1. **(20 points)** *Fill in the following table. You need not justify your results. In each cell, place either an X or a checkmark (✓). Place an X if the ring named in the column is not an algebra of the type named in the row, and a checkmark if the ring named in the column is an algebra of the type named in the row. Place one of these two marks in* every *cell of the table; empty cells will be automatically incorrect.*

	$\mathbb{R}$	$\mathbb{Z}[x]$	$\mathbb{Z}[\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \ldots]$	$\mathbb{Z}_7[x]$	$\mathbb{Q}[x]/\langle x^2 \rangle$
Principal ideal domain (PID)	✓	X	X	✓	X
Euclidean domain	✓	X	X	✓	X
Field	✓	X	X	X	X
Unique factorization domain (UFD)	✓	✓	X	✓	X

This justification is not necessary when doing the exam, but is included here for your study purposes.

$\mathbb{R}$ is a field. Because it is a field, it is vacuously a principal ideal domain (possessing only two ideals, the zero ideal and the whole field, both of which are in fact generated by a single element each), and is also vacuously a unique factorization domain (since it contains no nonunit elements, reducible or irreducible). In addition, the trivial constant measure assigning measure 0 to every element makes it a Euclidean domain, as any division in a field leaves zero remainder.

$\mathbb{Z}[x]$ is clearly not a field, since 2 has no inverse. It is also not a principal ideal domain, since the ideal of polynomials with even constant term, while it is finitely generated as $\langle x, 2 \rangle$, is not generated by a single element of $\mathbb{Z}[x]$. Since it is not a principal ideal domain, it cannot be a Euclidean domain. It is, however, a unique factorization domain, as has been seen in class (it inherits most of the factorization characteristics from $\mathbb{Q}[x]$), with the "primitivity" dodge to deal with constant multipliers.

$\mathbb{Z}[\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \sqrt[16]{2}, \ldots]$ is not a unique factorization domain, since 2 cannot be factored into irreducibles: $2 = \sqrt{2} \cdot \sqrt{2}$, $\sqrt{2} = \sqrt[4]{2}\sqrt[4]{2}$, etc. Since it is not a unique factorization domain, it is not a principal ideal domain, Euclidean domain, or field either.

$\mathbb{Z}_7[x]$ is clearly not a field, since x has no inverse. It is, however, a Euclidean domain, sionce there is a division algorithm using the degree of a polynomial as its measure. Because it is a Euclidean domain, it follows that it is also a principal ideal domain, and because it is a principal ideal domain, it is also a unique factorization domain.

$\mathbb{Q}[x]/\langle x^2 \rangle$ is not even an integral domain, since $x \cdot x = 0$, and thus it is not any of these specific types of integral domain either.

2. **(20 points)** *If R is a principal ideal domain, and I is a proper ideal of R (that is, an ideal smaller than the entirety of R), prove that I is contained (possibly nonstrictly) in a maximal ideal of R.*

There are several proofs of this fact, using different knowledge.

Proof. Since R is a principal ideal domain, it is Noetherian. Thus every ascending chain $I = I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ is finite, and so there is a finite chain which cannot be further extended (since arbitrary extendability would yield an infinite chain), and the second-to-last ideal in such a chain will be a proper subset of R which admits of no ideal insertable between it and R, i.e. a maximal ideal. □

Alternative proof. Since R is a principal ideal domain, $I = \langle a \rangle$ for some $a \in R$; since $I \neq R$, a is not a unit. Every principal ideal domain is also a unique factorization domain, and thus the nonunit a has an irreducible factor p. Since $p \mid a$, $a \in \langle p \rangle$, so that $\langle a \rangle \subseteq \langle p \rangle$, and, since p is irreducible, $\langle p \rangle$ is maximal. □

3. **(20 points)** *Let $f(x) \in \mathbb{Z}[x]$ be given by the formula $a_n x^n + \cdots + a_1 x + a_0$. Prove that if $\frac{p}{q} \in \mathbb{Q}$ is a fraction in lowest terms such that $f(\frac{p}{q}) = 0$, then $p \mid a_0$ and $q \mid a_n$. (This result is known as the* Rational Root Theorem*.)*

   Proof. The equality $f(\frac{p}{q}) = 0$ can be expanded into the rational equation

   $$a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0 = 0$$

   which can be converted into an equation in integers by multiplying both sides by q^n:

   $$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$$

   and so noting that every term except the first has a conspicuous factor of q, it must be the case that the first term is divisible by q as well, so that $q \mid a_n p^n$; likewise, every term except the last term on the left has a factor of p, so the last term must be divisible by p and so $p \mid a_0 q^n$. However, because the fraction $\frac{p}{q}$ is in lowest terms, p and q have no factors in common, so $q \mid a_n p^n$ implies that $q \mid a_n$, and $p \mid a_0 q^n$ implies that $p \mid a_0$. □

4. (a) **(10 points)** *Prove that $\mathbb{Z}_2[x]/\langle x^3 + x^2 + 1\rangle$ is a field. What is its order?*
   Since $\mathbb{Z}_2$ is a field, this assertion is equivalent to the claim that $x^3 + x^2 + 1$ is irrecudible in $\mathbb{Z}_2$. Since this polynomial is a cubic, it is reducible iff it has a root, and we may easily verify that it does not: $1^3 + 1^2 + 1 = 1$ and $0^3 + 0^2 + 1 = 1$. This quotient ring's elements are represented (via the division algorithm) by residues which are polynomials of degree 2 or less in $\mathbb{Z}_2$, or in other words, expressions of the form $ax^2 + bx + c$ where $a, b, c \in \mathbb{Z}_2$; there are $2^3 = 8$ such polynomials so this field has order 8.

   (b) **(10 points)** *Prove that $\mathbb{Z}_7[x]/\langle 3x^2 + x + 4\rangle$ is* not *a field. Is it an integral domain?*
   Note that $3 \cdot 4^2 + 4 + 4 = 0$ in $\mathbb{Z}_7$, so this polynomial has a zero and is thus reducible—in fact, we know that it has a factor of $(x - 4)$. Long division (or any other factorization technique) will show that $3x^2 + x + 4 = (x - 4)(3x - 1)$. This also serves to show it is not an integral domain, since in $\mathbb{Z}_7[x]/\langle 3x^2 + x + 4\rangle$ it is the case that $(x - 4)(3x - 1) = 0$.

5. **(20 points)** *Prove that every prime element of an integral domain is irreducible.*

   Let p be a prime element of integral domain D, and then let $p = ab$. We wish to show that either a or b must be a unit. Note that since $p \mid p$, $p \mid ab$, so since p is prime, either $p \mid a$ or $p \mid b$. WLOG assume $p \mid a$. Then, $a = pk$ for some $k \in D$, and $p = ab$, so $p = (pk)b = p(kb)$, so $kb = 1$ and b is thus a unit.

6. **(Bonus question, 10 extra points)** *Prove that every irreducible element of a principal ideal domain is prime.*

   Let p be an irreducible element of principal ideal domain D, and let $p \mid ab$ for some $a, b \in D$. We wish to show that either $p \mid a$ or $p \mid b$. Let us consider the set $I = \{px + ay : x, y \in D\}$; this set is obviously an ideal in D, and contains both p and a. Since D is a principal ideal domain, $I = \langle d\rangle$ for some d, and since $p \in I$, $p = dq$ for some $q \in D$. But, since r is irreducible, one of these two factors must be a unit, which leads to two cases:

   Case I: d is a unit. Then $I = \langle 1\rangle = D$, so $b \in I$, and thus there are x and y such that $px + ay = 1$, and then multiplying both sides by b, $pbx + aby = b$. However, since $p \mid p$ and $p \mid ab$, $p \mid (pbx + aby)$ and so $p \mid b$.

   Case II: q is a unit. Then since $p = dq$ and $d = pq^{-1}$, it is the case that both $p \mid d$ and $d \mid p$, so $I = \langle p\rangle$. Since $a \in I$, $p \mid a$.