Problem (Problem 1)**:** Let R be a ring in which every element a satisfies $a^2 = a$. Show that

(a) $2a = 0$ for every $a \in R$, so $a = -a$;

(b) R is commutative.

Solution:

(a) Let $a \in R$. We see that, since $a + a \in R$, $(a+a)^2 = a + a$, so that

$$\begin{aligned} a + a &= (a+a)^2 \\ &= (a+a)(a+a) \\ &= a^2 + a^2 + a^2 + a^2 \\ &= a + a + a + a, \end{aligned}$$

and since R is a ring, we see that $a + a = 0$, or that $a = -a$.

(b) Similarly, if $a, b \in R$, then since $(a+b)^2 = a + b$, we have

$$\begin{aligned} a + b &= (a+b)^2 \\ &= (a+b)(a+b) \\ &= a^2 + b^2 + ab + ba \\ &= a + b + ab + ba, \end{aligned}$$

so $ab = -ba$, but since $-ba = ba$ by the previous part, we have $ab = ba$, and so R is commutative.

Problem (Problem 2)**:** Let R be a ring with identity, and let $R^{\times}$ be the set of invertible elements of R. Show that $R^{\times}$ is a group under multiplication. What is $\mathbb{Z}[i]^{\times}$.

Solution: First, $R^{\times}$ is nonempty, as R contains a multiplicative identity. Next, if $a, b \in R^{\times}$, we see that ab admits the inverse $b^{-1}a^{-1}$, as

$$\begin{aligned} (ab)\left(b^{-1}a^{-1}\right) &= a\left(bb^{-1}\right)a^{-1} \\ &= aa^{-1} \\ &= 1, \end{aligned}$$

and similarly,

$$\begin{aligned} \left(b^{-1}a^{-1}\right)(ab) &= b^{-1}\left(a^{-1}a\right)b \\ &= b^{-1}b \\ &= 1, \end{aligned}$$

so $R^{\times}$ is closed under multiplication. Similarly, since $\left(b^{-1}\right)^{-1} = b$ for any $b \in R^{\times}$, every element of $R^{\times}$ has a multiplicative inverse, so $R^{\times}$ is a group.

To understand the picture of $\mathbb{Z}[i]^{\times}$, we try to understand when, given $a + bi \in \mathbb{Z}[i]$, $\frac{1}{a+bi} \in \mathbb{Z}[i]$. Doing the hand calculations, we see that

$$\frac{1}{a+bi} = \frac{1}{a^2+b^2}(a - bi).$$

Therefore, we see that this holds if and only if $a = \pm 1$ and $b = 0$, or $b = \pm 1$ and $a = 0$, meaning that $\mathbb{Z}[i]^{\times} = \{1, i, -1, -i\}$.

Problem (Problem 3)**:** Fix an integer $n > 1$. Recall that for $a, b \in \mathbb{Z}$, we write $a \equiv b$ modulo n if $a - b$ is divisible by n. Show that this relation is an equivalence relation on $\mathbb{Z}$. Furthermore, show that if $a \equiv b$

modulo n, and $c \equiv d$ modulo n, then

$$a + c \equiv b + d \text{ modulo } n, \text{ and } ac \equiv bd \text{ modulo } n.$$

Problem (Problem 4)**:** Show that a finite commutative ring with 1 and without zero divisors is a field.

Solution: Let $a \in R$, and consider the map $\varphi_a \colon R \setminus \{0\} \to R \setminus \{0\}$ given by $b \mapsto ab$. We see that if $ab = ac$, then $a(b - c) = 0$, and since $a \neq 0$, we see that $b = c$, so φ_a is injective. Since φ_a is an injective self-map of a finite set, φ_a is surjective, so φ_a is bijective, and thus $\varphi_a^{-1}(1)$ is well-defined, so $a\varphi_a^{-1}(1) = 1$, meaning a has a right-inverse. Since R is commutative, we have $\varphi_a^{-1}(1)a = 1$, so R is a field.

Problem (Problem 5)**:** Let $R = \text{Mat}_n(\mathbb{R})$ be the ring of real $n \times n$ matrices. Show that if A satisfies $\det(A) = 0$, then there exist nonzero $B, C \in R$ such that $AB = \mathbf{0}_n$ and $CA = \mathbf{0}_n$.

Solution: Consider the subring $R_0 \subseteq R$ consisting of all polynomials in A — i.e., polynomials $q(t) = a_0 + a_1t + \cdots + a_nt^n$ evaluated at A. We see that the sum of any two polynomials is a polynomial, and since A commutes with itself, and the product of any two polynomials is a polynomial, R_0 is a commutative subring of R.
Furthermore, we note two things:

- 0 is an eigenvalue of A;
- the minimal polynomial evaluated at A is contained in R_0.

Since 0 is an eigenvalue of A, we must have that $m_A(t) = tp(t)$ for some polynomial $p(t)$. Furthermore, $p(A)$ must not evaluate to 0, or else this would contradict minimality of A. The map $\varphi_A \colon R_0 \to R_0$ given by $q(A) \mapsto Aq(A)$ will have a nontrivial kernel as a result of the previous fact; by taking nonzero elements of the preimage $\varphi_A^{-1}(m_A(A))$, we find nonzero matrices B and C such that $AB = \mathbf{0}_n$ and $CA = \mathbf{0}_n$.

Problem (Problem 6)**:** An element $x \in R$ is called *nilpotent* if there exists $n > 0$ such that $x^n = 0$.

Assume R is a commutative ring with identity. Show that if $x \in R$ is nilpotent, then

(a) rx is nilpotent for any $r \in R$;

(b) $1 + x$ is invertible.

Solution:

(a) We see that, since R is commutative,

$$\begin{aligned}(rx)^n &= (rx)(rx)\cdots(rx)\\ &= r^nx^n\\ &= 0,\end{aligned}$$

so rx is nilpotent.

(b) We see that if a is nilpotent, then

$$\begin{aligned}1 &= 1 - a^n\\ &= (1 - a)\left(1 + a + \cdots + a^{n-1}\right),\end{aligned}$$

meaning that $1 - a$ is invertible. Furthermore, we note that if a is nilpotent, then so is $-a$, as since R is commutative and unital, $(-1)^na^n = (-a)^n = 0$. Therefore, if $x \in R$ is nilpotent, $1 - (-x) = 1 + x$ is invertible.

Problem (Problem 7)**:** Let $R = \text{Mat}_n(\mathbb{F})$, where $\mathbb{F}$ is a field. Show that if I is a nonzero 2-sided ideal of R, then $I = R$.

Solution: We show that if I is a nonzero two-sided ideal in $\text{Mat}_n(\mathbb{F})$, then $I_n \in I$.

Since I is nonzero, there is some matrix $\left(a_{ij}\right)_{i,j} \in I$ such that at particular indices i_0 and j_0, $a_{i_0 j_0} \neq 0$. Since $a_{ij} \in \mathbb{F}$ for all i, j, we have that $a_{i_0 j_0}^{-1}$ exists.

Let e_{ij} be the matrix unit with a position 1 at index (i, j) and zero elsewhere. Then, via some matrix algebra, we see that

$$a_{i_0 j_0} e_{kk} = \sum_{i,j=1}^{n} e_{ki} a_{ij} e_{jk},$$

which is necessarily in I, as I is a two-sided ideal. Therefore, since $\mathbb{F}$ is a field, we see that $(e_{kk})_{i,j} \in I$ for each k, so $\sum_{k=1}^{n} (e_{kk})_{i,j} \in I$, so $I_n \in I$, meaning $I = R$.

Problem (Problem 8)**:**

(a) Prove that $\operatorname{aut}_{\text{group}}(\mathbb{Z}^n) \cong \mathrm{GL}_n(\mathbb{Z})$.

(b) Prove that $\operatorname{aut}_{\text{ring}}(\mathbb{Z}^n) \cong \operatorname{Sym}(n)$.