Sample Exam 2
Math 127, Spring 2020

This sample compiles the relevant problems from the Exams 2 and 3 I gave last year. The actual exam will be shorter than Exam 1.

1. (10 points) Let F be a field, and let $\mathbf{u}, \mathbf{v}, \mathbf{w}$ be vectors in F^n. Define what it means for $\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$ to be linearly independent.

For questions 2–7, 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) If W is a subspace of $\mathbf{F}_{17}^9$ such that $\dim W = 4$, and $\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$ is a subset of W, then it must be the case that $\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$ does **not** span W.

3. (10 points) Let $\mathbf{u}$ and $\mathbf{v}$ be nonzero vectors in $\mathbf{F}_7^{11}$. Then it must be the case that the span of $\{\mathbf{u}, \mathbf{v}\}$ contains exactly two vectors.

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

5. (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.

6. (10 points) In $\mathbf{F}_{256}^\times$, the multiplicative group of the field of order 256, every element has order ≤ 85.

7. (10 points) Let $f(x)$ be a polynomial of degree 2 in $\mathbf{F}_{11}[x]$, and suppose that

$$f(x) = p_1(x)p_2(x) = q_1(x)q_2(x),$$

where each of $p_1(x)$, $p_2(x)$, $q_1(x)$, and $q_2(x)$ has degree 1. Then it must be the case that $p_1(x)$ is equal to either $q_1(x)$ or $q_2(x)$.

8. (12 points) Let $\mathcal{C}$ be the binary linear code of length 5 with parity check matrix

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

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

9. (12 points) Let A be a matrix with entries in $\mathbf{F}_5$ such that

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

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

10. (12 points) Consider $a(x) = x^5 + x^4 + x^3 + 1$ and $b(x) = x^3 + x^2$ in $\mathbf{F}_2[x]$, and note that

$$\begin{aligned} x^5 + x^4 + x^3 + 1 &= (x^2+1)(x^3+x^2) + (x^2+1), \\ x^3 + x^2 &= (x+1)(x^2+1) + (x+1), \\ x^2 + 1 &= (x+1)(x+1). \end{aligned}$$

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

Find $f(x), g(x) \in \mathbf{F}_2[x]$ such that $f(x)a(x) + g(x)b(x) = \gcd(a(x), b(x))$. Show your work and clearly indicate your answer.

11. (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.

12. (12 points) Let W be the subset of $\mathbf{F}_7^3$ defined by

$$W = \left\{ \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \in \mathbf{F}_7^3 \,\middle|\, x_1 = x_2 \right\}.$$

Prove that W is a subspace of $\mathbf{F}_7^3$, in the following steps:

(a) Explain why $\mathbf{0} \in W$.

(b) Suppose $\mathbf{x}, \mathbf{y} \in W$. Explain why $\mathbf{x} + \mathbf{y} \in W$.

(c) Suppose $\mathbf{x} \in W$ and $a \in \mathbf{F}_7$. Explain why $a\mathbf{x} \in W$.

13. (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.

14. (12 points) **PROOF QUESTION.** Let R be a ring, fix $a, b, c \in R$, and let

$$I = \{ra + sb + tc \mid r, s, t \in R\}. \tag{1}$$

(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 $u \in R$.

15. (12 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 $\mathbf{y} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$. 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.