Problem 1

Let $\mathbb{F}$ be a field, and let $R = \left\{ \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} : a, b, c, d, e, f \in \mathbb{F} \right\}$.

a) Show that R is a subring of the ring $M_3(\mathbb{F})$ of 3×3 matrices over $\mathbb{F}$.

Let $A = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}$, $A' = \begin{pmatrix} a' & b' & c' \\ 0 & d' & e' \\ 0 & 0 & f' \end{pmatrix}$ be elements of R. Then

$$AA' = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \begin{pmatrix} a' & b' & c' \\ 0 & d' & e' \\ 0 & 0 & f' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bd' & ac' + be' + cf' \\ 0 & dd' & de' + ef' \\ 0 & 0 & ff' \end{pmatrix} \in R$$

and

$$A - A' = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} - \begin{pmatrix} a' & b' & c' \\ 0 & d' & e' \\ 0 & 0 & f' \end{pmatrix} = \begin{pmatrix} a - a' & b - b' & c - c' \\ 0 & d - d' & e - e' \\ 0 & 0 & f - f' \end{pmatrix} \in R.$$

Also

$$1_{M_3(\mathbb{F})} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in R.$$

Hence R is a subring of $M_3(\mathbb{F})$.

Show that $I_1 = \left\{ \begin{pmatrix} 0 & b & c \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} : b, c \in \mathbb{F} \right\}$ is an ideal of R.

Let $A = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \in R$ and $X = \begin{pmatrix} 0 & p & q \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, X' = \begin{pmatrix} 0 & p' & q' \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in I_1$. Then

$$X - X' = \begin{pmatrix} 0 & p & q \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & p' & q' \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & p - p' & q - q' \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in I_1,$$

$$AX = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \begin{pmatrix} 0 & p & q \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ap & aq \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in I_1$$

and

$$XA = \begin{pmatrix} 0 & p & q \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} = \begin{pmatrix} 0 & pd & pe+qf \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in I_1.$$

Note that I_1 is also nonempty. Hence, I_1 is an ideal of R.

b) Show that I_1 is nilpotent.

Let $X = \begin{pmatrix} 0 & p & q \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & p' & q' \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in I_1$. Then

$$XY = \begin{pmatrix} 0 & p & q \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & p' & q' \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

It follows that $I_1^2 = 0$, so I_1 is nilpotent.

Determine whether or not R is a semisimple ring and whether or not R is a left artinian ring.

We see that R has a nonzero nilpotent ideal, I_1. By the Wedderburn-Artin theorem, a ring is semisimple if and only if it has no nonzero nilpotent ideals and is left artinian. Hence R is not semisimple.

The ring R is an $\mathbb{F}$-algebra with basis as $\mathbb{F}$-vector space given by the elementary matrices E_{11}, E_{12}, E_{13}, E_{22}, E_{23}, E_{33}. Hence it is a finite-dimensional $\mathbb{F}$-algebra and therefore left artinian.

c) Let $I_2 = \left\{ \begin{pmatrix} 0 & b & c \\ 0 & d & e \\ 0 & 0 & 0 \end{pmatrix} : b, c, d, e \in \mathbb{F} \right\}$. You may assume that I_2 is an ideal of R.

Determine whether or not R/I_2 is a semisimple ring and whether or not R/I_2 is a left artinian ring.

Define $\varphi : R \to \mathbb{F} \times \mathbb{F}$ by setting

$$\varphi\left(\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}\right) = (a, f).$$

Then

$$\varphi\left(\begin{pmatrix}a & b & c\\ 0 & d & e\\ 0 & 0 & f\end{pmatrix}\begin{pmatrix}a' & b' & c'\\ 0 & d' & e'\\ 0 & 0 & f'\end{pmatrix}\right) = \varphi\left(\begin{pmatrix}aa' & ab'+bd' & ac'+be'+cf'\\ 0 & dd' & de'+ef'\\ 0 & 0 & ff'\end{pmatrix}\right) = (aa', ff'),$$

while

$$\varphi\left(\begin{pmatrix}a & b & c\\ 0 & d & e\\ 0 & 0 & f\end{pmatrix}\right)\varphi\left(\begin{pmatrix}a' & b' & c'\\ 0 & d' & e'\\ 0 & 0 & f'\end{pmatrix}\right) = (a,f)(a',f') = (aa', ff').$$

So

$$\varphi\left(\begin{pmatrix}a & b & c\\ 0 & d & e\\ 0 & 0 & f\end{pmatrix}\begin{pmatrix}a' & b' & c'\\ 0 & d' & e'\\ 0 & 0 & f'\end{pmatrix}\right) = \varphi\left(\begin{pmatrix}a & b & c\\ 0 & d & e\\ 0 & 0 & f\end{pmatrix}\right)\varphi\left(\begin{pmatrix}a' & b' & c'\\ 0 & d' & e'\\ 0 & 0 & f'\end{pmatrix}\right).$$

We also have:

$$\varphi\left(\begin{pmatrix}a & b & c\\ 0 & d & e\\ 0 & 0 & f\end{pmatrix}+\begin{pmatrix}a' & b' & c'\\ 0 & d' & e'\\ 0 & 0 & f'\end{pmatrix}\right) = \varphi\left(\begin{pmatrix}a+a' & b+b' & c+c'\\ 0 & d+d' & e+e'\\ 0 & 0 & f+f'\end{pmatrix}\right) = (a{+}a', f{+}f'),$$

while

$$\varphi\left(\begin{pmatrix}a & b & c\\ 0 & d & e\\ 0 & 0 & f\end{pmatrix}\right)+\varphi\left(\begin{pmatrix}a' & b' & c'\\ 0 & d' & e'\\ 0 & 0 & f'\end{pmatrix}\right) = (a,f)+(a',f') = (a+a', f+f').$$

So

$$\varphi\left(\begin{pmatrix}a & b & c\\ 0 & d & e\\ 0 & 0 & f\end{pmatrix}+\begin{pmatrix}a' & b' & c'\\ 0 & d' & e'\\ 0 & 0 & f'\end{pmatrix}\right) = \varphi\left(\begin{pmatrix}a & b & c\\ 0 & d & e\\ 0 & 0 & f\end{pmatrix}\right)+\varphi\left(\begin{pmatrix}a' & b' & c'\\ 0 & d' & e'\\ 0 & 0 & f'\end{pmatrix}\right).$$

Since also $\varphi(1_R) = (1,1) = 1_{\mathbb{F}\times\mathbb{F}}$, we see that φ is a ring homomorphism.

We see easily that the kernel is I_2, and the image is $\mathbb{F}\times\mathbb{F}$, so by the Fundamental Theorem of Homomorphisms,

$$\frac{R}{I_2} \cong \mathbb{F}\times\mathbb{F}\,.$$

Since $\mathbb{F} \cong M_1(\mathbb{F})$ and any field is a division ring, the ring $\mathbb{F}\times\mathbb{F}$ is isomorphic to a finite direct product of matrix rings over division rings, and hence is a semisimple ring (see the Wedderburn-Artin Theorem). Again by the Wedderburn-Artin theorem, $\mathbb{F}\times\mathbb{F}$ is a left artinian ring.

d) $\boxed{\text{Is } I_2 \text{ a maximal ideal of } R\text{? If not, find the maximal ideals of } R \text{ containing } I_2.}$

The ideals of $\mathbb{F} \times \mathbb{F}$ are $J_1 \times J_2$ where J_1, J_2 are ideals of $\mathbb{F}$, i.e. where $J_1, J_2 \in \{\{0\}, \mathbb{F}\}$. By the Correspondence Theorem, the ideals of R containing I_2 are the preimages of these under φ, i.e. I_2, R and the ideals:

$$K_1 = \left\{ \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & 0 \end{pmatrix} : a, b, c, d, e \in \mathbb{F} \right\},$$

$$K_2 = \left\{ \begin{pmatrix} 0 & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} : b, c, d, e, f \in \mathbb{F} \right\}.$$

In particular, each of K_1 and K_2 strictly contains I_2 and is strictly contained in R. So I_2 is not a maximal ideal. Since these are all the ideals containing I_2 in R, we see that K_1 and K_2 are the maximal ideals of R containing I_2.

Problem 2

$\boxed{\text{Let } R \text{ be a ring and } M \text{ an } R\text{-module. Prove that } M \text{ is cyclic if and only if } M \cong {}_RR/I \text{ for a left ideal } I \text{ of } R.}$

Suppose that M is a cyclic R-module, so $M = Rm$ for some $m \in M$. Define a map $\varphi : {}_RR \to M$ by setting $\varphi(r) = rm$ for $r \in R$. Then, for $r, r' \in R$:

$$\varphi(r + r') = (r + r')m = rm + r'm = \varphi(r) + \varphi(r')$$

and, for $r, s \in R$:

$$\varphi(sr) = (sr)m = s(rm) = s\varphi(r),$$

so φ is an R-homomorphism. Since $M = Rm$, φ is onto, i.e. $\operatorname{im}(\varphi) = M$. The kernel $I = \ker(\varphi)$ is an R-submodule of ${}_RR$, hence a left ideal of R. Then, by the Fundamental Theorem of Homomorphisms,

$${}_RR/\ker(\varphi) \cong \operatorname{im}(\varphi) = M.$$

Conversely, let I be a left ideal in R. Then I is a left R-submodule of ${}_RR$, so we may consider the quotient module

$${}_RR/I = \{r + I : r \in R\}.$$

We can write this as

$$_RR/I = \{r(1+I) \,:\, r \in R\},$$

and we see that $_RR/I$ is a cyclic R-module. Hence any module isomorphic to $_RR/I$ is a cyclic R-module, as required.

Problem 3

a) Find the Smith normal form of the matrix $\begin{pmatrix} 4 & 4 & 4 \\ 2 & 4 & 3 \\ 4 & 4 & 2 \end{pmatrix}$ over $\mathbb{Z}$.

We apply row and column operations to reduce the matrix to Smith Normal Form:

$$\begin{pmatrix} 4 & 4 & 4 \\ 2 & 4 & 3 \\ 4 & 4 & 2 \end{pmatrix} \xrightarrow[R_1\leftrightarrow R_2]{} \begin{pmatrix} 2 & 4 & 3 \\ 4 & 4 & 4 \\ 4 & 4 & 2 \end{pmatrix} \xrightarrow[C_3-C_1]{C_2-2C_1} \begin{pmatrix} 2 & 0 & 1 \\ 4 & -4 & 0 \\ 4 & -4 & -2 \end{pmatrix} \xrightarrow[C_1\leftrightarrow C_3]{}$$

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & -4 & 4 \\ -2 & -4 & 4 \end{pmatrix} \xrightarrow[C_3-2C_1]{} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -4 & 4 \\ -2 & -4 & 8 \end{pmatrix} \xrightarrow[R_3+2R_1]{} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -4 & 4 \\ 0 & -4 & 8 \end{pmatrix} \xrightarrow[C_3+C_2]{}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & -4 & 4 \end{pmatrix} \xrightarrow[R_3-R_2]{} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & 4 \end{pmatrix} \xrightarrow[(-1)R_2]{} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

b) Let A be an $n \times n$ matrix over a field $\mathbb{F}$. State without proof how the characteristic polynomial of A and the minimum polynomial of A are related to the invariant factors of $A - xI$ over $\mathbb{F}[x]$.

The last invariant factor (i.e. the n, n entry of the Smith Normal Form of $A - xI_n$), if taken to be monic, is equal to the minimum polynomial of A. The product of the nonunit invariant factors of $A - xI_n$ (taken to be monic) is equal to $(-1)^n$ times the characteristic polynomial of A.

Let A be a 6×6 matrix over $\mathbb{Q}$ with minimum polynomial $(x^2 - 3x + 2)^2$. Find the possibilities for the invariant factors of $A - xI$ over $\mathbb{Q}[x]$ and compute the rational canonical form of A in one of the cases.

The nonunit invariant factors of $A - xI_6$ must all divide the minimum polynomial $(x^2 - 3x + 2)^2 = (x-1)^2(x-2)^2$, and their product must have degree 6. Each must divide the next. The unit invariant factors can all be taken to be 1. So the possibilities are as listed below.

We have $(x-1)^2 = x^2-2x+1$, $(x-2)^2 = x^2-4x+4$, $(x-1)(x-2) = x^2-3x+2$ and:

$$\begin{aligned}(x-1)^2(x-2)^2 &= (x^2-2x+1)(x^2-4x+4)\\ &= x^4-6x^3+13x^2-12x+4.\end{aligned}$$

The corresponding rational canonical forms are obtained by taking 2×2 block matrices with zero blocks off the diagonal and the companion matrices of the nonunit monic invariant factors of $A - xI_n$ on the diagonal (note only one was asked for).

$$1,1,1,1,(x-1)^2,(x-1)^2(x-2)^2, \begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 0\\ 1 & 2 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & -4\\ 0 & 0 & 1 & 0 & 0 & 12\\ 0 & 0 & 0 & 1 & 0 & -13\\ 0 & 0 & 0 & 0 & 1 & 6 \end{pmatrix}$$

$$1,1,1,1,(x-1)(x-2),(x-1)^2(x-2)^2, \begin{pmatrix} 0 & -2 & 0 & 0 & 0 & 0\\ 1 & 3 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & -4\\ 0 & 0 & 1 & 0 & 0 & 12\\ 0 & 0 & 0 & 1 & 0 & -13\\ 0 & 0 & 0 & 0 & 1 & 6 \end{pmatrix}$$

$$1,1,1,1,(x-2)^2,(x-1)^2(x-2)^2, \begin{pmatrix} 0 & -4 & 0 & 0 & 0 & 0\\ 1 & 4 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & -4\\ 0 & 0 & 1 & 0 & 0 & 12\\ 0 & 0 & 0 & 1 & 0 & -13\\ 0 & 0 & 0 & 0 & 1 & 6 \end{pmatrix}$$

$$1,1,1,(x-1),(x-1),(x-1)^2(x-2)^2, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & -4\\ 0 & 0 & 1 & 0 & 0 & 12\\ 0 & 0 & 0 & 1 & 0 & -13\\ 0 & 0 & 0 & 0 & 1 & 6 \end{pmatrix}$$

$$1, 1, 1, (x-2), (x-2), (x-1)^2(x-2)^2, \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -4 \\ 0 & 0 & 1 & 0 & 0 & 12 \\ 0 & 0 & 0 & 1 & 0 & -13 \\ 0 & 0 & 0 & 0 & 1 & 6 \end{pmatrix}$$

Problem 4

Let R be a ring and let M and N be R-modules.

a) Let $\varphi : M \to N$ be an R-homomorphism. Give the definition of the kernel of φ and show that it is a submodule of M.

The kernel of φ is:

$$\ker \varphi = \{m \in M \,:\, \varphi(m) = 0_N\}.$$

We have $\varphi(0_M) = 0_N$, so $\ker \varphi$ is nonempty. Let $m_1, m_2 \in \ker \varphi$. Then $\varphi(m_1) = \varphi(m_2) = 0_N$. We have

$$\varphi(m_1 - m_2) = \varphi(m_1) - \varphi(m_2) = 0_N - 0_N = 0_N,$$

so $m_1 - m_2 \in \ker \varphi$. Hence $\ker \varphi$ is a subgroup of M. For $r \in R$ and $m \in \ker \varphi$, we have

$$\varphi(rm) = r\varphi(m) = r0_N = 0_N,$$

so $rm \in \ker \varphi$. Hence $\ker \varphi$ is a submodule of M.

Show that if φ has an inverse $\varphi^{-1} : N \to M$ then φ^{-1} is an R-homomorphism.

Let $r \in R$ and $n \in N$. Then $\varphi(\varphi^{-1}(rn)) = rn$ and $\varphi(r\varphi^{-1}(n)) = r\varphi(\varphi^{-1}(n)) = rn$, so $\varphi^{-1}(rn) = r\varphi^{-1}(n)$, as φ is injective.

Let $n_1, n_2 \in N$. Then

$$\varphi(\varphi^{-1}(n_1 + n_2)) = n_1 + n_2$$

and

$$\varphi(\varphi^{-1}(n_1) + \varphi^{-1}(n_2)) = \varphi(\varphi^{-1}(n_1)) + \varphi(\varphi^{-1}(n_2)) = n_1 + n_2,$$

so

$$\varphi^{-1}(n_1+n_2)=\varphi^{-1}(n_1)+\varphi^{-1}(n_2),$$

as φ is injective.

Hence φ^{-1} is an R-homomorphism from N to M.

b) Suppose that M and N are simple R-modules. Prove that any R-homomorphism φ from M to N is either zero or an isomorphism.

Let M and N be simple R-modules and $\varphi : M \to N$ an R-homomorphism. Then M is nonzero and its only submodules are $\{0_M\}$ and M. Similarly, N is nonzero and its only submodules are $\{0_N\}$ and N. Since $\ker\varphi$ is a submodule of M and M is simple, we have that $\ker\varphi = \{0_M\}$ or M. Since $\operatorname{im}\varphi$ is a submodule of N and N is simple, we have that $\operatorname{im}\varphi = \{0_N\}$ or N.

If $\ker\varphi = M$ or $\operatorname{im}\varphi = \{0_N\}$ then φ is the map sending every element of M to zero. The only remaining possibility is that $\ker\varphi = \{0_M\}$ and $\operatorname{im}\varphi = N$. But then φ is injective and surjective, hence an isomorphism.

Let $\operatorname{End}_R(M)$ be the ring of R-homomorphisms from M to M. Prove that $\operatorname{End}_R(M)$ is a division ring.

If $M = N$, then, by the above, every nonzero R-homomorphism φ from M to M is an isomorphism and therefore (by part (a)) has an inverse in $\operatorname{End}_R(M)$. Since M is non-zero, the identity map from M to M is not the zero map. Therefore $\operatorname{End}_R(M)$ is a division ring.

c) Let n be a positive integer. Show that there is a ring isomorphism

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \operatorname{End}_{\mathbb{Z}}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right).$$

For $x \in \mathbb{Z}$, write $\overline{x}$ for the corresponding element of $\frac{\mathbb{Z}}{n\mathbb{Z}}$. We define a map

$$f : \mathbb{Z} \to \operatorname{End}_{\mathbb{Z}}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right).$$

Given $a \in \mathbb{Z}$, let $f(a) : \frac{\mathbb{Z}}{n\mathbb{Z}} \to \frac{\mathbb{Z}}{n\mathbb{Z}}$ be the map taking $\overline{x}$ to $a\overline{x}$. Then, for $\overline{x}, \overline{y} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$, $f(a)(\overline{x}+\overline{y}) = a(\overline{x}+\overline{y}) = a\overline{x}+a\overline{y} = f(a)(\overline{x})+f(a)(\overline{y})$. For $\overline{x} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ and $r \in \mathbb{Z}$,

$$f(a)(r\overline{x}) = a(r\overline{x}) = (ar)\overline{x} = (ra)\overline{x} = r(a\overline{x}) = rf(a)(\overline{x}).$$

Hence $f(a) \in \mathrm{End}_{\mathbb{Z}}(\frac{\mathbb{Z}}{n\mathbb{Z}})$.

For $a, b \in \mathbb{Z}$ and $\overline{x} \in \frac{Z}{n\mathbb{Z}}$, we have

$$f(a+b)(\overline{x}) = (a+b)\overline{x} = a\overline{x} + b\overline{x} = f(a)(\overline{x}) + f(b)(\overline{x}),$$

so $f(a+b) = f(a) + f(b)$. And

$$f(ab)(\overline{x}) = (ab)\overline{x} = a(b\overline{x}) = f(a)(f(b)(\overline{x})) = (f(a)f(b))(\overline{x}).$$

So $f(ab) = f(a)f(b)$. Also, $f(1)(\overline{x}) = 1\overline{x} = \mathrm{Id}(\overline{x})$, where Id is the identity element of $\mathrm{End}_{\mathbb{Z}}(\frac{\mathbb{Z}}{n\mathbb{Z}})$. So f is a ring homomorphism.

Let $a \in \mathbb{Z}$. Then $f(a)$ is the zero endomorphism of $\frac{\mathbb{Z}}{n\mathbb{Z}}$ if and only if $f(a)(\overline{1}) = 0$, if and only if $a = 0$ in $\frac{\mathbb{Z}}{n\mathbb{Z}}$, if and only if $a \in n\mathbb{Z}$. So the kernel of f is $n\mathbb{Z}$.

Let $\varphi \in \mathrm{End}_{\mathbb{Z}}(\frac{\mathbb{Z}}{n\mathbb{Z}})$. Then

$$\varphi(\overline{x}) = \varphi(\overline{x}1) = \varphi(x\overline{1}) = x\varphi(\overline{1}) = \varphi(\overline{1})\overline{x}$$

for all $x \in \mathbb{Z}$. So $\varphi = f(m)$, where $m \in \mathbb{Z}$ is any element such that $\overline{m} = \varphi(\overline{1})$. Hence f is onto. Applying the Fundamental theorem of ring homomorphisms, we obtain a ring isomorphism:

$$\overline{f} : \frac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathrm{End}_{\mathbb{Z}}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right),$$

as required. Note that $\overline{f}(\overline{a})$ is the map taking $\overline{x}$ to $\overline{ax}$.

Prove that there is exactly one such ring isomorphism.

Let

$$f' : \frac{\mathbb{Z}}{n\mathbb{Z}} \to \mathrm{End}_{\mathbb{Z}}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)$$

be an arbitrary ring isomorphism. Then $f'(\overline{1})$ is the identity map Id on $\frac{\mathbb{Z}}{n\mathbb{Z}}$. Let $0 \leq a \leq n-1$. Then

$$\begin{aligned} f'(\overline{a}) &= f'(\overline{1} + \overline{1} + \cdots + \overline{1}) \\ &= f'(\overline{1}) + f'(\overline{1}) + \cdots + f'(\overline{1}) \end{aligned}$$

(with a terms). So $f'(\overline{a}) = a\,\mathrm{Id}$, i.e. it is the map sending $\overline{x}$ to $a\overline{x} = \overline{ax}$. Hence $f' = \overline{f}$.

Prove that if n is not a prime number, then $\mathbb{Z}/n\mathbb{Z}$ is not a simple $\mathbb{Z}$-module.

Suppose that n is a positive integer which is not a prime number. If $n = 1$ then $\mathbb{Z}/n\mathbb{Z}$ is the zero module, hence not simple. If $n > 1$ then it can be written in the form $n = ab$ where $1 < a, b < n$ are integers. Then, regarding a, b as elements of $\mathbb{Z}/n\mathbb{Z}$, we have $ab = 0$ in $\mathbb{Z}/n\mathbb{Z}$. So if a had an inverse a^{-1}, we'd have $a^{-1}ab = 0$, and therefore $b = 0$ in $\mathbb{Z}/n\mathbb{Z}$, a contradiction (as $1 < b < n$). Hence $\mathbb{Z}/n\mathbb{Z}$ is not a division ring, as $a \neq 0$ in $\mathbb{Z}/n\mathbb{Z}$. Therefore, by part (b) (Schur's Lemma), $\mathbb{Z}/n\mathbb{Z}$ is not a simple $\mathbb{Z}$-module.