Section 39, Question 16

Firstly, notice that π^3 is transcendental over $\mathbb{Q}$, so

$$\mathbb{Q}(\pi^3) = \left\{ \frac{f(\pi^3)}{g(\pi^3)} : f(x), g(x) \in \mathbb{Q}[x] \right\}$$

Furthermore, π^2 is algebraic over $\mathbb{Q}(\pi^3)$ because $(\pi^3)^2 \in \mathbb{Q}(\pi^3)$ and for $f(x) = x^3 - (\pi^3)^2 \in \mathbb{Q}(\pi^3)[x]$, we have $f(\pi^2) = 0$.

We will now show that $f(x) = x^3 - (\pi^3)^2$ is of minimal degree. B.W.O.C., suppose there is a monic polynomial $g(x) \in \mathbb{Q}(\pi^3)[x]$ such that $g(x) = x^2 + q_1 x + q_0$ and $g(\pi^2) = 0$. Then $g(\pi^2) = \pi^4 + q_1\pi^2 + q_0 = 0$. Notice that,

$$q_1\pi^2 + q_0 = \frac{a_0\pi^2 + a_1\pi^5 + ... + a_n\pi^{3n+2}}{b_0 + b_1\pi^3 + ... + b_k\pi^{3k}} + \frac{c_0 + c_1\pi^3 + ... + c_l\pi^{3l}}{d_0 + d_1\pi^3 + ... + d_m\pi^{3m}}, a, b, c, d \in \mathbb{Q}$$

Furthermore, when we combine the fractions on the RHS, the terms in the numerator all are of the form $p\pi^n$ where either $n \equiv 0 \pmod 3$ or $n \equiv 2 \pmod 3$. Likewise, in the denominator the terms are of the form $b\pi^k$ where $k \equiv 0 \pmod 3$. However since $4 \equiv 1 \pmod 3$, we cannot have that $\pi^4 = q_1\pi^2 + q_2$. Hence, $g(\pi^2) \neq 0$. So, $f(x)$ is minimal and $\deg(\pi^2, \mathbb{Q}(\pi^3)) = \deg(f(x)) = 3$. □

Section 39, Question 25

(a) Let $f(x) = x^3 + x^2 + 1$. Since $\deg(f(x)) = 3$, $f(x)$ is irreducible over $\mathbb{Z}_2$ if and only if $f(x)$ has no zeros in $\mathbb{Z}_2$. Clearly, $f(0) = 1$ and $f(1) = 1$, so $f(x)$ is irreducible over $\mathbb{Z}_2$.

(b) We know that the extension field $\mathbb{Z}_2/\langle f(x)\rangle$ contains a zero of $f(x)$, namely, $\alpha = x + \langle f(x)\rangle = \overline{x}$. Hence, call $\mathbb{Z}_2(\alpha) = \mathbb{Z}_2/\langle f(x)\rangle$. The elements of $\mathbb{Z}_2(\alpha)$ are,

$$\mathbb{Z}_2(\alpha) = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}, \overline{x^2}, \overline{1+x^2}, \overline{x+x^2}, \overline{1+x+x^2}\}$$

For each $\overline{h(x)} \in \mathbb{Z}_2(\alpha)$, we relabel $\overline{h(x)} \coloneqq h(\alpha)$. Since α is a zero of $f(x)$, then $(x - \alpha)$ is a factor of $f(x)$. Dividing, we find,

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

Simply by trying other elements of $\mathbb{Z}_2(\alpha)$, we find that,

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

Hence,

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

□

Section 39, Question 30

By **Corollary 39.23**, $F(\alpha)$ is a vector space over F with basis $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$. Hence,

$$F(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{n-1}\alpha^{n-1} : a_i \in F\}$$

Since each element in a vector space is identified with a unique linear combination of the basis vectors, and there are q choices for each a_i, clearly there are q^n unique linear combinations of the basis vectors, and consequently q^n unique elements in $F(\alpha)$. □

Section 39, Question 36

Let $F' \leq F$ be the subfield of F such that $F' \simeq \mathbb{Z}_p$ as shown in **Theorem 31.19**. Furthermore, let $0_F \in F$ be the additive identity in F, $1_F \in F$ be unity in F and -1_F its unique additive inverse. Consider the group $\langle F^*, \cdot \rangle$ with order $n = p^m - 1$. Let $o(\alpha)$ denote the order of α. Recall that the order of an element in a group is the smallest number k such that $\alpha^k = e$, where e is the identity element. By Lagrange, we know that every element $a \in F^*$ has finite order which divides n, namely, $o(a) = k$ such that $n = kt$ for some $t \in \mathbb{Z}^+$. Hence, $a^n = (a^k)^t = (1_F)^t = 1_F$. It follows immediately that every element in F^* is a zero of the polynomial $f(x) = (1_F)x^n + (-1_F)$. Note that 0_F is a zero of the polynomial $g(x) = (1_F)x^n$. It remains to be shown that $f(x), g(x) \in F'[x]$, or equivalently, that $1_F, -1_F \in F'$.

However, since F' is a field, it contains unity $1_{F'} \in F'$. Furthermore, for any $a \in F'$, $(1_{F'})a = a = (1_F)a \implies 1_{F'} = 1_F$ by the right cancellation law. Since F' is a group under addition, $-1_F \in F'$, so $f(x), g(x) \in F'[x]$. So, every element in F is algebraic over the subfield of F that is isomorphic to $\mathbb{Z}_p$. □

Section 40, Question 6

Let $\alpha = \sqrt{2} + \sqrt{3}$. α is transcendental over $\mathbb{Q}$ as for $f(x) \coloneqq (x^2 - 5)^2 - 24 \in \mathbb{Q}[x]$, we have $f(\alpha) = 0$. $f(x)$ is minimal as in $(\sqrt{2} + \sqrt{3})^3$ we have a term $11\sqrt{2} + 9\sqrt{3}$ which cannot be cancelled by any lower powers.[1] Likewise, in $(\sqrt{2} + \sqrt{3})^2$, the product $\sqrt{2}\sqrt{3}$ appears which does not appear in the third power expansion. So, $f(x)$ is minimal and $\deg(\alpha, \mathbb{Q}) = \deg(f(x)) = 4$. By **Corollary 39.23**, a basis for the field extension $\mathbb{Q}(\alpha)$ is $\{1, \alpha, \alpha^2, \alpha^3\} = \{1, \sqrt{2} + \sqrt{3}, 5 + \sqrt{2}\sqrt{3}, 11\sqrt{2} + 9\sqrt{3}\}$. □

Section 40, Question 10

By the tower law,

$$[\mathbb{Q}(\sqrt{2}, \sqrt{6}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{6}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$$

Since $\sqrt{6} \notin \mathbb{Q}(\sqrt{2})$, we have that $\{1, \sqrt{2}, \sqrt{6}, \sqrt{2}\sqrt{6}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{6})$ over $\mathbb{Q}$. Furthermore, $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$, hence, $[\mathbb{Q}(\sqrt{2}, \sqrt{6}) : \mathbb{Q}(\sqrt{3})] = 2$. Finally, we see that $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{6})$ over $\mathbb{Q}(\sqrt{3})$ since $\sqrt{6} = \sqrt{3}\sqrt{2} \in (\mathbb{Q}(\sqrt{3}))(\sqrt{2})$. To demonstrate this fact, notice that

[1] In particular, it cannot be cancelled by a multiple of $(\sqrt{2} + \sqrt{3})$ since the coefficients are unequal.

$$\mathbb{Q}(\sqrt{2},\sqrt{6}) = \{a + b\sqrt{2} + c\sqrt{6} + d\sqrt{2}\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$$

and $d\sqrt{2}\sqrt{6} = 2d\sqrt{3}$. Furthermore,

$$\{x + y\sqrt{2} : x, y \in \mathbb{Q}(\sqrt{3})\} = \{(\alpha + \beta\sqrt{3}) + (\gamma + \delta\sqrt{3})\sqrt{2}, \alpha, \beta, \gamma, \delta \in \mathbb{Q}\}$$

Since $\sqrt{2}\sqrt{3} = \sqrt{6}$, the sets are identical. □

Section 40, Question 27

It is sufficient to show that $\mathbb{Q}(\sqrt{2},\sqrt{7})$ and $\mathbb{Q}(\sqrt{2}+\sqrt{7})$ have bases over $\mathbb{Q}$ which span the same extension field of $\mathbb{Q}$ to show that they are equal. Starting with $\mathbb{Q}(\sqrt{2},\sqrt{7})$, we know that $[\mathbb{Q}(\sqrt{2})] = 2$ and is generated by the basis $\{1, \sqrt{2}\}$ Furthermore, we have that $(\sqrt{2}+\sqrt{7})$ is a zero of the polynomial $x^4 - 18x^2 + 25$ which is irreducible over $\mathbb{Q}[x]$.[2] Hence, $[\mathbb{Q}(\sqrt{2}+\sqrt{7}) : \mathbb{Q}] = 4$. However, this implies that $(\sqrt{2}+\sqrt{7}) \notin \mathbb{Q}(\sqrt{2})$ since by the tower law,

$$[\mathbb{Q}(\sqrt{2}+\sqrt{7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}+\sqrt{7}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \implies [\mathbb{Q}(\sqrt{2}+\sqrt{7}) : \mathbb{Q}(\sqrt{2})] = 2$$

and if $(\sqrt{2}+\sqrt{7}) \in \mathbb{Q}(\sqrt{2})$, then $\deg(\sqrt{2}+\sqrt{7}, \mathbb{Q}) = 1$. Moreover, if $(\sqrt{2}+\sqrt{7}) \notin \mathbb{Q}(\sqrt{2})$, then $\sqrt{7} \notin \mathbb{Q}(\sqrt{2})$. This implies that $\{1, \sqrt{7}\}$ is a basis for $\mathbb{Q}(\sqrt{7})$ over $\mathbb{Q}(\sqrt{2})$. Finally, we see that $\{1, \sqrt{2}, \sqrt{7}, \sqrt{2}\sqrt{7}\}$ is a basis for $\mathbb{Q}(\sqrt{2},\sqrt{7})$ over $\mathbb{Q}$.

Turning our attention to $\mathbb{Q}(\sqrt{2}+\sqrt{7})$, since $(\sqrt{2}+\sqrt{7})$ is algebraic over $\mathbb{Q}$ and $\deg(\sqrt{2}+\sqrt{7}, \mathbb{Q}) = 4$, by **Corollary 39.23**, a basis for $\mathbb{Q}(\sqrt{2}+\sqrt{7})$ is $\{1, \sqrt{2}+\sqrt{7}, 9+\sqrt{2}\sqrt{7}, 16\sqrt{2}+11\sqrt{7}\}$. Clearly, every element in this basis is a linear combination of elements of the basis for $\mathbb{Q}(\sqrt{2},\sqrt{7})$. Likewise, every element in the basis for $\mathbb{Q}(\sqrt{2},\sqrt{7})$ is a linear combination of elements in the basis for $\mathbb{Q}(\sqrt{2}+\sqrt{7})$. In particular, notice that $\sqrt{2} = \frac{1}{6}(16\sqrt{2}+11\sqrt{7}) - \frac{11}{6}(\sqrt{2}+\sqrt{7})$. Hence, they are bases for the same subspace. It follows that $\mathbb{Q}(\sqrt{2}+\sqrt{7}) = \mathbb{Q}(\sqrt{2},\sqrt{7})$. □

Section 40, Question 35

Let F be a finite field of odd characteristic p, then $|F| = p^k$ for some $k \in \mathbb{Z}^+$. Clearly, we have p^k unique polynomials of the form $f_a(x) = x^2 - a \in F[x]$. Let $\alpha \in F$, then $f_a(\alpha) = 0$ implies that for all $b \in F$ with $b \neq a$, $f_b(\alpha) \neq 0$, since the square of an element in F cannot simultaneously take two different values in F. Hence, it suffices to show that there are two different elements $x, y \in F$ such that $f_a(x) = f_a(y)$. Then, there can be at most $p^k - 1$ equations in $H = \{f_\beta \in F[x] : \beta \in F\}$ with roots in F. Let $1 \in F$ be unity. Then $(1)^2 = 1 = (-1 \times -1) = (-1)^2$. Since $1 = -1$ implies that the characteristic of F is 2, then clearly $f_1(x) = x^2 - 1$ has two zeros in F. Hence, there is a polynomial $g \in H$ such that g has no zeros in F. So F cannot be algebraically closed. □

[2] If $f(x) = x^4 - 18x^2 + 25$ has linear factors in $\mathbb{Q}[x]$, then they must be of the form $(x - a)$ where $a \in \mathbb{Z}$ divides 25, however $\pm 1, \pm 5$ are not zeros of $f(x)$. Suppose $f(x) = (a_1x^2 + b_1x + c_1)(a_2x^2 + b_2x + c_2)$. We know that if $f(x)$ is irreducible in $\mathbb{Z}[x]$, it is irreducible in $\mathbb{Q}[x]$. Multiplying, we find $a_1 = a_2 = \pm 1$, $c_1 = c_2 = \pm 5$ and $b_1 = -b_2$. Eventually, we find $b_1^2 = 28$ or $b_1^2 = 8$, both of which have no integer solutions, so there is no quadratic factorization of $f(x)$ over $\mathbb{Q}[x]$, hence it is irreducible over $\mathbb{Q}[x]$.

Section 42, Question 2

We know that a finite field of order 3127 exists if and only if $3127 = p^k$ for some $k \in \mathbb{Z}^+$. Firstly, 3127 is not prime since $3127 = 53 \times 59$. Furthermore, checking with a calculator, we find that $3127^{\frac{1}{k}} \notin \mathbb{Z}^+$ for all $1 < k < 8$ and that $3127^{\frac{1}{8}} < 3$. Since 3127 is odd, then it cannot be the power of any prime. So there are no finite fields of order 3127. $\square$