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 $\mathbb{F}_4$. $\square$

Problem 1.2 *Set $\zeta = e^{\frac{2i\pi}{7}}$ and let $L = \mathbb{Q}(\zeta)$. Let $M = L \cap \mathbb{R}$.*

(a) Let p be prime. Prove $X^{p-1} + X^{p-2} + \cdots + X + 1 = \frac{X^p - 1}{X - 1}$ is irreducible over $\mathbb{Q}$ (hint: Eisenstein)

(b) Find the minimal polynomial of ζ over $\mathbb{Q}$ and the degree of L over $\mathbb{Q}$.

(c) Find the minimal polynomial of ζ over M (hint: $\zeta + \frac{1}{\zeta}$) and the degree $[L : M], [M : \mathbb{Q}]$.

(d) Let f be an automorphism of L over $\mathbb{Q}$. List all possibilities for $f(\zeta)$ then for $f(cos(2\pi/7))$.

Solution: For (a), Let $X = y + 1$, then the polynomial is

$$\frac{(1 + y)^p - 1}{1 + y - 1} = \frac{y^p + py^{p-1} + \cdots + py + 1 - 1}{y} = y^{p-1} + py^{p-2} + \cdots + p$$

Using Eisenstein criterion, it's irreducible, hence original polynomial must be irreducible.

For (b), it's a root of $X^7 - 1 = 0$, using (a), we know the minimal polynomial is $X^6 + X^5 + \cdots + 1$. And $[L : \mathbb{Q}] = 6$.

For (c), Because two dimension space need at most two independent vectors to generate. ζ have only degree 2 over $\mathbb{R}$. Actually because $\zeta + \frac{1}{\zeta} = \gamma \in L \cap \mathbb{R}$ we have $\zeta^2 + 1 = \gamma\zeta$ which means it's a minimal polynomial over $M = L \cap \mathbb{R}$. Then $[M : \mathbb{Q}] = 2$ and $[L : M] = 3$.

For (d), $f(\zeta)$ must be a root of $X^6 + X^5 + \cdots + 1$. And using stem field structure, any $\zeta \mapsto \zeta^i, i = 1, \dots, 6$ exists. So all possible $f(\zeta)$ are $\zeta^i, i = 1, \dots, 6$ And $f(\cos(2\pi/7)) = f(\frac{\zeta + \zeta^{-1}}{2})$, hence all possibilities are $\cos(2k\pi/7), k = 1, \dots, 6$. $\square$

Problem 1.3 *Which of the following algebras are fields? Products of fields? Describe these fields.*

(a) $\mathbb{Q}(\sqrt[3]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$

(b) $\mathbb{Q}(\sqrt[4]{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$

(c) $\mathbb{F}_2(\sqrt{T}) \otimes_{\mathbb{F}_2(T)} \mathbb{F}_2(\sqrt{T})$

(d) $\mathbb{F}_4(\sqrt[3]{T}) \otimes_{\mathbb{F}_4(T)} \mathbb{F}_4(\sqrt[3]{T})$

Solution: For (a), it's field, equal to $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$.

For (b), it's product of fields, equal to $\mathbb{Q}(\sqrt{2})[X]/(X^2-\sqrt{2})\times\mathbb{Q}(\sqrt{2})[X]/(X^2+\sqrt{2})$. This is from

$$\mathbb{Q}(\sqrt{2})\otimes_{\mathbb{Q}}\mathbb{Q}[X]/(X^4-2) = \mathbb{Q}(\sqrt{2})[X]/(X^4-2) = \mathbb{Q}(\sqrt{2})[X]/(X^2-\sqrt{2})\times\mathbb{Q}(\sqrt{2})[X]/(X^2+\sqrt{2})$$

For (c), it's neither field nor product of field. Actually it's

$$\begin{aligned}
&\mathbb{F}_2(\sqrt{T}) \otimes_{\mathbb{F}_2(T)} \mathbb{F}_2(\sqrt{T}) \\
=&\mathbb{F}_2(\sqrt{T}) \otimes_{\mathbb{F}_2(T)} \mathbb{F}_2(T)[X]/(X^2-T) \\
=&\mathbb{F}_2(\sqrt{T})[X]/(X^2-T) \\
=&\mathbb{F}_2(\sqrt{T})[X]/(X-\sqrt{T})^2
\end{aligned}$$

having nilpotents

For (d), it's product of fields, actually

$$\begin{aligned}
&\mathbb{F}_4(\sqrt[3]{T}) \otimes_{\mathbb{F}_4(T)} \mathbb{F}_4(\sqrt[3]{T}) \\
=&\mathbb{F}_4(\sqrt[3]{T}) \otimes_{\mathbb{F}_4(T)} \mathbb{F}_4(T)[X]/(X^3-T) \\
=&\mathbb{F}_4(\sqrt[3]{T})[X]/(X^3-T) \\
=&\mathbb{F}_4(\sqrt[3]{T})[X]/((X-\sqrt[3]{T})\cdot(X^2+\sqrt[3]{T}X+\sqrt[3]{T^2})) \\
=&\mathbb{F}_4(\sqrt[3]{T})[X]/((X-\sqrt[3]{T})\times\mathbb{F}_4(\sqrt[3]{T})[X]/(X^2+\sqrt[3]{T}X+\sqrt[3]{T^2}))
\end{aligned}$$

$\square$