1 Problem about Finite Fields

Question a)

P is irreducible over $\mathbb{F}_2$

It can be checked that P has no roots in $\mathbb{F}_2$, so it has no factors of order 1.

The only possible irreducible factor of order 2 is $X^2 + X + 1$, but

$$(X^2 + X + 1)^4 = X^4 + X^2 + 1 \neq X^4 + X^3 + 1.$$

Degression

The Polynomial P has degree 4, which means it has 4 roots in $\mathbb{F}_{16}$ which cicle under Frobenius isomorphism $f(x) = x^2$. Denote them by

$$A_1 \to A_2 \to A_3 \to A_4 \to A_1.$$

Moreover, we can express this roots:

Denote by $A_1 = a$ the first root and use it as ptimitive element of $\mathbb{F}_{16}$ over $\mathbb{F}_2$, so

$$a^4 = a^3 + 1.$$

Then

$$A_2 = a^2$$
$$A_3 = a^4 = a^3 + 1$$
$$A_4 = a^8 = (a^3 + 1)^2 = a^6 + 1 = a^3 + a^2 + a$$

Question b)

P has no roots in $\mathbb{F}_4$.

If it was the case then there would be a root A_i such that $f^2(A_i) = A_i^4 = A_i$. But we can see that this is not true.

Question c)

P is not irreducible in $\mathbb{F}_4$.

Note that $A_1 + A_3, A_2 + A_4, A_1A_3, A_2A_4 \in \mathbb{F}_4$ as

$$(A_1 + A_3)^2 = A_1^2 + A_3^2 = A_2 + A_4$$
$$(A_2 + A_4)^2 = A_2^2 + A_4^2 = A_3 + A_1$$
$$(A_1A_2)^2 = A_1^2A_3^2 = A_2A_4$$
$$(A_2A_4)^2 = A_2^2A_4^2 = A_3A_1$$

Moreover,

$$A_1 + A_3 = a^3 + a + 1 = a(a^3 + 1) = A_1A_3$$
$$A_2 + A_4 = a^3 + a = a^2(a^3 + a^2 + 1) = A_2A_4.$$

So we can factor P as

$$P(X) = (X+A_1)(X+A_2)(X+A_3)(X+A_4) = (X^2+(A_1+A_3)X+A_1A_3)(X^2+(A_2+A_4)X+A_2A_4) = \\ = (X^2+bX+b)(X^2+(b+1)X+b+1)$$

where b is a primitive element of $\mathbb{F}_4$ over $\mathbb{F}_2$.

question d)

P is Irreducible over $\mathbb{F}_8$.

$\mathbb{F}_8 = \mathbb{F}_{2^3}$ does not contain isomorphic copy of $\mathbb{F}_4 = \mathbb{F}_{2^2}$ as 2 and 3 are coprime. This means that it is impossible to properly embed A_1A_3 and A_2A_4 into $\mathbb{F}_8$ which implies irreducibility.

question e)

As it was shown in "Degression", P has four roots in $\mathbb{F}_{16}$.

question f)

P has no roots in $\mathbb{F}_{32} = \mathbb{F}_{2^5}$ as every root of P will generate subfield isomorphic to $\mathbb{F}_{16} = \mathbb{F}_{2^4}$, however 4 and 5 are coprime, so F_{32} has no such subfield.

question g)

P has no roots in $\mathbb{F}_{64} = \mathbb{F}_{2^6}$ as every root of P will generate subfield isomorphic to $\mathbb{F}_{16} = \mathbb{F}_{2^4}$, however 4 is not a divisor of 5, so F_{64} has no such subfield.

question h)

P is not irreducible in $\mathbb{F}_{64}$ as it contains an isomorphic copy of $\mathbb{F}_4$ so factorization from question c) will work.