

$$A) \text{ let } t^2 + 2, \text{ let } t^2 + t + 1 = (t^2 + 2) + t - 1$$

(6)

There ~~3~~⁶ more quadratic polynomials over \mathbb{Z}_3 :

$t^2 + 2t + 1$ which has a zero 2 (of multiplicity 2)

$t^2 + 2t$ which has a zero 0 (and 1)

$t^2 + t + 1$ which has a zero 1 (of multiplicity 2)

The three polynomials above are all reducible (since they have zeros in \mathbb{Z}_3) so f, g, h are the only irreducible polynomials over \mathbb{Z}_3

ii) $m(t) = t^4 + t + 2$

$m(0) = 0^4 + 0 + 2 = 2 \pmod{3}$

$m(1) = 1^4 + 1 + 2 = 4 \equiv 1 \pmod{3}$

$m(2) = 2^4 + 2 + 2 = 20 \equiv 2 \pmod{3}$

m has no zeros in \mathbb{Z}_3 . It is irreducible over \mathbb{Z}_3 .

9 expect better of you. All this says is that m has no zeros in \mathbb{Z}_3 . Must check whether m has quadratic factors, i.e. whether f, g, h are factors of m . But $m \equiv t^4 + t + 2 \pmod{3}$ and $f = (t^2 + 2t + 1) + t$

iii) Consider the Galois group of K over \mathbb{Z}_3 .

Since K is a finite field of order 3^4 , K has order 4 over \mathbb{Z}_3 so we can consider K as a vector space over \mathbb{Z}_3 of dimension 4, so $[K : \mathbb{Z}_3] = 4$, and there exists an irreducible polynomial of degree 4 over \mathbb{Z}_3 such that

the zeros of f are $\alpha, \alpha^3, \alpha^9, \alpha^{27}$. But all finite fields are cyclic, generated by a single element

$K = \mathbb{Z}_3(\alpha)$, and all finite fields of same order are isomorphic, so if α' is any other generating member of a field K' of order 81 (which will have prime subfield \mathbb{Z}_3) then $K' \cong K$ and

$\mathbb{Z}_3(\alpha) \cong \mathbb{Z}_3(\alpha')$, so there exists an element $\alpha \in K$ such that $K \cong \mathbb{Z}_3(\alpha)$ for any field K of order 81. m' also has degree 4 and m is irreducible so if α' is a zero of m' then $\mathbb{Z}_3(\alpha') \cong \mathbb{Z}_3(\alpha) = K$ and the case is proved.

Now take your iso $\phi: \mathbb{Z}_3(\alpha) \rightarrow K$. Then $\alpha = \phi(\alpha)$ is the required element. One problem is that the polynomial that gives rise to an extension of a field (in this case \mathbb{Z}_3) is not unique. e.g. $t^4 + 2t + 2$ is also irreducible of degree 4.

iv) $m(\alpha^3 + \alpha^2 + \alpha)$

$= (\alpha^3 + \alpha^2 + \alpha)^4 + \alpha^3 + \alpha^2 + \alpha + 2$

$= \alpha^4(\alpha^2 + \alpha + 1)^4 + \alpha^3 + \alpha^2 + \alpha + 2$

$\alpha^4 + \alpha + 2 = 0 \Rightarrow \alpha^4 = -\alpha - 2 = 2\alpha + 1$

$m(\alpha^3 + \alpha^2 + \alpha) = (2\alpha + 1)(\alpha^4 + \alpha^2 + 1 + 2\alpha^3 + 2\alpha^2 + 2\alpha)^2 + \alpha^3 + \alpha^2 + \alpha + 2$

$= (2\alpha + 1)(2\alpha + 1 + 2\alpha^3 + 2\alpha + 1)^2 + \alpha^3 + \alpha^2 + \alpha + 2$

$= (2\alpha + 1)(2\alpha^3 + \alpha + 2)^2 + \alpha^3 + \alpha^2 + \alpha + 2$

$= (2\alpha + 1)(\alpha^6 + \alpha^4 + 2\alpha^3 + \alpha^2 + \alpha + 1) + \alpha^3 + \alpha^2 + \alpha + 2$

$= (2\alpha + 1)(\alpha^6 + \alpha^4 + 2\alpha^3 + \alpha^2 + \alpha + 1) + \alpha^3 + \alpha^2 + \alpha + 2$