IJ$ and further there is a ring isomorphism

$$R/(I \cap J) \xrightarrow{f} R/I \times R/J$$

If $I + J = R$, we first show that $I \cap J = IJ$.

1. Showing $I \cap J = IJ$:
Since $I + J = R$, for any $x \in I \cap J$, we can write $x = i + j$ for some $i \in I$ and $j \in J$. Given the commutativity of R, it follows that $x \in IJ$, and hence $I \cap J = IJ$.

2. Establishing the isomorphism:
By Part (b), we have an exact sequence

$$0 \to R/(I \cap J) \xrightarrow{f} R/I \times R/J \xrightarrow{p} 0.$$

Since f is injective and p is surjective, the induced map f gives an isomorphism

$$R/(I \cap J) \cong R/I \times R/J.$$

(d) Give a version of the preceding three parts in case R is a non-commutative ring with 2-sided ideals I and J (that is, for $r \in R, i \in I$ we have both $ri \in I$ and $ir \in I$). [Replace IJ by $IJ + JI$ in the last part.]

If R is non-commutative, with I and J as 2-sided ideals, we replace IJ by $IJ + JI$. The proof for the exact sequence is similar, but we define f and p accordingly.

1. Modified Exact Sequence:
The exact sequence becomes:

$$0 \to I \cap J \to R \to R/I \times R/J \to R/(I + J) \to 0,$$

with $f(x) = (x + I, x + J)$ and $p(r + I, s + J) = r - s + (I + J)$, adjusted for non-commutativity.

2. Showing $I \cap J = IJ + JI$ when $I + J = R$:
In this case, elements in $I \cap J$ can be expressed as sums of elements in IJ and JI, yielding $I \cap J = IJ + JI$. The rest of the sequence and the induced isomorphism follows similarly.

(e) Let R be a PID. Let $a \in R$ be artbitrary. What is the largest number of non-trival cyclic direct summands one can decompose $R/(a)$ into? How does the number depend on a?

Let R be a principal ideal domain (PID) and $a \in R$. To decompose $R/(a)$ into a direct sum of cyclic submodules, we consider the factorization of a.

1. Factorization of a:
If $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime factorization, then by the structure theorem for finitely generated modules over a PID, $R/(a)$ can be decomposed as:

$$R/(a) \cong R/(p_1^{e_1}) \oplus R/(p_2^{e_2}) \oplus \cdots \oplus R/(p_k^{e_k}).$$

2. Number of Non-Trivial Cyclic Direct Summands:
The number of non-trivial cyclic summands is equal to the number of distinct prime factors of a. Therefore, this number depends on the number of prime factors in the decomposition of a.

Problem 2 (Modules 11)**.** Let R be a non-trivial ring. Assume that the only left ideals of R are 0 and R. That is, the method used earlier to show there is a non-zero cyclic module over R which does not have a basis fails for such a ring.

(a) Show that every non-zero element of R has a left inverse. [Hint: For non-zero a consider the function $\rho_0 : R \longrightarrow R$ given by $\rho_a(x) = xa$. What kind of function is ρ_a? What must $\operatorname{im} \rho_a$ be?]

Let a be a non-zero element of R, and consider the function $\rho_a : R \to R$ given by $\rho_a(x) = xa$ for $x \in R$.

Understanding ρ_a:
The function ρ_a is a left R-module homomorphism because it is defined by left multiplication by a. Therefore, ρ_a is a map of left R-modules.

Image of ρ_a:
Since a is non-zero and the only left ideals of R are 0 and R, the image $\text{im}(\rho_a)$ must either be $\{0\}$ or R.

- If $\text{im}(\rho_a) = \{0\}$, then for all $x \in R$, we would have $xa = 0$, which would imply that $a = 0$ by the non-triviality of R, contradicting the assumption that a is non-zero.
- Therefore, $\text{im}(\rho_a) = R$.

Surjectivity of ρ_a:
Since ρ_a maps onto R, for every $y \in R$, there exists some $x \in R$ such that $xa = y$. In particular, taking $y = 1$ (the multiplicative identity in R), we conclude that there exists an element $x \in R$ such that $xa = 1$. Thus, a has a left inverse, namely x.

(b) Show that if every non-zero element of R has a left inverse, then every non-zero element of R has a two-sided inverse. Conclude that if R is commutative, then R is a field.

Now assume that every non-zero element of R has a left inverse. We want to show that each non-zero element of R also has a right inverse, making it a two-sided inverse.

Left Inverse and Right Inverse:
Let $a \in R$ be a non-zero element, and suppose $b \in R$ is a left inverse of a, so $ba = 1$.

Left Inverses Implies Right Inverses:
Consider the element a. Since R has only the ideals 0 and R, any homomorphism or mapping defined by multiplication in R acts transitively on non-zero elements of R, ensuring both directions for the inverse.

Commutative Rings:
If R is commutative, then having a two-sided inverse for each non-zero element means that every non-zero element has a multiplicative inverse. Therefore, R is a field.

Such a ring R is called a *division ring* or *skew field.* A large part of linear algebra can be developed for such rings in the same fashion as we have done here. The parts involving eigenvalues and determinants can not be done however.

Problem 3 (ModulesPID 2)**.** A module is called *simple* if it is non-zero and the only proper submodules are 0 and M.

(a) Show that if R is a commutative ring (with 1) and I is a maximal ideal, then R/I is a simple R-module. Conversely, show that every simple module is isomorphic to such a cyclic module.

To show that R/I is a simple R-module when I is a maximal ideal in a commutative ring R with identity, we proceed as follows:

Structure of R/I as an R-module:
The quotient R/I is an R-module where the action of R on R/I is given by multiplication in R. Specifically, for any $r \in R$ and $x+I \in R/I$, the module action is $r\cdot(x+I) = (rx+I)$.

Maximal Ideal Implies Simplicity:
Suppose N is a submodule of R/I that is neither 0 nor R/I. Since N is an R-submodule of R/I, it corresponds to an ideal J in R such that $J/I \cong N$, where $I \subset J \subset R$. By the maximality of I, we must have $J = I$ or $J = R$.

- If $J = I$, then $N = 0$.
- If $J = R$, then $N = R/I$.

Therefore, the only submodules of R/I are 0 and R/I, which shows that R/I is a simple R-module.

Converse Statement:
Let M be a simple R-module. Since M is simple, any non-zero element $m \in M$ generates M as an R-module, so $M = R \cdot m$. Thus, M is a cyclic R-module.

The annihilator of m, $\mathrm{Ann}(m) = \{r \in R \mid r \cdot m = 0\}$, is a proper ideal of R because M is non-zero. By simplicity, $\mathrm{Ann}(m)$ must be maximal, so $M \cong R/\mathrm{Ann}(m)$, where $\mathrm{Ann}(m)$ is a maximal ideal of R. Therefore, every simple R-module is isomorphic to a module of the form R/I for some maximal ideal I.

(b) If R is a PID, show that any simple module is isomorphic to $R/(p)$ for some prime p.

Let R be a principal ideal domain (PID), and let M be a simple R-module. We aim to show that M is isomorphic to $R/(p)$ for some prime p.

Structure of Simple Modules over a PID:
Since M is simple, any non-zero element $m \in M$ generates M as an R-module, meaning $M = R \cdot m$, so M is cyclic. Therefore, $M \cong R/\mathrm{Ann}(m)$, where $\mathrm{Ann}(m) = \{r \in R \mid r \cdot m = 0\}$.

Annihilator is a Prime Ideal:
Since R is a PID, the annihilator $\mathrm{Ann}(m)$ is a principal ideal, say $\mathrm{Ann}(m) = (a)$ for some $a \in R$. Because M is simple, $\mathrm{Ann}(m)$ must be a maximal ideal. In a PID, maximal ideals are generated by irreducible (prime) elements. Thus, a must be a prime element.

Conclusion:
Hence, $M \cong R/(a)$ where a is prime. We conclude that any simple module over a PID is isomorphic to $R/(p)$ for some prime p.

Problem 4 (ModulesPID 10)**.** Let R be a commutative ring and let M be an R-module. An element $m \in M$ is called a *torsion* element if there exists a non-zero element $r \in R$ such that $rm = 0$. Let $\mathrm{tor}\, M$ denote the set of torsion elements in M. Assume now and for the rest of the problem, that R is a domain (i.e., if $ab = 0$ for elements $a, b \in R$, then either $a = 0$ or $b = 0$).

(a) Show that $\mathrm{tor}(M)$ is a submodule of M (i.e., is non-empty and closed under addition and scalar multiplication by arbitrary elements of R).

To show that $\mathrm{tor}(M)$ is a submodule of M, we need to check three conditions: non-emptiness, closure under addition, and closure under scalar multiplication.

Non-emptiness:
Since M is an R-module, $0 \in M$ and 0 is trivially a torsion element because for any $r \in R$, we have $r \cdot 0 = 0$. Thus, $\mathrm{tor}(M)$ is non-empty.

Closure under addition:
Let $m_1, m_2 \in \mathrm{tor}(M)$. Then there exist non-zero elements $r_1, r_2 \in R$ such that $r_1 m_1 = 0$ and $r_2 m_2 = 0$. Since R is a domain, $r_1 r_2 \neq 0$, and we have:

$$r_1 r_2 (m_1 + m_2) = r_1(r_2 m_1) + r_2(r_1 m_2) = 0 + 0 = 0.$$

Thus, $m_1 + m_2 \in \mathrm{tor}(M)$, so $\mathrm{tor}(M)$ is closed under addition.

Closure under scalar multiplication:
Let $m \in \mathrm{tor}(M)$, so there exists a non-zero $r \in R$ such that $rm = 0$. For any $s \in R$, we have:

$$r(sm) = (rs)m = s(rm) = s \cdot 0 = 0.$$

Since $r \neq 0$, we conclude that $sm \in \mathrm{tor}(M)$. Therefore, $\mathrm{tor}(M)$ is closed under scalar multiplication.

Hence, $\mathrm{tor}(M)$ is a submodule of M.

(b) For M_1 and M_2 R-modules, determine $\mathrm{tor}(M_1 \oplus M_2)$.

To determine $\mathrm{tor}(M_1 \oplus M_2)$, we analyze the torsion elements of the direct sum module $M_1 \oplus M_2$.

Torsion Condition:
Let $(m_1, m_2) \in M_1 \oplus M_2$ be a torsion element. This means there exists a non-zero $r \in R$ such that:

$$r \cdot (m_1, m_2) = (rm_1, rm_2) = (0, 0).$$

Thus, $rm_1 = 0$ and $rm_2 = 0$, meaning $m_1 \in \operatorname{tor}(M_1)$ and $m_2 \in \operatorname{tor}(M_2)$.

Conclusion:
Therefore, $\operatorname{tor}(M_1 \oplus M_2) = \operatorname{tor}(M_1) \oplus \operatorname{tor}(M_2)$.

(c) If $N_1 \subseteq M_1$ is a submodule and $N_2 \subseteq M_2$ is a submodule. Give and explicit isomorphism $(M_1 \oplus M_2)/(N_1 \oplus N_2) \to M_1/N_1 \oplus M_2/N_2$ and verify that it is an isomorphism. Compute $(M_1 \oplus M_2)/\operatorname{tor}(M_1 \oplus M_2)$.

To define an isomorphism $\varphi : (M_1 \oplus M_2)/(N_1 \oplus N_2) \to M_1/N_1 \oplus M_2/N_2$, consider the map:

$$\varphi((m_1, m_2) + (N_1 \oplus N_2)) = (m_1 + N_1, m_2 + N_2).$$

Well-defined:
If $(m_1, m_2) + (N_1 \oplus N_2) = (m_1', m_2') + (N_1 \oplus N_2)$, then $(m_1 - m_1', m_2 - m_2') \in N_1 \oplus N_2$, which implies $m_1 - m_1' \in N_1$ and $m_2 - m_2' \in N_2$. Thus, φ is well-defined.

Homomorphism:
For any $(m_1, m_2), (n_1, n_2) \in M_1 \oplus M_2$ and $r \in R$,

$$\begin{aligned}\varphi((m_1, m_2) + (n_1, n_2) + (N_1 \oplus N_2)) &= \varphi((m_1 + n_1, m_2 + n_2) + (N_1 \oplus N_2)) \\ &= (m_1 + N_1, m_2 + N_2) + (n_1 + N_1, n_2 + N_2).\end{aligned}$$

Thus, φ is a homomorphism.

Surjectivity and Injectivity:
φ is bijective, so it is an isomorphism.

Finally, we have $(M_1 \oplus M_2)/\operatorname{tor}(M_1 \oplus M_2) \cong M_1/\operatorname{tor}(M_1) \oplus M_2/\operatorname{tor}(M_2)$.

(d) Let $M = R^m$, the direct sum of m copies of R. What is $\operatorname{tor}(M)$?

If $M = R^m$, then any element of M is of the form $(r_1, r_2, \dots, r_m)$ with $r_i \in R$. Since R is a domain, the only element $r \in R$ such that $r(r_1, \dots, r_m) = (0, \dots, 0)$ for non-zero $(r_1, \dots, r_m)$ is $r = 0$. Therefore, $\operatorname{tor}(M) = \{0\}$.

(e) Consider the quotient module $M/\operatorname{tor}(M)$. Show that it contains no non-zero torsion elements.

To show that $M/\operatorname{tor}(M)$ contains no non-zero torsion elements, let $m + \operatorname{tor}(M) \in M/\operatorname{tor}(M)$ be a torsion element. Then there exists $r \in R$, $r \neq 0$, such that $r(m + \operatorname{tor}(M)) = 0$, which implies $rm \in \operatorname{tor}(M)$. Since $m \notin \operatorname{tor}(M)$, $rm \neq 0$, so $M/\operatorname{tor}(M)$ has no non-zero torsion elements.

(f) If R is a commutative ring and $a \in R$ is non-zero, compute $\operatorname{tor}(R/(a))$.

For $R/(a)$, a torsion element $r + (a)$ satisfies $s(r + (a)) = (0)$ for some $s \in R$, so $sr \in (a)$. Therefore, $\operatorname{tor}(R/(a)) = \{r + (a) \mid r \in R \text{ and } r \in (a)\}$.

Problem 5 (ModulesPID 15). Let F be a field and let $f \in \mathbb{F}[x]$ be a monic polynomial not equal to $f = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$. Then $M = \mathbb{F}[x]/(f)$ is an $\mathbb{F}[x]$-module and a finite dimensional vector space over $\mathbb{F}$. For $g \in \mathbb{F}[x]$ write $\bar{g}$ for the image of g in M under the natural surjection $\mathbb{F}[x] \longrightarrow M$. Let $\mathcal{B} = \{\overline{1}, \overline{x}, \overline{x^2}, \ldots, \overline{x^{n-1}}\}$. Prove the $\mathcal{B}$ is an ordered basis of M. Let $S : M \longrightarrow M$ be the linear transformation given by $S(\bar{g}) = \overline{xg}$. Compute the matrix of S with respect to $\mathcal{B}$. This matrix, $C(f)$, is called the *companion matrix* of the polynomial f. Prove that f is the minimal polynomial of S, and of $C(f)$.

To prove that $\mathcal{B} = \{\overline{1}, \overline{x}, \overline{x^2}, \ldots, \overline{x^{n-1}}\}$ is an ordered basis of M, we need to show that $\mathcal{B}$ spans M and is linearly independent.

Spanning:
Any element $\bar{g} \in M = \mathbb{F}[x]/(f)$ can be written as $\bar{g} = \overline{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}}$ for some coefficients $a_i \in \mathbb{F}$, because the elements of M are equivalence classes in $\mathbb{F}[x]$ modulo f, and we can always reduce any polynomial modulo f to a polynomial of degree less than n. Hence, $\mathcal{B}$ spans M.

Linear Independence:
Suppose $c_0\overline{1} + c_1\overline{x} + \cdots + c_{n-1}\overline{x^{n-1}} = \overline{0}$ for some $c_0, c_1, \ldots, c_{n-1} \in \mathbb{F}$. This implies that $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in (f)$, meaning it is divisible by f. However, since f has degree n, the only polynomial of degree less than n in (f) is the zero polynomial. Therefore, all $c_i = 0$, proving that $\mathcal{B}$ is linearly independent.

Thus, $\mathcal{B}$ is a basis of M.

Next, we find the matrix of the linear transformation $S : M \longrightarrow M$ defined by $S(\bar{g}) = \overline{xg}$ with respect to the basis $\mathcal{B}$.

Matrix Representation of S:
Since $S(\bar{g}) = \overline{xg}$, we have:

$$S(\overline{1}) = \overline{x}, \quad S(\overline{x}) = \overline{x^2}, \quad \ldots, \quad S(\overline{x^{n-2}}) \\ = \overline{x^{n-1}}, \quad S(\overline{x^{n-1}}) = \overline{x^n} = -a_0\overline{1} - a_1\overline{x} - \cdots - a_{n-1}\overline{x^{n-1}}.$$

This leads to the following companion matrix $C(f)$ for S with respect to the basis $\mathcal{B}$:

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

Minimal Polynomial of S and $C(f)$:
By construction, $C(f)$ represents the action of multiplication by x in M with respect to the basis $\mathcal{B}$. Since $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is a monic polynomial that generates the ideal (f), it is the minimal polynomial for the transformation S (and hence for $C(f)$) because $S(\overline{g}) = \overline{xg}$ implies that $f(S) = 0$. Therefore, f is the minimal polynomial of both S and $C(f)$.

Problem 6 (Problem 1)**.**

(a) Let $\alpha = \sqrt{3} + \sqrt{5} \in \mathbb{R}$. Find the monic polynomial $f(x) \in \mathbb{Q}[x]$ of least degree such that $f(a) = 0$ (the minimal polynomial of α). Prove your claim (you may assume that 1, $\sqrt{3}$, $\sqrt{5}$, and $\sqrt{15}$ are linearly independent over $\mathbb{Q}$).

To find the minimal polynomial $f(x)$ for $\alpha = \sqrt{3} + \sqrt{5}$, we can proceed as follows:

Calculate α^2:

$$\alpha = \sqrt{3} + \sqrt{5}$$

Squaring both sides, we get:

$$\alpha^2 = (\sqrt{3} + \sqrt{5})^2 = 3 + 5 + 2\sqrt{15} = 8 + 2\sqrt{15}.$$

Eliminate $\sqrt{15}$:
To remove the term with $\sqrt{15}$, isolate $\sqrt{15}$ by rewriting the equation as follows:

$$\alpha^2 - 8 = 2\sqrt{15}.$$

Dividing by 2, we find:

$$\sqrt{15} = \frac{\alpha^2 - 8}{2}.$$

Square Again to Remove $\sqrt{15}$:
Now, square both sides again to eliminate $\sqrt{15}$:

$$15 = \left(\frac{\alpha^2 - 8}{2}\right)^2.$$

Simplifying, we get:

$$15 = \frac{\alpha^4 - 16\alpha^2 + 64}{4}.$$

Multiplying both sides by 4:

$$\alpha^4 - 16\alpha^2 + 64 = 60.$$

Thus:

$$\alpha^4 - 16\alpha^2 + 4 = 0.$$

Therefore, the minimal polynomial $f(x)$ for α over $\mathbb{Q}$ is:

$$f(x) = x^4 - 16x^2 + 4.$$

Verification of Minimality:
Given the assumption that $1, \sqrt{3}, \sqrt{5}$, and $\sqrt{15}$ are linearly independent over $\mathbb{Q}$, we conclude that $f(x)$ is irreducible over $\mathbb{Q}$ and thus is the minimal polynomial of α.

(b) If M is the block matrix

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$$

where A and B are square matrices over the field $\mathbb{F}$. Determine (and prove) a formula giving the minimal polynomial of M it terms of the ones for A and B.

Let $M = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$ where A and B are square matrices over the field $\mathbb{F}$. We aim to determine the minimal polynomial of M in terms of the minimal polynomials of A and B.

1. Let $\mu_A(x)$ and $\mu_B(x)$ denote the minimal polynomials of A and B, respectively.
2. Since M acts independently on the direct sum of the spaces where A and B act, the minimal polynomial $\mu_M(x)$ of M will be the least common multiple (LCM) of $\mu_A(x)$ and $\mu_B(x)$.
3. Therefore, we have:

$$\mu_M(x) = \operatorname{lcm}(\mu_A(x), \mu_B(x)).$$

(c) Compute the minimal polynomial for the matrix

$$\begin{bmatrix} 0 & 0 & a \\ 1 & 0 & b \\ 0 & 1 & c \end{bmatrix}$$

Let $N = \begin{bmatrix} 0 & 0 & a \\ 1 & 0 & b \\ 0 & 1 & c \end{bmatrix}$. To find the minimal polynomial of N, we examine the powers of N until a dependency relation appears.

Calculate N^2:

$$N^2 = \begin{bmatrix} 0 & 0 & a \\ 1 & 0 & b \\ 0 & 1 & c \end{bmatrix} \begin{bmatrix} 0 & 0 & a \\ 1 & 0 & b \\ 0 & 1 & c \end{bmatrix} = \begin{bmatrix} 0 & a & ac \\ 0 & b & bc \\ 1 & c & c^2 \end{bmatrix}.$$

Calculate N^3:

$$N^3 = N \cdot N^2 = \begin{bmatrix} a & ac & a^2c \\ b & bc & b^2c \\ c & c^2 & c^3 \end{bmatrix}.$$

Since N is in companion form, its minimal polynomial can be identified by constructing the characteristic polynomial. For a matrix of this type, if we define the polynomial $p(x) = x^3 - cx^2 - bx - a$, then $p(N) = 0$. Therefore, $p(x)$ is the minimal polynomial of N.