1. **(40 points)** *Fill in the following table. You need not justify your results. In each cell, place either an X or a checkmark. Place a checkmark if a structure of the type named in the row* is always *a structure of the type named in the column, and an X if not. Fill in every cell. The tautological cells are pre-filled. To round off the values, you get 2 points just for being you.*

	is always…					
	a commutative ring	an integral domain	a PID	a UFD	a Noetherian domain	a field
An integral domain	✓	✓	X	X	X	X
A principal ideal domain	✓	✓	✓	✓	✓	X
A unique factorization domain	✓	✓	X	✓	X	X
A Euclidean domain	✓	✓	✓	✓	✓	X
A field	✓	✓	✓	✓	✓	✓
$F[x]$, where F is a field	✓	✓	✓	✓	✓	X
$D[x]$, where D is a PID	✓	✓	X	✓	✓	X

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

An integral domain must be commutative, but it need not have any of the other properties. $\mathbb{Z}[\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \ldots]$ is a good example of an integral domain which has none of the other listed properties.

A principal ideal domain is definitionally required to be an integral domain (and thus commutative), and every principal ideal domain has been proven to have unique factorization and the ascending chain condition. However, many principal ideal domains, like $\mathbb{Z}$ or $\mathbb{Q}[x]$, are not fields.

A unique factorization domain is definitionally required to be an integral domain (and thus commutative), but need not be a principal ideal domain: $\mathbb{Z}[x]$ is a good counterexample. Intriguingly, a unique factorization domain need not be Noetherian domain, although this is far from obvious: every element of $\mathbb{Q}[x_1, x_2, x_3, \ldots]$ has unique factorization, but there is an infinite ascending chain of ideals. It of course need not be a field either.

Euclidean domains have been shown to always be principal ideal domains, and thus must also be every structure that a principal ideal domain is known to be. They need not be fields, and $\mathbb{Z}$ is a simple counterexample.

Fields are vacuously principal ideal domains, since they possess only two ideals, both of which are generated by a single element. They thus are the same set of structures which a principal ideal must be.

It is known that the polynomial ring over a field is a Euclidean domain (using the division algorithm), and so it is all of the things a Euclidean domain is as well, but it will not be a field, since x is not a unit.

It is easy to see that $\mathbb{Z}[x]$ is neither a principal ideal domain nor a field, but that $D[x]$ will always be an integral domain. A somewhat more obscure result (Theorem 18.5 in the text) is that $D[x]$ must be a unique factorization domain. In addition, $D[x]$ must be Noetherian, since any ascending chain in $D[x]$ will necessaarily have a subchain in D and, if it contains any polynomial of degree n, can have at most n additional chain elements beyond the subchain in D.

2. **(20 points)** *Prove the following statements about rings:*

   (a) **(10 points)** *In a ring R (which may not be commutative or possess a unity) prove that for any $a \in R$, $a \cdot 0 = 0$.*

   Proof. We know that $0 + 0 = 0$, and by the distributive law, $a0 + a0 = a(0 + 0) = a0$. Adding $-(a0)$ to both sides, we find that $a0 = 0$. □

   (b) **(10 points)** *In a ring R with unity, prove that for any $a \in R$, $-a = -1 \cdot a$.*

   Proof. From the above (or a parallel result with order reversed) we know $0a = 0$. We also know that $1 + (-1) = 0$, so $0 = 0a = (1 + (-1))a = 1a + (-1)a = a + (-1)a$. Since $a + (-1)a$ is zero, $(-1)a$ is the additive inverse of a. □

3. **(20 points+10 bonus)** *Let D be an integral domain, and let $a, b \in D$.*

   (a) **(20 points)** *Prove that if $a^5 = b^5$ and $a^3 = b^3$, then $a = b$.*

   Proof. Note that if $a = 0$ then $b^5 = 0$ which will imply in an integral domain that $b = 0$, proving the result easily in this case. We may therefore henceforth assume a and b are nonzero. We rewrite b^5 as b^2b^3, so that $a^5 = b^2b^3 = b^2a^3$. Using the cancellation property of integral domains, we may cancel the nonzero term a^3 from both sides to get $a^2 = b^2$. Then, rewriting b^3 as bb^2, we may note that $a^3 = bb^2 = ba^2$, and again cancelling a^2 from both sides, we get $a = b$. □

   (b) **(10 points)** *Find (with proof) the best possible conditions on positive m and n such that if $a^m = b^m$ and $a^n = b^n$, then $a = b$.*

   The condition that m and n are relatively prime will suffice, and it is the best such condition possible, since, for instance,if m and n were both even, $a = -b$ would meet these conditions (likewise, if m and n had some factor k in common, a and b differing by a factor of a kth root of unity would meet these conditions).

   Proof. Given that m and n are relatively prime, let $mk - n\ell = 1$ for positive integers k and ℓ. Now $a^{mk} = b^{mk}$ and $a^{n\ell} = b^{n\ell}$, simply by multiplying the two known equations by themselves several times. Since $mk = 1 + n\ell$, we may rewrite a^{mk} as $aa^{n\ell}$, and so $bb^{n\ell} = b^{mk} = a^{mk} = aa^{n\ell} = ab^{n\ell}$, and canceling the $b^{n\ell}$ term on both sides yields $b = a$. □

4. **(20 points)** *Let R be the ring of all functions from $\mathbb{Q}$ to $\mathbb{Q}$, with the operations of multipliction and addition being $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x) \cdot g(x)$, and let $I = \{f(x) : f(0) = 0\}$.*

   (a) *Prove that I is an ideal.*

   Proof. We may note that I is closed under subtraction and multiplication, since if $f(0) = 0$ and $g(0) = 0$, then $(f - g)(0) = 0 + 0 = 0$; likewise $(fg)(0) = 0 \cdot 0 = 0$. In addition, I will be absorbing, since if $f \in I$ and $g \in R$, then $(fg)(0) = f(0)g(0) = 0 \cdot g(0) = 0$, so $fg \in I$. □

   (b) *Prove that I is a maximal ideal.*

   Proof. I is clearly a proper ideal of R, since there are functions (e.g. the constant function $f(x) = 1$) which are not in I. Now, suppose $I \subsetneq J$ for some ideal J. There is some $g(x) \in J - I$, and since $g(x) \notin I$, we know $g(0) \neq 0$. Let us consider an arbitrary function $f \in R$, and note the function $h(x) = f(x) - \frac{f(0)}{g(0)}g(x)$. $h(0) = 0$, so $h \in I$, but then since $f(x) = h(x) + \frac{f(0)}{g(0)}g(x)$, since we have written f as a sum of elements of J, $f \in J$, and since f was arbitrary, $J = R$. □

In the original version of this problem (with $\mathbb{Q}$ replaced by $\mathbb{Z}$), the above proof, which uses division by elements of the underlying ring, clearly doesn't work, and in fact, the statement is false! An example of a proper ideal which would strictly contain I would be $J = \{f(x) : f(0) \text{ is even}\}$.

5. (a) **(10 points)** *Determine whether $\mathbb{Q}[x]/\langle x^4 + 3x^2 + 3\rangle$ is a field.*
Using Eisenstein's criterion, since 3 divides the noninitial terms of $x^4 + 3x^2 + 3$ but 9 does not divide the constant term, this polynomial is irreducible, so the quotient ring in question will be a field.

   (b) **(10 points)** *Find the order of the ring $\mathbb{Z}_3[x]/\langle x^3 + 2x^2 + 1\rangle$, and determine whether it is a field.*
The ring's elements are each represented by a residue $ax^2 + bx + c$ for $a, b, c \in \mathbb{Z}_3$, admitting 27 distinct residues, so the ring has 27 elements. To determine if it is a field, we must check if $x^3 + 2x^2 + 1$ is irreducible. Since a cubic is reducible iff it has a zero, we check to see if this expression is zero at any value of $x \in \mathbb{Z}_3$: $0^3 + 2 \cdot 0^2 + 1 = 1$, $1^3 + 2 \cdot 1^2 + 1 = 1$, and $2^3 + 2 \cdot 2^2 + 1 = 2$, so since it is never zero, this is irreducible and is indeed a field.

6. **(20 points)** *Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree n, and let E be the splitting field of $f(x)$ over $\mathbb{Q}$.*

   (a) **(10 points)** *Prove that $[E : \mathbb{Q}]$ can be written as a product $k_1k_2k_3 \cdots k_n$, where each k_i is a positive integer less than or equal to i (hint: use induction on n).*

   Proof. We perform induction on n, andgeneralize to an arbitrary field F. If $n = 1$, then $f(x)$ is linear in F, so it is already "split" and $E = \mathbb{Q}$, making $[E : F]$ equal to 1.
   Let us now consider an arbitrary $n > 1$. Let α be a zero of $f(x)$. Then the minimal polynomial of α in F divides $f(x)$, and the minimal polynomial of α in F is an irreducible polynomial of degree less than or equal to n. Thus, $[F(\alpha) : F] \leq n$, and given that $f(x) = (x - \alpha)g(x)$ for some $g(x) \in F(\alpha)[x]$, we know that E is the splitting field of $g(x)$ over $F(\alpha)$. Invoking induction, we know that $[E : F(\alpha)] = k_1k_2 \cdots k_{n-1}$ for some values of $k_i \leq i$, and so $[E : F] = [E : F(\alpha)][F(\alpha) : F] = k_1k_2 \cdots k_{n-1}k_n$, where $k_n = [F(\alpha) : F]$, which, as noted above, is less than of equal to n. □

   (b) **(10 points)** *Prove that if $f(x)$ is irreducible, then $[E : \mathbb{Q}]$ is divisible by n.*

   Proof. We proceed as above, but note that, since $f(x)$ is irreducible in $\mathbb{Q}$, it is the minimal polynomial for α, so $[F(\alpha) : F] = n$. Then $[E : F] = (k_1k_2 \cdots k_{n-1})n$, which is clearly divisible by n. □

   (c) **(10 point bonus)** *The results above indicate that if $f(x)$ is an irreducible cubic, $[E : \mathbb{Q}]$ is 3 or 6. Are both possible? Prove or give examples.*
   It is very easy to find irreducible cubics whose splitting field has degree 6. The splitting field for $x^3 - 2$, for instance, is $\mathbb{Q}[\sqrt[3]{2}, \sqrt{3}i]$.
   Investigating the possibilities for an irreducible cubic to have a splitting field of degree 3 is much harder: in order for $[E : \mathbb{Q}]$ to equal 3, then it must be the case that for any zero α of $f(x)$, $E = \mathbb{Q}(\alpha)$, which is to say that the other two roots of $f(x)$ can be written in terms of α without radicals. There are such but they are *very* difficult to find; one example is $x^3 + 3x + 1$. The behavior of the splitting field is in fact based on the *cubic discriminant*, which for a polynomial $x^3 + px + q$ is $4p^3 - 27q^2$. If the discriminant is a perfect square, then the splitting field has degree 3. This one wasn't entirely meant to be fair.