Problem 1. (Ideals and Factor Rings) For each of the following rings $R$ and subsets $I \subseteq R$, determine whether $I$ is a subring of $R$ and whether $I$ is an ideal of $R$. If $I$ is an ideal, do the following:

- Find a set of generators for $I$ of minimal size, and determine whether $I$ is principal.
- Determine the factor ring $R/I$ by giving an appropriate homomorphism from $R$ to a familiar ring $S$.
- Determine whether $I$ is maximal, and if not, find a maximal ideal containing $I$.

1. $R = \mathbb{Z} \times \mathbb{Z}$, $I = \{(a, b) : a \equiv b \pmod{6}\}$.
2. $R = \mathbb{R}[x]$, $I = \{p(x) : p(0) = 0 \text{ and } p(7) = 0\}$.
3. $R = \mathbb{R}[x]$, $I = \{p(x) : p(0) = 0 \text{ or } p(7) = 0\}$.
4. $R = \mathbb{Q}[x]$, $I = \langle x^3 + x^2 - 2x - 2, x^2 + 2x + 1 \rangle$.
5. $R = \mathbb{Z}_{96}$, $I = \{0, 32, 64\}$.

Solution:
1. \( I \) is a subring but not an ideal, since for \( \alpha = (1, 2) \), \( \alpha I \not\subset I \).

2. A polynomial \( p(x) \) in \( R \) is such that \( p(0) = p(7) = 0 \) iff \( x(x-7) \) divides \( p(x) \). Thus \( I = x(x-7)R \) is an ideal generated by \( x(x-7) \). The quotient ring is the set of polynomials in \( R \) with degree one or zero where multiplication is taken mod \( x(x-7) \). The ideal is not maximal because \( I \) is contained in the ideal generated by \( x \).

The quotient ring is just isomorphic to \( R \times R \) – indeed, consider \( \phi : R[x] \to R \times R \) given by \( \phi(p) = (p(0), p(7)) \). It is easy to check that it is an homomorphism, \( \text{img}(\phi) = R \times R \), and by definition \( \text{ker} \phi = I \). 

3. \( I \) is not a subring because it is not closed under addition. Notice that \( x + (x-7) = 2x - 7 \not\in I \), while \( x \) and \( x-7 \in I \).

4. \( I = \langle x^3 + x^2 - 2x - 2, x^2 + 2x + 1 \rangle = \langle \gcd(x^3 + x^2 - 2x - 2, x^2 + 2x + 1) \rangle = \langle x+1 \rangle \). So, \( I \) and an ideal. and it is maximal because \( R/I = \mathbb{Q} \), which is a field.

5. \( I \) is an ideal, but it is not maximal because \( I \subset \langle 2 \rangle \). The quotient ring is \( \mathbb{Z}_{32} \) — the homomorphism \( \phi : \mathbb{Z}_{96} \to \mathbb{Z}_{32} \) given by \( \phi(x \mod 96) = x \mod 32 \) is surjective, and such that \( \ker \phi = I \).

Problem 2. (Computations in \( F[x] \) [AM106-A]) Note that the two parts of this problem are over different fields.

1. List all of the monic, irreducible polynomials of degree up to and including 5 over \( \mathbb{Z}_2[x] \).

2. Use the polynomial analogue of the Euclidean Algorithm to find a single polynomial \( h(x) \) such that the ideal \( \langle h(x) \rangle \) equals the ideal \( \langle x^6 + 2x^4 + 2x^3 + 2x + 1, x^5 + x^2 + 2x + 1 \rangle \) in \( \mathbb{Z}_3[x] \).

Show your work.

Solution:

1. List of irreducible polynomials of degree up to 5 over \( \mathbb{Z}_2 \):
   - Degree 1: all polynomials of degree 1 are irreducible.
     \[ x, x+1 \]
   - Degree 2 and 3: polynomials of degree 2 or 3 are irreducible iff they have no root.
     \[ x^2 + x + 1, x^3 + x^2 + 1, x^3 + x + 1 \]
   - Degree 4: irreducible polynomials of degree 4 cannot have a root, so it needs to have the shape \( x^4 + ax^3 + bx^2 + cx + 1 \), where \( a + b + c = 1 \) (mod 2). \[ x^4 + x + 1 = (x^2 + x + 1)^2, \]
   so it is reducible. The reducible possibilities are then,
   \[ x^4 + x^3 + x^2 + x + 1, x^4 + x^3 + 1, x^4 + x + 1 \]
• Degree 5: Irreducible polynomials of degree 5 cannot have a root, so it needs to have the form \( x^5 + ax^4 + bx^3 + cx^2 + dx + 1 \), where \( a + b + c + d = 1 \) (mod 2). If a polynomial of degree 5 is reducible but doesn’t have a root, it should be the product of a irreducible polynomial of degree 2 and a irreducible polynomials of degree 3. The possibilities of irreducible polynomials of degree 5 are then:

\[
x^5 + x^4 + x^3 + x^2 + x + 1, x^5 + x^3 + x^2 + x + 1, x^5 + x^4 + x^2 + x + 1, x^5 + x^4 + x^3 + x^2 + 1, x^5 + x^4 + x^3 + x + 1
\]

2. By the Euclidean algorithm, \( h(x) = \gcd(x^6 + 2x^4 + 2x^3 + 2x + 1, x^5 + x^2 + 2x + 1) \) can be written as a linear combination of \( x^6 + 2x^4 + 2x^3 + 2x + 1 \) and \( x^5 + x^2 + 2x + 1 \), i.e., we can write \( h(x) = q_1(x) \cdot (x^6 + 2x^4 + 2x^3 + 2x + 1) + q_2(x) \cdot (x^5 + x^2 + 2x + 1) \). Thus \( h(x) \in \langle x^6 + 2x^4 + 2x^3 + 2x + 1, x^5 + x^2 + 2x + 1 \rangle \), and \( \langle h(x) \rangle \in \langle x^6 + 2x^4 + 2x^3 + 2x + 1, x^5 + x^2 + 2x + 1 \rangle \). On the other hand, since \( h(x) \) divides both \( x^6 + 2x^4 + 2x^3 + 2x + 1 \) and \( x^5 + x^2 + 2x + 1 \), \( \langle x^6 + 2x^4 + 2x^3 + 2x + 1, x^5 + x^2 + 2x + 1, x^5 + x^2 + 2x + 1 \rangle \) divides \( \langle h(x) \rangle \). Therefore,

\[
\langle x^6 + 2x^4 + 2x^3 + 2x + 1, x^5 + x^2 + 2x + 1 \rangle = \langle h(x) \rangle.
\]

Now we just need to find \( h(x) = \gcd(x^6 + 2x^4 + 2x^3 + 2x + 1, x^5 + x^2 + 2x + 1) \). Using the Euclidean algorithm:

\[
x^6 + 2x^4 + 2x^3 + 2x + 1 = (x^5 + x^2 + 2x + 1) x + 2x^4 + x^3 + x^2 + x + 1.
\]

\[
x^5 + x^2 + 2x + 1 = (x + 2)(2x^4 + x^3 + x^2 + x + 1) + 2x^3 + x + 2.
\]

\[
2x^4 + x^3 + x^2 + x + 1 = (x + 2)(2x^3 + x + 2) + 0.
\]

Thus,

\[
\langle x^6 + 2x^4 + 2x^3 + 2x + 1, x^5 + x^2 + 2x + 1 \rangle = \langle h(x) \rangle = \langle 2x^3 + x + 2 \rangle = \langle x^3 + 2x + 1 \rangle.
\]

**Problem 3. (Polynomial Factorization [AM206-A])** In this problem, you will see one of the main ideas that go into polynomial-time randomized algorithms for polynomial factorization. Let \( \mathbb{F} \) be a finite field of odd order \( q \), and let \( p(x) = p_1(x)p_2(x) \), where \( p_1(x), p_2(x) \in \mathbb{F}[x] \) are distinct irreducible polynomials of degree \( n \).

1. Show that \( \mathbb{F}[x]/\langle p(x) \rangle \) is isomorphic to \( \mathbb{F}[x]/\langle p_1(x) \rangle \times \mathbb{F}[x]/\langle p_2(x) \rangle \). What theorem about the integers is this analogous to?

2. Show that if we pick a random polynomial \( f(x) \in \mathbb{F}[x] \) of degree smaller than \( 2n \), then with probability at least 1/2, either \( \gcd(f(x), p(x)) \in \{p_1(x), p_2(x)\} \) or \( \gcd(f(x)(q^{n/2}-1)-p(x)) \in \{p_1(x), p_2(x)\} \). You may use the fact that the group of units in any finite field is cyclic. (Hint: think of \( f(x) \) as a random element of \( \mathbb{F}[x]/\langle p(x) \rangle \).) Thus we can factor \( p \) with high probability by choosing several random \( f \)'s and computing these \( \gcd \)'s.

**Solution:**
1. Define the mapping $\varphi : F[x]/\langle p(x) \rangle \to F[x]/\langle p_1(x) \rangle \times F[x]/\langle p_2(x) \rangle$ as

$$\varphi(q(x)) = (q(x) \mod p_1(x), q(x) \mod p_2(x)).$$

This mapping is well defined because $p_1(x)$ and $p_2(x)$ divide $p(x)$. It is an homomorphism because:

- $\varphi(q_1(x) + q_2(x)) = (q_1(x) + q_2(x) \mod p_1(x), q_1(x) + q_2(x) \mod p_2(x)) = \varphi(q_1(x)) + \varphi(q_2(x)).$
- $\varphi(q_1(x) \cdot q_2(x)) = (q_1(x) \cdot q_2(x) \mod p_1(x), q_1(x) \cdot q_2(x) \mod p_2(x)) = \varphi(q_1(x)) \cdot \varphi(q_2(x)).$

Note that both rings $F[x]/\langle p(x) \rangle$ and $F[x]/\langle p_1(x) \rangle \times F[x]/\langle p_2(x) \rangle$ are finite and of the same cardinality. To show that mapping $\varphi$ defines an isomorphism it is enough to show that it is injective, or equivalently that $\ker(\varphi) = \{0\}$. Indeed, if $q(x) \in \ker(\varphi)$, it means that $q(x) \mod p_1(x) = 0$ and $q(x) \mod p_2(x) = 0$, as $p_1$ and $p_2$ are both irreducible, by uniqueness of factorization $q(x) \mod p_1(x)p_2(x) = 0$.

2. Suppose that $\gcd(f(x), p(x)) \notin \{p_1(x), p_2(x)\}$. Since $p_1$ and $p_2$ are irreducible, $f(x)$ must be a unit in the fields $F[x]/\langle p_1(x) \rangle$ and $F[x]/\langle p_2(x) \rangle$. Each one of those fields have $q^n$ elements, being $q^n - 1$ units. As it was stated in the problem, group of units of finite fields are cyclic. So, let $g_1(x)$ be a generator for the group of units of $F[x]/\langle p_1(x) \rangle$ and $g_2(x)$ be a generator for the group of units of $F[x]/\langle p_2(x) \rangle$, then $g_1(x)^{q^n-1} = 1$ in $F[x]/\langle p_1(x) \rangle$ and $g_2(x)^{q^n-1} = 1$ in $F[x]/\langle p_2(x) \rangle$. Thus $g_1(x)^{(q^n-1)/2} = +1$ or $-1$ in $F[x]/\langle p_1(x) \rangle$ and $g_2(x)^{(q^n-1)/2} = +1$ or $-1$ in $F[x]/\langle p_2(x) \rangle$, but since $g_1(x)$ and $g_2(x)$ must have order $q^n - 1$, we need to have $g_1(x)^{(q^n-1)/2} = -1$ in $F[x]/\langle p_1(x) \rangle$ and $g_2(x)^{(q^n-1)/2} = -1$ in $F[x]/\langle p_2(x) \rangle$.

Now let $f(x) = g_1(x)^{m_1}$ in $F[x]/\langle p_1(x) \rangle$ and $f(x) = g_2(x)^{m_2}$ in $F[x]/\langle p_2(x) \rangle$. If $m_1$ is and even number $2k$, then $f(x)^{(q^n-1)/2} = g(x)^{2k(q^n-1)/2} = g(x)^k(q^n-1) = 1$ in $F[x]/\langle p_1(x) \rangle$. Analogously, if $m_2$ is even $f(x)^{(q^n-1)/2} = 1$ in $F[x]/\langle p_2(x) \rangle$. Thus we have the following possibilities:

1) $m_1$ and $m_2$ even: in that case $f(x)^{(q^n-1)/2} - 1$ is multiple of $p_1(x)$ and $p_2(x)$, then $f(x)^{(q^n-1)/2} - 1$ is a multiple of $p(x)$ and $\gcd(f(x)^{(q^n-1)/2} - 1, p(x)) = p(x)$.

2) $m_1$ even and $m_2$ odd: in that case $f(x)^{(q^n-1)/2} - 1$ is multiple of $p_1(x)$ but is not multiple of $p_2(x)$. Thus $\gcd(f(x)^{(q^n-1)/2} - 1, p(x)) = p_1(x)$.

3) $m_1$ odd and $m_2$ even: in that case $f(x)^{(q^n-1)/2} - 1$ is multiple of $p_2(x)$ but is not multiple of $p_1(x)$. Thus $\gcd(f(x)^{(q^n-1)/2} - 1, p(x)) = p_2(x)$.

4) $m_1$ odd and $m_2$ odd: in that case $f(x)^{(q^n-1)/2} - 1$ is not multiple of $p_1(x)$ neither multiple of $p_2(x)$. Thus $\gcd(f(x)^{(q^n-1)/2} - 1, p(x))$ is neither $p_1(x)$ nor $p_2(x)$.

By the case analysis above, we can see that in at least half of the cases (items 2) and 3) $\gcd(f(x)^{(q^n-1)/2} - 1, p(x)) \in \{p_1(x), p_2(x)\}$. We assumed in the begining that $\gcd(f(x), p(x)) \notin \{p_1(x), p_2(x)\}$. So another case would be $\gcd(f(x), p(x)) \notin \{p_1(x), p_2(x)\}$.

So, with probability of either $\gcd(f(x), p(x)) \in \{p_1(x), p_2(x)\}$ or $\gcd(f(x)^{(q^n-1)/2} - 1, p(x)) \in \{p_1(x), p_2(x)\}$ is at least 1/2.
Problem 4. (Multivariate polynomials) Let $R$ be a commutative ring with unity. The ring $R[x_1, \ldots, x_n]$ of polynomials over $R$ in indeterminates $x_1, \ldots, x_n$ consists of all expressions of the form $p(x_1, \ldots, x_n) = \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n}$, where $a_{i_1, \ldots, i_n} \in R$, only finitely many of the $a_{i_1, \ldots, i_n}$ are nonzero, and addition and multiplication are defined as usual. The degree of such a polynomial $p$ is the maximum of $i_1 + \cdots + i_n$ over all nonzero coefficients $a_{i_1, \ldots, i_n}$.

1. Exhibit a nonzero degree 2 polynomial $p(x_1, x_2) \in \mathbb{Z}[x_1, x_2]$ that has infinitely many zeroes.

2. Despite the above, it can be shown that a low-degree polynomial cannot have too many roots in any finite “cube”. Specifically, show that if $R$ is an integral domain, $S \subseteq R$ is finite, and $p(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ is a nonzero polynomial of degree $d$, then the fraction of points $\alpha = (\alpha_1, \ldots, \alpha_n) \in S^n$ on which $p(\alpha) = 0$ is at most $d/|S|$. (Hint: group terms as $p(x_1, \ldots, x_n) = \sum_i q_i(x_1, \ldots, x_{n-1}) x_n^i$, and use induction on $n$.) Thus we can test whether a low-degree multivariate polynomial is zero by evaluating it on random points from $S^n$.

3. Find an ideal in $\mathbb{Q}[x_1, x_2]$ that is not principal.

Solution:

1. Consider $p(x_1, x_2) = x_1 \cdot x_2$, all elements of the form $(a, 0)$ of $(0, b)$ are roots of $p(x_1, x_2)$.

2. Consider random variables $X_1, \ldots, X_n$ independent, and each distributed uniformly over $S$. We wish to prove that $\mathbb{P}(p(X_1, \ldots, X_n) = 0) \leq \frac{d}{|S|}$. We will proceed by induction on the number of variables.

For $n = 1$, any nonzero univariate polynomial of degree $d$ over an integral domain has at most $d$ roots, so $\mathbb{P}(p(X_1) = 0) \leq \frac{d}{|S|}$. Consider $n > 1$, we can group monomial of $p$ according to degree of $x_n$ in each monomial. Let $\tilde{d}$ be the largest degree of $x_n$ in any monomial of $p$. We have

$$p(x_1, \ldots, x_n) = \sum_{k=0}^{\tilde{d}} q_k(x_1, \ldots, x_{n-1}) x_n^k$$

where $q_\tilde{d}(x_1, \ldots, x_{n-1})$ is a nonzero polynomial of degree at most $d - \tilde{d}$. Note that, by induction hypothesis, if we choose $x_1, \ldots, x_{n-1}$ uniformly at random from $S^{n-1}$, we have $\mathbb{P}(q_\tilde{d}(X_1, \ldots, X_{n-1}) = 0) \leq \frac{d-\tilde{d}}{|S|}$. Moreover, for any fixed sequence $\alpha_1, \ldots, \alpha_{n-1} \in R$ such that $q_\tilde{d}(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$, we know that

$$p(\alpha_1, \ldots, \alpha_{n-1}, x) = \sum_{k=0}^{\tilde{d}} q_k(\alpha_1, \ldots, \alpha_{n-1}) x^k$$

is a univariate, nonzero polynomial of degree $\tilde{d}$ — hence $\mathbb{P}(p(\alpha_1, \ldots, \alpha_{n-1}, X) = 0) \leq \frac{\tilde{d}}{|S|}$.

Finally

$$\mathbb{P}(p(X_1, \ldots, X_n) = 0) \leq \mathbb{P}(q_\tilde{d}(X_1, \ldots, X_{n-1}) = 0) + \mathbb{P}(p(X_1, \ldots, X_n) = 0 | q_\tilde{d}(X_1, \ldots, X_{n-1}) \neq 0)$$

$$\leq \frac{d-\tilde{d}}{|S|} + \frac{\tilde{d}}{|S|}$$
3. The ideal \( I = \langle x_1, x_2 \rangle \) is not principal. To prove this, let’s suppose it is principal and generated by some polynomial \( p(x_1, x_2) \). Since \( x_1 \in I \), there must be a \( q(x_1, x_2) \in \mathbb{Q}[x_1, x_2] \) such that \( x_1 = p(x_1, x_2) \cdot q(x_1, x_2) \). Thus \( x_2 \) cannot appear in any monomial of \( p(x_1, x_2) \) or \( q(x_1, x_2) \). Analogously, since \( x_2 \in I \), \( x_1 \) cannot appear in any monomial of \( p(x_1, x_2) \). Thus \( p \) is a constant polynomial. This is absurd, because otherwise we would have \( I = \langle p(x_1, x_2) \rangle = \mathbb{Q}[x_1, x_2] \).