1. Consider the veracity or falsehood of each of the following statements. For bonus, argue for those that you believe are true while providing a counterexample for those that you believe are false.

(1) There is an integral domain with 6 elements.

Let $k$ be a positive integer. Let $^{-}\colon \mathbb{Z} \to \mathbb{Z}_k$ be the mod function. Thus, *e.g.*, if $k = 7$, then $\overline{25} = 4$. This leads naturally to a homomorphism $^{-}\colon \mathbb{Z}[x] \to \mathbb{Z}_k[x]$. Thus, *e.g.*, if $k = 7$, then $\overline{25x^2 + 12} = 4x^2 + 5 = -3x^2 - 2$. Consider the veracity or falsehood of each of the following statements. For those that are true give an argument, for those that are false, give a counterexample. Let $p(x) \in \mathbb{Z}[x]$ be monic.

(2) If $p(x)$ has a root in $\mathbb{Z}$, then $\overline{p}(x)$ has a root in $\mathbb{Z}_k$.

(3) If $\overline{p}(x)$ has a root in $\mathbb{Z}_k$, then $p(x)$ has a root in $\mathbb{Z}$.

(4) If $p(x)$ is irreducible, then so is $\overline{p}(x)$.

(5) If $\overline{p}(x)$ is irreducible, then so is $p(x)$.

**Solution.**

(1) False.
**Proof.** Assume to the contrary that $R$ is an integral domain with 6 elements. Since $R$ is finite it follows that it is a field, a contradiction since 6 cannot be written as a positive power of any prime; thus $R$ is not an integral domain. $\square$

For the remaining problems, let

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x].$$

(2) True.
**Proof.** Suppose that $c \in \mathbb{Z}$ is a root of $p(c)$. It follows immediately that $\overline{c}$ is also a root of $\overline{p}(x)$ because

$$\begin{aligned} \overline{p}(\overline{c}) &= \overline{a_0} + \overline{a_1} \cdot \overline{c} + \cdots + \overline{a_n} \cdot \overline{c}^n \\ &= \overline{a_0 + a_1 c + \cdots + a_n c^n} \\ &= \overline{p(c)} = \overline{0}. \end{aligned}$$

$\square$

(3) False.
**Counterexample.** Let $p(x) = x^2 + 1$. Then $\overline{p}(x)$ has a root, $\overline{1}$, in $\mathbb{Z}_2$ but $p(x)$ has no root in $\mathbb{Z}$.

(4) False.
**Counterexample.** Let $p(x) = x^2 + 1$. Then $p(x)$ is irreducible in $\mathbb{Z}[x]$ but $\overline{p}(x) = (x + 1)^2$ is not irreducible in $\mathbb{Z}_2[x]$.

(5) False.

**Proof.** Let $p(x) = 49x^2 + 14x + 1$. Then $\overline{p}(x) = \overline{1}$ is irreducible in $\mathbb{Z}_7[x]$ but $p(x) = (7x+1)^2$ is not irreducible in $\mathbb{Z}[x]$.

2. Consider the integral domain $R = \mathbb{Z}[\sqrt{3}]$. Let $A = \begin{pmatrix} 5 & 3 \\ 9 & 5 \end{pmatrix}$.

(1) Find a nontrivial unit, and show it has infinite order.

(2) Compute $\dfrac{A}{\begin{pmatrix} 20 & 6 \\ 18 & 20 \end{pmatrix}}$ and its reciprocal $\dfrac{\begin{pmatrix} 20 & 6 \\ 18 & 20 \end{pmatrix}}{A}$. These elements may not be in the domain, but they are certainly in the field of quotients.

(3) Decide if $A$ and $\begin{pmatrix} 19 & 11 \\ 33 & 19 \end{pmatrix}$ are associates.

(4) Is $\begin{pmatrix} 7789 & 4488 \\ 13464 & 7789 \end{pmatrix} \equiv \begin{pmatrix} 57 & 24 \\ 72 & 57 \end{pmatrix}$ mod $A$? Give reasons for your answer.

**Solution.**

(1) The matrix $B = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}$ is a unit in $\mathbb{Z}[\sqrt{3}]$ because $B^{-1} = \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix} \in \mathbb{Z}[\sqrt{3}]$. Let $n$ be a positive integer. Observe that the integer in the first row and first column of $B^n$ will never be less than 2 because all the entries in $B$ are positive integers. Thus $B^n \neq I$, so that $|B| = \infty$.

(2) We have

$$\frac{A}{\begin{pmatrix} 20 & 6 \\ 18 & 20 \end{pmatrix}} = \frac{1}{146}\begin{pmatrix} 23 & 15 \\ 45 & 23 \end{pmatrix} \quad \text{and} \quad \frac{\begin{pmatrix} 20 & 6 \\ 18 & 20 \end{pmatrix}}{A} = \begin{pmatrix} -23 & 15 \\ 45 & -23 \end{pmatrix}.$$

(3) $A$ and $\begin{pmatrix} 19 & 11 \\ 33 & 19 \end{pmatrix}$ are associates if and only if there exists a unit $X = \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \in \mathbb{Z}[\sqrt{3}]$ such that

$$AX = \begin{pmatrix} 19 & 11 \\ 33 & 19 \end{pmatrix}.$$

Multiplying $A$ and $X$ and equating corresponding entries will yield the equations $3a + 5b = 11$ and $5a + 9b = 19$, and whose solution is $a = 2$ and $b = 1$. Since $\det(X) = a^2 - 3b^2 = 1$, it follows that $X$ is a unit. Thus $A$ and $\begin{pmatrix} 19 & 11 \\ 33 & 19 \end{pmatrix}$ are associates.

(4) A quick computation will show us that

$$\begin{pmatrix} 7789 & 4488 \\ 13464 & 7789 \end{pmatrix} \equiv \begin{pmatrix} 57 & 24 \\ 72 & 57 \end{pmatrix} \mod A$$

because

$$\begin{pmatrix} 7789 & 4488 \\ 13464 & 7789 \end{pmatrix} - \begin{pmatrix} 57 & 24 \\ 72 & 57 \end{pmatrix} = \begin{pmatrix} 7732 & 4464 \\ 13392 & 7732 \end{pmatrix} = A \begin{pmatrix} 758 & 438 \\ 1314 & 758 \end{pmatrix}.$$

3. Consider the following element $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ of $GL(3, \mathbb{Z}_2)$.

(1) Compute all of its powers.

(2) How many elements would you have to add for this set of powers to be closed under addition?

(3) Find the characteristic polynomial of each of the powers.

(4) Find the lowest degree polynomial that all of the powers satify.

(5) Have you constructed a field?

**Bonus.** Show that every irreducible cubic over $\mathbb{Z}_2$ has a root among these powers.

**Solution.** Let $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$

(1) The powers of $A$ are:

$$A^1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, A^3 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, A^4 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

$$A^5 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, A^6 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, A^7 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

(2) We notice that the set of powers is closed under addition of two *distinct* matrices. However, since each matrix added to itself yields the zero matrix, we need to add only the zero matrix so that this set of powers is closed under addition.

(3) If we let $\operatorname{char}(X)$ denote the charactersitic polynomial of a matrix $X$, then it follows that $\operatorname{char}(A^7) = x^3 + x^2 + x + 1$,

$$\operatorname{char}(A) = \operatorname{char}(A^2) = \operatorname{char}(A^4) = x^3 + x + 1, \text{and}$$

$$\operatorname{char}(A^3) = \operatorname{char}(A^5) = \operatorname{char}(A^6) = x^3 + x^2 + 1.$$

(4) The lowest degree polynomial that $A^7$ satisfies is $x+1$, while the lowest degree polynomial that the remaining powers satisfy is their respective characteristic polynomials. Thus the lowest degree polynomial that all the powers of $A$ satisfy is

$$(x+1)(x^3+x+1)(x^3+x^2+1) = x^7+1.$$

(5) Yes. It is clear that the set of powers of $A$ (including the 0 matrix) is a commutative ring; since each element in the set of powers of $A$ is a unit, it follows that the set of powers union the 0 matrix is a field.

**Bonus.** The only cubics with nontrivial factorizations in $\mathbb{Z}_2[x]$ are:

$$\begin{array}{lcl} x^3 & = & (x)(x)(x) \\ x^3+1 & = & (x+1)(x^2+x+1) \\ x^3+x & = & x(x+1)^2 \\ x^3+x^2 & = & x^2(x+1) \\ x^3+x^2+x & = & x(x^2+x+1) \\ x^3+x^2+x+1 & = & (x+1)^3, \end{array}$$

so that $x^3+x+1$ and $x^3+x^2+1$ are irreducible in $\mathbb{Z}_2[x]$. But these irreducibles are the characteristic polynomials of $A$ and $A^3$, so it follows by the Cayley-Hamilton theorem that $A$ is a root of $x^3+x+1$ and $A^3$ is a root of $x^3+x^2+1$.

4. On $\mathbb{Z}_2[x]$. Consider the ring of polynomials $\mathbb{Z}_2[x]$ with coefficients in $\mathbb{Z}_2$,

$$p(x) = a_0 + a_1x + \cdots + a_nx^n.$$

(1) How many polynomials of degree $n$ are there? **Hint.** Consider $n = 1, 2, 3, \ldots$.

(2) Consider the function $E : \mathbb{Z}_2[x] \to \mathbb{Z}_2$ that sends any polynomial $p(x)$ to $p(1)$. Decide if it is a (ring) homomorphism or not. Decide if it is one-to-one and onto. Argue your case.

(3) Consider the function $S : \mathbb{Z}_2[x] \to \mathbb{Z}_2[x]$ that sends any polynomial $p(x)$ to $p^2(x)$, it square. Decide if it is a (ring) homomorphism or not. Decide if it is one-to-one and onto. Argue your case.

(4) Count the number of irreducible quadratics in $\mathbb{Z}_2[x]$.

(5) Count the number of irreducible cubics in $\mathbb{Z}_2[x]$.

(6) Count the number of irreducible quartics in $\mathbb{Z}_2[x]$.

**Solution.**

(1) Since each polynomial has $n+1$ unique coefficients and since there are 2 choices for each coefficients, it follows that there are $2^{n+1}$ polynomials of degree $n$.

(2) It is clear that $E$ is onto since $E(0) = 0$ and $E(1) = 1$. However $E$ is not injective because $E(x) = E(1) = 1$ but $x \neq 1$. Now we claim that $E$ is a homomorphism of rings.

**Proof.** Consider two elements $q(x), r(x) \in \mathbb{Z}_2[x]$ where

$$q(x) = q_0 + q_1 x + \cdots + q_n x^n \text{ and } r(x) = r_0 + r_1 x + \cdots + r_n x^n.$$

We have that

$$\begin{aligned}
E(q(x) + r(x)) &= E((q_0 + r_0) + (q_1 + r_1)x + \cdots + (q_n + r_n)x^n) \\
&= (q_0 + r_0) + (q_1 + r_1) + \cdots + (q_n + r_n) \\
&= (q_0 + q_1 + \cdots + q_n) + (r_0 + r_1 + \cdots + r_n) \\
&= E(q(x)) + E(r(x)) \text{ and} \\
E(q(x)r(x)) &= E\left(q_0 r_0 + (q_0 r_1 + q_1 r_0)x + \cdots + \left(\sum_{i=0}^{n} q_i r_{n-i}\right) x^n\right) \\
&= q_0 r_0 + (q_0 r_1 + q_1 r_0) + \cdots + \left(\sum_{i=0}^{n} q_i r_{n-i}\right) \\
&= q(1) r(1) = E(q(x))E(r(x)),
\end{aligned}$$

so that $E$ is a surjective ring homomorphism. □

3 Claim that $S$ is an injective homomorphism of rings.
**Proof.** Consider two elements $q(x), r(x) \in \mathbb{Z}_2[x]$ where

$$q(x) = q_0 + q_1 x + \cdots + q_n x^n \text{ and } r(x) = r_0 + r_1 x + \cdots + r_n x^n.$$

Thus

$$\begin{aligned}
S(q(x) + r(x)) &= (q(x) + r(x))^2 \\
&= q(x)^2 + r(x)^2 + 2q(x)r(x) \\
&= q(x)^2 + r(x)^2 \\
&= S(q(x)) + S(r(x)) \text{ and} \\
S(q(x)r(x)) &= (q(x)r(x))^2 \\
&= q(x)^2 r(x)^2 \\
&= S(q(x))S(r(x)),
\end{aligned}$$

so that $S$ is a ring homomorphism. Now suppose that $S(q(x)) = S(r(x))$; then we have that $q(x)^2 = r(x)^2$, so that $(q(x) - r(x))(q(x) + r(x)) = 0$. Since we are in $\mathbb{Z}_2[x]$, notice that the additive of every polynomial is itself. Thus we must have that $(q(x) - r(x))(q(x) - r(x)) = (q(x) - r(x))(q(x) + r(x)) = 0$. And since $\mathbb{Z}_2[x]$ is an integral domain, it follows that $q(x) - r(x) = 0$; i.e., $q(x) = r(x)$ so that $S$ is injective. Clearly $S$ is not surjective since the polynomial $x + 1$ has no preimage under $S$. □

4 The only irreducible quadratic in $\mathbb{Z}_2[x]$ is $x^2 + x + 1$.

5 We know from the Bonus part of Problem 3 that there are two irreducible cubics in $\mathbb{Z}_2[x]$ and they are:

$$x^3 + x + 1 \text{ and } x^3 + x^2 + 1.$$

6 There are three irreducible quartics in $\mathbb{Z}_2[x]$ and they are:

$$x^4 + x + 1, x^4 + x^3 + 1, \text{ and } x^4 + x^3 + x^2 + x + 1.$$