Math 127, Spring 2020 **Name:** _____
Exam 2

This test consists of 7 questions on 3 pages, totalling 100 points. You are allowed to use **ONE** handwritten page of notes (both sides), but you are otherwise not allowed to use books, notes, or calculators. Unless otherwise stated, you may take as given anything that has been proven in class, in the homework, or in the reading.

1. (14 points) Let A be a matrix with entries in $\mathbf{F}_5$ such that

$$A = \begin{bmatrix} 3 & 4 & 3 & 3 & 4 & 1 & 0 \\ 3 & 4 & 4 & 2 & 1 & 1 & 1 \\ 0 & 0 & 3 & 1 & 1 & 4 & 0 \\ 3 & 4 & 3 & 2 & 4 & 0 & 2 \end{bmatrix}, \qquad RREF(A) = \begin{bmatrix} 1 & 3 & 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 0 & 2 & 1 & 4 \\ 0 & 0 & 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Find bases for $\mathrm{Col}(A)$ and $\mathrm{Null}(A)$. Show your work.

2. (14 points) Suppose $\mathbf{x}, \mathbf{y}, \mathbf{z} \in F_{11}^4$.

(a) Write down the definition of what it means for $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ to be linearly independent. (You can just copy this from your notes!)

(b) Now suppose also that

$$\mathbf{x} = \begin{bmatrix} 0 \\ 1 \\ r \\ 0 \end{bmatrix} \qquad \mathbf{y} = \begin{bmatrix} 1 \\ 0 \\ s \\ 0 \end{bmatrix} \qquad \mathbf{z} = \begin{bmatrix} 0 \\ 0 \\ t \\ 1 \end{bmatrix},$$

where $r, s, t \in \mathbf{F}_{11}$ are unspecified constants. Use the definition of linear independence to prove that $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ is linearly independent.

3. (14 points) Let $\mathbf{F}_{32}$ be the field with 32 elements, and suppose $a \in \mathbf{F}_{32}^\times$, $a \neq 1$.

(a) What can you say about the order of a? Be as specific as possible.

(b) What can you say about $\langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}$, the cyclic subgroup of $\mathbf{F}_{32}^\times$ generated by a? Be as specific as possible.

4. (14 points) Note that in $\mathbf{F}_2[x]$, we have

$$x^5 + x^2 + 1 = (x^2 + x + 1)(x^3 + x^2 + 1) + (x^2 + x),$$
$$x^3 + x^2 + 1 = (x)(x^2 + x) + 1.$$

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

Let $\mathbf{F}_{32} = \mathbf{F}_2[\alpha]$, where α is a root of x^5+x^2+1. Find the multiplicative inverse of $\alpha^3 + \alpha^2 + 1$. Show all your work.

5. (14 points) Recall that the parity check matrix of the Hamming 7-code $\mathcal{H}_7$ is

$$H_7 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Suppose Yolanda is receiving transmissions sent using the Hamming 7-code, and she receives $\mathbf{y} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$. Correct $\mathbf{y}$ to a codeword $\mathbf{y}'$, if necessary, and read off the message bits 3, 5, 6, and 7 to find the intended message $\mathbf{m}'$. Show all your work.

6. (14 points) Let $\mathcal{C}$ be the binary linear code of length 7 with parity check matrix

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Find a generator matrix for $\mathcal{C}$. Show your work.

7. (16 points) **PROOF QUESTION.** Let R and R' be rings, and let $\rho : R \to R'$ be a homomorphism. Define

$$K = \{x \in R \mid \rho(x) = 0\}.$$

(a) Write down the definition of what it means for ρ to be a homomorphism. (You can just copy this from your notes!)

(b) Prove that K is closed under addition. (Suggestion: What do two random elements $x, y \in K$ look like?)

(c) Prove that K is closed under multiplication by $r \in R$.