NAP 2019 - MODULE V - PROBLEM SET 1
DUE TUESDAY JULY 23, 2019, AT 24:00 KATHMANDU TIME

Justify all answers!

Exercise 1

Let $K_1 = \mathbb{F}_3(\alpha)$, $K_2 = \mathbb{F}_3(\beta)$, where α is a root of $X^2 + 1$ and β is a root of $X^2 + X + 2$.

a) Find the roots of $X^2 + 1$ in K_2.
b) How many isomorphisms are there between K_1 and K_2? Construct them explicitly.
c) Factorize the poynomial $X^9 - X$ over $\mathbb{F}_3$. How many irreducible polynomials of degree two are there in $\mathbb{F}_3[X]$?

Exercise 2

a) Prove that $X^6 + X^3 + 1$ is irreducible in $\mathbb{F}_2[X]$.
b) Let $K = \mathbb{F}_2(\alpha)$ where α is a root of $g(X)$. List the elements of each subfield of K. For each subfield L, determine an element β such that $L = \mathbb{F}_2(\beta)$.
c) Find elements of order 7 and 9 in $K^\times$. Determine a generator of the multiplicative group $K^\times$.

Exercise 3

Both $g(X) = X^3 - 2$ and $h(X) = X^3 + X^2 + 6X + 5$ are irreducible over $\mathbb{F}_7$. Let α be a root of $g(X)$ over $\mathbb{F}_7$.

a) Explain why the polynomial $h(X)$ must have 3 roots in $\mathbb{F}_7(\alpha)$.
b) Verify that one root is $\alpha^2 + \alpha + 2$.
c) Find the others two roots, (i.e. write them as $\mathbb{F}_7$-linear combinations of $1, \alpha, \alpha^2$).