Show your work - explain what you are doing. Scattered formulas without clear logical order and clear justifications will be ignored (ZERO CREDIT!)

It is YOUR responsibility to demonstrate that you have mastered the material of this class. A total of 140 points are available on this test and 100 points constitute a perfect score (A+). Work as many parts as you can - but fewer completely correct answers will earn more credit than more incomplete answers.

1. a. Suppose that $a$ and $b$ are nonzero integers. In no more than half a page outline an explanation, in as elementary terms as possible, why there exist integers $u$ and $v$ such that $\gcd(a, b) = ua + vb$.
   
b. Using part a., prove that if $a$, $b$, and $p$ are integers, $p$ is prime and $p \mid ab$ and $p \nmid a$ then $p \mid b$.
   
c. Show that if $I \leq R$ is a prime ideal in a commutative ring $R$ with unity then $R/I$ is an integral domain.
   
   You may assume without proof that $R/I$ is a commutative ring with unity.

2. Factor each polynomial as a product of irreducibles in the specified ring.
   
   Prove that the factors are indeed irreducible – demonstrate knowledge of a diversity of arguments.
   
   a. $x^3 + x + 1$ in $\mathbb{Z}_2[x]$.
   
   b. $x^6 + x^2 + 1$ in $\mathbb{Z}_2[x]$.
   
   c. $x^3 - 16x^2 + 9x + 5$ in $\mathbb{Q}[x]$.

3. Consider the polynomial $p(x) = x^3 + x + 1$ in the ring $\mathbb{Z}_2[x]$.
   
   a. Briefly explain why $F = \mathbb{Z}_2[x]/\langle p(x) \rangle$ is a field.
   
   b. Find the multiplicative inverse of $x + \langle p(x) \rangle$ in $F$, or explain why it does not exist.
   
   c. Let $\alpha = x + \langle p(x) \rangle \in F$. Verify that both $\alpha$ and $\alpha^2$ are roots of $p(x)$ in $F$.
   
   Bonus. Find the third root of $p(x)$ in $F$.

4. Consider the ring $S = \mathbb{Q}[x]/\langle p(x) \rangle$ of congruence classes in $\mathbb{Q}[x]$ modulo $p(x) = x^2 - 3$.
   
   a. For $a, b \in \mathbb{Q}$, not both zero, find the multiplicative inverse of $a + bx + \langle x^2 - 3 \rangle$ in $S$.
   
   b. Show that $S$ is isomorphic to $T = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$ considered as a subring of the reals $\mathbb{R}$.
   
   (Justify why your map is well-defined, if applicable, and focus on the multiplicative properties.)

5. Suppose $\Phi: R \map R S$ is a homomorphism between rings $R$ and $S$ and $I \leq R$ and $J \leq S$ are ideals.
   
   You may assume without proof that $\Phi^{-1}(J) \leq R$ and $\Phi(I) \leq S$ are subrings.
   
   a. Show that the preimage $\Phi^{-1}(J)$ is an ideal of $R$.
   
   b. Give a counterexample that shows that the image $\Phi(I)$ need not be an ideal of $S$.
   
   c. Consider the special case of $R = S = \mathbb{Z}_{10}$.
   
   Explain the difference: $\Phi: x \map 6x \text{ (mod 10)}$ is a homomorphism, but $\Psi: x \map 4x \text{ (mod 10)}$ is not.
   
   Verify that the image $J = \Phi(\mathbb{Z}_{10})$ is an ideal in $\mathbb{Z}_{10}$.
   
   Is the ring of congruence classes $\mathbb{Z}_{10}/J$ an integral domain? Is it a field? Justify your answer.

6. For each pair of rings $R$ and $S$ listed below, either give an explicit (nonzero) isomorphism between them, or explain why there does not exist any. If there is no isomorphism, find nonzero homomorphisms from $R \text{ to } S$, and from $S \text{ to } R$, or explain why either is or both are impossible.
   
   a. $R = \mathbb{Z}$, $S = \mathbb{Z} \times \mathbb{Z}$.
   
   b. $R = \mathbb{Z}_{10}$, $S = \mathbb{Z}_5$.
   
   c. $R = \mathbb{Z}_3 \times \mathbb{Z}_4$, $S = \mathbb{Z}_{12}$.