- Please put your name and ID number on your blue book.
- The exam is CLOSED BOOK except for two pages of notes.
- Calculators are NOT allowed.
- *In a multipart problem, you can do later parts without doing earlier ones.*
- **You must show your work to receive credit.**

1. (4 pts.) Find a multiplicative inverse of $1+2x$ in $\mathbb{Z}_4[x]$. You must do the calculations that show your answer is a multiplicative inverse.

2. (4 pts.) Compute the Hamming distance between the two words $u = 01000101$ and $v = 11110011$. Also, either (a) find one word that is simultaneously within Hamming distance two of both u and v or (b) explain why there is no such word.

3. (6 pts.) Find the splitting field of $x^3 - 2$ over $\mathbb{Q}$. You should use real and/or complex numbers in your description of the field. For example, give the splitting field of $x^2 - 3$ over $\mathbb{Q}$ as "$\mathbb{Q}(\sqrt{3})$," NOT as "$\mathbb{Q}[x]/\langle x^2 - 3\rangle$" and NOT as "$\mathbb{Q}(a)$ where a is a zero of $x^2 - 3$."

4. (18 pts.) Let $E = \mathbb{Q}(\sqrt{2} + \sqrt{5})$ and $F = \mathbb{Q}(\sqrt{10})$.
   (a) Prove that F is a subfield of E.
   (b) Find a basis for E as a vector space over F. You need not prove that it is a basis.
   (c) Find a basis for E as a vector space over $\mathbb{Q}$. You need not prove that it is a basis.

5. (18 pts.) Suppose F and K are fields and that F is a finite field of characteristic p.
   (a) Describe explicitly all the values that $|F|$ can have. For example, DO NOT say "the size of any field with characteristic p. If it were correct (which it is NOT), you could say something like "p and $p^2 - 1$."
   (b) Prove: If K is a finite extension of F, then $|K| = |F|^n$ for some integer n.
   (b) Prove: If $|K| = |F|^n$ for some integer n, then K is a finite extension of F.

END OF EXAM