Rings and modules - Problem set 5 solutions

Solved on Friday 10.11

Problem 1. (After Chapter 11.3.) Let R be a PID. Let $r, s \in R$ and let $d = \gcd(r, s)$. Show that $(r) + (s) = (d)$.

Solution. We have that $(r) + (s)$ is an ideal (as it is the sum of two ideals). Since R is a PID, we have that $(r) + (s) = (t)$ for some $t \in R$ and it is enough to show that t is a greatest common divisor of r and s. First we have that

$$r = 1r + 0s \in (r) + (s) = (t),$$

and so $r \in (t)$. Then $r = tx$ for some $x \in R$ and so $t \mid r$. Similarly we show that $t \mid s$. Now let $t' \in R$ be such that $t' \mid r$ and $t' \mid s$ and we need to show that $t' \mid t$. First, since $t' \mid r$, there exists $a \in R$ such that $r = t'a$. Moreover, since $t' \mid s$, there exists $b \in R$ such that $s = t'b$. Since

$$t \in (t) = (r) + (s),$$

there exist $y, z \in R$ such that $t = yr + zs$. Then

$$t = yr + zs = y(t'a) + z(t'b) = t'(ya + zb),$$

and so $t' \mid t$, as required.

Problem 2. (After Chapter 20.3) (Exercise 20.3.1 in the book.) Obtain the Smith normal form and rank for the following matrices over a PID R:

(a) $\left(\begin{smallmatrix} 0 & 2 & -1 \\ -3 & 8 & 3 \\ 2 & -4 & -1 \end{smallmatrix}\right)$, where $R = \mathbb{Z}$.

(b) $\left(\begin{smallmatrix} -X-3 & 2 & 0 \\ 1 & -X & 1 \\ 1 & -3 & -X-2 \end{smallmatrix}\right)$, where $R = \mathbb{Q}[X]$.

Solution.

(a)

$$\begin{pmatrix} 0 & 2 & -1 \\ -3 & 8 & 3 \\ 2 & -4 & -1 \end{pmatrix} \overset{C_1 \leftrightarrow C_3}{\longrightarrow} \begin{pmatrix} -1 & 2 & 0 \\ 3 & 8 & -3 \\ -1 & -4 & 2 \end{pmatrix} \overset{\substack{R_2 \to R_2 + 3R_1 \\ R_3 \to R_3 - R_1}}{\longrightarrow} \begin{pmatrix} -1 & 2 & 0 \\ 0 & 14 & -3 \\ 0 & -6 & 2 \end{pmatrix} \overset{C_2 \to C_2 + 2C_1}{\longrightarrow} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 14 & -3 \\ 0 & -6 & 2 \end{pmatrix} \overset{R_2 \to R_2 + R_3}{\longrightarrow}$$
$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 8 & -1 \\ 0 & -6 & 2 \end{pmatrix} \overset{C_2 \leftrightarrow C_3}{\longrightarrow} \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 8 \\ 0 & 2 & -6 \end{pmatrix} \overset{R_3 \to R_3 + 2R_1}{\longrightarrow} \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 8 \\ 0 & 0 & 10 \end{pmatrix} \overset{C_3 \to C_3 + 8C_2}{\longrightarrow} \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 10 \end{pmatrix} \overset{\substack{R_1 \to -R_1 \\ R_2 \to -R_2}}{\longrightarrow}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 10 \end{pmatrix}.$$

(b)

$$\begin{pmatrix} -X-3 & 2 & 0 \\ 1 & -X & 1 \\ 1 & -3 & -X-2 \end{pmatrix} \overset{R_1 \leftrightarrow R_2}{\longrightarrow} \begin{pmatrix} 1 & -X & 1 \\ -X-3 & 2 & 0 \\ 1 & -3 & -X-2 \end{pmatrix} \overset{\substack{C_2 \to C_2 + XC_1 \\ C_3 \to C_3 - C_1}}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ -X-3 & -X^2-3X+2 & X+3 \\ 1 & X-3 & -X-3 \end{pmatrix}$$

$$\overset{\substack{R_2 \to R_2 + (X+3)R_1 \\ R_3 \to R_3 - R_1}}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -X^2-3X+2 & X+3 \\ 0 & X-3 & -X-3 \end{pmatrix} \overset{C_2 \to C_2 + XC_3}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & X+3 \\ 0 & -X^2-2X-3 & -X-3 \end{pmatrix} \overset{C_3 \to C_3 - \frac{X+3}{2}C_2}{\longrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & -X^2-2X-3 & \frac{1}{2}(X^3+5X^2+7X+3) \end{pmatrix} \overset{R_2 \to \frac{1}{2}R_2}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -X^2-2X-3 & \frac{1}{2}(X^3+5X^2+7X+3) \end{pmatrix} \overset{R_3 \to R_3 + (X^2+2}{\longrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{2}(X^3+5X^2+7X+3) \end{pmatrix} \overset{R_3 \to 2R_3}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & X^3+5X^2+7X+3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (X+1)^2(X+3) \end{pmatrix}.$$

Problem 3. (After Chapter 20.3) (Exercise 20.3.3 in the book.) Find the rank of the subgroup of $\mathbb{Z}^4$ generated by each of the following lists of elements.

(a) $(3,6,9,0), (-4,-8,-12,0)$.

(b) $(2,3,1,4), (1,2,3,0), (1,1,1,4)$.

(c) $(-1,2,0,0), (2,-3,1,0), (1,1,1,1)$.

Solution. $\mathbb{Z}^4$ is a $\mathbb{Z}$-module and the rank of each subgroup is just the rank of the submodule of $\mathbb{Z}^4$ generated by these elements. Hence the rank of each subgroup is equal to the rank of the matrix with these vectors as row vectors.

(a) We have

$$\begin{pmatrix} 3 & 6 & 9 & 0 \\ -4 & -8 & -12 & 0 \end{pmatrix} \overset{R_2 \to R_2 + R_1}{\longrightarrow} \begin{pmatrix} 3 & 6 & 9 & 0 \\ -1 & -2 & -3 & 0 \end{pmatrix} \overset{R_1 \leftrightarrow R_2}{\longrightarrow} \begin{pmatrix} -1 & -2 & -3 & 0 \\ 3 & 6 & 9 & 0 \end{pmatrix} \overset{R_1 \to -R_1}{\longrightarrow}$$

$$\begin{pmatrix} 1 & 2 & 3 & 0 \\ 3 & 6 & 9 & 0 \end{pmatrix} \overset{R_2 \to R_3 - 3R_1}{\longrightarrow} \begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \overset{\substack{C_2 \to C_2 - 2C_1 \\ C_3 \to C_3 - 3C_1}}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

and so the rank in this case is 1.

(b) We have

$$\begin{pmatrix} 2 & 3 & 1 & 4 \\ 1 & 2 & 3 & 0 \\ 1 & 1 & 1 & 4 \end{pmatrix} \overset{R_1 \leftrightarrow R_2}{\longrightarrow} \begin{pmatrix} 1 & 2 & 3 & 0 \\ 2 & 3 & 1 & 4 \\ 1 & 1 & 1 & 4 \end{pmatrix} \overset{\substack{R_2 \to R_2 - 2R_1 \\ R_3 \to R_3 - R_1}}{\longrightarrow} \begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & -1 & -5 & 4 \\ 0 & -1 & -2 & 4 \end{pmatrix} \overset{R_2 \to -R_2}{\longrightarrow} \begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & 1 & 5 & -4 \\ 0 & -1 & -2 & 4 \end{pmatrix} \overset{\substack{C_2 \to C_2 - 2C_1 \\ C_3 \to C_3 - 3C_1}}{\longrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 5 & -4 \\ 0 & -1 & -2 & 4 \end{pmatrix} \overset{R_3 \to R_3 + R_2}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 5 & -4 \\ 0 & 0 & 3 & 0 \end{pmatrix} \overset{\substack{C_3 \to C_3 - 5C_2 \\ C_4 \to C_4 + 4C_2}}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 \end{pmatrix},$$

and so the rank in this case is 3.

(c) We have

$$\begin{pmatrix} -1 & 2 & 0 & 0 \\ 2 & -3 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \overset{R_1 \to -R_1}{\longrightarrow} \begin{pmatrix} 1 & -2 & 0 & 0 \\ 2 & -3 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \overset{C_2 \to C_2 + 2C_1}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 3 & 1 & 1 \end{pmatrix} \overset{\substack{R_2 \to R_2 - 2R_1 \\ R_3 \to R_3 - R_1}}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 3 & 1 & 1 \end{pmatrix} \overset{C_3 \to C_3 - C_2}{\longrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 3 & -2 & 1 \end{pmatrix} \overset{\substack{C_2 \to C_2 - 3C_4 \\ C_3 \to C_3 + 2C_4}}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \overset{C_3 \leftrightarrow C_4}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

and so the rank in this case is 3.

Problem 4. (After Chapter 20.3) (Exercise 20.3.2 in the book.) Find the invariant factors of the following matrix over $\mathbb{Q}[X]$: $\begin{pmatrix} 5-X & 1 & -2 & 4 \\ 0 & 5-X & 2 & 2 \\ 0 & 0 & 5-X & 3 \\ 0 & 0 & 0 & 4 \end{pmatrix}$.

Solution. We have

$$\begin{pmatrix} 5-X & 1 & -2 & 4 \\ 0 & 5-X & 2 & 2 \\ 0 & 0 & 5-X & 3 \\ 0 & 0 & 0 & 4 \end{pmatrix} \overset{C_1 \leftrightarrow C_2}{\longrightarrow} \begin{pmatrix} 1 & 5-X & -2 & 4 \\ 5-X & 0 & 2 & 2 \\ 0 & 0 & 5-X & 3 \\ 0 & 0 & 0 & 4 \end{pmatrix} \overset{R_2 \to R_2-(5-X)R_1}{\longrightarrow} \begin{pmatrix} 1 & 5-X & -2 & 4 \\ 0 & -(5-X)^2 & 12-X & 4X-18 \\ 0 & 0 & 5-X & 3 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$

$$\overset{\substack{C_2 \to C_2-(5-X)C_1 \\ C_3 \to C_3+2C_1 \\ C_4 \to C_4-4C_1}}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -(5-X)^2 & 12-X & 4X-18 \\ 0 & 0 & 5-X & 3 \\ 0 & 0 & 0 & 4 \end{pmatrix} \overset{C_2 \leftrightarrow C_4}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4X-18 & 12-X & -(5-X)^2 \\ 0 & 3 & 5-X & 0 \\ 0 & 4 & 0 & 0 \end{pmatrix} \overset{R_2 \leftrightarrow R_4}{\longrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 4X-18 & 12-X & -(5-X)^2 \\ 0 & 3 & 5-X & 0 \end{pmatrix} \overset{R_2 \to \frac{1}{4}R_2}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 4X-18 & 12-X & -(5-X)^2 \\ 0 & 3 & 5-X & 0 \end{pmatrix} \overset{\substack{R_3 \to R_3-(RX-18)R_2 \\ R_4 \to R_4-3R_4}}{\longrightarrow}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 12-X & -(5-X)^2 \\ 0 & 0 & 5-X & 0 \end{pmatrix} \overset{R_2 \to R_2-R_3}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 7 & -(5-X)^2 \\ 0 & 0 & 5-X & 0 \end{pmatrix} \overset{R_3 \to \frac{1}{7}R_3}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -\frac{1}{7}(5-X)^2 \\ 0 & 0 & 5-X & 0 \end{pmatrix}$$

$$\overset{R_4 \to R_4-(5-X)R_3}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -\frac{1}{7}(5-X)^2 \\ 0 & 0 & 0 & \frac{1}{7}(5-X)^3 \end{pmatrix} \overset{C_4 \to C_4+\frac{1}{7}(5-X)^2C_3}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{1}{7}(5-X)^3 \end{pmatrix} \overset{R_4 \to 7R_4}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & (5-X)^3 \end{pmatrix},$$

and so the invariant factors of this matrix are $(1, 1, 1, (5-X)^3)$.

Problem 5. (After Chapter 14.3.) (Exam November 2005, Problem 1.) Let q be a fixed non-zero element in $\mathbb{C}$, the set of complex numbers. Define the subset R_q of the ring of 4×4-matrices over $\mathbb{C}$ by

$$R_q = \left\{ \begin{pmatrix} a & 0 & 0 & 0 \\ b & a & 0 & 0 \\ c & 0 & a & 0 \\ d & c & -qb & a \end{pmatrix} \mid a, b, c, d \in \mathbb{C} \right\}.$$

(a) Show that R_q is a unital ring.

(b) For which q in $\mathbb{C}$ is R_q a commutative ring?

(c) For a given element α in $\mathbb{C}$ define the subset

$$I_\alpha = \left\{ \begin{pmatrix} 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 \\ \alpha x & 0 & 0 & 0 \\ y & \alpha x & -qx & 0 \end{pmatrix} \mid x, y \in \mathbb{C} \right\}$$

of R_q. Show that I_α is a left ideal in R_q for all $\alpha \in \mathbb{C}$.

(d) Show that each of the left ideals I_α is generated by one element as a left ideal. Show that $I_\alpha \cong R_q/I_{\alpha q}$ as left R_q-modules.

Solution.

(a) Since the identity matrix $I_4 \in M_4(\mathbb{C})$ is in R_q, it is enough to show that R_q is a subring of $M_4(\mathbb{C})$. Let $\left(\begin{smallmatrix} a & 0 & 0 & 0 \\ b & a & 0 & 0 \\ c & 0 & a & 0 \\ d & c & -qb & a \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} a' & 0 & 0 & 0 \\ b' & a' & 0 & 0 \\ c' & 0 & a' & 0 \\ d' & c' & -qb' & a' \end{smallmatrix}\right)$ be elements of R_q. Then we have

$$\begin{pmatrix} a & 0 & 0 & 0 \\ b & a & 0 & 0 \\ c & 0 & a & 0 \\ d & c & -qb & a \end{pmatrix} + \begin{pmatrix} a' & 0 & 0 & 0 \\ b' & a' & 0 & 0 \\ c' & 0 & a' & 0 \\ d' & c' & -qb' & a' \end{pmatrix} = \begin{pmatrix} a+a' & 0 & 0 & 0 \\ b+b' & a+a' & 0 & 0 \\ c+c' & 0 & a+a' & 0 \\ d+d' & c+c' & -q(b+b') & a+a' \end{pmatrix} \in R_q,$$

and

$$\begin{pmatrix} a & 0 & 0 & 0 \\ b & a & 0 & 0 \\ c & 0 & a & 0 \\ d & c & -qb & a \end{pmatrix} \begin{pmatrix} a' & 0 & 0 & 0 \\ b' & a' & 0 & 0 \\ c' & 0 & a' & 0 \\ d' & c' & -qb' & a' \end{pmatrix} = \begin{pmatrix} aa' & 0 & 0 & 0 \\ ba'+ab' & aa' & 0 & 0 \\ ca'+ac' & 0 & aa' & 0 \\ da'+cb'-qbc'+ad' & ca'+ac' & -q(ba'+ab') & aa' \end{pmatrix} \in R_q,$$

and so R_q is indeed a subring of $M_4(\mathbb{C})$.

(b) Let $A = \left(\begin{smallmatrix} a & 0 & 0 & 0 \\ b & a & 0 & 0 \\ c & 0 & a & 0 \\ d & c & -qb & a \end{smallmatrix}\right)$ and $A' = \left(\begin{smallmatrix} a' & 0 & 0 & 0 \\ b' & a' & 0 & 0 \\ c' & 0 & a' & 0 \\ d' & c' & -qb' & a' \end{smallmatrix}\right)$ be elements of R_q. Then we compute

$$AA' = \begin{pmatrix} a & 0 & 0 & 0 \\ b & a & 0 & 0 \\ c & 0 & a & 0 \\ d & c & -qb & a \end{pmatrix} \begin{pmatrix} a' & 0 & 0 & 0 \\ b' & a' & 0 & 0 \\ c' & 0 & a' & 0 \\ d' & c' & -qb' & a' \end{pmatrix} = \begin{pmatrix} aa' & 0 & 0 & 0 \\ ba'+ab' & aa' & 0 & 0 \\ ca'+ac' & 0 & aa' & 0 \\ da'+cb'-qbc'+ad' & ca'+ac' & -q(ba'+ab') & aa' \end{pmatrix},$$

and

$$A'A = \begin{pmatrix} a' & 0 & 0 & 0 \\ b' & a' & 0 & 0 \\ c' & 0 & a' & 0 \\ d' & c' & -qb' & a' \end{pmatrix} \begin{pmatrix} a & 0 & 0 & 0 \\ b & a & 0 & 0 \\ c & 0 & a & 0 \\ d & c & -qb & a \end{pmatrix} = \begin{pmatrix} a'a & 0 & 0 & 0 \\ b'a+a'b & a'a & 0 & 0 \\ c'a+a'c & 0 & a'a & 0 \\ d'a+c'b-qb'c+a'd & c'a+a'c & -q(b'a+a'b) & a'a \end{pmatrix}.$$

We observe that all the coefficients of the matrices AA' and $A'A$ agree, except for row 4 column 1. Hence $AA' = A'A$ if and only if

$$\begin{aligned} da'+cb'-qbc'+ad' = d'a+c'b-qb'c+a'd &\iff cb'-qbc' = c'b-qb'c \\ &\iff cb'-c'b = qbc'-qb'c \\ \iff cb'-c'b = q(bc'-b'c) &\iff cb'-c'b = -q(cb'-c'b) \end{aligned}$$

and this last equality must hold for all $b, b', c, c' \in \mathbb{C}$. We conclude that this is true if and only if $q = -1$ and since the matrices A and A' were arbitrary, we obtain that R_q is commutative if and only if $q = -1$.

(c) First of all the zero matrix is clearly in I_α. Hence $I_\alpha \neq 0$. Next, let $\left(\begin{smallmatrix} 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 \\ \alpha x & 0 & 0 & 0 \\ y & \alpha x & -qx & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 & 0 & 0 \\ x' & 0 & 0 & 0 \\ \alpha x' & 0 & 0 & 0 \\ y' & \alpha x' & -qx' & 0 \end{smallmatrix}\right) \in I_\alpha$ and $\left(\begin{smallmatrix} a & 0 & 0 & 0 \\ b & a & 0 & 0 \\ c & 0 & a & 0 \\ d & c & -qb & a \end{smallmatrix}\right) \in R_q$. We have

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 \\ \alpha x & 0 & 0 & 0 \\ y & \alpha x & -qx & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ x' & 0 & 0 & 0 \\ \alpha x' & 0 & 0 & 0 \\ y' & \alpha x' & -qx' & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ x+x' & 0 & 0 & 0 \\ \alpha(x+x') & 0 & 0 & 0 \\ y+y' & \alpha(x+x') & -q(x+x') & 0 \end{pmatrix} \in I_\alpha,$$

and

$$\begin{pmatrix} a & 0 & 0 & 0 \\ b & a & 0 & 0 \\ c & 0 & a & 0 \\ d & c & -qb & a \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 \\ \alpha x & 0 & 0 & 0 \\ y & \alpha x & -qx & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ ax & 0 & 0 & 0 \\ \alpha(ax) & 0 & 0 & 0 \\ cx-q\alpha bx+ay & \alpha(ax) & -q(ax) & 0 \end{pmatrix} \in I_\alpha.$$

Hence I_α is a left ideal in R_q.

(d) We claim that that I_α is generated as a left ideal by the matrix $M_\alpha = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \alpha & 0 & 0 & 0 \\ 0 & \alpha & -q & 0 \end{pmatrix}$. Clearly $M_\alpha \in I_\alpha$ and so $R_q M_\alpha \subseteq I_\alpha$. For the other inclusion, let $X = \begin{pmatrix} 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 \\ \alpha x & 0 & 0 & 0 \\ y & \alpha x & -qx & 0 \end{pmatrix} \in I_\alpha$. Then for $A = \begin{pmatrix} x & 0 & 0 & 0 \\ 0 & x & 0 & 0 \\ y & 0 & x & 0 \\ 0 & y & 0 & x \end{pmatrix} \in R_q$ we have

$$AM_\alpha = \begin{pmatrix} x & 0 & 0 & 0 \\ 0 & x & 0 & 0 \\ y & 0 & x & 0 \\ 0 & y & 0 & x \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \alpha & 0 & 0 & 0 \\ 0 & \alpha & -q & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 \\ \alpha x & 0 & 0 & 0 \\ y & \alpha x & -qx & 0 \end{pmatrix} = X.$$

Since $X = AM_\alpha \in R_q M_\alpha$, we conclude that $I_\alpha \subseteq R_q M_\alpha$ and so I_α is generated as a left ideal by M_α.

Now consider the map $\phi : R \to I_\alpha$ given by left multiplication with M_α, that is for $A \in R_q$ we set $\phi(A) = AM_\alpha$. Then ϕ is a homomorphism of left R_q-modules since for any $A, B \in R_q$ we have

$$\phi(A+B) = (A+B)M_\alpha = AM_\alpha + BM_\alpha = \phi(A) + \phi(B),$$

and

$$\phi(AB) = (AB)M_\alpha = A(BM_\alpha) = A\phi(B).$$

Moreover, since

$$I_\alpha = R_q M_\alpha = \{AM_\alpha \mid A \in R_q\},$$

it follows that ϕ is surjective. Now let $A = \begin{pmatrix} a & 0 & 0 & 0 \\ b & a & 0 & 0 \\ c & 0 & a & 0 \\ d & c & -qb & a \end{pmatrix} \in \ker(\phi)$. Then $\phi(A) = 0$ or $AM_\alpha = 0$, that is,

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 & 0 & 0 \\ b & a & 0 & 0 \\ c & 0 & a & 0 \\ d & c & -qb & a \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \alpha & 0 & 0 & 0 \\ 0 & \alpha & -q & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ a & 0 & 0 & 0 \\ \alpha a & 0 & 0 & 0 \\ c - q\alpha b & a\alpha & -q\alpha & 0 \end{pmatrix}$$

from which we obtain that $a = 0$ and $c = q\alpha b$. Then

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ b & 0 & 0 & 0 \\ (\alpha q)b & 0 & 0 & 0 \\ d & (\alpha q)b & -qb & 0 \end{pmatrix} \in I_{\alpha q}.$$

Hence $\ker(\phi) \subseteq I_{\alpha q}$. For the other inclusion, let $X' = \begin{pmatrix} 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 \\ (\alpha q)x & 0 & 0 & 0 \\ y & (\alpha q)x & -qx & 0 \end{pmatrix} \in I_{\alpha q}$. Then

$$\phi(X') = X'M_\alpha = \begin{pmatrix} 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 \\ (\alpha q)x & 0 & 0 & 0 \\ y & (\alpha q)x & -qx & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \alpha & 0 & 0 & 0 \\ 0 & \alpha & -q & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

which shows that $\ker(\phi) \subseteq I_{\alpha q}$. Therefore $I_{\alpha q} = \ker(\phi)$. Then by the first isomorphism theorem for modules we obtain that

$$R_q / I_{\alpha q} = R_q / \ker(\phi) \cong \mathrm{Im}(\phi) = I_\alpha,$$

as required.

Problem 6. (After Chapter 10.2.)

(a) Let R be a unital ring. An idempotent e of R is called *central* if $e \in Z(R)$. We say that R is *connected* if there exist no nonzero unital rings T_1, T_2 such that $R \cong T_1 \times T_2$. Show that the following are equivalent

(i) R is connected.

(ii) the only central idempotents of R are 0 and 1.

(Hint: to show that (i) implies (ii), assume instead that there exists a central idempotent $e \in R$ with $e \notin \{0,1\}$ and consider the ring $eR \times (1-e)R$.)

(b) Let $R_1, \ldots, R_p$ be unital rings. Show that the following are equivalent.

(i) The ring $R_1 \times \cdots \times R_p$ has exactly 2^p central idempotents.

(ii) $R_1, \ldots, R_p$ are all connected rings.

(Hint: show first that $R_1 \times \cdots \times R_p$ has at least 2^p idempotents irrespectively of $R_1, \ldots, R_p$ being connected.)

(c) Let $R_1, \ldots, R_p$ and $S_1, \ldots, S_q$ be connected unital rings. Show that if there is a ring isomorphism

$$R_1 \times \cdots \times R_p \cong S_1 \times \cdots \times S_q,$$

then $p = q$.

(d) Let D be a division ring and $n > 0$ a positive integer. Show that the ring $M_n(D)$ is connected. *(Hint: use Problem 8 from Problem Set 1 to describe the center of $M_n(R)$, using the obvious generalization from the case 2 to the case n.)*

(e) Let $D_1, \ldots, D_p$ and $D'_1, \ldots, D'_q$ be division rings and let $n_1, \ldots, n_p$ and $k_1, \ldots, k_q$ be positive integers. Show that if there is a ring isomorphism

$$M_{n_1}(D_1) \times \cdots \times M_{n_p}(D_p) \cong M_{k_1}(D'_1) \times \cdots \times M_{k_q}(D'_q),$$

then $p = q$.

Solution.

(a) Assume first that (i) holds. Assume to a contradiction that there exists an idempotent $e \in Z(R)$ with $e \notin \{0,1\}$. Then $(1-e)^2 = 1 - e - e + e^2 = 1 - 2e + e = 1 - e$ is also an idempotent and, since $e \notin \{0,1\}$, we also have that $1 - e \notin \{0,1\}$. Moreover, for any $r \in R$ we have

$$(1-e)r = r - er = r - re = r(1-e),$$

and so $(1-e)$ is central as well. Consider the ideals eR and $(1-e)R$ of R. Clearly $eR \neq 0$ since $0 \neq e = e^2 \in eR$ and similarly $(1-e)R \neq 0$ since $0 \neq (1-e) = (1-e)^2 \in (1-e)R$. We define $f : R \to eR \times (1-e)R$ via $f(r) = (er, (1-e)r)$. We claim that f is a ring homomorphism. Let $r, s \in R$. Then

$$f(r+s) = (e(r+s), (1-e)(r+s)) = (er, (1-e)r) + (es, (1-e)s) = f(r) + f(s),$$

and, using that $e, (1-e) \in Z(R)$, we have

$$f(rs) = (ers, (1-e)rs) = (e^2rs, (1-e)^2rs) = ((er)(es), (1-e)r(1-e)s) = (er, (1-e)r)(es, (1-e)s) = f(r)f(s).$$

We now claim that f is a ring isomorphism. Assume that $f(r) = (0,0)$. Then $(0,0) = f(r) = (er, (1-e)r)$ gives that $er = 0$ and $(1-e)r = 0$. Hence

$$r = 1r = (1 - e + e)r = (1-e)r + er = 0 + 0 = 0,$$

and so $\ker f = \{0\}$. This shows that f is injective. Now let $(es, (1-e)t) \in eR \times (1-e)R$. Then

$$f(es+(1-e)t) = (e(es+(1-e)t), (1-e)(es+(1-e)t)) = (e^2s+(e-e^2)t, (e-e^2)s+(1-e)^2t) = (es, (1-e)t),$$

showing that f is surjective. Hence f is indeed a ring isomorphism. But then $R \cong eR \times (1-e)R$ contradicts (i). Hence such a central idempotent e does not exist and so (ii) holds.

Now assume that (ii) holds. Assume to a contradiction that R is not connected and so there exist nonzero rings T_1, T_2 such that $R \cong T_1 \times T_2$. Consider the element $(1,0) \in T_1 \times T_2$. We have $(1,0)^2 = (1,0)$ and so $(1,0)$ is an idempotent with $(1,0) \neq (0,0)$ and $(1,0) \neq (1,1)$. Moreover, for every $(t_1, t_2) \in T_1 \times T_2$ we have

$$(1,0)(t_1,t_2) = (1t_1, 0t_2) = (t_1, 0) = (t_1 1, t_2 0) = (t_1, t_2)(1,0),$$

and so $(1,0) \in Z(R)$. But this contradicts (ii). Hence such rings T_1 and T_2 do not exist and so R is connected

(b) For $i \in \{1, \ldots, p\}$ let $e_i \in R_i$ be a central idempotent. Then

$$(e_1, \ldots, e_p)^2 = (e_1^2, \ldots, e_p^2) = (e_1, \ldots, e_p)$$

which shows that $(e_1, \ldots, e_p)$ is an idempotent. Moreover for all $(r_1, \ldots, r_p) \in R_1 \times \cdots \times R_p$ we have

$$(e_1, \ldots, e_p)(r_1, \ldots, r_p) = (e_1 r_1, \ldots, e_p r_p) = (r_1 e_1, \ldots, r_p e_p) = (r_1, \ldots, r_p)(e_1, \ldots, e_p),$$

and so $(e_1, \ldots, e_p) \in Z(R_1 \times \cdots \times R_p)$. Since 0 and 1 are both central idempotents of R_i, we conclude that there are at least 2^p idempotents in $R_1 \times \cdots \times R_p$.

Assume now that (i) holds. Assume to a contradiction that the ring R_i is not connected for some $i \in \{1, \ldots, p\}$. Then by part (a) there exists a central idempotent $e \in R_i$ with $e \neq \{0, 1\}$. But then

$$(0, \ldots, 0, e, 0, \ldots, 0)$$

is a central idempotent of $R_1 \times \cdots \times R_p$ in addition to the ones from the previous paragraph. Then $R_1 \times \cdots \times R_p$ has at least $2^p + 1$ central idempotents, which is a contradiction. Hence (ii) holds.

Assume now that (ii) holds. Assume to a contradiction that (i) fails, that is, there exist at lest $2^p + 1$ central idempotents in $R_1 \times \cdots \times R_p$ (since we know that there exist at least 2^p). Then there exists a central idempotent $(e_1, \ldots, e_p) \in R_1 \times \cdots \times R_p$ different from with some $e_i \notin \{0, 1\}$. Then

$$(e_1, \ldots, e_i, \ldots, e_p) = (e_1, \ldots, e_i, \ldots, e_p)^2 = (e_1^2, \ldots, e_i^2, \ldots, e_p^2)$$

gives $e_i = e_i^2$ and so e_i is an idempotent of R_i different than 0 or 1. Moreover, for any $r \in R_i$ we have

$$(0, \ldots, re_i, \ldots, 0) = (0, \ldots, r, \ldots, 0)(e_1, \ldots, e_i, \ldots, e_p) = (e_1, \ldots, e_i, \ldots, e_p)(0, \ldots, r, \ldots, 0) = (0, \ldots, e_i r, \ldots, 0)$$

and so $re_i = e_i r$. Hence $e_i \in Z(R_i)$. But by part (a) we conclude that R_i is not connected, which contradicts (ii). Hence (i) holds.

(c) By part (b) we know that there exist 2^p central idempotents in $R_1 \times \cdots \times R_p$ and that there exist 2^q central idempotents in $S_1 \times \cdots \times S_q$. Since the two rings are isomorphic we conclude that $2^p = 2^q$ and so $p = q$.

(d) By Problem 8 in Problem Set 1 (generalizing from 2 to n) we know that

$$Z(M_n(R)) = \left\{ \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a \end{pmatrix} \middle| \, a \in Z(R) \right\}.$$

Now let $A = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a \end{pmatrix} \in Z(M_n(R))$ be an idempotent. We have

$$\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a \end{pmatrix} = A = A^2 = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a \end{pmatrix}^2 = \begin{pmatrix} a^2 & 0 & \cdots & 0 \\ 0 & a^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a^2 \end{pmatrix}$$

and so $a = a^2$. It follows that $a(1 - a) = 0$. Since D is an integral domain, we obtain that $a = 0$ or $a = 1$. Hence $A = 0$ or $A = I_n$ are the only central idempotents of $M_n(R)$. By part (a) we obtain that $M_n(R)$ is connected.

(e) Each of the rings $M_{n_1}(D_1), \ldots, M_{n_p}(D_p), M_{k_1}(D_1'), \ldots, M_{k_q}(D_q')$ is a connected unital ring by part (d). We conclude by part (c) that $p = q$ as required.

Problem 7. (After Chapter 19.2.) (Exam November 2005, Problem 4.) Let R be a unital ring and let M be a noetherian left R-module. Show that any surjective homomorphism of R-modules $f : M \to M$ is an isomorphism. (Hint: Consider the chain $\ker(f) \subseteq \ker(f^2) \subseteq \ker(f^3) \subseteq \cdots$ of submodules of M).

Solution. Since f is a surjective homomorphism of R-modules, it is enough to show that f is injective. Let $m \in \ker f$ such that $f(m) = 0$. Since M is a noetherian left R-module, the sequence

$$\ker(f) \subseteq \ker(f^2) \subseteq \ker(f^3) \subseteq \cdots$$

stabilizes. That is, there exists n such that

$$\ker(f^n) = \ker(f^{n+1}) = \ker(f^{n+2}) = \cdots .$$

Since f is surjective, there exists $m_1 \in M$ such that

$$f(m_1) = m.$$

Furthermore, there exists $m_2 \in M$ such that $f(m_2) = m_1$ and so

$$f^2(m_2) = f(f(m_2)) = f(m_1) = m.$$

Continuing this way, we conclude that there exists $m_n \in M$ such that $f^n(m_n) = m$. Then

$$f^{n+1}(m_n) = f(f^n(m_n)) = f(m) = 0$$

and so $m_n \in \ker(f^{n+1}) = \ker(f^n)$. Since $m \in \ker(f^n)$ we obtain

$$m = f^n(m_n) = 0.$$

Therefore $m = 0$. Since $m \in \ker(f)$ was arbitrary, we conclude that $\ker(f) = \{0\}$ and so f is injective.

Problem 8. (After Chapter 19.3.) (Exam November 2005, Problem 3.) Let $\mathbb{C}$ be the field of complex numbers and $\mathbb{C}[X]$ the polynomial ring over $\mathbb{C}$ in one variable X. Let $\alpha \in \mathbb{C}$ be a complex number.

(a) Show that the map $\phi_\alpha : \mathbb{C}[X] \to \mathbb{C}$ defined by $\phi_\alpha(f(X)) = f(\alpha)$ is a surjective ring homomorphism, and use this to show that the ideal generated by $X - \alpha$ is a maximal ideal in $\mathbb{C}[X]$.

(b) For which $n \geq 1$ is the ring

$$\begin{pmatrix} \frac{\mathbb{C}[X]}{((X-\alpha)^n)} & \frac{\mathbb{C}[X]}{((X-\alpha)^n)} \\ \frac{\mathbb{C}[X]}{((X-\alpha)^n)} & \frac{\mathbb{C}[X]}{((X-\alpha)^n)} \end{pmatrix}$$

semisimple?

Solution.

(a) First let us show that ϕ_α is a ring homomorphism. For any $f(X), g(X) \in \mathbb{C}[X]$ we have

$$\phi_\alpha(f(X) + g(X)) = \phi_\alpha((f+g)(X)) = (f+g)(\alpha) = f(\alpha) + g(\alpha) = \phi_\alpha(f(X)) + \phi_\alpha(g(X)),$$

and

$$\phi_\alpha(f(X)g(X)) = \phi_\alpha((fg)(X)) = (fg)(\alpha) = f(\alpha)g(\alpha) = \phi_\alpha(f(X))\phi_\alpha(g(X)),$$

and so ϕ_α is indeed a ring homomorphism.

Now we show that ϕ_α is surjective. Let $z \in \mathbb{C}$. Set $f_z(X) = X - (\alpha - z) \in \mathbb{C}[X]$. Then

$$\phi_\alpha(f_z(X)) = f_z(\alpha) = \alpha - (\alpha - z) = z,$$

and so $\phi_\alpha(f_z(X)) = z$, which shows that ϕ_α is surjective. In other words we have that $\operatorname{Im} \phi_\alpha = \mathbb{C}$.

Now we claim that $\ker \phi_\alpha = (X-\alpha)$, that is the kernel of ϕ_α is the ideal of $\mathbb{C}[X]$ generated by $X-\alpha$. First let $f(X) \in (X-\alpha)$. Then $f(X) = g(X)(X-\alpha)$ for some $g(X) \in \mathbb{C}[X]$ and so

$$\phi_\alpha(f(X)) = \phi_\alpha(g(X)(X-\alpha)) = g(\alpha)(\alpha-\alpha) = 0,$$

and so $f(X) \in \ker \phi_\alpha$. This shows that $(X-\alpha) \subseteq \ker \phi_\alpha$. For the other inclusion let $h(X) \in \ker \phi_\alpha$. Then

$$\phi_\alpha(h(X)) = 0 \implies h(\alpha) = 0.$$

It follows that $X-\alpha \mid h(X)$ and so $h(X) = g(X)(X-\alpha)$ for some $h(X) \in \mathbb{C}[X]$, and so $h(X) \in (X-\alpha)$. This shows that $\ker \phi_\alpha \subseteq (X-\alpha)$ and so $\ker \phi_\alpha = (X-\alpha)$. By the first isomorphism theorem for rings, we obtain that

$$\tfrac{\mathbb{C}[X]}{(X-\alpha)} = \tfrac{\mathbb{C}[X]}{\ker \phi_\alpha} \cong \operatorname{Im} \phi_\alpha = \mathbb{C},$$

and so $\frac{\mathbb{C}[X]}{(X-\alpha)}$ is a field. By Theorem 6.3 we conclude that $(X-\alpha)$ is a maximal ideal in $\mathbb{C}[X]$.

(b) Set $U_n = \frac{\mathbb{C}[X]}{((X-\alpha)^n)}$ and $R_n = M_2(U_n)$ so that the question becomes for which $n \geq 1$ is the ring R_n semisimple.

Let $n = 1$. Then by part (a) we have that $U_1 \cong \mathbb{C}$ and so $R_1 = M_2(\mathbb{C})$. Since $\mathbb{C}$ is a field, it follows that R_1 is semisimple by the Wedderburn–Artin theorem.

Now let $n > 1$. We claim that R_n is not semisimple. By Proposition 14.5 we have that R_n is semisimple if and only if R_n is left artinian and there exist no nonzero nilpotent ideals in R_n. Hence it is enough to construct a nonzero nilpotent ideal in R_n. Let

$$I = \left(\begin{pmatrix} \overline{X-\alpha} & \overline{X-\alpha} \\ \overline{X-\alpha} & \overline{X-\alpha} \end{pmatrix} \right),$$

that is I is the two-sided ideal generated by the matrix $M = \left(\begin{smallmatrix} \overline{X-\alpha} & \overline{X-\alpha} \\ \overline{X-\alpha} & \overline{X-\alpha} \end{smallmatrix} \right) \in R_n$. We claim that $M \neq 0$. It is enough to show that $\overline{X-\alpha} \in U_n = \frac{\mathbb{C}[X]}{((X-\alpha)^n)}$ is nonzero. Assume to a contradiction that $\overline{X-\alpha} = 0$. Then $X-\alpha \in (X-\alpha)^n$ and so

$$X-\alpha = f(X)(X-\alpha)^n$$

for some $f(X) \in \mathbb{C}[X]$. Clearly $f(X) \neq 0$, and so the degree of the left hand-side is 1 while the degree of the right hand side is at least $n \geq 2$, which is a contradiction. Hence $\overline{X-\alpha} \neq 0$. Now we claim that $I^n = 0$. An element of I^n is a sum of elements of the form

$$M_1 M_2 \cdots M_n$$

where $M_i \in I$. Since $M_i \in I = R_n M$, we have that

$$\begin{aligned} M_i = \begin{pmatrix} \overline{p_i(X)} & \overline{q_i(X)} \\ \overline{r_i(X)} & \overline{s_i(X)} \end{pmatrix} \begin{pmatrix} \overline{X-\alpha} & \overline{X-\alpha} \\ \overline{X-\alpha} & \overline{X-\alpha} \end{pmatrix} &= \begin{pmatrix} (\overline{p_i(X)+q_i(X)})(\overline{X-\alpha}) & (\overline{p_i(X)+q_i(X)})(\overline{X-\alpha}) \\ (\overline{r_i(X)+s_i(X)})(\overline{X-\alpha}) & (\overline{r_i(X)+s_i(X)})(\overline{X-\alpha}) \end{pmatrix} \\ &= \begin{pmatrix} \overline{f_i(X)}(\overline{X-\alpha}) & \overline{f_i(X)}(\overline{X-\alpha}) \\ \overline{g_i(X)}(\overline{X-\alpha}) & \overline{g_i(X)}(\overline{X-\alpha}) \end{pmatrix}, \end{aligned}$$

Where $f_i(X) = p_i(X) + g_i(X)$ and $g_i(X) = r_i(X) + s_i(X)$. Then

$$\begin{aligned} M_1 M_2 &= \begin{pmatrix} \overline{f_1(X)}(\overline{X-\alpha}) & \overline{f_1(X)}(\overline{X-\alpha}) \\ \overline{g_1(X)}(\overline{X-\alpha}) & \overline{g_1(X)}(\overline{X-\alpha}) \end{pmatrix} \begin{pmatrix} \overline{f_2(X)}(\overline{X-\alpha}) & \overline{f_2(X)}(\overline{X-\alpha}) \\ \overline{g_2(X)}(\overline{X-\alpha}) & \overline{g_2(X)}(\overline{X-\alpha}) \end{pmatrix} \\ &= \begin{pmatrix} (\overline{f_1(X)f_2(X)+f_1(X)g_2(X)})\overline{(X-\alpha)^2} & (\overline{f_1(X)f_2(X)+f_1(X)g_2(X)})\overline{(X-\alpha)^2} \\ (\overline{g_1(X)f_2(X)+g_1(X)g_2(X)})\overline{(X-\alpha)^2} & (\overline{g_1(X)f_2(X)+g_1(X)g_2(X)})\overline{(X-\alpha)^2} \end{pmatrix}. \end{aligned}$$

Continuing this way, we see that

$$M_1 M_2 \cdots M_n = \begin{pmatrix} \overline{h_1(X)}(\overline{(X-\alpha)^n} & \overline{h_2(X)}(\overline{(X-\alpha)^n} \\ \overline{h_3(X)}((X-\alpha)^n & \overline{h_4(X)}((X-\alpha)^n \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

where the last equality follows since $\overline{h_i(X)(X-\alpha)^n} \in \frac{\mathbb{C}[X]}{((X-\alpha)^n)}$. Therefore $M_1M_2\cdots M_n = 0$ and so every element of I^n is equal to zero as it is the sum of elements of this form. We conclude that I is a nilpotent nonzero ideal and hence R_n is not a semisimple ring.

Problem 9. (After Chapter 19.3.) (Exam December 2015, Problem 2.) Let $\Lambda = \left\{ \left(\begin{smallmatrix} a & b & c \\ c & a & b \\ b & c & a \end{smallmatrix} \right) \mid a, b, c \in \mathbb{Z}_6 \right\} \subseteq M_3(\mathbb{Z}_6)$ be the ring of 3×3 matrices over $\mathbb{Z}_6$.

(a) Prove that Λ is a commutative subring of $M_3(\mathbb{Z}_6)$, the ring of 3×3-matrices over $\mathbb{Z}_6$.

(b) Define $\Psi : \Lambda \to \mathbb{Z}_6$ by $\Psi\left(\left(\begin{smallmatrix} a & b & c \\ c & a & b \\ b & c & a \end{smallmatrix} \right) \right) = a + b + c$. Prove that Ψ is a surjective ring homomorphism and find a set of generators for the kernel of Ψ.

(c) How many maximal ideals in Λ contain the kernel of Ψ? You have to give an argument for your answer.

(d) Is Λ a semisimple ring? You have to give an argument for your answer. *(Hint: find how many idempotents Λ has.)*

Solution.

(a) Clearly $\Lambda \neq \varnothing$ since $0 \in \Lambda$. Now let $\left(\begin{smallmatrix} a & b & c \\ c & a & b \\ b & c & a \end{smallmatrix} \right), \left(\begin{smallmatrix} a' & b' & c' \\ c' & a' & b' \\ b' & c' & a' \end{smallmatrix} \right) \in \Lambda$. We have

$$\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} + \begin{pmatrix} a' & b' & c' \\ c' & a' & b' \\ b' & c' & a' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' & c+c' \\ c+c' & a+a' & b+b' \\ b+b' & c+c' & a+a' \end{pmatrix} \in \Lambda,$$

and

$$\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \begin{pmatrix} a' & b' & c' \\ c' & a' & b' \\ b' & c' & a' \end{pmatrix} = \begin{pmatrix} aa'+bc'+cb' & ab'+a'b+cc' & ac'+bb'+ca' \\ ca'+c'a+bb' & cb'+aa'+bc' & cc'+ab'+ba' \\ ba'+cc'+ab' & bb'+ca'+ac' & bc'+cb'+aa' \end{pmatrix} \in \Lambda,$$

which show that Λ is a subring of $M_3(\mathbb{Z}_6)$. Moreover, we also have

$$\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \begin{pmatrix} a' & b' & c' \\ c' & a' & b' \\ b' & c' & a' \end{pmatrix} = \begin{pmatrix} aa'+bc'+cb' & ab'+a'b+cc' & ac'+bb'+ca' \\ ca'+c'a+bb' & cb'+aa'+bc' & cc'+ab'+ba' \\ ba'+cc'+ab' & bb'+ca'+ac' & bc'+cb'+aa' \end{pmatrix} = \begin{pmatrix} a' & b' & c' \\ c' & a' & b' \\ b' & c' & a' \end{pmatrix} \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix},$$

which shows that Λ is a commutative ring.

(b) We first show that Ψ is a ring homomorphism. Let $\left(\begin{smallmatrix} a & b & c \\ c & a & b \\ b & c & a \end{smallmatrix} \right), \left(\begin{smallmatrix} a' & b' & c' \\ c' & a' & b' \\ b' & c' & a' \end{smallmatrix} \right) \in \Lambda$. We have

$$\begin{aligned} \Psi\left(\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} + \begin{pmatrix} a' & b' & c' \\ c' & a' & b' \\ b' & c' & a' \end{pmatrix} \right) &= \Psi\left(\begin{pmatrix} a+a' & b+b' & c+c' \\ c+c' & a+a' & b+b' \\ b+b' & c+c' & a+a' \end{pmatrix} \right) \\ &= (a+a') + (b+b') + (c+c') \\ &= (a+b+c) + (a'+b'+c') \\ &= \Psi\left(\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \right) + \Psi\left(\begin{pmatrix} a' & b' & c' \\ c' & a' & b' \\ b' & c' & a' \end{pmatrix} \right), \end{aligned}$$

and

$$\begin{aligned} \Psi\left(\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \begin{pmatrix} a' & b' & c' \\ c' & a' & b' \\ b' & c' & a' \end{pmatrix} \right) &= \Psi\left(\begin{pmatrix} aa'+bc'+cb' & ab'+a'b+cc' & ac'+bb'+ca' \\ ca'+c'a+bb' & cb'+aa'+bc' & cc'+ab'+ba' \\ ba'+cc'+ab' & bb'+ca'+ac' & bc'+cb'+aa' \end{pmatrix} \right) \\ &= (aa'+bc'+cb') + (ab'+a'b+cc') + (ac'+bb'+ca') \\ &= (a+b+c)(a'+b'+c') \\ &= \Psi\left(\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \right) \Psi\left(\begin{pmatrix} a' & b' & c' \\ c' & a' & b' \\ b' & c' & a' \end{pmatrix} \right), \end{aligned}$$

which show that Ψ is a ring homomorphism. Now for $a \in \mathbb{Z}$ we have that $\left(\begin{smallmatrix} a & 0 & \\ 0 & a & 0 \\ 0 & 0 & a \end{smallmatrix}\right) \in \Lambda$ and

$$\Psi\left(\begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}\right) = a + 0 + 0 = a,$$

and so Ψ is surjective. Finally, assume that $\left(\begin{smallmatrix} a & b & c \\ c & a & b \\ b & c & a \end{smallmatrix}\right) \in \ker \Psi$, so that

$$\Psi\left(\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}\right) = 0.$$

Then $a + b + c = 0$ and so

$$\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} = \begin{pmatrix} -b-c & b & c \\ c & -b-c & b \\ b & c & -b-c \end{pmatrix} = b\begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix} + c\begin{pmatrix} -1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix},$$

and so $\left\{\left(\begin{smallmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{smallmatrix}\right)\right\}$ is a generating set for $\ker \Psi$.

(c) By the correspondence theorem (Theorem 4.5) we obtain that maximal ideals of Λ that contain $\ker \Psi$ are in bijection with maximal ideals of $\operatorname{Im} \Psi = \mathbb{Z}_6$. The ideals of $\mathbb{Z}_6$ which are generated by a single element are

$$(\overline{0}) = \{\overline{0}\}, (\overline{1}) = \mathbb{Z}_6 = (\overline{5}), (\overline{2}) = \{\overline{0}, \overline{2}, \overline{4}\} = (\overline{4}), (\overline{3}) = \{\overline{0}, \overline{3}\},$$

and we have that

$$(\overline{2}, \overline{3}) = (\overline{4}, \overline{3}) = \mathbb{Z}_6,$$

hence all and all the ideals of $\mathbb{Z}_6$ are

$$\{\overline{0}\}, \{\overline{0}, \overline{3}\}, \{\overline{0}, \overline{2}, \overline{4}\}, \mathbb{Z}_6.$$

It follows that there are exactly two maximal ideals of $\mathbb{Z}_6$ and so there are exactly two maximal ideals of Λ containing $\ker \Psi$.

(d) We first compute the non-trivial idempotents of Λ. Let $E = \left(\begin{smallmatrix} a & b & c \\ c & a & b \\ b & c & a \end{smallmatrix}\right) \in \Lambda$ be such that $E^2 = E$ and $E \notin \{0, I_3\}$. Then

$$\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} = \begin{pmatrix} a^2 + \overline{2}bc & c^2 + \overline{2}ab & b^2 + \overline{2}ac \\ b^2 + \overline{2}ac & a^2 + \overline{2}bc & c^2 + \overline{2}ab \\ c^2 + \overline{2}ab & b^2 + \overline{2}ac & a^2 + \overline{2}bc \end{pmatrix}$$

gives

$$\begin{cases} a &= a^2 + \overline{2}bc, \\ b &= c^2 + \overline{2}ab, \\ c &= b^2 + \overline{2}ac. \end{cases}$$

Assume first that $a \in \{\overline{0}, \overline{1}, \overline{3}, \overline{4}\}$. Then $a^2 = a$ and so the first equation gives $\overline{2}bc = 0$. Hence either $b = \overline{3}$ or $c = \overline{3}$. Assume that $b = \overline{3}$. Then the second equation gives $c^2 = \overline{3}$ and so $c = \overline{3}$. Similarly, the case $c = \overline{3}$ gives $b = \overline{3}$. Hence we obtain the nontrivial idempotent elements of Λ

$$\begin{pmatrix} \overline{0} & \overline{3} & \overline{3} \\ \overline{3} & \overline{0} & \overline{3} \\ \overline{3} & \overline{3} & \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{1} & \overline{3} & \overline{3} \\ \overline{3} & \overline{1} & \overline{3} \\ \overline{3} & \overline{3} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{3} & \overline{3} & \overline{3} \\ \overline{3} & \overline{3} & \overline{3} \\ \overline{3} & \overline{3} & \overline{3} \end{pmatrix}, \begin{pmatrix} \overline{4} & \overline{3} & \overline{3} \\ \overline{3} & \overline{4} & \overline{3} \\ \overline{3} & \overline{3} & \overline{4} \end{pmatrix}.$$

Now assume that $a \in \{\overline{2}, \overline{5}\}$. Then the system becomes

$$\begin{cases} \overline{0} &= \overline{2} + \overline{2}bc, \\ \overline{0} &= c^2 + \overline{3}b, \\ \overline{0} &= b^2 + \overline{3}c. \end{cases}$$

If $b \in \{\overline{0}, \overline{3}\}$, then the first equation fails. If $b \in \{\overline{1}, \overline{5}\}$, then the second equation gives $c = \overline{3}$ and the first equation fails again. Finally, if $b \in \{2, \overline{4}\}$, then the second equation gives $c = \overline{0}$ and the first equation fails again. So there are no idempotent elements of Λ in this case. We conclude that in total there are 4 nontrivial idempotents in Λ.

Now assume to a contradiction that Λ is semisimple. Then by the Wedderburn–Artin theorem we obtain that

$$\Lambda \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$$

, for some division rings $D_1, \ldots, D_k$ and some positive integers $n_1, \ldots, n_k > 0$. We claim that $k \geq 3$. Assume to a contradiction first that $k = 1$. Then $\Lambda \cong M_{n_1}(D_1)$, and by Theorem 3.4(3), the only two-sided ideals of $M_{n_1}(D_1)$ are 0 and $M_{n_1}(D_1)$. Since none of these are maximal while Λ has two maximal ideals by part (c), we reach a contradiction. Now assume to a contradiction that $k = 2$. Then $\Lambda \cong M_{n_1}(D_1) \times M_{n_2}(D_2)$ and the only two-sided ideals in this case are

$$M_{n_1}(D_1) \times M_{n_2}(D_2), M_{n_1}(D_1) \times 0, 0 \times M_{n_2}(D_2), 0 \times 0.$$

Hence the maximal ideals are $M_{n_1}(D_1) \times 0$ and $0 \times M_{n_2}(D_2)$, and their intersection is 0×0. But this again contradicts part (b) since there exist two maximal ideals of Λ with $0 \neq \ker \Psi$ included in their intersection. We conclude that indeed $k \geq 3$. Hence there exist at least 8 idempotents in $M_{n_1}(D_1) \times \cdots M_{n_k}(D_k)$, given by all possible combinations of 0's and 1's. On the other hand, we have shown that Λ has exactly 6 idempotents. This contradicts Λ being semisimple and hence Λ is not semisimple.

Extra problems

The following problems may be a bit more challenging, in case you feel like you need something more.

Problem 10. (After Chapter 19.3.) Let K be a field. A K-algebra Λ is called a *division algebra* if Λ is a division ring as a ring, that is $\Lambda \neq 0$ is a unital ring and for every nonzero $r \in \Lambda$ there exists a multiplicative inverse $r^{-1} \in \Lambda$.

(a) Show that if Λ is a semisimple finite-dimensional unital algebra over K, then there exist finite-dimensional division algebras $D_1, \ldots, D_k$ over K and positive integers $n_1, \ldots, n_k$ such that

$$\Lambda \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k).$$

(b) Show that if Λ is a semisimple finite-dimensional algebra over $\mathbb{C}$, then there exist positive integers $n_1, \ldots, n_k$ such that

$$\Lambda \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C}).$$

(Hint: use the fundamental theorem of algebra.)

Solution.

(a) By the Wedderburn–Artin theorem we know that

$$\Lambda \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k),$$

where $D_1, \ldots, D_k$ are division rings and $n_1, \ldots, n_k$ are positive integers. It is enough to show that D_i is also a K-algebra. Recall that by the proof of the Wedderburn–Artin theorem we have that

$$D_i \cong \mathrm{End}_\Lambda(S)^{\mathrm{op}},$$

for some simple left Λ-module S, which is a submodule of Λ. Hence it is enough to show that $\mathrm{End}_\Lambda(S)$ is a finite-dimensional K-algebra, since then clearly $\mathrm{End}_\Lambda(S)^{\mathrm{op}}$ is a finite-dimensional K-algebra too. First notice that S is a K-submodule of Λ since for every $k \in K$ and $s \in S$ we have

$$ks = (k1_\Lambda)s \in S.$$

Since Λ is a finite-dimensional K-module, it follows that S is a finite-dimensional K-module.

Now let $f \in \mathrm{End}_\Lambda(S)$. Then we claim that $f \in \mathrm{End}_K(S)$. Indeed, additivity of f holds by definition and for $k \in K$ and $s \in S$ we have

$$f(ks) = f((k1_\Lambda)s) = (k1_\Lambda)f(s) = kf(s),$$

where we use the fact that f is a homomorphism of left Λ-modules. Therefore $\mathrm{End}_\Lambda(S) \subseteq \mathrm{End}_K(S)$. Since a composition of homomorphisms of left Λ-modules is still a homomorphism of left Λ-modules, we conclude that $\mathrm{End}_\Lambda(S)$ is a subring of $\mathrm{End}_K(S)$. On the other hand we have that $\mathrm{End}_K(S)$ is also a K-vector space via

$$\lambda g(s) = g(\lambda s)$$

for $\lambda \in K$ and $g \in \mathrm{End}_K(S)$. Moreover, $\mathrm{End}_K(S)$ is finite-dimensional since S is finite-dimensional. We claim that $\mathrm{End}_\Lambda(S)$ is a subspace of $\mathrm{End}_K(S)$. That is, for $f \in \mathrm{End}_\Lambda(S)$ and $\lambda \in K$ we claim that $\lambda f \in \mathrm{End}_\Lambda(S)$. Indeed, if $s, t \in S$ and $r \in \Lambda$, then using the fact that f is a homomorphism of left Λ-modules and that Λ is a K-algebra we obtain that

$$(\lambda f)(s+t) = f(\lambda(s+t)) = f(\lambda s + \lambda t) = f((\lambda 1_\Lambda)s + (\lambda 1_\Lambda)t) = f((\lambda 1_\Lambda)s) + f((\lambda 1_\Lambda)t),$$

and

$$(\lambda f)(rs) = f(\lambda(rs)) = f((\lambda 1_\Lambda r)s) = f(r(\lambda 1_\Lambda)s) = rf(\lambda s) = r(\lambda f)(s).$$

We conclude that $\mathrm{End}_\Lambda(S)$ is a K-subspace of $\mathrm{End}_K(S)$. Notice that for every $f \in \mathrm{End}_\Lambda(S)$, for every $\lambda \in K$ and for every $s \in S$ we have

$$(\lambda f)(s) = f(\lambda s) = f((\lambda 1_\Lambda)s) = (\lambda 1_\Lambda)f(s) = \lambda f(s).$$

Hence for every $f, g \in \mathrm{End}_\Lambda(S)$ and every $\lambda \in K$ we have

$$((\lambda f) \circ g)(s) = (\lambda f)(g(s)) = f(\lambda g(s)) = f(g(\lambda s)) = (f \circ g)(\lambda s) = (\lambda(f \circ g))(s),$$

and so $\lambda f \circ g = \lambda(f \circ g)$. Similarly we show that $f \circ (\lambda g) = \lambda(f \circ g)$. This shows that $\mathrm{End}_\Lambda(S)$ is a K-algebra. Since it is a subspace of a finite-dimensional vector space, it is also finite-dimensional as required.

(b) By part (a) it is enough to show that every finite-dimensional division algebra over $\mathbb{C}$ is isomorphic to $\mathbb{C}$. Let D be a division algebra over $\mathbb{C}$. Consider the map $\eta : \mathbb{C} \to D$ given by $\eta(\lambda) = \lambda 1_D$ for every $\lambda \in \mathbb{C}$. For every $\lambda, \mu \in \mathbb{C}$ we have

$$\eta(\lambda + \mu) = (\lambda + \mu)1_D = \lambda 1_{Da} + \mu 1_D = \eta(\lambda) + \eta(\mu),$$

and

$$\eta(\lambda\mu) = (\lambda\mu)1_D = \lambda(\mu 1_D) = (\lambda 1_D)(\mu 1_D) = \eta(\lambda)\eta(\mu),$$

showing that η is a ring homomorphism. Moreover, since $\mathbb{C}$ is a field and $\ker \eta$ is an ideal of $\mathbb{C}$ we have that $\ker \eta = 0$ or $\ker \eta = \mathbb{C}$. But $\eta(1) = 11_D = 1_D \neq 0$ and so $1 \notin \ker \eta$. We conclude that $\ker \eta = 0$ and so η is injective. It remains to show that η is surjective.

Let $d \in D$. Since D is a finite-dimensional $\mathbb{C}$-vector space, there exists a positive integer n such that the set $\{1, d, d^2, \ldots, d^n\}$ is linearly dependent over $\mathbb{C}$. That is, there exist $\lambda_0, \lambda_1, \ldots, \lambda_n \in \mathbb{C}$ such that

$$\lambda_0 1_D + \lambda_1 d + \cdots + \lambda_n d^n = 0.$$

Set $p(X) = \lambda_0 + \lambda_1 X + \cdots + \lambda_n X^n \in \mathbb{C}[X]$. By the fundamental theorem of algebra, there exist $z_0, z_1, \ldots, z_n \in \mathbb{C}$ such that

$$p(X) = (X - z_0)(X - z_1)\cdots(X - z_n).$$

Then

$$p(d) = (d - z_0 1_D)(d - z_1 1_D)\cdots(d - z_n 1_D) = \lambda_0 1_D + \lambda_1 d + \cdots + \lambda_n d^n = 0.$$

Since D is a division algebra, it is also an integral domain and so we conclude that $d - z_i 1_D = 0$ for some $i \in \{0, 1, \ldots, n\}$. Then $d = z_i 1_D$ or $\eta(z_i) = d$, showing that η is surjective. Hence we conclude that $D \cong \mathbb{C}$ as required.

Problem 11. (After Chapter 19.3.) The aim of this problem is to prove Maschke's theorem. Let F be a field and G be a finite group such that the characteristic of F does not divide the order of G. Recall that

$$F[G] = \{f : G \to F \mid f(g) = 0 \text{ for all but finitely many } g \in G\}$$

with addition given by

$$(f + h)(g) = f(g) + h(g)$$

and multiplication given by

$$(fh)(g) = \sum_{g=g_1 g_2} f(g_1)h(g_2),$$

where $f, h \in F[G]$ and $g \in G$. Let M be a finitely generated left $F[G]$-module where $F[G]$ is the group algebra.

(a) Show that $F[G]$ is isomorphic to the ring

$$FG = \left\{ \sum_{g\in G} \lambda_g g \;\middle|\; \lambda g \in F \right\},$$

with addition given by

$$\left(\sum_{g\in G} \lambda_g g\right) + \left(\sum_{g\in G} \mu_g g\right) = \sum_{g\in G} (\lambda_g + \mu_g)g$$

with $0_{FG} = \sum_{g\in G} 0g$ and multiplication given by

$$\left(\sum_{g\in G} \lambda_g g\right)\left(\sum_{g\in G} \mu_g g\right) = \sum_{g\in G}\left(\sum_{g_1 g_2 = g\in G} \lambda_{g_1}\mu_{g_2}\right) g,$$

with $1_{FG} = e = e_g$. Conclude that $F[G]$ is a finite-dimensional vector space over F. Use this description of $F[G]$ for the rest of the problem.

(b) Show that M is a finite-dimensional vector space over F.

(c) Show that M is a left artinian $F[G]$-module. Conclude that either $M = 0$ or M has a simple submodule.

(d) Let $f \in \mathrm{End}_F(M)$. Define $\tilde{f} : M \to M$ via

$$\tilde{f}(m) = \frac{1}{|G|} \sum_{g\in G} gf(g^{-1}m).$$

Show that $\tilde{f} \in \mathrm{End}_{F[G]}(M)$.

(e) Assume that there exists a simple submodule $S \subseteq M$. In particular, S is a subspace of M and so there exists a subspace $N \subseteq M$ such that $M = S \oplus N$ (as vector spaces). Let $\pi : M \to S$ and $\iota : S \to M$ be the canonical projection and inclusion maps. Show that if $f = \iota \circ \pi$, then $\mathrm{Im}\, \tilde{f} = S$ and $\tilde{f}^2 = \tilde{f}$.

(f) Show that there if there exists a simple submodule $S \subseteq M$, then there is an isomorphism of left $F[G]$-modules

$$M \cong \mathrm{Im}\, \tilde{f} \oplus \mathrm{Im}(1_M - \tilde{f}).$$

Conclude that every finitely generated $F[G]$-module is semisimple.

Solution.

(a) Since G is finite, we obtain that $F[G] = \{f : G \to F\}$. For $f \in F[G]$ and $g \in G$ we set $f_g \coloneqq f(g)$. Define $\phi : F[G] \to FG$ by

$$\phi(f) = \sum_{g \in G} f_g g.$$

Then for $f, h \in F[G]$ and $g \in G$ we have

$$(f+h)_g = (f+h)(g) = f(g) + h(g) = f_g + h_g,$$

and so

$$\phi(f+g) = \sum_{g \in G} (f+h)_g = \sum_{g \in G} (f_g + h_g)g = \sum_{g \in G} f_g g + \sum_{g \in G} h_g = \phi(f) + \phi(g).$$

Similarly we have

$$(fh)_g = \sum_{g_1 g_2 = g \in G} (f(g_1)h(g_2)) = \sum_{g_1 g_2 = g \in G} (f_{g_1} h_{g_2}),$$

and so

$$\phi(fh) = \sum_{g \in G} (fh)_g = \sum_{g \in G} \left(\sum_{g_1 g_2 = g \in G} (f_{g_1} h_{g_2}) g \right) = \left(\sum_{g_\epsilon G} f_g g \right) \left(\sum_{g \in G} h_g g \right) = \phi(f)\phi(h).$$

This shows that ϕ is a ring homomorphism. If $\sum_{g \in G} \lambda_g g \in FG$, then define $\lambda : G \to F$ via $\lambda(g) = \lambda_g$. It follows that $\phi(\lambda) = \sum_{g \in G} \lambda_g g$ and so ϕ is surjective. On the other hand, if $\phi(f) = 0$, then we obtain that $f_g = 0$ for all $g \in G$ and so $f = 0_{F[G]}$, showing that ϕ is injective. We conclude that ϕ is a ring isomorphism.

FG is an abelian group by the definition of addition in FG. For $\lambda \in F$ and $\sum_{g \in G} \lambda_g g \in FG$ we define a scalar multiplication by

$$\lambda \left(\sum_{g \in G} \lambda_g g \right) = \sum_{g \in G} (\lambda \lambda_g) g,$$

which makes FG into a vector space over F. The whole group G generates FG as an F-vector space, since an element $\sum_{g \in G} \lambda_g g \in FG$ is just an F-linear combination with summands $\lambda_g g$ for $g \in G$. Since FG is a finitely generated vector space, it follows that it is finite-dimensional.

(b) Let $m \in M$ and $\lambda \in F$. We define a scalar multiplication via

$$\lambda m = (\lambda e) m.$$

Since M is finitely generated, there exists a set $\{m_1, \ldots, m_n\} \subseteq M$ that generates M as an FG-module. Let $m \in M$. Then there exist $f^1, \ldots, f^n \in FG$ such that

$$m = \sum_{i=1}^{n} f^i m_i.$$

By part (a) we have that FG is finite-dimensional as an F-vector space. Therefore there exists an F-basis $\{b_1, \ldots, b_u\} \in FG$. Hence for every $i \in \{1, \ldots, n\}$ there exist $c_{i1}, \ldots, c_{iu} \in F$ such that

$$f^i = \sum_{j=1}^{u} c_{ij} b_j.$$

Then we have that

$$m = \sum_{i=1}^{n} f^i m_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{u} c_{ij} b_j \right) m_i = \sum_{i=1}^{n} \sum_{j=1}^{u} c_{ij} (b_j m_i).$$

Hence the set $\{b_j m_i \mid 1 \leq i \leq n, 1 \leq j \leq u\}$ generates M as an F-vector space. Since this set is finite, it follows that M is a finite-dimensional F-vector space.

(c) Let

$$M = M_1 \supseteq M_2 \supseteq M_3 \supseteq \cdots \tag{1}$$

be a decreasing sequence of FG-submodules of M. Let $i \in \{2, 3, \dots, \}$. Then M_i is closed under scalar multiplications by elements of FG. In particular, M_i is closed under scalar multiplication by the elements $\{\lambda e \mid \lambda \in F\} \subseteq FG$, and so M_i is closed under scalar multiplication with F. Hence M_i is an F-subspace of M_{i-1}. Since M_1 is a finite-dimensional vector space over F, it follows that each M_i is a finite-dimensional vector space over F. Hence for the sequence (1) we have that there exists $r \geq 1$ such that $M_r = M_{r+1} = M_{r+2} = \cdots$. Hence M is left artinian.

Now assume that $M \neq 0$ and we show that M has a simple submodule. Let $\mathcal{S}$ be the collection of all nonzero submodules of M. Clearly $\mathcal{S} \neq 0$ since $0 \neq M \in \mathcal{S}$. By Theorem 13.5 we have that $\mathcal{S}$ has a minimal element S. Then if $L \subseteq S$ is a submodule, it follows that $L \subseteq M$ is a submodule and so either $L \in \mathcal{S}$ or $L = 0$. If $L \in \mathcal{S}$, by minimality of S we obtain that $L = S$. Hence S is a simple module, as required.

(d) Let $m_1, m_2 \in M$ and $\lambda \in F$. Using the fact that f is additive we have that

$$\tilde{f}(m_1 + m_2) = \frac{1}{|G|} \sum_{g \in G} gf(g^{-1}(m_1 + m_2)) = \frac{1}{|G|} \sum_{g \in G} gf(g^{-1}m_1) + \frac{1}{|G|} \sum_{g \in G} gf(g^{-1}m_2) = \tilde{f}(m_1) + \tilde{f}(m_2).$$

Now for $\lambda \in F$, $g \in G$ and $m \in M$ we have

$$\lambda(gm) = (\lambda e)(gm) = (\lambda eg)m = (g\lambda e)m = g(\lambda em) = g(\lambda m)$$

and so using the fact that f is F-linear we obtain

$$\tilde{f}(\lambda m) = \frac{1}{|G|} \sum_{g \in G} gf(g^{-1}(\lambda m)) = \frac{1}{|G|} \sum_{g \in G} gf(\lambda(g^{-1}m)) = \frac{\lambda}{|G|} \sum_{g \in G} gf(g^{-1}m) = \lambda \tilde{f}(m).$$

Next let $g \in G$ and $m \in M$ and we show that $\tilde{f}(gm) = g\tilde{f}(m)$. We have

$$\tilde{f}(gm) = \frac{1}{|G|} \sum_{x \in G} xf(x^{-1}(gm)) = \frac{1}{|G|} \sum_{x \in G} xf((x^{-1}g)m). \tag{2}$$

Notice that $G = \{y = g^{-1}x \mid x \in G\}$. Indeed, for any $g' \in G$ we have that there exists $x = gg' \in G$ such that $y = g^{-1}gg' = g'$. Therefore, we may perform the change of variables $y = g^{-1}x$. Then we obtain that $x = gy$ and so $x^{-1} = y^{-1}g^{-1}$. Replacing this in (2) we obtain

$$\tilde{f}(gm) = \frac{1}{|G|} \sum_{y \in G} gyf((y^{-1}g^{-1}g)m) = g\frac{1}{|G|} \sum_{y \in G} yf(y^{-1}m) = g\tilde{f}(m),$$

as claimed. Now for $\lambda \in F$, $g \in G$ and $m \in M$ we have shown that

$$\tilde{f}((\lambda g)m) = (\lambda g)\tilde{f}(m).$$

Combining this with the fact that we have shown additivity of $\tilde{f}$ we obtain for every $\sum_{g \in G} \lambda_g g \in FG$ and every $m \in M$ that

$$\tilde{f}\left(\left(\sum_{g \in G} \lambda_g g\right) m\right) = \tilde{f}\left(\sum_{g \in G} ((\lambda_g g)m)\right) = \sum_{g \in G} \tilde{f}\left((\lambda_g g)m\right) = \sum_{g \in G} \left(\lambda_g g(\tilde{f}(m))\right) = \left(\sum_{g \in G} \lambda_g g\right) \tilde{f}(m),$$

which shows that $\tilde{f}$ is a homomorphism of FG-modules.

(e) We first claim that $\operatorname{Im} \tilde{f} \subseteq S$. Let $m \in M$. Then $\pi(g^{-1}m) \in S$ for all $g \in G$, since $\pi : M \to S$. Then $\iota \circ \pi(g^{-1}m)) = \pi(g^{-1}m) \in S$ since $\iota : S \to M$ is just the inclusion of S into M. Since S is an FG-submodule of M, we have that $g\tilde{f}(g^{-1}m) = g\pi(g^{-1}m) \in S$ for any $g \in G$. Then

$$\tilde{f}(m) = \frac{1}{|G|} \sum_{g \in G} g\tilde{f}(g^{-1}m) \in S,$$

showing that $\operatorname{Im}\tilde{f} \subseteq S$. Now let $s \in S$. Then for every $g \in G$ we have $g^{-1}s \in S$. Hence $g\iota \circ \pi(g^{-1}s) = gg^{-1}s = s$. We now compute

$$\tilde{f}(s) = \frac{1}{|G|}\sum_{g\in G} g\iota \circ \pi(g^{-1}s) = \frac{1}{|G|}\sum_{g\in G} s = \frac{1}{|G|}|G|s = s,$$

and so $s \in \operatorname{Im}\tilde{f}$. This shows that $S \subseteq \operatorname{Im}\tilde{f}$ and so $S = \operatorname{Im}\tilde{f}$. Now notice that we have showed that for $s \in S$ we have $\tilde{f}(s) = s$. For any $m \in M$ we have that $\tilde{f}(m) \in \operatorname{Im}\tilde{f} = S$ and so

$$\tilde{f}^2(m) = \tilde{f}(\underbrace{\tilde{f}(m)}_{\in S}) = \tilde{f}(m),$$

showing that $\tilde{f}^2 = \tilde{f}$.

(f) If $M = 0$, then M is semisimple. Assume that $M \neq 0$. Then by part (c) there exists a simple submodule $S \subseteq M$. By part (d) we have that $\tilde{f}$ is a homomorphism of left FG-modules. It follows that $1_M - \tilde{f}$ is also a homomorphism of left FG-modules. Hence both $\operatorname{Im}\tilde{f}$ and $\operatorname{Im}(1_M - \tilde{f})$ are FG-submodules of M. Now let $x \in \operatorname{Im}\tilde{f} \cap \operatorname{Im}(1_M - \tilde{f})$. Then there exists $y \in M$ such that $x = \tilde{f}(y)$ and there exists $z \in M$ such that $x = (1_M - \tilde{f})(z) = z - \tilde{f}(z)$. Then by part (e) we have

$$\tilde{f}(x) = \tilde{f}(\tilde{f}(y)) = \tilde{f}^2(y) = \tilde{f}(y) = x$$

and

$$\tilde{f}(x) = \tilde{f}((1_M - \tilde{f})(z)) = \tilde{f}(z - \tilde{f}(z)) = \tilde{f}(z) - \tilde{f}^2(z) = \tilde{f}(z) - \tilde{f}(z) = 0,$$

and combining the too we obtain that $\tilde{f}(x) = 0$. We conclude that $\operatorname{Im}\tilde{f} \cap \operatorname{Im}(1_M - \tilde{f}) = \{0\}$. Next, let $m \in M$. We can write

$$m = \tilde{f}(m) + m - \tilde{f}(m) = \underbrace{\tilde{f}(m)}_{\in \operatorname{Im}\tilde{f}} + \underbrace{(1_M - \tilde{f})(m)}_{\in \operatorname{Im}(1_M - \tilde{f})},$$

which shows that $M = \operatorname{Im}\tilde{f} + \operatorname{Im}(1_M - \tilde{f})$. This shows that $M = \operatorname{Im}\tilde{f} \oplus \operatorname{Im}(1_M - \tilde{f})$.

Set $S_1 = S$ and $U_1 = \operatorname{Im}(1_M - \tilde{f})$. By part (e) we have that $\operatorname{Im}\tilde{f} = S = S_1$. If $U_1 = 0$, then $M = S$ is semisimple. Otherwise, there exists a simple submodule $S_2 \subseteq U_1$ and another submodule $U_2 \subseteq U_1$ such that $U_1 = S_2 \oplus U_2$ and so $M = S_1 \oplus S_2 \oplus U_2$. We may continue this process, which has to terminate since M is left artinian by part (c). We conclude that M is semisimple.