COMPUTATIONAL ALGEBRA: HOMEWORKS

1. (a) Prove that $f = x^5 - x + 1$ is an irreducible polynomial in $\mathbb{F}_3[x]$, and it is reducible in $\mathbb{F}_2[x]$.
   (b) Decompose f in irreducible factors in $\mathbb{F}_2[x]$

2. Consider the field $\mathbb{F}_9 \cong \mathbb{F}_3[x]/(f)$, where $f = x^2 + 1 \in \mathbb{F}_3[x]$.
   (a) Determine the elements of $\mathbb{F}_9$ and their sums.
   (b) Let $\alpha = \overline{x}$. Compute $(1 + \alpha)(2 + \alpha)$ and $(1 + \alpha)^2$.
   (c) Determine $(1 + 2\alpha)^{-1}$.

3. Find the lattice of the subfields of: $\mathbb{F}_{2^7}$, $\mathbb{F}_{2^{15}}$, $\mathbb{F}_{2^{18}}$.

4. Determine the splitting field of:
   (a) $x^4 + x^3 + 1$ over $\mathbb{F}_2$
   (b) $x^3 + x^2 + x + 1$ over $\mathbb{F}_3$
   (c) $x^4 + 2x^2 + 2x + 2$ over $\mathbb{F}_3$

5. (a) Show that $f = x^4 + x + 1$ is irreducible over $\mathbb{F}_2$.
   (b) Find the primitive elements of $\mathbb{F}_{16} \cong \mathbb{F}_2[x]/(f)$.
   (c) Find the subfields of $\mathbb{F}_{16}$. For any subfield find its elements.
   (d) Decompose $x^{15} - 1$ in irreducible factors over $\mathbb{F}_2$.
   (e) Decompose $x^{15} - 1$ in irreducible factors over $\mathbb{F}_4$.

6. How many irreducible factor over $\mathbb{F}_2$ does the polynomial $x^{63} - 1$ admit? Which are their degrees?

7. An element $\xi \in \mathbb{F}_q$ is an *nth root of unity* if $\xi^n = 1$. The element ξ is a *primitive nth root of unity* provided $\xi^n = 1$ and $\xi^s \neq 1$ for any $0 < s < n$.

   Show that $\mathbb{F}_q$ contains a primitive nth root of unity if and only if n divides $q - 1$. In such a case find a primitve nth root of unity.

8. (a) What is the smallest field of characteristic 2 containing a primitive 9th root of unity?
   (b) What is the smallest field of characteristic 3 containing a primitive 11th root of unity?

9. Show that $\Sigma_{\alpha \in \mathbb{F}_q} \alpha = 0$, for any $q \neq 2$.

10. Let p be a prime number, $n \in \mathbb{N}$. Recall that $\mathbb{F}_{p^n}$ is an extension of $\mathbb{F}_p$ such that the Galois group $G = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is generated by the Frobenius automorphism $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $x \mapsto x^p$.

    Let m be a divisor of n. Consider the subgroup $H =< \varphi^m >$ and $L = Fix_{\mathbb{F}_{p^n}}(H)$ the subfield of $\mathbb{F}_{p^n}$ consisting on the elements fixed by all the automorphisms in H. Recall that $|L : \mathbb{F}_p| = |G : H|$. Show that:
    (a) H has order $\frac{n}{m}$
    (b) L has p^m elements
    (c) L is the unique subfield of $\mathbb{F}_{p^n}$ with p^m elements.