Rings and modules - Problem set 1 solutions

Solved on Tuesday 05.09

Problem 1. Let R be a ring. Show that the polynomial ring $R[X]$ is commutative if and only if R is commutative, and is unital if and only if R is unital.

Solution. Assume first that $R[X]$ is commutative. Then for any polynomials $p(X)$ and $q(X)$ in $R[X]$, we have $p(X)q(X) = q(X)p(X)$. Now let $r, s \in R$ and consider the polynomials $p(X) = r$ and $q(X) = s$ in $R[X]$. Then

$$rs = p(X)q(X) = q(X)p(X) = sr,$$

and since $r, s \in R$ were arbitrary, we conclude that R is commutative.

Assume now that $R[X]$ is commutative. Let $p(X), q(X) \in R[X]$ and write

$$p(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n, q(X) = b_0 + b_1X + b_2X^2 + \ldots + b_mX^m.$$

Then

$$p(X)q(X) = c_0 + c_1X + c_2X^2 + \ldots + c_{n+m}X^{n+m},$$

where $c_i = \sum_{j+k=i} a_jb_k$. On the other hand, we have

$$q(X)p(X) = c'_0 + c'_1X + c'_2X^2 + \ldots + c'_{n+m}X^{n+m},$$

where $c'_i = \sum_{j+k=i} b_ja_k$. Since $a_jb_k = b_ka_j$ (because R is commutative), we have

$$c_i = \sum_{j+k=i} a_jb_k = \sum_{j+k=i} b_ka_j = \sum_{j+k=i} b_ja_k = c'_i,$$

and so $p(X)q(X) = q(X)p(X)$ and $R[X]$ is commutative.

Now suppose that the polynomial ring $R[X]$ is unital with multiplicative identity $1_{R[X]}(X)$. Write

$$1_{R[X]}(X) = a_0 + a_1X + \ldots + a_nX^n.$$

Then $1_{R[X]}(X) \cdot X = X$ and so

$$X = 1_{R[X]}(X) \cdot X = a_0X + a_1X^2 + \ldots + a_nX^{n+1}.$$

Hence we conclude that $a_0 = 1$ and $a_i = 0$ for $i \geq 1$. Then $1_{R[X]}(X) = a_0 \in R$. Now let $r \in R$ and consider the polynomial $p_r(X) = r \in R[X]$. We have

$$a_0r = 1_{R[X]}(X)r = r \text{ and } ra_0 = r1_{R[X]}(X) = r$$

and so a_0 is the multiplicative identity in R. Hence R is unital.

Finally assume that R has a multiplicative unity, denoted as 1_R. Consider the polynomial $I(X) = 1_R$. For any $P(X) \in R[X]$ we have

$$I(X) \cdot P(X) = 1_R \cdot P(X) = P(X),$$

and

$$P(X) \cdot I(X) = P(X) \cdot 1_R = P(X).$$

This shows that the polynomial $I(X)$ acts as a multiplicative identity for $R[X]$, and so $R[X]$ is unital.

Problem 2. Let R be a ring. Show that the following are equivalent.

(a) R is an integral domain.

(b) The left cancellation property holds in R, that is if $a, b, c \in R$, $a \neq 0$ and $ab = ac$ holds, then $b = c$.

(c) The right cancellation property holds in R, that is if $a, b, c \in R$, $a \neq 0$ and $ba = ca$ holds, then $b = c$.

Solution. We only show the equivalence between (a) and (b) as the equivalence between (a) and (c) is similar.

(a) implies (b): Let $a, b, c \in R$, $a \neq 0$ and assume that $ab = ac$. Then $ab - ac = 0$ or $a(b - c) = 0$. Since R is an integral domain we obtain that $a = 0$ or $b - c = 0$. Since $a \neq 0$, we conclude that $b - c = 0$ or $b = c$, as required.

(b) implies (a): Let $r, s \in R$ be such that $rs = 0$. To show that R is an integral domain, we need to show that $r = 0$ or $s = 0$. If $r = 0$ there is nothing to show. Assume that $r \neq 0$. Then $rs = 0 = r0$ and so by the left cancellation property we obtain that $s = 0$, as required.

Problem 3. (Exercise 9.4.5(a) in the book.) Determine the idempotents, nilpotent elements and invertible elements of the following rings.

(i) $\mathbb{Z}/(4)$.

(ii) $\mathbb{Z}/(20)$.

Solution.

(i) We have $\mathbb{Z}/(4) = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. We compute $\pmod 4$:

$$\begin{aligned}
\overline{0}^2 &\equiv \overline{0^2} \equiv \overline{0}, \\
\overline{1}^2 &\equiv \overline{1^2} \equiv \overline{1}, \\
\overline{2}^2 &\equiv \overline{2^2} \equiv \overline{4} \equiv \overline{0}, \\
\overline{3}^2 &\equiv \overline{3^2} \equiv \overline{9} \equiv \overline{1}.
\end{aligned}$$

So the only idempotents are $\overline{0}$ and $\overline{1}$. Also by the above we see that $\overline{0}$ and $\overline{2}$ are nilpotent and that $\overline{1}^k = \overline{1}$ and so $\overline{1}$ is not nilpotent, and

$$\overline{3}^k = \begin{cases} \overline{1}, & \text{if } k \text{ is odd}, \\ \overline{3}, & \text{if } k \text{ is even}, \end{cases}$$

and so $\overline{3}$ is also not nilpotent. Finally, by the above we have that $\overline{1}^{-1} = \overline{1}$ and that $\overline{3}^{-1} = \overline{3}$ and so $\overline{1}$ and $\overline{3}$ are invertible. However $\overline{2}$ is not invertible since

$$\overline{2} \cdot \overline{1} \equiv \overline{2}, \;\; \overline{2} \cdot \overline{2} \equiv \overline{0}, \;\; \overline{2} \cdot \overline{3} \equiv \overline{6} \equiv \overline{2}.$$

(ii) We have $\mathbb{Z}/(20) = \{\bar{i} \mid 0 \leq i \leq 19\}$. We compute $\pmod{20}$:

$$\begin{aligned}
\overline{0}^2 &\equiv \overline{0^2} \equiv \overline{0},\\
\overline{1}^2 &\equiv \overline{1^2} \equiv \overline{1},\\
\overline{2}^2 &\equiv \overline{2^2} \equiv \overline{4},\\
\overline{3}^2 &\equiv \overline{3^2} \equiv \overline{9},\\
\overline{4}^2 &\equiv \overline{4^2} \equiv \overline{16},\\
\overline{5}^2 &\equiv \overline{5^2} \equiv \overline{25} \equiv \overline{5},\\
\overline{6}^2 &\equiv \overline{6^2} \equiv \overline{36} \equiv \overline{16},\\
\overline{7}^2 &\equiv \overline{7^2} \equiv \overline{49} \equiv \overline{9},\\
\overline{8}^2 &\equiv \overline{8^2} \equiv \overline{64} \equiv \overline{4},\\
\overline{9}^2 &\equiv \overline{9^2} \equiv \overline{181} \equiv \overline{1},\\
\overline{10}^2 &\equiv \overline{10^2} \equiv \overline{100} \equiv \overline{0},\\
\overline{11}^2 &\equiv \overline{11^2} \equiv \overline{121} \equiv \overline{1},\\
\overline{12}^2 &\equiv \overline{12^2} \equiv \overline{144} \equiv \overline{4},\\
\overline{13}^2 &\equiv \overline{13^2} \equiv \overline{169} \equiv \overline{9},\\
\overline{14}^2 &\equiv \overline{14^2} \equiv \overline{196} \equiv \overline{16},\\
\overline{15}^2 &\equiv \overline{15^2} \equiv \overline{225} \equiv \overline{5},\\
\overline{16}^2 &\equiv \overline{16^2} \equiv \overline{256} \equiv \overline{16},\\
\overline{17}^2 &\equiv \overline{17^2} \equiv \overline{289} \equiv \overline{9},\\
\overline{18}^2 &\equiv \overline{18^2} \equiv \overline{324} \equiv \overline{4},\\
\overline{19}^2 &\equiv \overline{19^2} \equiv \overline{361} \equiv \overline{1}.
\end{aligned}$$

So the only idempotents are $\overline{0}$, $\overline{1}$, $\overline{5}$ and $\overline{16}$. Also by the above we see that $\overline{0}$ and $\overline{10}$ are nilpotent. Next, we have

$$\begin{aligned}
\overline{2}^2 &\equiv \overline{4},\\
\overline{2}^3 &\equiv \overline{8},\\
\overline{2}^4 &\equiv \overline{16},\\
\overline{2}^5 &\equiv \overline{32} \equiv \overline{12},\\
\overline{2}^6 &\equiv \overline{64} \equiv \overline{4} \equiv \overline{2}^2,
\end{aligned}$$

and so the powers of $\overline{2}$ keep repeating after this. None of these is equal to $\overline{0}$, and so $\overline{2}$ is not nilpotent. In particular, none of the powers of $\overline{2}$ is nilpotent either, and so none of $\overline{4}$, $\overline{8}$, $\overline{12}$ and $\overline{16}$ are nilpotent. Moreover, since $\overline{6}^2 = \overline{16}$, $\overline{14}^2 = \overline{16}$ and $\overline{18}^2 = \overline{4}$, none of the elements $\overline{6}$, $\overline{14}$ and $\overline{18}$ are nilpotent. Next, we have

$$\begin{aligned}
\overline{3}^2 &\equiv \overline{9},\\
\overline{3}^3 &\equiv \overline{27} \equiv \overline{7},\\
\overline{3}^4 &\equiv \overline{81} \equiv \overline{1},\\
\overline{3}^5 &\equiv \overline{243} \equiv \overline{3},
\end{aligned}$$

and so the powers of $\overline{3}$ keep repeating after this. None of these is equal to $\overline{0}$ and so none of $\overline{1}$, $\overline{3}$, $\overline{7}$, $\overline{9}$ is nilpotent. Since $\overline{11}^2 = \overline{1}$, $\overline{13}^2 = \overline{9}$, $\overline{17}^2 = \overline{9}$ and $\overline{19}^2 = \overline{1}$, none of the elements $\overline{11}$, $\overline{13}$, $\overline{17}$ and $\overline{19}$ are nilpotent. Next, we have that $\overline{5}$ is idempotent and so it cannot be nilpotent since it is not zero. Since $\overline{15}^2 = \overline{5}$, we have that $\overline{15}$ is not nilpotent either. We conclude that the only nilpotent elements are $\overline{0}$ and $\overline{10}$.

Finally, by the above we have that

$$\overline{1}^{-1} = \overline{1}, \ \ \overline{9}^{-1} = \overline{9}, \ \ \overline{11}^{-1} = \overline{11}, \ \ \overline{19}^{-1} = \overline{19}.$$

Hence the elements $\overline{1}$, $\overline{9}$, $\overline{11}$ and $\overline{19}$ are invertible. A computation shows that

$$\overline{3} \cdot \overline{7} \equiv \overline{21} \equiv \overline{1},$$

and so the elements $\overline{3}$ and $\overline{7}$ are also invertible. Moreover, we also compute

$$\overline{13} \cdot \overline{17} \equiv \overline{221} \equiv 1$$

and so the elements $\overline{13}$ and $\overline{17}$ are also invertible. Next, let $1 \leq k \leq 9$. Then $\overline{2k} \equiv \overline{1}$ implies that 20 divides $2k-1$ which is impossible, since $2k-1$ is not even. Hence $\overline{2k}$ is not invertible, and so $\overline{2}$, $\overline{4}$, $\overline{6}$, $\overline{8}$, $\overline{10}$, $\overline{12}$, $\overline{14}$, $\overline{16}$ and $\overline{18}$ are not invertible. Next, let $1 \leq k \leq 3$. Then $\overline{5k} \equiv \overline{1}$ implies that 20 divides $5k-1$ which is impossible since $5k-1$ is not divisible by 5. Hence $\overline{5k}$ is not invertible, and so $\overline{5}$ and $\overline{15}$ are not invertible. We conclude that $\overline{1}$, $\overline{3}$, $\overline{7}$, $\overline{9}$, $\overline{11}$, $\overline{13}$, $\overline{17}$ and $\overline{19}$ are the only invertible elements in $\mathbb{Z}_{20}$.

Problem 4. Let R be a ring and $r \in R$. Let $\langle r \rangle$ be the subring generated by $\{r\}$. Show that $\langle r \rangle = X$ where

$$X = \{n_1 r + n_2 r^2 + \cdots + n_k r^k \mid n_i \in \mathbb{Z}, k > 0\}.$$

Solution. First we show that $X \subseteq \langle r \rangle$. Let $n_1 r + n_2 r^2 + \cdots + n_k r^k \in X$. Since $\langle r \rangle$ is a ring and it contains r, we have that $r, r^2, \ldots, r^k \in \langle r \rangle$. Furthermore, we have that $n_i r^i \in \langle r \rangle$ and also that $n_1 r + \cdots + n_k r^k \in \langle r \rangle$. This shows the inclusion $X \subseteq \langle r \rangle$.

Now we show that $\langle r \rangle \subseteq X$. Since $\langle r \rangle$ is the smallest subring of R that contains r, and since X contains r, it is enough to show that X is a subring of R. Clearly we have that $X \neq \varnothing$ since $r \in X$. Let $n_1 r + \cdots + n_k r^k, m_1 r + \cdots + m_t r^t \in X$, and without loss of generality assume that $k \geq t$. Then

$$n_1 r + \cdots + n_k r^k - (m_1 r + \cdots + m_t r^t) = (n_1 - m_1) r + \cdots + (n_t - m_t) r^t + \cdots + n_k r^k \in X,$$

and

$$(n_1 r + \cdots + n_k r^k)(m_1 r + \cdots + m_t r^t) = c_1 r + \cdots + c_{k+t} r^{k+t} \in X,$$

where $c_i = \sum_{a+b=i} n_a m_b$. By Proposition 2.3 we conclude that X is a subring of R.

Problem 5. Let $R = M_2(\mathbb{Z})$ be the ring of 2×2 integer matrices. Recall that R is unital with $1_R = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

(a) Show that the subset $S \subseteq R$ defined by

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$$

is a subring of R. Show that S is not unital. Conclude that the subring of a unital ring does not need to be unital.

(b) Show that the subset $T \subseteq S$ defined by

$$T = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a0 \in \mathbb{Z} \right\}$$

is a subring of T. Show that T is unital with $1_T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Conclude that the subring of a ring which is not unital, may be unital. Conclude also that the subring of a unital ring may be unital with a different multiplicative identity.

Solution.

(a) We use Proposition 2.3 to show that S is a subring of R. Clearly we have $S \neq \varnothing$ since $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in S$. Let $\left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} c & d \\ 0 & 0 \end{smallmatrix}\right) \in S$. Then

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ 0 & 0 \end{pmatrix} \in S,$$

and

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix} \in S,$$

and so S is a subring of R. Now assume towards a contradiction that S is unital with unit $1_S = \left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right)$. Then for every $X = \left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right) \in S$ we have $X = X1_S$, from which we get

$$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} xa & xb \\ 0 & 0 \end{pmatrix}.$$

Hence for every $x, y \in \mathbb{Z}$ we have $xa = x$ and $xb = y$. This gives $a = 1$ but the second equality cannot hold for every $x, y \in \mathbb{Z}$ for a constant b. Hence such an element 1_S does not exist and so S is not unital. Since S is a subring of a unital ring, we conclude that a subring of a unital ring does not need to be unital.

(b) We use Proposition 2.3 to show that T is a subring of S. Clearly we have $T \neq \varnothing$ since $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in T$. Let $\left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} b & 0 \\ 0 & 0 \end{smallmatrix}\right) \in T$. Then

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a-b & 0 \\ 0 & 0 \end{pmatrix} \in T,$$

and

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in T,$$

and so T is a subring of R. We claim that $1_T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ is a multiplicative identity of T. Indeed, for every $X = \left(\begin{smallmatrix} x & 0 \\ 0 & 0 \end{smallmatrix}\right) \in T$ we have

$$1_T X = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1x & 0 \\ 0 & 0 \end{pmatrix} = X = \begin{pmatrix} x1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = X1_T,$$

as required. Since T is a subring of the non-unital ring S, we conclude that the subring of a ring which is not unital may be unital. Also, since T is a subring of the unital ring R and since $1_T \neq 1_R$, we conclude that the subring of a unital ring may be unital with a different multiplicative identity.

Problem 6. Let R_i, $i = 1, 2, \ldots$ be an infinite family of unital rings.

(a) Recall that the direct product $R = \prod_{i=1}^{\infty} R_i$ is a ring under the operations

$$(a_1, a_2, \ldots) + (b_1, b_2, \ldots) = (a_1 + b_1, a_2 + b_2, \ldots)$$
$$(a_1, a_2, \ldots)(b_1, b_2, \ldots) = (a_1 b_1, a_2 b_2, \ldots),$$

for $(a_1, a_2, \ldots), (b_1, b_2, \ldots) \in R$. Is R a unital ring?

(b) Recall that the direct sum $S = \bigoplus_{i=1}^{\infty} R_i$ defined by

$$S = \{(a_1, a_2, \ldots) \in R \mid a_i = 0 \text{ for all but finitely many } i\}$$

is a subring of R. Is S a unital ring?

Solution.

(a) Consider the element $(1, 1, \ldots) \in R$. Then for any $(a_1, a_2, \ldots) \in R$ we have

$$(1, 1, \ldots)(a_1, a_2, \ldots) = (1a_1, 1a_2, \ldots) = (a_1, a_2, \ldots)$$

and similarly $(a_1, a_2, \ldots)(1, 1, \ldots) = (a_1, a_2, \ldots)$. Hence $1_R = (1, 1, \ldots)$ and R is unital.

(b) Assume to a contradiction that there exists an element $x = (x_1, x_2, \ldots) \in S$ such that $xa = a$ for all $a \in S$. For $i = 1, 2, \ldots$ let $e_i \in S$ be the element with 1 in position i and 0 everywhere else. Then

$$(0, 0, \ldots, 0, 1, 0, \ldots) = e_i = xe_i = (x_1, x_2, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots)(0, 0, \ldots, 0, 1, 0, \ldots) = (0, 0, \ldots, 0, x_i, 0, \ldots),$$

and so $x_i = 1$. But then $x = (1, 1, \ldots)$ contradicting $x \in S$. Hence S is not unital.

Problem 7. (Exercise 9.4.5(b) in the book.) Show that the set of units $U(R)$ of a unital ring R forms a multiplicative group.

Solution. Let $r, s \in U(R)$. We claim that $rs \in U(R)$ as well. Since $r, s \in U(R)$, there exist $r^{-1}, s^{-1} \in R$. Then

$$(rs)(s^{-1}r^{-1}) = r(ss^{-1})r^{-1} = r1r^{-1} = rr^{-1} = 1,$$

and similarly we have $(s^{-1}r^{-1})(rs) = 1$. Therefore rs is invertible and so $rs \in U(R)$. Hence the multiplication operation is well-defined in $U(R)$. Since multiplication in R is associative, multiplication in $U(R)$ is also associative. Since $1 \in R$ is invertible with inverse $1^{-1} = 1$, we have that $1 \in U(R)$. And since for $r \in U(R)$ there exists $r^{-1} \in R$ with r^{-1} also a unit, we have $r^{-1} \in U(R)$ and so there is an inverse for every element $r \in U(R)$. We conclude that $U(R)$ is a multiplicative group.

Problem 8. Let R be a unital ring. Find the center of the ring $M_2(R)$ of 2×2 matrices over R.

Solution. Let $Z = Z(M_2(R))$ be the center of $M_2(R)$. Let $X = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in Z$. Then $e_{11}X = Xe_{11}$ and so

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

gives $b = 0$ and $c = 0$. Moreover we have $e_{12}X = Xe_{12}$ and so

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

gives $c = 0$ and $a = d$. Hence $X = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$. Next, for any $r \in R$ we have that $\left(\begin{smallmatrix} r & 0 \\ 0 & 0 \end{smallmatrix}\right)X = X\left(\begin{smallmatrix} r & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and so

$$\begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} ra & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ar & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}$$

and so $ra = ar$. Hence $a \in Z(R)$. We claim that

$$Z = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in Z(R) \right\}.$$

We have already shown the "$\subseteq$" inclusion. For the other side notice that for any $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in M_2(R)$ we have

$$\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} rx & ry \\ rz & rw \end{pmatrix} = \begin{pmatrix} xr & yr \\ zr & wr \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix},$$

as required.

Problem 9. (a) Let R be a unital ring with $\mathrm{char}(R) \neq 0$. Show that $\mathrm{char}(R) = \min\{n > 0 \mid n1 = 0\}$.

(b) Show that $\mathrm{char}(\mathbb{Z}/(n)) = n$.

Solution.

(a) Set $x = \min\{n > 0 \mid n1 = 0\}$. We have

$$\{n > 0 \mid nr = 0 \ \ \forall r \in R\} \subseteq \{n > 0 \mid n1 = 0\},$$

and hence

$$x = \min\{n > 0 \mid n1 = 0\} \leq \min\{n > 0 \mid nr = 0 \ \ \forall r \in R\} = \mathrm{char}(R).$$

On the other hand, for any $r \in R$ we have

$$xr = x(1r) = (x1)r = 0r = 0,$$

and so $x \in \{n > 0 \mid nr = 0 \ \ \forall r \in R\}$. Therefore

$$\text{char}(R) = \min\{n > 0 \mid nr = 0 \ \ \forall r \in R\} \leq x.$$

Since we have showed that both $x \leq \text{char}(R)$ and $\text{char}(R) \leq x$ hold, we conclude that $x = \text{char}(R)$.

(b) In $\mathbb{Z}/(n)$ we have that $\overline{n} = 0$ and $\overline{k} \neq 0$ for all $1 \leq k \leq n-1$. Hence $\min\{n > 0 \mid n\overline{1} = 0\} = n$ and the result follows by part (a).

Problem 10. Let $n \geq 2$ be an integer. Show that the ring Z_n is a field if and only if n is a prime number.

Solution. Assume first that $\mathbb{Z}_n$ is a field but assume instead that n is not a prime number. Then $n = ab$ for some integers $1 < a, b < n$. Then

$$\overline{a}\overline{b} \equiv \overline{ab} \equiv \overline{n} \equiv 0 \pmod{n},$$

with $\overline{a}$ and $\overline{b}$ nonzero. But this contradicts that $\mathbb{Z}_n$ is an integral domain.

Now assume that $n = p$ is a prime number. Let $\overline{a}, \overline{b} \in \mathbb{Z}_p$ be nonzero. We claim that $\overline{a}\overline{b} = \overline{ab}$ is nonzero in $\mathbb{Z}_p$. Assume to a contradiction that $\overline{ab} = 0$ in $\mathbb{Z}_p$. Then p divides ab and since p is prime, we have that p divides a or p divides b. But then at least one of a and b is zero in $\mathbb{Z}_p$, which contradicts our assumption. Hence $\mathbb{Z}_p$ is an integral domain. Now let $\overline{x} \in \mathbb{Z}_p$ be nonzero. We claim that the set $\overline{x}\mathbb{Z}_p \coloneqq \{\overline{x}\overline{k} \mid 0 \leq k \leq p-1\}$ has exactly p elements. Indeed, if $\overline{x}\overline{k} = \overline{xm}$ for some $0 \leq k, m \leq p-1$, then we obtain that $\overline{k} = \overline{m}$ by the cancelation property of integral domains. But then $k = m$ since $0 \leq k, m \leq p-1$. Therefore, no two terms in $\overline{x}\mathbb{Z}_p$ are equal, and so it has p elements. Hence $\overline{x}\mathbb{Z}_p = \mathbb{Z}_p$. But then there exists $\overline{y} \in \mathbb{Z}_p$ such that $\overline{xy} = 1$, which proves that $\overline{x}$ is a unit and hence $\mathbb{Z}_p$ is a field.

Problem 11. (Exercise 9.4.7 in the book.) Let R be a commutative ring and $r, s \in R$. If r and s are nilpotent, show that $r + s$ is also nilpotent. Show that this does not necessarily hold if R is not commutative.

Solution. Since r and s are nilpotent, there exist $n, k \geq 0$ such that $r^n = 0$ and $s^k = 0$. Consider the product

$$\underbrace{(r+s)(r+s)\cdots(r+s)}_{z \text{ terms}}.$$

Using distributivity, a term of this product is obtaining by choosing r or s in each of the brackets, for a total of z choices. But then using commutativity we may rewrite this product into the form $r^x s^y$ (where still $x + y = z$ and where $0 \leq x, y \leq z$). Hence

$$(r+s)^{k+n} = \sum_{i=0}^{k+n} c_i r^i s^{k+n-i},$$

for some coefficients c_i. If $i \geq n$, then $r^i = 0$ and so all the terms after $i = n$ become 0. If $i < n$, then $k + n - i > k$ and so $s^{k+n-i} = 0$ and all the terms before $i = n$ become 0. Hence $(r+s)^{k+n} = 0$ and $r + s$ is nilpotent.

For an example where this does not hold if R is not commutative, let F be a field and $R = M_2(F)$. Then

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

so these two matrices are nilpotent. But their sum is

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and we have

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Hence A^k is either A or the identity matrix, and hence A is not nilpotent.

Extra problems

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

Problem 12. Let $\mathbb{H} \subseteq M_2(\mathbb{C})$ be the set

$$\mathbb{H} = \left\{ \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \mid z, w \in \mathbb{C} \right\}$$

where $\overline{a+bi} = a - bi$ indicates complex conjugation.

(a) Show that $\mathbb{H}$ is a subring of $M_2(\mathbb{C})$. Is $\mathbb{H}$ commutative? Is $\mathbb{H}$ unital?

(b) Is $\mathbb{H}$ a division ring? Is $\mathbb{H}$ a field?

(c) Find the center $Z(\mathbb{H})$ of $\mathbb{H}$.

Solution.

(a) We use Proposition 2.3 to show that $\mathbb{H}$ is a subring of $M_2(\mathbb{C})$. Clearly we have $\mathbb{H} \neq \varnothing$ since $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in \mathbb{H}$. Let $\left(\begin{smallmatrix} z & w \\ -\overline{w} & \overline{z} \end{smallmatrix}\right), \left(\begin{smallmatrix} v & u \\ -\overline{u} & \overline{v} \end{smallmatrix}\right) \in \mathbb{H}$. Then

$$\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} - \begin{pmatrix} v & u \\ -\overline{u} & \overline{v} \end{pmatrix} = \begin{pmatrix} z-v & w-u \\ -\overline{w}+\overline{u} & \overline{z}-\overline{v} \end{pmatrix} == \begin{pmatrix} z-v & w-u \\ -\overline{(w-u)} & \overline{z-v} \end{pmatrix} \in \mathbb{H},$$

and

$$\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \begin{pmatrix} v & u \\ -\overline{u} & \overline{v} \end{pmatrix} = \begin{pmatrix} zv - w\overline{u} & zu + w\overline{v} \\ -\overline{w}v - \overline{zu} & -\overline{w}u + \overline{zv} \end{pmatrix} = \begin{pmatrix} zv - w\overline{u} & zu + w\overline{v} \\ -\overline{(zu + w\overline{v})} & \overline{zv - w\overline{u}} \end{pmatrix} \in \mathbb{H},$$

and so $\mathbb{H}$ is a subring of $M_2(\mathbb{C})$. We have $\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathbb{H}$ and

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

hence $\mathbb{H}$ is not commutative. Since $1_{M_2(\mathbb{C})} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathbb{H}$, we conclude that $\mathbb{H}$ is unital.

(b) Let $A = \left(\begin{smallmatrix} z & w \\ -\overline{w} & \overline{z} \end{smallmatrix}\right) \in \mathbb{H}$. Then the determinant of this matrix is

$$\det(A) = z\overline{z} - w(-\overline{w}) = |z|^2 + |w|^2$$

which is zero if and only if $z = w = 0$. Hence every nonzero matrix in $\mathbb{H}$ has nonzero determinant and hence is invertible in $M_2(\mathbb{C})$. Notice that $\det(A)$ is a real number and set $\det(A) = s \in \mathbb{R}$. Using the formula for the inverse of a 2×2 matrix, we obtain

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} \overline{z} & -w \\ \overline{w} & z \end{pmatrix} = \frac{1}{s} \begin{pmatrix} \overline{z} & -w \\ -\overline{(-w)} & \overline{\overline{z}} \end{pmatrix} = \begin{pmatrix} \frac{\overline{z}}{s} & -\frac{w}{s} \\ -\overline{\left(\frac{-w}{s}\right)} & \overline{\left(\frac{\overline{z}}{s}\right)} \end{pmatrix} \in \mathbb{H}.$$

Hence every $A \in \mathbb{H}$ is invertible. Since $\mathbb{H}$ is unital by part (a), we conclude that $\mathbb{H}$ is a division ring. Since $\mathbb{H}$ is not commutative by part (a), we conclude that $\mathbb{H}$ is not a field.

(c) Let $A = \left(\begin{smallmatrix} z & w \\ -\overline{w} & \overline{z} \end{smallmatrix}\right) \in Z(\mathbb{H})$. Then, since $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathbb{H}$, we have $A\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)A$ and so

$$\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -w & z \\ -\overline{z} & -\overline{w} \end{pmatrix} = \begin{pmatrix} -\overline{w} & \overline{z} \\ -z & -w \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$$

gives $z = \overline{z}$ and $w = \overline{w}$, that is z and w are real numbers. Hence $z = a \in \mathbb{R}$ and $w = b \in \mathbb{R}$ and so $A = \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$. Moreover, since $A \in Z(\mathbb{H})$ and $\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right) \in \mathbb{H}$, we have $A\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right) = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)A$ and so

$$\begin{pmatrix} a & b \\ -a & b \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} ai & -bi \\ -bi & -ai \end{pmatrix} = \begin{pmatrix} ai & bi \\ bi & -ai \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

gives $bi = -bi$ or $b = 0$. Hence $A = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$. We then claim that

$$Z(\mathbb{H}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R} \right\}.$$

We have already shown the "$\subseteq$" inclusion. For the other side notice that for any $\left(\begin{smallmatrix} z & w \\ -\overline{w} & \overline{z} \end{smallmatrix}\right) \in \mathbb{H}$ we have

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} = \begin{pmatrix} az & aw \\ -a\overline{w} & a\overline{z} \end{pmatrix} = \begin{pmatrix} za & wa \\ -\overline{w}a & \overline{z}a \end{pmatrix} = \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix},$$

as required.

Problem 13. (Exercise 9.4.5(c) in the book.) Let $n \geq 1$ be an integer. Prove that an element $\overline{x} \in \mathbb{Z}/(n)$ is invertible if and only if $\gcd(x, n) = 1$. Show also that if $\gcd(x, n) = 1$, then $x^{\phi(n)} \equiv 1 \pmod{n}$ where $\phi(n)$ is Euler's function.

Solution. Assume first that $\gcd(x, n) = 1$. We first prove *Bézout's identity*, that is the fact that there exist integers a and b such that $ax + bn = 1$. Let

$$S \coloneqq \{ax + bn > 0 \mid a, b \in \mathbb{Z}\}.$$

For $a = 0$, $b = 1$ we obtain $n \in S$ and so $S \neq \varnothing$. Let $m = a_0x + b_0n = \min(S)$. It suffices to show that $\gcd(x, n) = m$. We may perform integer division of n by m to obtain

$$n = qm + r$$

where $0 \leq r < m$. In particular, we have that

$$r = n - qm = n - q(a_0x + b_0n) = (-qa_0)x + (1 - qb_0)n \in S,$$

and since $0 \leq r < m = \min(S)$, we conclude that $r = 0$. Hence $n = qm$ and m so divides n. By switching the roles of n and x we obtain that m divides x. Now let d be a common divisor of x and n. Then $td = x$ and $sd = n$ for some $t, s \in \mathbb{Z}$. Hence

$$m = a_0x + b_0n = a_0td + b_0sd = d(a_0t + b_0s),$$

and so d divides m. Therefore $m = \gcd(x, n) = 1$ as required. Hence $a_0x + b_0n = 1$ and so in $\mathbb{Z}/(n)$ we have $\overline{a_0} \cdot \overline{x} \equiv \overline{1} \pmod{n}$ and so $\overline{x}$ is invertible with $\overline{x}^{-1} = \overline{a_0}$.

Now assume that $\overline{x}$ is invertible and let $\overline{x}^{-1} = \overline{y}$. Then $\overline{x} \cdot \overline{y} \equiv 1 \pmod{n}$. In particular, n divides $xy - 1$ and so $xy - 1 = ln$ for some $l \in \mathbb{Z}$ or $1 = xy - ln$. Now let d be a common divisor of n and x. Then $td = x$ and $sd = n$ for some $t, s \in \mathbb{Z}$. Hence

$$1 = xy - ln = tdy - lsd = d(ty - ls)$$

and so d divides 1. Since any common divisor of x and n divides 1, we conclude that $\gcd(x, n) = 1$.

For the second part, recall that $\phi(n)$ is defined to be the number of elements which are relatively prime to n, that is

$$\phi(n) = |\{0 < x < n \mid \gcd(x, n) = 1\}|.$$

We have shown that the set

$$\{\overline{x} \mid 0 < x < n \text{ and } \gcd(x, n) = 1\}$$

consists of all the units of $\mathbb{Z}/(n)$, in other words it is equal to $U(\mathbb{Z}/(n))$ where $U(\mathbb{Z}/(n))$ is as in Problem 7. Hence $|U(\mathbb{Z}/(n))| = \phi(n)$. By Problem 7 we have that $U(\mathbb{Z}/(n))$ is a multiplicative group, and hence we obtain by Lagrange's theorem that for any $\overline{x} \in U(\mathbb{Z}/(n))$ we have

$$\overline{x}^{|U(\mathbb{Z}/(n))|} \equiv 1 \pmod{n}.$$

Since $|U(\mathbb{Z}/(n))| = \phi(n)$, the claim follows.