Problem 1

a) F
b) T
c) F
d) T
e) T

Problem 2

a) The minimal polynomial of α over F is the monic polynomial $p(x)$ of smallest degree satisfying $p(\alpha)=0$.

b) If $\varphi: R \to S$ is a ring homomorphism and $I \subseteq R$ is an ideal containing $\ker(\varphi)$, then φ descends to the quotient to a ring homomorphism

$$\bar{\varphi}: R/I \to S$$

defined by $\bar{\varphi}(r+I) = \varphi(r)$

(c) $R = \mathbb{Z}[x]$, $I = \langle x \rangle$ is prime but not maximal

because $R/I \cong \mathbb{Z}$ integral domain but not field

Problem 3

(a) $\operatorname{irr}(\sqrt{\sqrt{3}+\sqrt{5}}, \mathbb{Q}) = (x^4-8)^2 - 60$
$= x^8 - 16x^4 + 4$

so $[E:\mathbb{Q}] = 8$

(b)

$\frac{1}{2}\left[(\sqrt{\sqrt{3}+\sqrt{5}})^4 - 8\right] = \sqrt{15} \in E$ so therefore

$\frac{1}{2}\left[\sqrt{15}\,(\sqrt{3}+\sqrt{5}) - 3(\sqrt{3}+\sqrt{5})\right] = \sqrt{3} \in E$

Thus $\mathbb{Q}(\sqrt{3}) \subseteq E$.

(c) $\operatorname{irr}(\sqrt{3}, \mathbb{Q}) = x^2 - 3$ so $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$.

Since $[E:\mathbb{Q}] = [E:\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}]$
we see $8 = [E:\mathbb{Q}(\sqrt{3})] \cdot 2$ so $[E:\mathbb{Q}(\sqrt{3})] = 4$.

Alternative proof: $\operatorname{irr}(\sqrt{3}+\sqrt{5}, \mathbb{Q}(\sqrt{3})) = (x^2 - \sqrt{3})^2 - 5$

$= x^4 - 2\sqrt{3}x^2 - 2$

and since $E = \mathbb{Q}(\sqrt{3})(\sqrt{3}+\sqrt{5})$, $[E:\mathbb{Q}(\sqrt{3})] = 4$.

Problem 4: By Euclidean algorithm
$f(x) = g(x)(x^2+x+1) + h(x)$ with $\deg(h(x)) \leq 1$.

a) so
$f(x) + I = h(x) + I$ with $\deg(h(x)) \leq 1$.

Thus without loss of generality

$$f(x) + I = ax + b + I$$

Also since $3 \in I$, a and b can be reduced modulo 3, making

$$R/I = \{ax+b+I \mid a, b \in \{0,1,2\}\}$$

b) Note $x^2+x+1 = (x-1)^2 + 3x$ so

$$((x-1)+I)((x-1)+I) = (x-1)^2 + I$$
$$= x^2+x+1 - 3x + I = 0 + I$$

Thus R/I has zero divisors and I is not prime.

c) Let $J = \langle 3, x-1 \rangle$. Then

$$R/J = \{ a + I \mid a \in \{0,1,2\} \} \cong \mathbb{Z}/_3$$

is a field, so J is maximal. Also

$$3 \in J \quad \text{and} \quad x^2+x+1 = (x-1)^2 + 3x \in J$$

and therefore $I \subseteq J$.

Problem 5: Find all automorphisms $\mathbb{Q}(\alpha)$, $\alpha = \sqrt{1-\sqrt{5}}$

$\operatorname{irr}(\alpha, \mathbb{Q}) = (x^2-1)^2 - 5 = x^4 - 2x^2 - 4$ so

$\mathbb{Q}(\alpha) = \operatorname{span}_{\mathbb{Q}} \{1, \alpha, \alpha^2, \alpha^3\}$.

Let $\varphi \in \operatorname{Aut}(\mathbb{Q}(\alpha))$. Then

$$\varphi(a + b\alpha + c\alpha^2 + d\alpha^3) = a + b\varphi(\alpha) + c\varphi(\alpha)^2 + d\varphi(\alpha)^3$$

so φ is determined by $\varphi(\alpha)$!!

Note $(\varphi(\alpha)^2 - 1)^2 - 5 = \varphi(\alpha)^4 - 2\varphi(\alpha)^2 + 1 - 5$
$= \varphi(\alpha^4 - 2\alpha^2 - 4) = \varphi(0) = 0$

and therefore $\varphi(\alpha)$ is a root of $(x^2-1)^2 - 5 = x^4 - 2x^2 - 4$.
Hence we have four possible maps, corresponding to these roots: $\sqrt{1-\sqrt{5}}$, $\sqrt{1+\sqrt{5}}$, $-\sqrt{1-\sqrt{5}}$, $-\sqrt{1+\sqrt{5}}$

The automorphisms are given explicitly by

$$\varphi(a+\alpha b+\alpha^2c+\alpha^3d) = a+\sqrt{1-\sqrt5}\,b+\left(\sqrt{1-\sqrt5}\right)^2c+\left(\sqrt{1-\sqrt5}\right)^3d$$
$$\varphi(a+\alpha b+\alpha^2c+\alpha^3d) = a+\sqrt{1+\sqrt5}\,b+\left(\sqrt{1+\sqrt5}\right)^2c+\left(\sqrt{1+\sqrt5}\right)^3d$$
$$\varphi(a+\alpha b+\alpha^2c+\alpha^3d) = a-\sqrt{1-\sqrt5}\,b+\left(-\sqrt{1-\sqrt5}\right)^2c+\left(-\sqrt{1-\sqrt5}\right)^3d$$
$$\varphi(a+\alpha b+\alpha^2c+\alpha^3d) = a-\sqrt{1+\sqrt5}\,b+\left(-\sqrt{1+\sqrt5}\right)^2c+\left(-\sqrt{1+\sqrt5}\right)^3d$$

Problem 6:

Since β is algebraic over F, it is also algebraic over $F(\alpha)$. Therefore

$$[F(\alpha):F] = \deg \operatorname{irr}(\alpha,F) < \infty$$

and also

$$[F(\alpha,\beta):F(\alpha)] = [F(\alpha)(\beta):F(\alpha)] = \deg \operatorname{irr}(\beta,F(\alpha)) < \infty$$

Hence

$$[F(\alpha,\beta):F] = [F(\alpha,\beta):F(\alpha)][F(\alpha):F] < \infty.$$

It follows $F(\alpha,\beta)$ is an algebraic extension of F and thus $\alpha+\beta$ is algebraic over F.

Problem 7:

(a) $\mathbb{Z}_4$ satisfies $2^2=0$ so it is not reduced.

(b) Assume R/I is reduced.

If $r^n\in I$ then

$$0+I = r^n+I = (r+I)^n$$

and since R/I has no nonzero nilpotent elements, $r+I=0+I$. Thus $r\in I$.

Hence $r^n\in I \Rightarrow r\in I$ and I is radical.

Conversely, assume I is radical.

Then if $r+I \in R/I$ satisfies $(r+I)^n = 0+I$ we must have

$$r^n + I = (r+I)^n = 0+I$$

and therefore $r^n \in I$. Since I is radical, this means $r \in I$ so $r+I = 0+I$.

Thus the only nilpotent element is $0+I$ and R/I is reduced.