Sample Exam 3
Math 127, Spring 2021

1. (10 points) Let $\mathcal{C}$ be a cyclic code of length n over $\mathbf{F}_q$, and suppose that $g(x)$ is the generator polynomial of $\mathcal{C}$. Describe, in terms of $g(x)$, exactly when $f(x) \in \mathbf{F}_q[x]/(x^n - 1)$ is an element of $\mathcal{C}$. You can either give a precise verbal description or a description of the form

$$\mathcal{C} = \{\, f(x) \in \mathbf{F}_q[x]/(x^n - 1) \mid \text{(defining condition)} \,\}.$$

For questions 2–4, you are given a statement. If the statement is true, you need only write "True", though a justification may earn you partial credit if the correct answer is "False". If the statement is false, write "False", and justify your answer **as specifically as possible**. (Do not just write "T" or "F", as you may not receive any credit; write out the entire word "True" or "False".)

2. (10 points) $\mathbf{F}_4$ (the field with four elements) is isomorphic to $\mathbf{Z}/(4)$.

3. (10 points) Let $I = (x^2)$, the principal ideal of $\mathbf{F}_2[x]$ generated by x^2. Then x and $x^4 + x^2 + x$ are in the same coset of I.

4. (10 points) In $\mathbf{F}_{256}^{\times}$, the multiplicative group of the field of order 256, every element has order ≤ 85.

5. (12 points) Let α be a primitive element of $\mathbf{F}_{64}$. 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.

6. (12 points) Let $\mathbf{F}_{16} = \mathbf{F}_2[\alpha]$, where α is a root of $x^4 + x + 1$. Find the order of $\beta = \alpha^3$ by calculating powers of β. Show all your work.

7. (12 points) Let $E = \mathbf{F}_{32}$, and let α be a primitive root of unity of E. Let $\mathcal{C}$ be the corresponding BCH code of designed distance $\delta = 9$ 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 $k = \dim \mathcal{C}$.

8. (12 points) Note that in $\mathbf{F}_2[x]$, we have

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

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

Let $\mathbf{F}_{16} = \mathbf{F}_2[\alpha]$, where α is a root of $x^4 + x + 1$. Find the multiplicative inverse of $\alpha^2 + 1$. Show all your work.

9. (12 points) **PROOF QUESTION.** Let R be a ring, fix $a, b, c \in R$, and let

$$I = \{ra + sb + tc \mid r, s, t \in R\}.$$

(a) Prove that I is closed under addition. (Suggestion: What do two random elements of I look like?)

(b) Prove that I is closed under multiplication by $u \in R$.