NAP 2019 - MODULE V - Problem Set 1- Solutions

Due Tuesday July 23, 2019, at 24:00 Kathmandu time

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 $\mathbb{F}_3[X]$?

Solution

a) The generic element of K_2 is $a + b\beta$ with $a, b \in \mathbb{Z}_3$. We have

$$\begin{aligned}(a + b\beta)^2 &= a^2 + b^2\beta^2 + 2ab\beta \\ &= a^2 + b^2(-\beta - 2) + 2ab\beta \\ &= a^2 + b^2 + (b^2 - ab)\beta.\end{aligned}$$

By imposing $(a + b\beta)^2 = 2$ we find

$$\begin{cases} a^2 + b^2 &= 2 \\ b(a - b) &= 0 \end{cases} \qquad \text{that is} \quad a = b = \pm 1.$$

Therefore the two roots are $\pm(1 + \beta)$.

b) An isomorphism $K_1 \to K_2$ must send α in a root of $X^2 + 1$, that is one of $\pm(\beta + 1)$. Therefore there are two isomorphism θ_1, θ_2, defined by

$$\begin{aligned}\theta_1(a + b\alpha) &= a + b(\beta + 1) = a + b + b\beta \\ \theta_2(a + b\alpha) &= a - b(\beta + 1) = a - b - b\beta.\end{aligned}$$

c) We have

$$\begin{aligned}X^9 - X &= X(X^8 - 1) \\ &= X(X + 2)(X + 1)(X^2 + 1)(X^4 + 1) \\ &= X(X + 2)(X + 1)(X^2 + 1)(X^2 + X + 2)(X^2 + 2X + 2).\end{aligned}$$

Every irreducible polynomials of degree two in $\mathbb{Z}_3[X]$ must appear in the decomposition of $X^9 - X$: there are 3 such polynomials.

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 $K^\times$.

Solution.

a) If the polynomial $X^6 + X^3 + 1$ was reducible, then either it would have a factor of degree ≤ 2, or it would be a product of two irreducible polynomials of degree 3. It is immediately seen that it has no roots in $\mathbb{F}_2$ and that it is not divisible by X^2+X+1, which is the unique irreducible polynomial of degree 2. Moreover it is not a square, because it contains a term of odd degree. There are two irreducible polynomials of degree 3 in $\mathbb{F}_2[X]$: $X^3 + X + 1$ and $X^3 + X^2 + 1$, and

$$(X^3 + X + 1)(X^3 + X^2 + 1) \neq X^6 + X^3 + 1.$$

b) $\mathrm{Gal}(K/\mathbb{F}_2)$ is a cyclic group of order 6 generated by the Frobenius automorphism Φ. The lattice of subgroups is

$$\begin{tikzcd}
 & G \arrow[dl, dash] \arrow[dr, dash] & \\
H_1 \arrow[dr, dash] & & H_2 \arrow[dl, dash] \\
 & \{1\} &
\end{tikzcd}$$

where $H_1 = \langle \Phi^2 \rangle$ has order 3 and $H_2 = \langle \Phi^3 \rangle$ has order 2.
By Galois correspondence, K has two proper subfields

- $K_1 = K^{H_1} = \{\lambda \in K \mid \lambda^4 = \lambda\}$, such that $[K_1 : \mathbb{F}_2] = 2$; and
- $K_2 = K^{H_2} = \{\lambda \in K \mid \lambda^8 = \lambda\}$, such that $[K_2 : \mathbb{F}_2] = 3$.

The generic element of K can be written as

$$\lambda = a + b\alpha + c\alpha^2 + d\alpha^3.$$

We have

$$\begin{aligned}\alpha^6 =& \alpha^3+1\\ \alpha^7 =& \alpha^4+\alpha\\ \alpha^8 =& \alpha^5+\alpha^2\\ \alpha^9 =& \alpha^6+\alpha^3=1.\end{aligned}$$

Then we find

$$\lambda^4 = a + e\alpha + (c+f)\alpha^2 + d\alpha^3 + (b+e)\alpha^4 + c\alpha^5.$$

By imposing $\lambda = \lambda^4$ we obtain $b=c=e=f=0$, so that

$$K_1 = \{a + d\alpha^3 \mid a, d \in \mathbb{F}_2\} = \mathbb{F}_2(\alpha^3).$$

Moreover we have

$$\lambda^8 = (a+d) + c\alpha + b\alpha^2 + d\alpha^3 + (c+f)\alpha^4 + (b+e)\alpha^5.$$

By imposing $\lambda = \lambda^8$ we obtain $b = c = e+f, d = 0$, so that

$$K_2 = \{a+(e+f)\alpha+(e+f)\alpha^2+e\alpha^4+f\alpha^5 \mid a, d \in \mathbb{F}_2\} = \mathbb{F}_2(\alpha+\alpha^2+\alpha^4).$$

c) We already found that α as order 9 in $K^\times$. In order to find an element of order 7 notice that $K_2^\times$ is cyclic of order 7 (a prime number) so that it is generated by any its non trivial element. We can take for example $\alpha+\alpha^2+\alpha^4$. Since 7 and 9 are coprime, (and $K^\times$ is an abelian group!) $\alpha(\alpha+\alpha^2+\alpha^4) = \alpha^2+\alpha^3+\alpha^5$ has order 63, hence it is a generator of $K^\times$.

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 $1, \alpha, \alpha^2$).

Solution

a) Let β be a root of $h(X)$ in a splitting field of $h(X)$ over $\mathbb{F}_7$. Then $|\mathbb{F}_7(\beta)| = 7^3 = |\mathbb{F}_7(\alpha)|$. Since two finite fields of the same order are isomorphic, $\mathbb{F}_7(\alpha)$ contains a root of $h(X)$. Since $\mathbb{F}_7(\alpha)/\mathbb{F}_p$ is normal, it contains all the roots.
b) Using the fact that $\alpha^3 = 2$ we obtain

$$(\alpha^2 + \alpha + 2)^2 = 5\alpha^2 + 6\alpha + 1$$
$$(\alpha^2 + \alpha + 2)^3 = 3\alpha^2 + 2\alpha + 3.$$

and the claim follows
c) The other two roots are the conjugates of $\alpha^2+\alpha+2$ over $\mathbb{F}_7$, that is its images through the authomophisms in $\mathrm{Gal}(\mathbb{F}_7(\alpha)/\mathbb{F}_7) = \langle\Phi\rangle$; namely

$$\begin{aligned}\Phi(\alpha^2 + \alpha + 2) &= \alpha^{14} + \alpha^7 + 2\\ &= 2\alpha^2 + 4\alpha + 2\\ \Phi^2(\alpha^2 + \alpha + 2) &= \alpha^{98} + \alpha^{49} + 2\\ &= 4\alpha^2 + 2\alpha + 2.\end{aligned}$$