MAD 6607: Coding Theory

Edoardo Persichetti Test 2 Solutions

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

a) We have $\mathbb{F}_2[x]/(x^4+1) = \{0, 1, x, x^2, x^3, x+1, x^2+1, x^3+1, x^2+x, x^3+x, x^3+x^2, x^3+x+1, x^2+x+1, x^3+x^2+x, x^3+x^2+1, x^3+x^2+x+1\}$.

b) This is not a field since x^4+1 is not irreducible (1 is a root).

c) The principal ideal $(x+1)$ is entirely generated by $x+1$ so we have $\{0, x+1, x^2+1, x^2+x, x^3+x^2+x+1, x^3+x^2, x^3+x, x^3+1\}$.

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

a) $\mathbb{Q}$: irreducible since the two roots $(-1 \pm \sqrt{17})/2$ are not rational.

b) $\mathbb{R}$: reducible (see above).

c) $\mathbb{F}_5$: irreducible since no element is a root (check $0, 1, 2, 3, 4$).

Exercise 3 It follows that $\mathcal{R} = \mathbb{F}_5[x]/(x^2+x-4)$ is a field, specifically $\mathbb{F}_{5^2} = \mathbb{F}_{25}$.

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

a) Since this is a quadratic extension the general form of an element in this ring is $\{a+b\alpha, a, b \in \mathbb{F}_5\}$.

b) No, α is not a primitive element since it has order 3, in fact $\alpha^3 = \alpha \cdot \alpha^2 = \alpha \cdot (4\alpha+4) = 4\alpha^2 + 4\alpha = 4 \cdot 4 = 1$.

An irreducible polynomial that works is x^2+x+2, then it is possible to define the field in terms of its root β.

Exercise 5 Consider the field F you just built.

a) The prime subfield is $\mathbb{F}_5$ (it's the only one by definition).

b) The conjugates of γ^7 are γ^7 and $(\gamma^7)^5 = \gamma^{35} = \gamma^{11}$.

c) The automorphisms are $\sigma_0 = id$ and $\sigma_1 : \gamma \to \gamma^5$ - they form a group of order 2.

d) We have $Tr_{\mathbb{F}_5}(\gamma^7) = \gamma^7 + \gamma^{11} = 3$ and $N_{\mathbb{F}_5}(\gamma^7) = \gamma^7 \cdot \gamma^{11} = \gamma^{18} = 3$.

e) A polynomial basis is $(1, \gamma)$ and a normal basis is (γ, γ^5). Verify that the normal basis generates a matrix of determinant $\neq 0$.