Question 1. We define two operations $\boxplus$ and $\boxtimes$ on $\mathbb{Z}$ as

$$a \boxplus b = a + b - 1$$
$$a \boxtimes b = ab - a - b + 2$$

for $a, b \in \mathbb{Z}$.

(a) Show that $\mathbb{Z}$ together with addition $\boxplus$ and multiplication $\boxtimes$ is a ring.
(b) Determine if this ring is
  (i) A commutative ring
  (ii) A ring with identity
  (iii) An integral domain.
  (iv) A field.

Solution. (a) To see that $(\mathbb{Z}, \boxplus, \boxtimes)$ is a ring, we verify the six properties of a ring.

(i) (Associativity Over $\boxplus$) Let $x, y, z \in \mathbb{Z}$ be arbitrary. We show that

$$(x \boxplus y) \boxplus z = x \boxplus (y \boxplus z)$$

Using the properties of the usual addition on $\mathbb{Z}$,

$$\begin{aligned}(x \boxplus y) \boxplus z &= (x + y - 1) \boxplus z \\ &= (x + y - 1) + z - 1 \\ &= x + y - 1 + z - 1 \\ &= x + y + z - 1 - 1 \\ &= x + (y + z - 1) - 1 \\ &= x + (y \boxplus z) - 1 \\ &= x \boxplus (y \boxplus z)\end{aligned}$$

(ii) (Identity Over $\boxplus$) We claim that the identity over $\boxplus$ is $1 \in \mathbb{Z}$ because for any $x \in \mathbb{Z}$,

$$x \boxplus 1 = x + 1 - 1 = x$$

and

$$1 \boxplus x = 1 + x - 1 = x$$

(iii) (Inverse Over $\boxplus$) We first find the inverse element over $\boxplus$. Let $x \in \mathbb{Z}$ be arbitrary. Then there exists an element $y \in \mathbb{Z}$ such that $x \boxplus y = 1$. Then

$$\begin{aligned}x \boxplus y &= 1 \\ x + y - 1 &= 1 \\ y &= 2 - x\end{aligned}$$

So the inverse element over $\boxplus$ is $2 - x \in \mathbb{Z}$. Furthermore,

$$x \boxplus (2 - x) = x + (2 - x) - 1 = x + 2 - x - 1 = 1$$

and

$$(2 - x) \boxplus x = (2 - x) + x - 1 = 2 - x + x - 1 = 1$$

(iv) (Abelian Over $\boxplus$) Let $x, y \in \mathbb{Z}$ be arbitrary. We show that

$$x \boxplus y = y \boxplus x$$

Indeed,

$$x \boxplus y = x + y - 1 = y + x - 1 = y \boxplus x$$

(v) (Associativity Over $\boxtimes$) Let $x, y, z \in \mathbb{Z}$ be arbitrary. Then we show that

$$(x \boxtimes y) \boxtimes z = x \boxtimes (y \boxtimes z)$$

Indeed,

$$\begin{aligned}
(x \boxtimes y) \boxtimes z &= (xy - x - y + 2) \boxtimes z \\
&= (xy - x - y + 2)z - (xy - x - y + 2) - z + 2 \\
&= xyz - xz - yz + 2z - xy + x + y - 2 - z + 2 \\
&= xyz - xy - xz + x - yz + y + z - 2 + 2 \\
&= xyz - xy - xz + 2x - x - yz + y + z - 2 + 2 \\
&= x(yz - y - z + 2) - x - (yz - y - z + 2) + 2 \\
&= x \boxtimes (yz - y - z + 2) \\
&= x \boxtimes (y \boxtimes z)
\end{aligned}$$

as required.

(vi) (Distributive Property) Let $x, y, z \in \mathbb{Z}$ be arbitrary. Then we show that

$$x \boxtimes (y \boxplus z) = (x \boxtimes y) \boxplus (x \boxtimes z)$$

and

$$(x \boxplus y) \boxtimes z = (x \boxtimes z) \boxplus (y \boxtimes z)$$

Indeed,

$$\begin{aligned}
x \boxtimes (y \boxplus z) &= x \boxtimes (y + z - 1) \\
&= x(y + z - 1) - x(y + z - 1) + 2 \\
&= xy + xz - x - x - y - z + 1 + 2 \\
&= xy + xz - x - x - y - z + 2 - 1 + 2 \\
&= (xy - x - y + 2) + (xz - x - z + 2) - 1 \\
&= (x \boxtimes y) + (x \boxtimes z) - 1 \\
&= (x \boxtimes y) \boxplus (x \boxtimes z)
\end{aligned}$$

and similarly,

$$\begin{aligned}
(x \boxtimes y) \boxtimes z &= (x + y - 1) \boxtimes z \\
&= (x + y - 1)z - (x + y - 1) - z + 2 \\
&= xz + yz - z - x - y + 1 - z + 2 \\
&= xz + yz - z - x - y + 2 - 1 - z + 2 \\
&= (xz - x - z + 2) + (yz - y - z + 2) - 1 \\
&= (x \boxtimes z) + (y \boxtimes z) - 1 \\
&= (x \boxtimes z) \boxplus (y \boxtimes z)
\end{aligned}$$

Therefore, we have show that $(\mathbb{Z}, \boxplus, \boxtimes)$ is a ring.

(b) (i) We claim that $(\mathbb{Z}, \boxplus, \boxtimes)$ is a commutative ring. Let $x, y \in \mathbb{Z}$ be arbitrary. Then we show that

$$x \boxtimes y = y \boxtimes x$$

Indeed,

$$x \boxtimes y = xy - x - y + 2 = yx - y - x + 2 = y \boxtimes x$$

Therefore, $(\mathbb{Z}, \boxplus, \boxtimes)$ is a commutative ring.

(ii) We claim that $(\mathbb{Z}, \boxplus, \boxtimes)$ is a ring with identity. To see this, let $x \in \mathbb{Z}$ be arbitrary. Then if such a $y \in \mathbb{Z}$ exists such that $x \boxtimes y = y \boxtimes x = x$, then

$$\begin{aligned} x \boxtimes y &= x \\ xy - x - y + 2 &= x \\ xy - 2x - y + 2 &= 0 \\ x(y-2) - (y-2) &= 0 \\ (x-1)(y-2) &= 0 \end{aligned}$$

So from the above equation, we have that $y = 2$ is the identity over $\boxtimes$. Then observe that $2 \neq 0$, and for any $x \in \mathbb{Z}$,

$$x \boxtimes 2 = x2 - x - 2 + 2 = x$$

and

$$2 \boxtimes x = 2x - 2 - x + 2 = x$$

as desired.

(iii) We claim that $(\mathbb{Z}, \boxplus, \boxtimes)$ is an integral domain. To see this, note that from (i) and (ii) it is a commutative ring with identity. Assume that for $x, y \in \mathbb{Z}$ such that $x \boxtimes y = 0$. Then

$$x \boxtimes y = xy - x - y + 2 = 0$$

But then the equation above can be expressed as $y = \dfrac{x-2}{x-1}$ with $x \neq 1$, in which by some brief analysis, has a zero at $x = 2$, which would then yield that $y = 0$. So we have that $x \neq 2$ but $y = 0$. On the other hand, we can also express the equation as $x = \dfrac{y-2}{y-1}$ with $y \neq 1$, and similarly, we would obtain that $x = 0$ but $2 \neq 0$. Therefore, we have shown that either $x = 0$ or $y = 0$.

(iv) We claim that $(\mathbb{Z}, \boxplus, \boxtimes)$ is a not a field. To see this, note that from (i) and (ii), it is a commutative ring with identity. To show that $(\mathbb{Z}, \boxplus, \boxtimes)$ is a field, we need to show that it is a division ring. So let $x \neq 0 \in \mathbb{Z}$ be arbitrary. Then we seek a $y \in \mathbb{Z}$ so that $x \boxtimes y = y \boxtimes x = 2$ (because 2 is the identity over $\boxtimes$). Then solving for y,

$$\begin{aligned} xy - x - y + 2 &= 2 \\ xy - x - y &= 0 \\ y(x-1) &= x \\ y &= \frac{x}{x-1} \end{aligned}$$

However, note that by taking $x = 3$, we obtain that $y = \dfrac{3}{2} \notin \mathbb{Z}$, which is absurd. Therefore, $(\mathbb{Z}, \boxplus, \boxtimes)$ cannot be a field.

Question 2. Let $\mathbb{Z}_n[i] = \{a + ib : a, b \in \mathbb{Z}_n, i^2 = -1\}$ denote the Gaussian integers modulo n.

(a) Generate the multiplication table of $\mathbb{Z}_n[i]$ for $n = 2, 3, ..., 7$. (Use computer. Submit the tables for only $n = 2, 3$.)

(b) Determine all integers $n \geq 2$ for which $\mathbb{Z}_n[i]$ is an integral domain, hence, a field. (Hint: Fermat's theorem on the sum of squares. You may assume that $a^2 + b^2 = 0 \bmod p$ implies $a = b = 0 \bmod p$.)

Solution. (a) We have the following tables generated for $n = 2$ and $n = 3$ as follows:

$\cdot_2$	0	1	i	$1+i$
0	0	0	0	0
1	0	1	i	$1+i$
i	0	i	1	$1+i$
$1+i$	0	$1+i$	$1+i$	0

$\cdot_3$	0	1	2	i	$2i$	$1+i$	$1+2i$	$2+i$	$2+2i$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	i	$2i$	$1+i$	$1+2i$	$2+i$	$2+2i$
2	0	2	1	$2i$	i	$2+2i$	$2+i$	$1+2i$	$1+i$
i	0	i	$2i$	2	1	$2+i$	$1+i$	$2+2i$	$1+2i$
$2i$	0	$2i$	i	1	2	$1+2i$	$2+2i$	$1+i$	$2+i$
$1+i$	0	$1+i$	$2+2i$	$2+i$	$1+2i$	$2i$	2	1	i
$1+2i$	0	$1+2i$	$2+i$	$1+i$	$2+2i$	2	i	$2i$	1
$2+i$	0	$2+i$	$1+2i$	$2+2i$	$1+i$	1	$2i$	i	2
$2+2i$	0	$2+2i$	$1+i$	$1+2i$	$2+i$	i	1	2	$2i$

(b) We will break down the proof into three cases.

Case 1: (If n is an even integer) First consider the case when $n = 2$. We claim that $\mathbb{Z}_2[i]$ is not an integral domain. To see this, let us take $a = b = 1 + i \in \mathbb{Z}_2[i]$ such that $(1 + i)^2 = 0$. However, $1 + i \neq 0$, so $\mathbb{Z}_2[i]$ cannot be an integral domain. Recall that $\mathbb{Z}_p$ is an integral domain if and only if p is prime. Now if $n = 2k$ for some integer $k \in \mathbb{Z}$, then note that $\mathbb{Z}_{2k}$ would not be an integral domain as well, because $2k$ is a composite number, and therefore, $\mathbb{Z}_{2k}$ cannot be an integral domain. Furthermore, because $\mathbb{Z}_{2k} \subset \mathbb{Z}_{2k}[i]$, then $\mathbb{Z}_{2k}[i]$ cannot be an integral domain as well.

Case 2: (If $p = 4k + 1$ is a prime for some $k \in \mathbb{Z}$) Using Fermat's Theorem of Sum of Squares, then for integers $a, b \in \mathbb{Z}_p$,

$$a^2 + b^2 = p$$
$$a^2 + b^2 = p$$
$$(a + ib)(a - ib) = p$$

So then this implies that both $a + ib$ and $a - ib$ are zero divisors in $\mathbb{Z}_p[i]$, and thus, $\mathbb{Z}_p[i]$, where $p = 4k + 1$ for some integer k, cannot be an integral domain.

Case 3: (If $p = 4k + 3$ is a prime for some $k \in \mathbb{Z}$) We claim that $\mathbb{Z}_p[i]$, where $p = 4k + 3$ for some $k \in \mathbb{Z}$, is an integral domain. If this were not the case, let us assume that $a + ib \in \mathbb{Z}_p[i]$ is a zero divisor. Then for $c + id \in \mathbb{Z}_p[i]$ such that $c + id \neq 0$, we then have that

$$(a + ib)(c + id) = 0$$

which is in $\mathbb{Z}_p[i]$. So then,

$$(a+ib)(c+id) = (ac-bd) + i(ad+bc) = 0$$

and thus, $(ac-bd) \bmod p$ and $(ad+bc) \bmod p$, or equivalently:

$$ac - bd \equiv 0 \pmod{p} \tag{1}$$

$$ad + bc \equiv 0 \pmod{p} \tag{2}$$

Because $a+ib \in \mathbb{Z}_p[i]$ is a zero divisor, then at least one of a or b is not zero in $\mathbb{Z}_p$. Assume, without loss of generality, that $a \neq 0$. Then using (1)

$$\begin{aligned}
ac - bd &\equiv 0 \pmod{p}\\
ac &\equiv bd \pmod{p}\\
(ac)a^{-1} &\equiv (bd)a^{-1} \pmod{p}\\
(aa^{-1})c &\equiv bda^{-1} \pmod{p}\\
c &\equiv bda^{-1} \pmod{p}
\end{aligned}$$

Then substituting to (2), we obtain

$$\begin{aligned}
ad + bc &\equiv 0 \pmod{p}\\
ad + b(bda^{-1}) &\equiv 0 \pmod{p}\\
ad + b^2da^{-1} &\equiv 0 \pmod{p}
\end{aligned}$$

Note that $d \neq 0$ in this case. Otherwise, $c + id = 0$, which is absurd. Thus, note that

$$\begin{aligned}
ad + b^2da^{-1} &\equiv 0 \pmod{p}\\
d(a + b^2a^{-1}) &\equiv 0 \pmod{p}\\
a + b^2a^{-1} &\equiv 0 \pmod{p}\\
(a + b^2a^{-1})a^{-1} &\equiv 0 \pmod{p}\\
1 + b^2(a^{-1})^2 &\equiv 0 \pmod{p}\\
(ba^{-1})^2 &\equiv -1 \pmod{p}
\end{aligned}$$

But then from here, because $p = 4k+3$ is a prime for some $k \in \mathbb{Z}$, then we note that the last equation $(ba^{-1})^2 \equiv -1 \pmod{p}$ has no solutions, since -1 is not a quadratic residue mod p. Therefore, no such zero divisors exists when $p = 4k+3$ is a prime for some $k \in \mathbb{Z}$. Furthermore, since we have that $\mathbb{Z}_p \subset \mathbb{Z}_p[i]$ and since $\mathbb{Z}_p$ is a field, then we also obtain that $\mathbb{Z}_p[i]$ is a field.

Question 3. Let R be a ring. Define the *center of* R to be

$$Z(R) = \{a \in R : ar = ra \text{ for all } r \in R\}$$

Prove that $Z(R)$ is a commutative subring of R.

Solution. To show that $Z(R) \leq R$[1] is a commutative subring, we need to verify the following properties:

(1) Clearly, $Z(R) \neq \emptyset$ because $0 \in Z(R)$, which implies that $0 \in R$ as well, but satisfies the condition that $0r = r0 = 0$, which is true for any $r \in R$.

(2) Let $a, b \in Z(R)$ be arbitrary. We need to show that $ab \in Z(R)$. Indeed, if $a, b \in Z(R)$, then observe that for any $r \in R$,

$$(ab)r = a(br) = a(rb) = (ar)b = (ra)b = r(ab)$$

by using the associative property of R.

(3) Let $a, b \in Z(R)$ be arbitrary. We need to show that $a - b \in Z(R)$. Indeed, if $a, b \in Z(R)$, then for any $r \in R$,

$$(a - b)r = ar - br = ra - rb = r(a - b)$$

by using the distributive property of the ring R.

(4) Finally, note that $Z(R)$ is commutative by its definition, because for any $a \in R$, $ar = ra$ for any $r \in R$, so $Z(R)$ is commutative.

Therefore, we have shown that $Z(R) \leq R$.

[1] This notation is similar to saying that H is a subgroup of G, or $H \leq G$. So if S is a subring of R, we will use the notation $S \leq R$.

Question 4. An element a is an *idempotent* if $a^2 = a$.

(a) Prove that the only idempotents in an integral domain are 0 and 1.
(b) Find a ring with an idempotent that is not equal to 0 nor 1.
(c) Let R be a commutative ring with characteristic 2. Prove that the set $S = \{a \in R : a^2 = a\}$ is a subring of R.

Solution. (a) Let R be an integral domain, and let $a \in R$. Assume that $a^2 = a$. Then $a^2 - a = 0$, and so by factoring, $a(a-1) = 0$, so either $a = 0$ or $a - 1 = 0$ (thus, $a = 1$). Therefore, $a = 0$ and $a = 1$ are the only idempotents in the integral domain.

(b) Take $\mathbb{Z}_{15} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$. Then we have

- $0^2 = 0$
- $1^2 = 1$
- $2^2 = 4$
- $3^2 = 9$
- $4^2 = 16 \equiv 1$
- $5^2 = 25 \equiv 10$
- $6^2 = 36 \equiv 6$
- $7^2 = 49 \equiv 4$
- $8^2 = 64 \equiv 4$
- $9^2 = 81 \equiv 6$
- $10^2 = 100 \equiv 10$
- $11^2 = 121 \equiv 1$
- $12^2 = 144 \equiv 9$
- $13^2 = 169 \equiv 4$
- $14^2 = 196 \equiv 1$

Here, we observe that $6^2 = 6$ and $10^2 = 10$ are idempotents in $\mathbb{Z}_{15}$.

(c) To show that $S \leq R$, we need to verify the following properties.

(1) $S \neq \emptyset$ because $0, 1 \in S$ means that $0^2 = 0$ and $1^2 = 1$.
(2) Let $a, b \in S$ be arbitrary. We need to show that $ab \in S$. If $a, b \in S$, then

$$(ab)^2 = a^2b^2 = ab$$

(3) Let $a, b \in S$ be arbitrary. We need to show that $a + b \in S$ (rather than showing $a - b \in S$). If $a, b \in S$, then $a^2 = a$ and $b^2 = b$. Furthermore, because R has characteristic 2, then $2ab = 0$. Therefore,

$$(a+b)^2 = a^2 + 2ab + b^2 = a^2 + b^2 = a + b$$

Therefore, we have shown that $S \leq R$.

Question 5. (a) Let R be a commutative ring with identity. Show that the set of units in R, $U(R)$, is an abelian group under $\times_R$.

(b) Let F be a finite field with n elements. Show that $a^{n-1} = 1$ for all $a \neq 0 \in F$.

Solution. (a) Recall that $U(R) = \{n \in R : \gcd(k, n) = 1\}$. We show that $(U(R), \times_R)$ is an abelian group as follows:

(1) (Associativity) Since R is a commutative ring with identity, then R is also associative, and therefore, $U(R)$ is also associative, as it is inherited from R.

(2) (Identity) The element $1 \in U(R)$ because $1 \in R$, so for any $x \in U(R)$

$$1 \times_R a = a \quad a \times_R 1 = a$$

(3) (Inverse) Let $a \in U(R)$ be arbitrary. Then because R is a commutative ring with identity, then there exists an element $b \in R$ such that

$$a \times_R b = b \times_R a = 1$$

so $b \in U(R)$ as well, so an inverse exists.

(4) (Abelian) Since R is a commutative ring with identity, then $U(R)$ is also an abelian group under $\times_R$.

(b) Let $a \neq 0 \in F$ be arbitrary. Since F is a field with n elements, then it is a multiplicative group of order $n - 1$. Then the order of a must be a divisor of $n - 1$. Assume that the order of a is $m \in \mathbb{N}$, then because a is a divisor of $n - 1$, we have $m \mid n - 1$, so there exists an integer $b \in \mathbb{N}$ such that $bm = n - 1$, and so

$$a^{n-1} = b^m = (a^m)^b = 1^b = 1$$

So $a^{n-1} = 1$ for every $a \neq 0 \in F$, as desired.

Question 6. Let F be a field and let K be a subset of F with at least two elements. Prove that K is a subfield of F if for any $a, b \in K$, $a - b \in K$ and $ab^{-1} \in K$.

Solution. Let $a, b \in K$ be arbitrary. Then we need to show that $a - b \in K$ and $ab^{-1} \in K$ (assuming that $b \neq 0$). First, note that if $a \in K$, then $a - a = 0 \in K$ and also $-a = 0 - a \in K$. Then if $a, b \in K$ are arbitrary, then $-b \in K$ as well, and so $a + (-b) = a - b \in K$, as required. Now let $b \in K$ such that $b \neq 0$. Since K contains at least two elements, and because F is a field, then $b \cdot b^{-1} = 1 \in K$, and also $b^{-1} = 1 \cdot b^{-1} \in K$ as well. Now let $a, b \in K$ be arbitrary such that $b \neq 0$. Then because $b \neq 0$ and F is a field, then b^{-1} exists in K, and $ab^{-1} \in K$. Therefore, we have shown that $a - b \in K$ and $ab^{-1} \in K$, so $K \leq F$, as required.

Question 7. (a) Let R be a commutative ring with prime characteristic p. Show that for $r, s \in R$,

(i) $(r+s)^p = r^p + s^p$

(ii) $(r+s)^{p^m} = r^{p^m} + s^{p^m}$ for all positive integers m.

(iii) The Frobenius map $x \mapsto x^p$ is a ring homomorphism from R to R.

(b) Give an example of a ring of characteristic 4 and elements r and s such that $(r+s)^4 \neq r^4+s^4$.

Solution. (a) We first require the following lemma in order to prove (i).

Claim 1. If $p \geq 2$ is prime, then $p \mid \binom{p}{k}$ for $0 \leq k \leq p$

Given the claim, for p prime and $r, s \in R$ where R is a commutative ring with prime characteristic, we have by the binomial theorem,

$$\begin{aligned}
(r+s)^p &= \sum_{k=0}^{p} \binom{p}{k} r^{p-k} s^k \\
&= \binom{p}{0} r^p + \sum_{k=1}^{p-1} \binom{p-1}{k} r^{p-k} s^k + \binom{p}{p} s^p \\
&= r^p + s^p + \sum_{k=1}^{p-1} \binom{p}{k} r^{p-k} s^k
\end{aligned}$$

Then, since $p \mid \binom{p}{k}$, then it follows that $p \mid \sum_{k=0}^{p-1} \binom{p}{k} r^{p-k} s^k$, so there exists an integer $m \in \mathbb{Z}$ such that

$$\sum_{k=1}^{p-1} \binom{p}{k} r^{p-k} s^k = mp$$

Furthermore, since R is a commutative ring with characteristic p, then

$$\sum_{k=1}^{p-1} \binom{p}{k} r^{p-k} s^k = 0$$

Hence,

$$(r+s)^p = r^p + s^p$$

as desired.

Now to prove the claim, observe that

$$p(p-1)! = \binom{p}{k} k!(p-k)!$$

which then implies that $p \mid \binom{p}{k} k!(p-k)!$ and furthermore, because p is prime, we have either $p \mid \binom{p}{k}$, $p \mid k!$, or $p \mid (p-k)!$. However, $p \nmid k!$ and $p \nmid (p-k)!$. To see this, assume otherwise that $p \mid k!$. Since p is prime, then $p \mid i$ for some $1 \leq i \leq k$. But then $1 \leq p \leq i$, which is absurd, because $1 \leq k \leq p$. Similarly, $1 \leq (p-k) < p$ so $p \nmid (p-k)!$.

(ii) In a similar manner as in part (i), we use the binomial theorem to see that

$$(r+s)^{p^m} = r^{p^m} + \sum_{k=1}^{p^m-1} \binom{p^m}{k} r^{p^m-k}s^k + s^{p^m}$$

Now we just need to show that $\sum_{k=1}^{p^m-1} \binom{p^m}{k} r^{p^m-k}s^k = 0$. However, note that $p^m \mid \sum_{k=0}^{p^m-1} \binom{p^m}{k} r^{p^m-k}s^k$ for each $1 \leq k \leq p^m - 1$, so each of these coefficients are also divisible by p. Therefore, there is some $n \in \mathbb{Z}$ such that $\sum_{k=0}^{p^m-1} \binom{p^m}{k} r^{p^m-k}s^k = np$, and thus,

$$\begin{aligned}
(r+s)^{p^m} &= r^{p^m} + \sum_{k=1}^{p^m-1} \binom{p^m}{k} r^{p^m-k}s^k + s^{p^m} \\
&= r^{p^m} + np + s^{p^m} \\
&= r^{p^m} + 0 + s^{p^m} \\
&= r^{p^m} + s^{p^m}
\end{aligned}$$

as required.

(iii) Let $\phi : R \to R$ be a mapping defined by $\phi(x) = x^p$, where p is prime. We want to show that ϕ is a ring homomorphism, i.e. for all $x, y \in R$,

$$\phi(x+y) = \phi(x) + \phi(y) \quad \phi(xy) = \phi(x)\phi(y)$$

To show the addition, observe that

$$\begin{aligned}
\phi(x+y) &= (x+y)^p \\
&= x^p + y^p && \text{(from (i))} \\
&= \phi(x) + \phi(y)
\end{aligned}$$

To show the multiplication, observe that

$$\begin{aligned}
\phi(xy) &= (xy)^p \\
&= x^p y^p && \text{(because } R \text{ is commutative)} \\
&= \phi(x)\phi(y)
\end{aligned}$$

Therefore, we have shown that ϕ is a ring homomorphism.

Question 8. Let $\phi : R \to S$ be a ring homomorphism. Let $\phi(R) = \{\phi(r) : r \in R\}$. Prove each of the following statements:

(a) $\phi(0_R) = 0_S$
(b) $\phi(-b) = -\phi(b)$ for all $b \in R$
(c) $\phi(R)$ is a subring of S
(d) If R is a commutative subring, then $\phi(R)$ is a commutative subring.
(e) Suppose R and S are rings with identities. If ϕ is onto, then $\phi(1_R) = 1_S$.
(f) If R is a field and $\phi(R) \neq \{0_S\}$ then $\phi(R)$ is a field.

Solution. (a) To show that $\phi(0_R) = 0_S$, observe that

$$\begin{aligned}\phi(0_R) &= \phi(0_R + 0_R) \\ &= \phi(0_R) + \phi(0_R)\end{aligned}$$

Since S is a ring, then $\phi(0_R)$ has an additive inverse, namely $-\phi(0_R)$, and therefore, applying $-\phi(0_R)$ to both sides of the equation yields

$$\begin{aligned}\phi(0_R) - \phi(0_R) &= \phi(0_R) + \phi(0_R) - \phi(0_R) \\ 0_S &= \phi(0_R)\end{aligned}$$

as desired.

(b) Since $0_R = b + (-b)$, then $\phi(0_R) = \phi(b + (-b)) = \phi(b) + \phi(-b)$. Since $\phi(0_R) = 0_S$, then $0_S = \phi(b) + \phi(-b)$, and thus, $\phi(-b) = -\phi(b)$, as required.

(c) To show that $\phi(R) \leq S$, we need to verify the three properties:

(1) Here, $\phi(R) \neq \emptyset$ because $0_R \in R$, and $\phi(0_R) = 0_S$.
(2) Let $\phi(x), \phi(y) \in \phi(R)$ be arbitrary, and hence, $-\phi(y) \in \phi(R)$. Then we show that $\phi(x) - \phi(y) \in \phi(R)$. Since ϕ is a homomorphism, then

$$\phi(x + (-y)) = \phi(x) + \phi(-y) = \phi(x) - \phi(y) \in \phi(R)$$

(3) Let $\phi(x), \phi(y) \in \phi(R)$ be arbitrary. Then we show that $\phi(x)\phi(y) \in \phi(R)$. Since ϕ is a homomorphism,

$$\phi(xy) = \phi(x)\phi(y) \in \phi(R)$$

Therefore, we have shown that $\phi(R) \leq S$, as desired.

(d) To show that $\phi(R)$ is a commutative subring, let $x, y \in R$ be arbitrary. Then $\phi(x), \phi(y) \in \phi(R)$, and since R is a commutative subring, and ϕ is a homomorphism,

$$\begin{aligned}\phi(x)\phi(y) &= \phi(xy) \\ &= \phi(yx) \\ &= \phi(y)\phi(x)\end{aligned}$$

as required.

(e) Let $a = \phi(1_R)$ and let $r \in R$ be such that $\phi(r) = 1_S$ (because ϕ is onto, such an r exists). Then, because ϕ is a homomorphism

$$\begin{aligned}1_S &= \phi(r) \\ &= \phi(1_R \cdot r) \\ &= \phi(1_R) \cdot \phi(r) \\ &= a\phi(r) \\ &= a \cdot 1_S \\ &= a\end{aligned}$$

Therefore, $a = \phi(1_R) = 1_S$, as required.

(f) Note that because R is a field, then R is a commutative divison ring, so $\phi(R)$ is also commutative from (d). Now assume that $\phi(1) = 0$. Then for $r \in R$,

$$\phi(r) = \phi(r)\phi(1) = 0$$

which is absurd because it would contradict that ϕ is not the zero function. Therefore, $\phi(1) \neq 0$. Now let $\phi(r) \in \phi(R)$ be such that $\phi(r) \neq 0$. Since $\phi(r) \neq 0$, then $r \neq 0$. But then r has an inverse r^{-1}, because R is a field, so then

$$\phi(1) = \phi(r \cdot r^{-1}) = \phi(r)\phi(r^{-1})$$

Therefore, $\phi(r)$ has an inverse in $\phi(R)$, and so $\phi(R)$ is a field.

Question 9. Consider the ring $S = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$ with matrix addition and matrix multiplication. Show that $\phi : \mathbb{C} \to S$ given by

$$\phi(a+ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

is a ring isomorphism.

Solution. To show that ϕ is a ring isomorphism, we check the following.

(1) One-to-One: If $\phi(a+ib) = \phi(c+id)$, then $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$, so $a = c$ and $b = d$, so $a + ib = c + id$.

(2) Onto: Because ϕ is an injection, if $\phi(a+ib) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, then $a = 0$ and $b = 0$ and so ϕ is onto.

(3) Let $a + ib, c + id \in \mathbb{C}$. Then observe that

$$\begin{aligned} \phi((a+ib)+(c+id)) &= \phi((a+c)+i(b+d)) \\ &= \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\ &= \phi(a+ib) + \phi(c+id) \end{aligned}$$

Let $a + ib, c + id \in \mathbb{C}$, then observe that

$$\begin{aligned} \phi((a+ib)(c+id)) &= \phi((ac-bd)+i(ad+bc)) \\ &= \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\ &= \phi(a+ib)\phi(c+id) \end{aligned}$$

Therefore, we have shown that $\phi : \mathbb{C} \to S$ is a ring isomorphism.

Question 10. Show that $\mathbb{Z}_3[i]$ is ring isomorphic to $\mathbb{Z}_3[x]/\langle x^2+1\rangle$.

Solution. To show that $\mathbb{Z}_3[i] \simeq \mathbb{Z}_3[x]/\langle x^2+1\rangle$, let $\phi : \mathbb{Z}_3[x] \to \mathbb{Z}_3[i]$ be the mapping defined by $\phi(a+bx) = a+bi$. Then

$$\ker(\phi) = \{a+bx : \phi(a+bx) = 0\} = \langle x^2+1\rangle$$

because for any polynomial such that $p(i) = 0$ has i as a root, and therefore $-i$ because it has integer coefficients and is divisible by x^2+1 so we can factor and we would obtain the isomorphism as required.