Sample Final Exam
Math 127, Spring 2020

This sample compiles the relevant problems from the final exam I gave last year.

1. (12 points) Let $\mathbf{v}_1 = \begin{bmatrix}1\\1\\3\\2\\0\end{bmatrix}$, $\mathbf{v}_2 = \begin{bmatrix}0\\1\\2\\0\\3\end{bmatrix}$, and $\mathbf{v}_3 = \begin{bmatrix}0\\0\\1\\6\\4\end{bmatrix}$ be vectors in $\mathbf{F}_7^5$, and let

$$W = \text{span}\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}.$$

How many vectors are there in W? Briefly **JUSTIFY** your answer.

2. (12 points) Recall that the various forms of the Division Theorem for a ring R all say that when we divide $a \in R$ by some nonzero $d \in R$, we get

$$a = qd + r$$

for some $q, r \in R$ such that r is, in some sense, "smaller" than d. Complete the statement of the Division Theorem for the following rings R.

(a) For $R = \mathbf{Z}$, in what sense is r smaller than d? (There are two possible correct answers here; you may choose whichever one you prefer.)

(b) For F a field and $R = F[x]$, in what sense is $r(x)$ smaller than $d(x)$?

3. (12 points) Complete the following description of how to construct the field of order $q = 2^e$ by filling in the blanks. Make sure your answer is clearly readable.

- For $q = 2^e$, to construct the field $\mathbf{F}_q$ of order q, we construct the quotient ring: $\boxed{}$
- Where $m(x)$ is a/an $\boxed{}$ polynomial
- Of degree $\boxed{}$.

4. (12 points) Let G be a group, let H be a subgroup of G, and let a be an element of G. Define the left multiplicative coset aH.

5. (12 points) Let A be a matrix with entries in $\mathbf{F}_5$ such that

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

Find a basis for Null(A). Show your work.

6. (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 $\delta = 5$ over $\mathbf{F}_2$.

(a) Find the generating polynomial $g(x)$ of $\mathcal{C}$ as a product of minimal polynomials $m_i(x)$.

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

7. (12 points) Consider $a(x) = x^4+x^3+x+1$ and $b(x) = x^2+x$ in $\mathbf{F}_2[x]$. Use the Euclidean Algorithm to find $d = \gcd(a(x), b(x))$. Show all your work.

8. (12 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.

9. (12 points) Let $\mathcal{C}$ be the binary linear code of length 7 with generator matrix

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

In other words, $\mathcal{C}$ is spanned by the columns of G.

(a) Find the dimension of $\mathcal{C}$. **JUSTIFY** your answer.

(b) Find a nonzero codeword in $\mathcal{C}$ that is *not* one of the columns of G. Show your work.

10. (14 points) Let $\mathbf{F}_{16} = \mathbf{F}_2[\alpha]$, where α is a root of $x^4 + x + 1$.

(a) Let $\beta = \alpha^2 + \alpha$, and suppose that you are given that the order of β is ≤ 5. Find the order of β by calculating powers of β and using the given information. Show all your work.

(b) Is there an element of $\mathbf{F}_{16}^{\times}$ whose order is greater than 5? **JUSTIFY** your answer.

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

12. (14 points) Find $d = \gcd(177, 78)$, and find $x, y \in \mathbf{Z}$ such that $177x + 78y = d$. Show all your work.

13. (14 points) **PROOF QUESTION.** Let I be the set of all $f(x) \in \mathbf{F}_{13}[x]$ such that $f(5) = 0$. In other words, let

$$I = \{f(x) \in \mathbf{F}_{11}[x] \mid f(5) = 0\}. \tag{1}$$

(a) Prove that I is closed under addition. (Suggestion: What does it mean to say that $f_1(x)$ and $f_2(x)$ are in I?)

(b) Prove that I is closed under multiplication by $h(x) \in \mathbf{F}_{11}[x]$. (That is, explain why we can be sure that if $f(x) \in I$ and $h(x) \in \mathbf{F}_{11}[x]$, then $h(x)f(x) \in I$.)