1 Introduction to Galois theory assignmens 1

Problem 1.1 *Consider polynomial $P(X) = X^4 + X^3 + 1$. Is it true P*

(a) irreducible over $\mathbb{F}_2$

(b) has a root in $\mathbb{F}_4$

(c) irred. over $\mathbb{F}_4$

(d) irred. over $\mathbb{F}_8$

(e) has a root in $\mathbb{F}_{16}$

(f) has a root in $\mathbb{F}_{32}$

(g) has a root in $\mathbb{F}_{64}$

(h) irred. over $\mathbb{F}_{64}$

Solution: For (a), True. Because if not it can be factored as polynomial with degree 1 and 3 or degree 2 and degree 2.

All possible linear factor are only X and $X+1$, but $P = X(X^3+X^2)+1$ and $P = (X+1)X^3+1$ hence not factorable by degree 1×3. All possible quadratic polynomials are $X^2, X^2+1, X^2+X, X^2+X+1$, but $P = X^2(X^2+X)+1$ and $P = (X^2+1)(X^2+X+1)+X$ hence can not be factored as 2×2.

For (b), False. Because $\mathbb{F}_4 = \mathbb{F}_2/(X^2+X+1) = \mathbb{F}_2[\alpha] = \{0, 1, \alpha, 1-\alpha\}$ and $\alpha(1-\alpha) = 1$, hence $P(\alpha) = \alpha \neq 0$ and $P(1-\alpha) = 1-\alpha \neq 0$.

For (c), False. Although it doesn't have root, and having no linear factor. But note in $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$, $\alpha^2 = 1-\alpha = 1+\alpha$ and $(1+\alpha)^2 = \alpha$, and $\alpha^3 = \alpha(1-\alpha) = 1$. And it's easy to see

$$P = (X^2 + \alpha X + \alpha) \cdot (X^2 + \alpha^2 X + \alpha^2)$$

For (d), True. Because P is irred. on $\mathbb{F}_2$, any field containing one root must be at least of dimension 4. Hence no linear factor.

Let $\mathbb{F}_8 = \mathbb{F}_{2^3} = \mathbb{F}[\alpha]$ where α is a root of X^3+X^2+1. Because $(\mathbb{F}_8)^*$ is cyclic, it is generated by α. But the addtive group structure is generate by base vector

$$\begin{array}{rcl} (1,0,0) & = & 1 \\ (0,1,0) & = & \alpha \\ (0,0,1) & = & \alpha^2 \end{array}$$

And more over we have,

$$\begin{array}{rcccl} \alpha^3 & = & 1+\alpha^2 & = & (1,0,1) \\ \alpha^4 & = & 1+\alpha+\alpha^2 & = & (1,1,1) \\ \alpha^5 & = & 1+\alpha & = & (1,1,0) \\ \alpha^6 & = & \alpha+\alpha^2 & = & (0,1,1) \end{array}$$

If $P = (X^2 + AX + C)(X^2 + BX + D)$ then we have

$$CD = 1, (AD + BC) = 0, (D + C + AB) = 0, (A + B) = 1$$

Because any quadratic with two terms is reducible, we assume $ABCD \neq 0$ and Let $A = \alpha^a, B = \alpha^b, C = \alpha^c, D = \alpha^d$, using the above lookup table it's easy to enumerate all possbile $a, b, c, d \in \{0, \dots, 6\}$ and confirm there is no such satisfying the required relation.

For (e), True. $\mathbb{F}_{2^4}$ is stem and splittig field of any irred. polynomial of degree 4.

For (f), False. Because $4 \nmid 5$ hence $\mathbb{F}_{2^4} \not\subseteq \mathbb{F}_{2^5}$.

For (g), False. Because $4 \nmid 6$ hence $\mathbb{F}_{2^4} \not\subseteq \mathbb{F}_{2^6}$.

For (h), False. Because $2 \mid 6$ hence $\mathbb{F}_{2^2} \subset \mathbb{F}_{2^6}$. And P factors over $\mathbb{F}_4$. $\square$