Exercise 4 - Finite Fields

Q1. Consider $\mathbb{F}_{17}$

i) What is the sum of all the elements?

ii) What is the product of the nonzero elements?

iii) What is the order of 2 ?

iv) What are the possible orders of the elements?

v) Determine for all the possible orders an element of that order.

vi) How many primitive elements are there?

vii) Try to solve the equation $x^2 + x + 1 = 0$.

Q2. Determine all binary irreducible polynomials of degree 3.

Q3. How many zeros of the polynomial $z^4 + z^3 + 1$ in $\mathbb{F}_{16}$?

Q4. How many zeros of $z^4 + z^2 + z$ in $\mathbb{F}_{16}$?

Q5. Consider the finite fields $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$. Define the mapping $\mathrm{Tr} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ by

$$\mathrm{Tr}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}$$

i) Show that $\mathrm{Tr}(x) \in \mathbb{F}_q$

ii) Show that $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$

iii) Show that $\mathrm{Tr}(\gamma x) = \gamma\,\mathrm{Tr}(x)$ for $\gamma \in \mathbb{F}_q$

Q6. Show that $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$.

Q7. Let C be a linear (n, k, d) code over $\mathbb{F}_q$.

i) Show that d equals the minimal number of linearly dependent columns of a parity matrix H.

ii) What is the maximal length of an $(n, k, 3)$ code over $\mathbb{F}_q$?

*The above questions are taken from the textbook Ch. 2.

Programming Tasks

T1. Use SageMath to check whether $x^5 + x^3 + x^2 + 1$ is irreducible over $\mathbb{F}_2$.

T2. Use SageMath to create $\mathbb{F}_{2^{10}}$ based on a polynomial $f(x) = x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1$. Suppose α is a root of $f(x)$. Use Sagemath to answer the following questions:

i) the vectorial form of α^{18}

ii) the vectorial form of α^{36}

iii) $\alpha^{18} + \alpha^{36}$

iv) $\alpha^{18}(\alpha^5 + \alpha^{36})$

T3. Use SageMath to create $\mathbb{F}_{2^{10}}$ based on a polynomial $f(x) = x^{10} + x^6 + x^2 + x + 1$. Suppose β is a root of $f(x)$. Use Sagemath to answer the following questions:

i) the vectorial form of β^{18}

ii) the vectorial form of β^{36}

iii) $\beta^{18} + \beta^{36}$

iv) $\beta^{18}(\beta^5 + \beta^{36})$