(1) Describe the elements of $\mathbb{Q}(\sqrt[3]{5})$.

$$\alpha^3 - 5 = 0$$

$$\pm \frac{\text{divisors of } 5}{\text{divisors of } 1} = \pm 5, \pm 1$$

clearly none of $\pm 5, \pm 1$ satisfy $\alpha^3 - 5 = 0$

so it is irreducible.

$$[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$$

$$1, \alpha, \alpha^2$$

$p(\alpha) = a + b\alpha + c\alpha^2 = 0$, $a, b, c \in \mathbb{Q}$

note α is a root

so $p \in \mathbb{Q}[x]$ and degree at most 2.

so, $\alpha = \sqrt[3]{5}$ bc $\Rightarrow x^3 - 5 = 0$

so, the min irreducible over $\mathbb{Q}$, $f(\alpha) = \alpha^3 - 5$

$\Longrightarrow$ p is a multiple of f.

and since $p(\alpha) = 0$, either $p(\alpha)$ is the zero poly or

$f(\alpha) \mid p(\alpha)$ in $\mathbb{Q}[x]$

but nonzero mults of f must have degree of at least 3.

so $P(\alpha)=0$ must be zero poly.

$\implies a=b=c=0.$

$\mathbb{Q}(\sqrt[3]{5})$ is spanned by $\{1, \alpha, \alpha^2\}$

$S=\{a+b\alpha+c\alpha^2 : a, b, c \in \mathbb{Q}\}$

so, $\dim(\mathbb{Q}(\alpha))=3$ and $|\{1, \alpha, \alpha^2\}|=3$

$\implies \{1, \alpha, \alpha^2\}$ is a basis!

thus elts will look like

$$\mathbb{Q}(\sqrt[3]{5}) = \{a+\sqrt[3]{5}(b)+\sqrt[3]{25}(c) : a, b, c \in \mathbb{Q}\}$$

(2) Show that $\mathbb{Q}(4-\sqrt{-1}) = \mathbb{Q}(\sqrt{-1})$

1) $\mathbb{Q}(4-\sqrt{-1}) \subseteq \mathbb{Q}(\sqrt{-1}) = \{a+bi : a,b \in \mathbb{Q}\}$

so $4-i = 4+(-1)i$

$a=4$, $b=-1 \in \mathbb{Q} \Rightarrow 4-i \in \mathbb{Q}(i)$

so, $\mathbb{Q}(i)$ field, contains $\mathbb{Q}$, and $4-i \Rightarrow \mathbb{Q}(4-i) \subseteq \mathbb{Q}(i)$

2) $\mathbb{Q}(i) \subseteq \mathbb{Q}(4-\sqrt{-1})$

Sup. $\alpha = 4-i$

$$\left.\begin{array}{l} \text{so } \alpha \in \mathbb{Q}(4-i) \text{ by defn.} \\ 4 \in \mathbb{Q}(4-i) \text{ by defn.} \end{array}\right\} (*)$$

so, $i = 4-\alpha \in \mathbb{Q}(4-i) \Rightarrow$

so, $i \in \mathbb{Q}(4-i) \Rightarrow \mathbb{Q}(i) \subseteq \mathbb{Q}(4-i)$

(3) Show that $f(x)$ and $f(x+a)$ have the same splitting field if $a \in \mathbb{F}$ and $f \in \mathbb{F}[x]$

$\mathbb{F}[x]$, $f(x) = c_n x^n + \dots + c_1 x + c_0$ w/ $c_i \in \mathbb{F}$.

Suppose $a \in \mathbb{F}$ and $f \in \mathbb{F}[x]$ and suppose that α is a root of f.

so, $f(\alpha) = 0$.

so, let $\beta + a = \alpha$

so, $f(\beta + a) = f(\alpha) = 0 \Rightarrow \beta$ is a root of $f(x+a)$

Let E be splitting field of $f(x)$ over $\mathbb{F}$.

so, $E = F(\alpha_1, \dots, \alpha_n)$, α_i roots of f.

Note each $\alpha_i = (\alpha_i - a) + a$, and since $a \in F$

so, $F(\alpha_1, \dots, \alpha_n) = F(\alpha_1 - a, \dots, \alpha_n - a)$

and each $\alpha_i - a$ are the roots of $f(\beta + a)$

Similarly, any splitting field of g is also one for f.

so, the splitting fields $f(x)$ and $f(x+a)$ must coincide.

(4) Find an extension field where $f(x) = x^3+2x+1 \in \mathbb{Z}/3\mathbb{Z}$ factors, and indicate the factors into which f splits. ($\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$)

$f(0) = 1$, $f(1) = 1+2+1 = 4$, $f(2) = 8+4+1 = 13 \equiv 1$

No root in $\mathbb{F}_3 \Rightarrow f$ irreducible in $\mathbb{F}_3$.

Let $E = \mathbb{F}_3[t]/(t^3+2t+1)$, $\alpha \leftarrow$ class of t.

then $\alpha^3 + 2\alpha + 1 = 0 \Rightarrow \alpha$ root of f

So in $E[x]$, $f(x) = x^3+2x+1 = (x-\alpha)\underbrace{g(x)}_{\text{some quadratic fcn.} \in E[x]}$

By Synthetic division over E.

$$g(x) = x^2 + \alpha x + (\alpha^2+2)$$

So, $f(x) = (x-a)\,(x^2 + \alpha x + \alpha^2 + 2)$

$$\text{disc} = \alpha^2 - 4(\alpha^2+2)$$

$4 \equiv 1 \Rightarrow \text{disc} = \alpha^2 - (\alpha^2+2) = -2 \equiv 1$

Roots $\Rightarrow$ $x = \dfrac{-\alpha \pm \sqrt{\text{disc}}}{2} = \dfrac{-\alpha \pm 1}{2}$

Note in $\mathbb{F}_3$ $2^{-1} \equiv 2$, so $\beta_1 = 2(-\alpha+1) = 2 - 2\alpha$

$$\beta_2 = 2(-\alpha - 1) = -2\alpha - 2 \equiv 1 - 2\alpha$$

So, $x^2 + \alpha x + \alpha^2 + 2 = (x - \beta_1)(x - \beta_2)$

$$= (x - (2 - 2\alpha))(x - (1 - 2\alpha))$$

So, $x^3 + 2x + 1 = (x - \alpha)(x - (2 - 2\alpha))(x - (1 - 2\alpha))$

splits into

(5) Show that $x^{21} + 2x^8 + 1$ only has simple roots in any extension of $\mathbb{Z}/3\mathbb{Z}$. On the other hand, show that $f(x) = x^{21} + 2x^9 + 1$ does have multiple roots over some extension of $\mathbb{Z}/3\mathbb{Z}$.

1) $f(x) = x^{21} + 2x^8 + 1$

$f'(x) = 21x^{20} + 16x^7 \equiv 0x^{20} + (1)x^7$

$f'(x) = x^7$

$g(0) = 1 \in \mathbb{F}$

so let $h(x)$ be a poly.

if $h(x) \mid x^7$ and $h(x) \mid f(x) \Rightarrow h(x) \mid g(0) = 1$

But only divisors of 1 in a poly. ring are units

$\Rightarrow \gcd(f(x), x^7) = 1 \Rightarrow$ No multiple roots in any extension field of $\mathbb{F}$.

2) $f(x) = x^{21} + 2x^9 + 1 \in \mathbb{F}[x]$

$f'(x) = 21x^{20} + 18x^8 \equiv 0x^{20} + 0x^8 \equiv 0$

$f'(x) = 0 \leftarrow$ zero poly!

$\gcd(f, f') = \gcd(f, 0) = f \neq 1$

$\Rightarrow$ f must have multiple roots in some extension.

factor f: $(a+b+c)^3 = a^3 + b^3 + c^3$

because coeffs. $\binom{3}{1}, \binom{3}{2} \equiv 0$ in $\mathbb{F}_3$.

$$(x^7 + 2x^3 + 1)^3 = (x^7)^3 + (2x^3)^3 + 1^3$$
$$= x^{21} + 2^3 x^9 + 1$$
$$\equiv x^{21} + 2x^9 + 1 = f(x)$$

Next, let E be the splitting field of $x^7 + 2x^3 + 1 = h(x)$

By defn $\Rightarrow$ α is a root $\in E$

$f(x) = h(x)^3$ and $h(x) = (x - \alpha)\, q(x)$

$\Longrightarrow f(x) = h(x)^3 = (x-\alpha)^3 q(x)^3$

so in E, α is a root of mult 3.

$\Longrightarrow$ must have multiple roots in E.