1. For each of the following rings determine if the ring is an integral domain and if the ring is a field. If not an integral domain identify one zero divisor and if not a field identify one non-unit. [10 pts]

(a) \( \mathbb{Z}_5[x]/\langle x^2 + x + 1 \rangle \)
   **Solution:** Field.

(b) \( \mathbb{Z}_{43}[x] \)
   **Solution:** Integral domain but not a field.
   \( p(x) = x \) is not a unit.

(c) \( \mathbb{Z}_5[x]/\langle x^2 + 3x + 1 \rangle \)
   **Solution:** Not an integral domain and not a field.
   \( x + 4 + \langle x^2 + 3x + 1 \rangle \) is a zero-divisor and is not a unit.

(d) \( \mathbb{Z} \)
   **Solution:** Integral domain but not a field.
   2 is not a unit.

(e) \( \mathbb{Z}_{31} \)
   **Solution:** Field.

(f) \( \mathbb{Z}_{143} \)
   **Solution:** Not an integral domain and not a field.
   11 is a zero-divisor and is not a unit.
2. Consider the polynomial \( p(x) = x^3 + 2x + 6 \in \mathbb{Z}_7[x] \). [10 pts]

(a) Show that \( p(x) \) is irreducible over \( \mathbb{Z}_7[x] \).

**Solution:** We can test all of \( x = 0, \ldots, 6 \) and we see there are no roots:
\[
\begin{align*}
p(0) &\equiv 6 \mod 7 \\
p(1) &\equiv 2 \mod 7 \\
p(2) &\equiv 4 \mod 7 \\
p(3) &\equiv 4 \mod 7 \\
p(4) &\equiv 1 \mod 7 \\
p(5) &\equiv 1 \mod 7 \\
p(6) &\equiv 3 \mod 7
\end{align*}
\]
Hence the polynomial is irreducible by the degree 2/3 test.

(b) Describe an element in \( \mathbb{Z}_7[x]/\langle x^3 + 2x + 6 \rangle \) as succinctly as possible. How many such elements are there?

**Solution:** An element will have the form \( c_2x^2 + c_1x + c_0 + \langle x^3 + 2x + 6 \rangle \) where \( c_0, c_1, c_2 \in \mathbb{Z}_7 \). There are 343 such elements.

(c) Calculate the simplest form of the product:
\[
(x^2 + 6x + 5 + \langle x^3 + 2x + 6 \rangle)(x^2 + 6x + 3 + \langle x^3 + 2x + 6 \rangle)
\]

**Solution:** We have
\[
(x^2 + 6x + 5 + \langle x^3 + 2x + 6 \rangle)(x^2 + 6x + 3 + \langle x^3 + 2x + 6 \rangle)
\]
\[
= x^4 + 5x^3 + 2x^2 + 6x + 1 + \langle x^3 + 2x + 6 \rangle
\]
\[
= \ldots
\]
\[
= 4x + 6 + \langle x^3 + 2x + 6 \rangle
\]
3. Prove that the ideal $I = \langle x^2 + 2x + 1 \rangle$ is not prime in $\mathbb{Z}_7[x]$. Provide evidence for any [10 pts] assertions you make relative to the definition of a prime ideal.

**Solution:** We have $x^2 + 2x + 1 = (x + 1)(x + 1)$ so that $x^2 + 2x + 1 \in I$ but $x + 1, x + 1 \not\in I$.

WLOG we know that $x + 1 \not\in I$ because if $x + 1 \in I$ then $\exists p(x) \in \mathbb{Z}_7[x]$ such that

$$x + 1 = p(x)(x^2 + 2x + 1)$$

which is impossible since $\mathbb{Z}_7[x]$ is an integral domain and degrees add.
4. Prove that the polynomial \( p(x) = 8x^3 + 15x^2 + 14x + 29 \) is irreducible over \( \mathbb{Q} \). [10 pts]

**Solution:** We use the mod-\( p \) test with \( p = 7 \) to reduce to \( \bar{p}(x) = x^3 + x^2 + 1 \). At this point we use the degree 2/3 test by checking all of 0, ..., 6:

\[
\begin{align*}
\bar{p}(0) &\equiv 1 \mod 7 \\
\bar{p}(1) &\equiv 3 \mod 7 \\
\bar{p}(2) &\equiv 6 \mod 7 \\
\bar{p}(3) &\equiv 2 \mod 7 \\
\bar{p}(4) &\equiv 4 \mod 7 \\
\bar{p}(5) &\equiv 4 \mod 7 \\
\bar{p}(6) &\equiv 1 \mod 7 \\
\end{align*}
\]

None of these yield a root and so \( \bar{p}(x) \) is irreducible over \( \mathbb{Z}_7 \) and so \( p(x) \) is irreducible over \( \mathbb{Q} \).

Note 1: This might work for smaller \( p \). The algorithm which created the problem just made sure that some reasonable low \( p \) worked, not that it was the lowest that worked!

Note 2: Eisenstein may work on some people’s problems by pure chance.
5. Find an extension field of $\mathbb{Z}_3$ over which $x^3 + 2x + 1$ factors and factor it. [10 pts]

**Solution:** We see that $x^3 + 2x + 1$ is irreducible over $\mathbb{Z}_3$ by the 2/3-test:

\[
\bar{p}(0) \equiv 1 \mod 3 \\
\bar{p}(1) \equiv 1 \mod 3 \\
\bar{p}(2) \equiv 1 \mod 3
\]

It therefore has the root $x + \langle x^3 + 2x + 1 \rangle$ in the extension field $\mathbb{Z}_3[x]/(x^3 + 2x + 1)$. In order to not confuse the variables we’ll write the polynomial as:

\[
z^3 + (2 + \langle x^3 + 2x + 1 \rangle)z + (1 + \langle x^3 + 2x + 1 \rangle)
\]

By long division (work omitted) it factors as:

\[
[z - (x + \langle >)] \cdot [z^2 + (x + \langle >)z + (x^2 + 2 + \langle >)]
\]
6. Prove that the ideal \( \langle x^2 + 2 \rangle \) is maximal in \( \mathbb{R}[x] \) using the definition of a maximal ideal. \([10 \text{ pts}]\)

**Solution:** Suppose not, then there is some ideal \( B \) with:

\[
\langle x^2 + 2 \rangle \subsetneq B \subseteq \mathbb{R}[x]
\]

We claim \( B = \mathbb{R}[x] \). Since \( \langle x^2 + 2 \rangle \subsetneq B \) there is some \( p(x) \in B \) with \( p(x) \notin \langle x^2 + 2 \rangle \) and so \( p(x) \) is not a multiple of \( x^2 + 2 \).

We claim that \( B \) contains a nonzero constant because it then contains all of \( \mathbb{R}[x] \).

Applying the division algorithm then yields:

\[
p(x) = q(x)(x^2 + 2) + r(x)
\]

with \( r(x) \neq 0 \) and \( \deg(r(x)) < \deg(x^2 + 2) = 2 \).

It follows that the degree of \( r(x) \) is zero or one and that also we have:

\[
r(x) = p(x) - q(x)(x^2 + 2)
\]

and since \( p(x) \in B \) and \( x^2 + 2 \in B \) we also have \( r(x) \in B \).

If the degree of \( r(x) \) is zero then \( r(x) = b \) and then \( B \) contains a nonzero constant and we are done.

If the degree of \( r(x) \) is one then \( r(x) = ax + b \) and then observe that:

\[
\underbrace{x^2 + 2}_{\in B} - \underbrace{\frac{x}{a} (ax + b)}_{\in B} - \underbrace{\frac{b}{a^2} (ax + b)}_{\in B} = 2 + \frac{b^2}{a^2} \in B
\]

and then \( B \) contains a nonzero constant and we are done.

Note: This can be more succinctly by appealing to the irreducibility of the polynomial. As long as you used the definition of maximality in the proof then doing that was fine. However you had to do something significant with the definition of maximal.
7. Prove that $\mathbb{Z}_2$ is isomorphic to a subring of $\mathbb{Z}_{30}$.

**Solution:** Define $\phi : \mathbb{Z}_2 \to \mathbb{Z}_{30}$ by $\phi(x) = 15x$. We claim that $\phi$ is a ring homomorphism and then the result follows.

First we claim that $\phi(x + y) = \phi(x) + \phi(y)$ for $x, y \in \mathbb{Z}_2$. We write $x + y = 2q + r$ where $0 \leq r < 2$ so that:

$$
\begin{align*}
\phi(x + y) &= \phi(2q + r) \\
&= \phi(r) \\
&= 15r \\
&= 15(x + y - 2q) \\
&= 15x + 15y - 30q \\
&= 15x + 15y \\
&= \phi(x) + \phi(y)
\end{align*}
$$

Next we claim that $\phi(xy) = \phi(x)\phi(y)$ for $x, y \in \mathbb{Z}_2$. We write $xy = 2q + r$ where $0 \leq r < 2$ so that:

$$
\begin{align*}
\phi(xy) &= \phi(2q + r) \\
&= \phi(r) \\
&= 15r \\
&= 15(xy - 2q) \\
&= 15xy - 30q \\
&= 15xy \\
&= 15^2xy \\
&= (15x)(15y) \\
&= \phi(x)\phi(y)
\end{align*}
$$

The reason that $15 = 15^2$ is that $2 \mid 15^2 - 15$ and $15 \mid 15^2 - 15$ and $\gcd(2, 15) = 1$.

Note: This can also be done by checking the mapping at all pairs of elements.
8. Suppose $R$ is a ring in which $a^2 = a$ for all $a \in R$. [10 pts]

(a) Show that $a + a = 0$ for all $a \in R$.

Solution: We have $-a = (-a)^2 = a^2 = a$ so $a + a = 0$.

(b) Show that $R$ is commutative.

Solution: We have

\[
\begin{align*}
  a + b &= (a + b)^2 \\
  a + b &= a^2 + ab + ba + b^2 \\
  a + b &= a + ab + ba + b \\
  0 &= ab + ba \\
  ab &= ab + ab + ba \\
  ab &= ba
\end{align*}
\]
9. Suppose $R$ and $S$ are commutative rings where $S \neq \{0\}$ and $R$ has unity $1$. Suppose $\phi : R \to S$ is a ring homomorphism. 

(a) Prove that if $\phi$ is onto then $\phi(1)$ is the unity in $S$.

Solution: Given $y \in S$ we claim that $\phi(1)y = y$. Since $y \in S$ and $\phi$ is onto we have some $x \in R$ with $\phi(x) = y$. Then $\phi(1)y = \phi(1)\phi(x) = \phi(1x) = \phi(x) = y$ as desired.

(b) Give a counterexample when $\phi$ is not onto.

Solution: Consider $\phi : \mathbb{Z} \to \mathbb{Z}$ given by $\phi(x) = 0$. 
10. If \( ab \) is algebraic over \( F \) and \( b \neq 0 \), prove that \( a \) is algebraic over \( F(b) \). [5 pts]

**Solution:** If \( ab \) is algebraic over \( F \) then there are constants \( c_i \in F \) with:

\[
c_0 + c_1(ab) + c_2(ab)^2 + ... + c_n(ab)^n = 0
\]

This may be rewritten:

\[
c_0 + (c_1b)a + (c_2b^2)a^2 + ... + (c_nb^n)a^n = 0
\]

Since \( c_0, c_1b, c_2b^2, ..., c_nb^n \in F(b) \) we have \( a \) algebraic over \( F(b) \).
11. Suppose that a field extension \( E \subseteq \mathbb{C} \) satisfies \([E : \mathbb{Q}] = 2\). Show that there is a square-free \( d \) such that \( E = \mathbb{Q}(\sqrt{d}) \).

**Solution:** Pick \( x_0 \in E - \mathbb{Q} \) and consider the set \( \{1, x_0\} \). We claim this forms a basis for \( E \) over \( \mathbb{Q} \). Since \([E : \mathbb{Q}] = 2\) it suffices to show that the set is linearly independent.

Suppose \( \alpha(1) + \beta(x_0) = 0 \) for some \( \alpha, \beta \in \mathbb{Q} \). If \( \beta \neq 0 \) then \( x_0 = -\alpha/\beta \in \mathbb{Q} \), a contradiction, and so \( \beta = 0 \) and then we must have \( \alpha = 0 \).

Now then since the extension has degree 2 we know the set \( \{1, x_0, x_0^2\} \) is linearly dependent and so there are nonzero constants \( a, b, c \in \mathbb{Q} \) with \( ax_0^2 + bx_0 + c = 0 \). We know \( a \neq 0 \) since otherwise we would have \( b = c = 0 \) as above, and so WLOG we can divide by \( a \) and relabel to get \( x_0^2 + bx_0 + c = 0 \).

Consider then that \( \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{b^2 - 4c}) \subseteq E \) and since \([E : \mathbb{Q}] = 2\) we must have \( \mathbb{Q}(\sqrt{b^2 - 4c}) = E \).

Thus let \( d = b^2 - 4c \). If \( d \) is not square-free we may simply divide it out.

Note: It’s tempting to state that \( \mathbb{Q}(x_0) = E \) without justification but it’s not necessarily the case in general, it’s the \([E : \mathbb{Q}] = 2\) which guarantees it.