Math 504 Final Exam Fall 2001
Some comments on the questions and answers

PART I (12 points)
Questions in this section are worth two points each.
Give examples of the following:

1. A quotient of $k[x, y, z]$ that is a UFD but not a PID.
2. A quotient of $k[x, y, z]$ that is a domain but not a UFD.
3. A radical ideal in $k[x, y, z]$ that is not prime.
4. A non-noetherian $\mathbb{Z}$-module.

The most popular answer was the infinite polynomial ring $R = \mathbb{Z}[x_1, x_2, \ldots]$. I guess the philosophy was to just take something really, really big and hope for the best! You are correct that $R$ is a not a noetherian $\mathbb{Z}$-module (it is not even noetherian as a module over itself because the ideal $(x_1, x_2, \ldots)$ is not finitely generated). But a much better example is $M = \mathbb{Q}$ with infinite ascending chain

$$\mathbb{Z} \subset \frac{1}{2}\mathbb{Z} \subset \frac{1}{4}\mathbb{Z} \subset \frac{1}{8}\mathbb{Z} \subset \ldots$$

This is better because it perchers more delicately on the boundary of non-noetherianity. As a module over itself $\mathbb{Q}$ is noetherian. But $R$ is not noetherian as a module over itself. If you understand the real reason that $R$ is not a noetherian $\mathbb{Z}$-module you would also understand that $\mathbb{Z}[x]$ is not a noetherian $\mathbb{Z}$-module. So, I suspect that those who gave $R$ as the answer did not understand the real reason it fails to be noetherian, because if they did, they would simply have given $\mathbb{Z}[x]$ as the example. By the way, $\mathbb{Z}[x]$ fails to be noetherian because of the chain $M_0 \subset M_1 \subset \ldots$ where $M_n = \mathbb{Z} \oplus \mathbb{Z}x \oplus \cdots \oplus \mathbb{Z}x^n$.

5. A finite extension of $\mathbb{Q}$ that is not normal.
6. A field extension $k \subset K$ and an element $\alpha \in K$ such that $k(\alpha) \neq k[\alpha]$.

Just take $\alpha$ to be any transcendental over $k$, e.g. $\mathbb{Q}[\pi] \neq \mathbb{Q}(\pi)$.

PART II (16 points)
Questions in this section are worth two points each.
State the following:

1. The Chinese remainder theorem.
2. The classification theorem for finite fields (including their description as splitting fields).

I was surprised that few people got this completely correct... you need to say there is a field of order $p^n$ for all primes $p$ and all $n \geq 1$, and any finite field has order $p^n$ for some such $p$ and $n$, and there is only one field of order $p^n$ up to isomorphism, and it is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

3. The strong form of Hilbert’s Nullstellensatz.

4. The first result about integrality of an element $a$ in a ring $S$ containing a subring $R$. There should be three equivalent conditions.

Lots got this wrong. You need to say that $R[a]$ is finitely generated as an $R$-module.

5. Noether’s normalization theorem.

6. The main result about splitting fields.

Existence and uniqueness.

7. The result relating morphisms between closed subvarieties of $\mathbb{A}^n$ and $\mathbb{A}^m$ and ..... (fill in the rest of this question yourself)....it should have something to do with their coordinate rings.

A tough question for most people.

8. The most general form of Eisenstein’s criterion.

State it not for $\mathbb{Z}$ but for an arbitrary UFD.

PART III (10 points)
State whether each of the following statements is True or False. You get one point for each correct answer and −1 point for each incorrect answer. These questions proved pretty tough for most people.

1. If $f, g \in \mathbb{Q}[x]$ and the rings $\mathbb{Q}[x]/(f)$ and $\mathbb{Q}[x]/(g)$ are isomorphic, then $f = \lambda g$ for some $\lambda \in \mathbb{Q}$.

FALSE. For example, let $f$ and $g$ be the minimal polynomials of $\sqrt{2}$ and $\sqrt{2}+1$ respectively. Check that $f \neq g$. But $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}+1)$, $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(f)$ and $\mathbb{Q}(\sqrt{2}+1) \cong \mathbb{Q}[x]/(g)$.

2. A commutative ring with 1001 elements can never be a domain.

TRUE. A finite domain is a field, but 1001 is not a prime power ($1001 = 7 \times 11 \times 13$).
3. The rings \( \mathbb{Z}[x]/(x^2 - 2x + 1) \) and \( \mathbb{Z} \oplus \mathbb{Z} \) are isomorphic.

   FALSE. In \( \mathbb{Z}[x]/(x^2 - 2x + 1) \) we have \((x-1)^2 = 0\) so \(\sqrt{0} \neq 0\). But in \( \mathbb{Z} \oplus \mathbb{Z} \), \(\sqrt{0} = 0\). Oh, an isomorphism of rings \( R \to S \) sends the radical of zero to the radical of zero.

4. The rings \( \mathbb{Z}[x]/(x^2 - 2x) \) and \( \mathbb{Z} \oplus \mathbb{Z} \) are isomorphic.

   TRUE. Define \( \phi : \mathbb{Z}[x] \to \mathbb{Z} \oplus \mathbb{Z} \) by \( x \mapsto (0, 2) \). Or use the Chinese Remainder because \((x) + (x - 2) = \mathbb{Z}[x] \) and \( \mathbb{Z}[x]/(x) \cong \mathbb{Z} \cong \mathbb{Z}[x]/(x - 2) \).

5. The cubic curve \( y = x^3 - x^2 \) is isomorphic to the affine line as an algebraic variety.

   TRUE. \( k[x, y]/(y - x^3 + x^2) \cong k[x] \).

6. There are infinitely many maximal ideals in the ring \( \mathbb{F}_2[x] \).

7. The degree of the minimal polynomial of \( e^{2\pi i/5} + e^{8\pi i/5} \) over \( \mathbb{Q} \) is four.

   FALSE. If \( \xi = e^{2\pi i/5} \), then \( \alpha = e^{2\pi i/5} + e^{8\pi i/5} = \xi + \xi^4 \). Now \( 1 + \xi + \xi^2 + \xi^3 + \xi^4 = 0 \) and \( \alpha^2 = (\xi + \xi^4)^2 = \xi^2 + 2 + \xi^3 \). So \( 1 + \alpha + \alpha^2 - 2 = 0 \).

8. There is a commutative ring \( R \) with 64 elements containing \( \mathbb{F}_{16} \).

   FALSE. \( R \) would be a vector space over \( \mathbb{F}_{16} \), but \( \mathbb{F}_{16}^2 \) already has 256 elements.

9. A prime ideal contains an ideal \( J \) if and only if it contains \( \sqrt{J} \).

10. The fields \( \mathbb{Q}(\sqrt{3}) \) and \( \mathbb{Q}(\sqrt{5}) \) are isomorphic.

   FALSE. Just compute to see that \( \mathbb{Q}(\sqrt{3}) \) cannot contain an element \( a + b\sqrt{3} \) whose square is 5.

**PART IV (12 points)**

Questions in this section are worth two points each.

Give short (one or two sentence) answers to each of the following questions:

1. What are the Zariski closed subsets of the affine line \( \mathbb{A}^1 \)? Why?

2. How are the irreducible components of a closed subvariety \( X \subset \mathbb{A}^n \) related to the ideals in \( \mathcal{O}(X) \).

   Everyone got this wrong. The irreducible components are in bijection with the **minimal** prime ideals of \( \mathcal{O}(X) \).

3. If \( I \) and \( J \) are ideals in \( k[x_1, \ldots, x_n] \), what is \( V(IJ) \) in terms of \( V(I) \) and \( V(J) \)?

4. Let \( K/k \) be an extension field and \( \alpha \in K \). If \( f \in k[x] \) is such that \( f(\alpha) = 0 \), how is \( f \) related to the minimal polynomial of \( \alpha \)?
5. Suppose that \( f \in k[x] \) is not a unit. Give an example of an extension field \( K/k \) in which \( f \) has a zero. (Do not say “the splitting field of \( f \)!” – be more explicit.)

Notice \( f \) is not necessarily irreducible so \( k[x]/(f) \) need not be a field. But let \( g \) be an irreducible factor of \( f \) and take \( K = k[x]/(g) \).

6. Let \( k(x) \) be the rational function field in an indeterminate \( x \) over \( k \), and define \( t = x^3/(x + 1) \). What is the minimal polynomial of \( x \) over \( k(t) \)?

Yikes! This is easy. I have given you the polynomial \( x \) satisfies, namely \( x^3 - tx - t \).
PART V (50 points)

1. (10 pts) Prove that every ideal in $k[x_1, \ldots, x_n]$ is finitely generated.

2. (10 pts) Define the noetherian property for a module, and state and prove its equivalence to two other conditions.

   Many people forgot to specify that the collection of submodules that has a maximal member must first be assumed non-empty.

3. (10 pts) Prove that a finite extension $K/k$ is normal if and only if it is the splitting field of some polynomial in $k[x]$. State clearly any preliminary results you make use of.

   A difficult question for most of you.

4. (10 pts) Let $R$ be a principal ideal domain. Prove that greatest common divisors (g.c.d.s) exist in $R$, and if $d = \gcd(a, b)$, then $d = ax + by$ for some $x, y \in R$. It would be a good idea to start your proof with the definition of a greatest common divisor. Once you know that g.c.d.s exist, what important property of PIDs can then be proved?

5. (10 pts) Prove that the polynomial ring $k[x]$ is a principal ideal domain. First prove that if $d = \gcd(f, g)$, then $d = af + bg$ for some $a, b \in k[x]$. You may use the fact that the Euclidean algorithm works in $k[x]$.

   This was a lousy question! Sorry. You can show directly that $k[x]$ is a principal ideal domain as follows: if $I$ is a non-zero ideal pick $f \in I$ of least degree; if $g \in I$ and one writes $g = af + r$ with $\deg r < \deg f$, then $r = g - af \in I$, so $r = 0$. 