MAD 6607: Coding Theory

Edoardo Persichetti Test 2

Exercise 1 Consider the finite field $\mathbb{F}_2$.

a) Build the quotient ring $\mathbb{F}_2[x]/(x^4+1)$.

b) Is this ring a field? Explain why.

c) Describe the principal ideal $(x+1)$.

Hint: remember that a principal ideal is entirely generated by its defining element.

Exercise 2 Let $p(x) = x^2 + x - 4$. In which of the following fields is $p(x)$ irreducible and why?

a) $\mathbb{Q}$

b) $\mathbb{R}$

c) $\mathbb{F}_5$

Exercise 3 Using the result from above, indicate whether $\mathcal{R} = \mathbb{F}_5[x]/(x^2+x-4)$ is a field or not. If not, why? If so, what would be the field that we obtain?

Exercise 4 Consider the ring $\mathcal{R}$ as above and let α be a root of $x^2 + x - 4$.

a) What is the general form of an element in this ring?

b) Is α a primitive element? Explain.

If the answer to part b) was yes, describe the ring using powers of α. If not, find an irreducible quadratic polynomial whose root, say β, is a primitive element, then describe the ring (in this case a field) using powers of β.

Exercise 5 Consider the field F you just built.

a) What is the prime subfield of F? Are there any other subfields, and why?

b) Let γ be the primitive element used to define the field[1]. List all of the conjugates of γ^7.

c) List all the automorphisms of F over its prime field. What structure do they form?

d) Compute the trace and norm of γ^7 over its prime field.

e) Write a polynomial basis and a normal basis for F over its prime field.

[1] This is either α or β, depending on your answer to question 4.