Sample Exam 3
Math 127, Fall 2024

1. (10 points) Let $\mathbf{F}_{32}$ be a field of order 32. Is $\mathbf{Z}/(32)$ isomorphic to $\mathbf{F}_{32}$? Briefly **EXPLAIN** why or why not.

2. (10 points) Let $I = (x^3 + x)$ be the principal ideal of $R = \mathbf{F}_2[x]$ generated by $x^3 + x$. Find an element $f(x)$ of the coset $x^2 + I$ such that $\deg f(x) \geq 4$, and briefly **EXPLAIN** how you know that $f(x) \in x^2 + I$. (If you don't know how to find such an $f(x)$, you may recite the definitions of ideal and coset for partial credit.)

3. (10 points) Let $\mathbf{F}_{32} = \mathbf{F}_2[\alpha]$, where α is a root of $x^5 + x^3 + 1$. Find part of the antilog table with respect to α by computing the reduced forms of α^5, α^6, α^7, α^8, and α^9. Show all your work.

4. (12 points) Let $\mathbf{F}_{256}$ be the field of order $256 = 2^8$, and let $\mathbf{F}_{256}^\times$ be the multiplicative group of $\mathbf{F}_{256}$.

(a) Let α be a primitive element of $\mathbf{F}_{256}$. What is the order of α? Briefly **EXPLAIN** your answer.

(b) Exactly one of the following is true.

- There exists an element $\beta \in \mathbf{F}_{256}^\times$ of order 17.
- There exists an element $\beta \in \mathbf{F}_{256}^\times$ of order 32.

Circle the true statement and explain how to find such an element β in terms of the primitive element α.

5. (12 points) Let $R = \mathbf{F}_2[\alpha]$, where α is a root of $m(x) = x^6 + x^3 + x$. In other words, $R = \mathbf{F}_2[x]/(m(x))$.

(a) How many elements are there in the ring R? Briefly **JUSTIFY** your answer.

(b) Is R a field? Briefly **EXPLAIN** why or why not.

6. (14 points) Let $q = 2^e$ for some $e \geq 1$, and let α be an element of $\mathbf{F}_q^\times$ of order 39. Find the minimal polynomial $m(x)$ of α^3 over $\mathbf{F}_2$, expressed as a product of terms of the form $(x - \alpha^i)$. Show all your work.

7. (14 points) Note that in $\mathbf{F}_2[x]$, we have

$$\begin{aligned} x^6 + x + 1 &= (x^2)(x^4 + 1) + (x^2 + x + 1), \\ x^4 + 1 &= (x^2 + x)(x^2 + x + 1) + (x + 1), \\ x^2 + x + 1 &= (x)(x + 1) + 1. \end{aligned}$$

(I.e., you are given the above facts and do not need to check them yourself.)

Let $\mathbf{F}_{64} = \mathbf{F}_2[\alpha]$, where α is a root of x^6+x+1. Find the multiplicative inverse of $\beta = \alpha^4+1$. Show all your work.

8. (18 points) Let $E = \mathbf{F}_{4096}$, let β be a primitive element of E, and let $\alpha = \beta^{63}$. Note that the order of α is 65 (i.e., you are given this fact and do not need to check it or justify it). Let $\mathcal{C}$ be the BCH code given by E, α, and $\delta = 5$ over $\mathbf{F}_2$.

(a) Find the generating polynomial $g(x)$ of $\mathcal{C}$, expressed as a product of minimal polynomials $m_i(x)$, where $m_i(x)$ is the minimal polynomial of α^i. (You do not need to expand each $m_i(x)$ as a product of terms of the form $(x - \alpha^j)$.) Show all your work, especially your orbit calculations.

(b) Find $k = \dim \mathcal{C}$.