Problem 1. Let R be a finite ring. Suppose that $a \in R$ is not a zero divisor (neither left nor right). Prove that R is unital and a is invertible. **Hint.** Prove that $a^k = a$ for some integer $k > 1$. Then prove that a^{k-1} is the identity element of R.

Solution: Consider the sequence $a, a^2, a^3, \ldots$. Since R is finite, there exist $m < n$ such that $a^m = a^n$. Thus $a^{m-1}(a^{n-m+1} - a) = 0$. Since a is not a zero divisor, a^{m-1} is not a zero divisor and therefore we must have $a^{n-m+1} - a = 0$, i.e. $a^k = a$, where $k = n - m + 1 > 1$.

Let now $r \in R$. Then $a(a^{k-1}r - r) = a^k r - ar = ar - ar = 0$ and $(ra^{k-1} - r)a = ra^k - ra = ra - ra = 0$. Since a is not a zero divisor, we must have $a^{k-1}r - r = 0 = ra^{k-1} - r$. In other words, $a^{k-1}r = r = ra^{k-1}$ for all $r \in R$. This means that a^{k-1} is the identity element of R. In particular, R is unital. Also, if $k = 2$ then a itself is the identity element, hence it is invertible. If $k > 2$ then $1 = a^{k-1} = aa^{k-2} = a^{k-2}a$, so a is invertible.

Remark. Note that the problem implies in particular that any finite domain is a division ring. So we have another proof of a result from class.

Problem 2. Let I be an ideal in the ring $M_2(\mathbb{R})$. Prove that either $I = \{0\}$ or $I = M_2(\mathbb{R})$.

Solution: Suppose that $I \neq \{0\}$. Then there is a non-zero matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in I. Note that

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

and

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

Since I is an ideal, the matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} b & a \\ d & c \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} c & d \\ a & b \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} d & c \\ b & a \end{smallmatrix}\right)$ belong to I. Since at least one of a, b, c, d is not zero, we see that I contains a matrix $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ with $x \neq 0$. Thus

$$\begin{pmatrix} \frac{1}{x} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I.$$

It follows that

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in I, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in I,$$

and

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in I.$$

Now, for any $a, b, c, d \in \mathbb{R}$ we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in I.$$

Thus every matrix belongs to I, i.e. $I = M_2(\mathbb{R})$.

Solution to Problem 2.18 Our map $\theta : \mathbb{R}[x] \longrightarrow \mathbb{C}$ is defined by $\theta(f) = f(i)$. It is a homomorphism:

$$\theta(f + g) = (f + g)(i) = f(i) + g(i) = \theta(f) + \theta(g),$$

$$\theta(f \cdot g) = (f \cdot g)(i) = f(i) \cdot g(i) = \theta(f) \cdot \theta(g).$$

Given a complex number $a+bi$ we have $\theta(a+bx) = a+bi$ so θ is surjective. Suppose now that $f \in \ker\theta$, i.e. $\theta(f) = 0$. Thus $f(i) = 0$. Applying complex conjugation to this equality and using the fact that the coefficients of f are real, we get that $f(-i) = 0$. Thus i and $-i$ are roots of f and therefore $f(x) = (x-i)(x+i)g(x) = (x^2+1)g(x)$ for some polynomial in $\mathbb{C}[x]$. Applying complex conjugation we easily see that g has in fact real coefficients. Thus $f \in (x^2+1)\mathbb{R}[x]$. Conversely, if $f \in (x^2+1)\mathbb{R}[x]$ then $f(x) = (x^2+1)g(x)$ for some $g \in R[x]$ and therefore $f(i) = (i^2+1)g(i) = 0$, i.e. $f \in \ker\theta$. This proves that $(x^2+1)\mathbb{R}[x] = \ker\theta$.

Another way of computing $\ker\theta$ is to use the division algorithm for polynomials, according to which any polynomial $f \in \mathbb{R}[x]$ can be written (in a unique way) as $f = (x^2+1)g(x) + ax + b$ for some $g \in R[x]$ and some $a, b \in R$. It follows that $f(i) = 0$ iff $ai + b =$, iff $a = 0 = b$, iff $f \in (x^2+1)\mathbb{R}[x]$.

The first homomorphism theorem implies now that $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ and $\mathbb{C}$ are isomorphic. Explicitely, define a map $\phi : \mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ by $\phi(f + (x^2+1)\mathbb{R}[x]) = f(i) = \theta(f)$. It is weel defined, since if $f + (x^2+1)\mathbb{R}[x] = h + (x^2+1)\mathbb{R}[x]$ then $f - h = (x^2+1)g(x)$ for some polynomial g hence $f(i) = g(i)$. It is now starightforward to check that ϕ is an isomorphism (do it though).

Solution to Problem 2.21 Let $\left(\begin{smallmatrix} 0 & a \\ 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right)$ be in I and let $\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right) \in R$. Clearly

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

and

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} 0 & az \\ 0 & 0 \end{pmatrix} \in I, \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & xa \\ 0 & 0 \end{pmatrix} \in I.$$

This proves that I is an ideal.

Let $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right)$ be in S. Then

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} - \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} = \begin{pmatrix} a-x & 0 \\ 0 & b-y \end{pmatrix} \in S$$

and

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} = \begin{pmatrix} ax & 0 \\ 0 & by \end{pmatrix} \in S.$$

Thus S is a subring of R. It is not an ideal since $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in S$, $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \in R$ but

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \notin S.$$

Define a function $f : R/I \longrightarrow S$ by

$$f(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + I) = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}.$$

Note that it is well defined, since if $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) + I = \left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right) + I$ then

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} - \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} a-x & b-y \\ 0 & c-z \end{pmatrix} \in I$$

so $a - x = 0 = c - z$, i.e. $a = x$ and $c = z$. It is straightforward to check now that f is a homomorphism (do it !) and it is clear that it is surjective. If $A = \left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right) + I$ is in the kernel of f then $x = 0 = z$, so $\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right) \in I$ and therefore $A = 0$. This shows that f is injective and consequently an isomorphism.