1. *Compute with justification* $[\mathbb{Q}(\sqrt{2+\sqrt{3}}):\mathbb{Q}]$.

Proof:
Let $f(x) = x^4 - 4x^2 + 1$. Then

$f(\sqrt{2+\sqrt{3}}) = (\sqrt{2+\sqrt{3}})^4 - 4(\sqrt{2+\sqrt{3}})^2 + 1 = 7 + 4\sqrt{3} - 4(2+\sqrt{3}) + 1 = 0.$

Since $f(x+1) = x^4 + 4x^3 + 2x^2 - 4x - 2$ is irreducible by Eisenstein's Criterion with $p = 2$, then f is irreducible.

$\therefore\ [\mathbb{Q}(\sqrt{2+\sqrt{3}}):\mathbb{Q}] = \deg f(x) = 4.$

2. *Let E be an extension of F. Prove the set of all algebraic elements of E over F form a subfield of E.*

Proof:
Let $T = \{a \in E \mid a \text{ is algebraic over } F\}$.

Clearly $T \subseteq E$, so we only need to show T is a field.

If $f(x) = x$, then $f(0) = 0$, and so $0 \in T$. Thus $T \neq \varnothing$.

If $a, b \in E$, then $[F(a):F] = n < \infty$ and $[F(b):F] = m < \infty$ as a, b are algebraic over F.

We know $[F(a, b):F(a)] = [F(a)(b):F(a)] \leq [F(b):F]$ (as proven in an exercise).

And $[F(a, b):F] = [F(a, b):F(a)][F(a):F]$.

So then $[F(a, b):F] \leq m \bullet n < \infty$, hence $F(a, b)$ is an algebraic extension of F.

Since $a - b \in F(a, b)$ and $ab \in F(a, b)$ by closure, then $a - b, ab \in T$.

If $c \in T$ such that $c \neq 0$, then $F(c)$ is an algebraic extension of F.

And since $F(c)$ is a field, then $c^{-1} \in F(c)$, thus c^{-1} is algebraic over F, hence $c^{-1} \in T$.

$\therefore$ T is a subfield of E.

3. *Let E be an extension of F. Let a, b ∈ E.*
(a) *Prove that [F(a, b):F] ≤ [F(a):F][F(b):F].*

Proof:
If $[F(a):F] = \infty$ or $[F(b):F] = \infty$ the result is true. Assume both are finite.

Let $[F(a):F] = m$ and $[F(b):F] = n$.

Then $\exists\ p(x) = \text{irr}(b, F)$ such that $\deg p(x) = n$.

Since $p(x)$ is also an element of $F(a, b)[x]$ where $\deg p(x) = n$ and $p(b) = 0$, but not necessarily irreducible in $F(b)$, then we can only conclude $[F(a, b):F(a)] = \deg h(x)$ where $p(x) = h(x)j(x)$ for some $h(x), j(x) \in F(a)[x]$, $h(x)$ irreducible in $F(a)[x]$.

Thus $\deg h(x) \le \deg p(x)$, hence $[F(a, b):F(a)] \le [F(b):F]$.

It follows that $[F(a, b):F] = [F(a, b):F(a)][F(a):F] \le [F(b):F][F(a):F]$.

(b) *Let [F(a, b):F] = n and [F(b):F] = m. Prove that if m and n are relatively prime, then [F(a, b):F] = mn.*

Proof:
Since $[F(a, b):F] = n$ and $[F(b):F] = m$, then a and b are algebraic over F.

Thus $[F(a, b):F] = t < \infty$.

So then $[F(a, b):F] = [F(a, b):F(a)][F(a):F] = n \bullet [F(a, b):F(a)]$ and

$[F(a, b):F] = [F(a, b):F(b)][F(b):F] = m \bullet [F(a, b):F(b)]$.

Thus, $n \mid [F(a, b):F]$ and $m \mid [F(a, b):F]$.

Since m and n are relatively prime, then by Euclid's Lemma, $mn \mid [F(a, b):F]$.

By part (a) $[F(a, b):F] \le [F(a):F][F(b):F] = mn$.

Let $d = [F(a, b):F]$. Then $mn \mid d \Rightarrow d = mnr$ for some integer r and $nm \ge d \Rightarrow r = 1$.

$\therefore\ [F(a, b):F] = mn$.

4. *Let p be prime.*

(a) *Prove that if $\mathbb{F}_{p^n}$ is a subfield of $\mathbb{F}_{p^m}$, then n|m.*

Proof:

We know that $\mathbb{Z}_p$ is isomorphic to a subfield of $\mathbb{F}_{p^m}$ and isomorphic to a subfield of $\mathbb{F}_{p^n}$.

So then $[\mathbb{F}_{p^m}: \mathbb{Z}_p] = m$ and $[\mathbb{F}_{p^n}: \mathbb{Z}_p] = n$.

And since $\mathbb{F}_{p^n}$ is a subfield of $\mathbb{F}_{p^m}$, then $[\mathbb{F}_{p^m}: \mathbb{Z}_p] = [\mathbb{F}_{p^m}: \mathbb{F}_{p^n}][\mathbb{F}_{p^n}: \mathbb{Z}_p]$ where $[\mathbb{F}_{p^m}: \mathbb{F}_{p^n}]$ is a positive integer.

$\therefore n \mid m$.

(b) *Let f (x) be an irreducible polynomial of degree 2 in $\mathbb{Z}_p[x]$. Prove that f (x) is irreducible in $\mathbb{F}_{p^3}[x]$.*

Proof:

Since f is an irreducible polynomial of degree 2 in $\mathbb{Z}_p[x]$,

then $\mathbb{Z}_p[x]/(f) \cong \mathbb{Z}_p(\alpha)$ for some α where $f(\alpha) = 0$ and $|\mathbb{Z}_p(\alpha)| = p^2$.

Since $\deg f(x) = 2$, the $f(x) = (x - \alpha)(x - \beta)$ for some β.

If f is reducible in $\mathbb{F}_{p3}[x]$, then since $\mathbb{F}_{p3}[x]$ is a UFD, $f(x) = (x - \alpha)(x - \beta)$ is the only factorization, hence $\alpha, \beta \in \mathbb{F}_{p^3}$. This gives us that $\mathbb{Z}_p(\alpha)$ is a subfield of $\mathbb{F}_{p^3}$.

Hence $[\mathbb{F}_{p^3} : \mathbb{Z}_p] = [\mathbb{F}_{p^3} : \mathbb{Z}_p(\alpha)][\mathbb{Z}_p(\alpha): \mathbb{Z}_p]$.

Since $[\mathbb{F}_{p^3} : \mathbb{Z}_p] = 3$, $[\mathbb{Z}_p(\alpha): \mathbb{Z}_p] = 2$, and $[\mathbb{F}_{p^3} : \mathbb{Z}_p(\alpha)] = m$ for some positive integer m, then $3 = 2m$, a contradiction.

$\therefore f$ is irreducible over $\mathbb{F}_{p^3}$.

5. *Prove any two field of order p^n are isomorphic.*

Proof:

Let E be a field of order p^n. Let $f(x) = x^{p^n} - x$.

Since $|E^*| = p^n - 1$, then $\forall\ a \in E^*$, $a^{p^n-1} = 1$, hence $a^{p^n} = a$.

Consequently $f(a) = 0$.

Therefore, every element of E^* is a root of f.

Since $0^{p^n} - 0 = 0$, then every element of E is a root of f.

Since f has at most p^n roots and $|E| = p^n$, then E contains all the roots of f.

Since char $E = p$, then $f'(x) = p^n x^{p^n-1} - 1 = -1$, hence f has no repeated roots.

Thus E contains no elements other than roots of f.

$\therefore$ E is the splitting field of f.

If E' is another field of order p^n such that $E' \neq E$, then E' is also a splitting field of f.

Since any two splitting fields are isomorphic, then $E \cong E'$.

6. *Let E be an extension of $\mathbb{Z}_p$ such that $|E| = p^n$.*

(a) *Prove that $E = \mathbb{Z}_p(\alpha)$ for some $\alpha \in E$.*

Proof:

We have shown previously that E^* is cyclic.

Thus $\exists\ \alpha \in E^*$ that generates E^*. That is, $E^* = \langle \alpha \rangle$.

Since E is an extension of $\mathbb{Z}_p$, then $\mathbb{Z}_p \subseteq E$. And since $\alpha \in E$, then $\mathbb{Z}_p(\alpha) \subseteq E$.

To show the reverse containment, let $w \in E^*$.

Then $w = \alpha^k$ for some non-negative integer k.

Thus $E^* \subseteq \mathbb{Z}_p(\alpha)$.

Since $0 \in \mathbb{Z}_p(\alpha)$, then $E \subseteq \mathbb{Z}_p(\alpha)$.

$\therefore\ E = \mathbb{Z}_p(\alpha)$.

(b) *Prove there exists an irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ such that deg $(f(x)) = n$.*

Proof:

Since $|E| = p^n$ and E is an extension of $\mathbb{Z}_p$, then $[E:\mathbb{Z}_p] = n$.

By part (a), $E = \mathbb{Z}_p(\alpha)$.

Thus $[\mathbb{Z}_p(\alpha): \mathbb{Z}_p] = n < \infty$ which gives us that α is algebraic over $\mathbb{Z}_p$.

So then $\exists\ f \in \mathbb{Z}_p[x]$ such that $f(\alpha) = 0$.

Since $\mathbb{Z}_p$ is a field, $\mathbb{Z}_p[x]$ is a euclidean ring, so there is an irreducible factor g of f such that $g(\alpha) = 0$.

Since $\mathbb{Z}_p(\alpha) \cong \mathbb{Z}_p[x]/(g)$ and $|\mathbb{Z}_p(\alpha)| = p^n$, then $n = [\mathbb{Z}_p(\alpha):\mathbb{Z}_p] = \deg g$.