Q3

Ch 21.5

Q3.

(a) $x^4 - 10x^2 + 21 = 0$

$x^4 - 10x^2 + 25 = 4$

$(x^2 - 5)^2 = 4$

$x^2 - 5 = \pm 2$

$x^2 = 3, 7$

$x = \pm\sqrt{3}, \pm\sqrt{7}$

The splitting field is $\mathbb{Q}(\sqrt{3}, \sqrt{7})$

(b) $x^4 + 1 = 0$

$x^4 = -1$

$x = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i, -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$

The splitting field is $\mathbb{Q}(\sqrt{2}, i)$

(c) $\mathbb{F}_{27} = \mathbb{Z}_3 / (x^3 + 2x + 2) = \mathbb{Z}_3(\bar{x})$.

$\bar{x}$ is a root of x^3+2x+2 in $\mathbb{F}_{27}$. Thus $\bar{x}^3 + 2\bar{x} + 2 = 0$.

char $\mathbb{F}_{27} = 3$.

$(\bar{x}^3 + 2\bar{x} + 2)^3 = \bar{x}^9 + 6\bar{x}^7 + 6\bar{x}^6 + 12\bar{x}^5 + 24\bar{x}^4 + 20\bar{x}^3 + 24\bar{x}^2 + 24\bar{x} + 8$

$= \bar{x}^9 + 20\bar{x}^3 + 8$

$= \bar{x}^9 + 2\bar{x}^3 + 2$

$= (\bar{x}^3)^3 + 2\bar{x}^3 + 2$

$= (\overline{x+1})^3 + 2(\overline{x+1}) + 2$

$= 0$

$\overline{x+1}$ is a root of x^3+2x+2.

Similarly, we get $(\overline{x+1}^3)^3 + 2(\overline{x+1}^3) + 2 = 0$. Thus, $\overline{x+1}^3 = \overline{x+2}$ is a root of x^3+2x+2.

Thus, $\mathbb{Z}_3(\text{all roots}) \subseteq \mathbb{F}_{27}$. Since $\mathbb{F}_{27} = \mathbb{Z}_3(\bar{x})$, $\mathbb{F}_{27} \subseteq \mathbb{Z}_3(\text{all roots})$.

Therefore $\mathbb{Z}_3$ (all roots) = $\mathbb{F}_{27}$.

$\mathbb{F}_{27} = \mathbb{Z}_3/(x^3+2x+2)$ is the splitting field.

(d) $x^3 - 3 = 0$

$\frac{1}{3}x^3 = 1$

$(\frac{1}{\sqrt[3]{3}}x)^3 = 1$

$\frac{1}{\sqrt[3]{3}}x = 1, \zeta_3, \zeta_3^2$

$x = \sqrt[3]{3}, \sqrt[3]{3}\zeta_3, \sqrt[3]{3}\zeta_3^2$

Thus, splitting field is $\mathbb{Q}(\sqrt[3]{3}, \zeta_3)$.

Q17

17.

Proposition 3. *Let E be the algebraic closure of a field F. Then every polynomial $p(x)$ in $F[x]$ splits in E.*

Proof. Suppose $p(x) \in F[x]$.
We will proceed with proof by induction on $\deg p(x)$.
Base case:
If $\deg p(x) = 1$, then we have by definition that $p(x)$ is itself a linear factor in $E[x]$ (as $F \subset E$), and therefore $p(x)$ splits in E.
Inductive hypothesis:
Suppose polynomials of degree n split in E.
Suppose $\deg p(x) = n + 1$.
We know that $p(x)$ has some root α in an extension field E' of F.
Then we may observe that α is by definition algebraic over F and thus $\alpha \in E$ as E contains all the elements algebraic over F.
Hence $p(x)$ has a root in E and thus $p(x) = (x - \alpha)g(x)$ with $g(x) \in E[x]$.
Observe by the additivity of degree over multiplication that $\deg g(x) = n$.
By the inductive hypothesis we have that $g(x)$ splits in E, and thus we have shown that $p(x)$ splits in E.

$\square$

Q25

25.

Proposition 7. *Let E be a field extension of F and $\alpha \in E$. Determine $[F(\alpha) : F(\alpha^3)]$.*

Proof. First observe that $f(x) = x^3 - \alpha^3 \in F(\alpha^3)[x]$ has a root at $x = \alpha$. As the minimal polynomial for α over $F(\alpha^3)$ by definition is the polynomial with α as a root of minimal degree, it follows that the minimal polynomial for α over $F(\alpha^3)$ has degree at most 3, and therefore

$$1 \leq [F(\alpha) : F(\alpha^3)] \leq 3$$

To show that this is indeed the tightest bound we can give, it suffices to provide examples of F and α with degree of extension $1, 2$, and 3.

Example 1:
Let $F = \mathbb{Q}$ and $\alpha = 1$.
Obviously then $\alpha^3 = \alpha$ and thus $F(\alpha) = F(\alpha^3)$, or $[F(\alpha) : F(\alpha^3)] = 1$.
Example 2:
Let $F = \mathbb{Q}$ and $\alpha = \zeta_3$, the third root of unity.
We know $\Phi_3(x)$ is the minimal polynomial of ζ_3 over $\mathbb{Q}$ and has degree 2.
Furthermore $(\zeta_3)^3 = 1$, so $\mathbb{Q}((\zeta_3)^3) = \mathbb{Q}$.
Hence $[F(\alpha) : F(\alpha^3)] = 2$.
Example 3:
Let $F = \mathbb{Q}$ and $\alpha = \sqrt[3]{2}$.
Note Eisenstein's Criterion with $p = 2$ gives us that $f(x) = x^3 - 2$ is irreducible, and thus $f(x)$ is a degree 3 minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$.
Furthermore $(\sqrt[3]{2})^3 = 2$, so $\mathbb{Q}((\sqrt[3]{2})^3) = \mathbb{Q}$, and thus $[F(\alpha) : F(\alpha^3)] = 3$.

We have thus shown that the tightest bound is $1 \leq [F(\alpha) : F(\alpha^3)] \leq 3$. $\square$