Solutions to Sample Exam

1. We solve to obtain $\alpha = 3\beta + 2$, so

$$0 \;=\; (3\beta+2)^2 + 2(3\beta+2) + 3 \;=\; 4\beta^2 + 3\beta + 1 \;=\; 4(\beta^2 + 2\beta + 4).$$

Thus β is a root of $m(x) = x^2 + 2x + 4 \in F[x]$. In fact, $m(x)$ is the minimal polynomial of β over F. If not, then β would be a root of a polynomial in $F[x]$ of degree 1, forcing $\beta \in F$, implying that $\alpha = 3\beta + 2 \in F$, a contradiction. Another way to see that $m(x)$ is irreducible in $F[x]$ is to observe that its discriminant $2^2 - 4{\cdot}4 = 3$ is a nonsquare in F. (The only squares in F are $0, 1, 4$.)

2. Write $\alpha = \theta^2 + \theta$ where $\theta = 2^{1/3}$. Then

$$\alpha^3 \;=\; \theta^6 + 3\theta^5 + 3\theta^4 + \theta^3 \;=\; 4 + 6\theta^2 + 6\theta + 2 = 6\alpha + 6$$

so α is a root of $m(x) = x^3 - 6x - 6$. This polynomial is irreducible in $\mathbb{Q}[x]$ (the divisors of 6 are $\pm1, \pm2, \pm3, \pm6$, none of which are roots of $m(x)$) so $m(x)$ is in fact the minimial polynomial of α over $\mathbb{Q}$.

3. This example is attributed to Daniel Shanks, who was the first person to compute the first 100,000 decimal places of π. I have no idea how he found the remarkable identity in (b).

(a) We have

$$\begin{aligned}
\alpha - \sqrt{5} &= \sqrt{22 + 2\sqrt{5}} \\
\alpha^2 - 2\alpha\sqrt{5} + 5 &= 22 + 2\sqrt{5} \\
\alpha^2 - 17 &= 2(\alpha+1)\sqrt{5} \\
(\alpha^2 - 17)^2 &= 20(\alpha+1)^2 \\
\alpha^4 - 34\alpha^2 + 289 &= 20\alpha^2 + 40\alpha + 20 \\
\alpha^4 - 54\alpha^2 - 40\alpha + 269 &= 0,
\end{aligned}$$

so α is a root of $m(x) = x^4 - 54x^2 - 40x + 269 \in \mathbb{Q}[x]$. You can use the usual procedure to show that $m(x)$ is irreducible in $\mathbb{Q}[x]$; but let me show you a trick that simplifies the arithmetic. The substitution $y = 4x + 3$, i.e. $x = \frac{y-3}{4}$, allows us to rewrite $m(x) = 256f(y)$ where $f(y) = y^4 + 3y^3 - 4y - 1$. Now $m(x)$ is irreducible in $\mathbb{Q}[x]$ iff $f(y)$ is irreducible in $\mathbb{Q}[y]$. (Any nontrivial factorization $m(x) = m_1(x)m_2(x)$ in $\mathbb{Q}[x]$ gives a nontrivial factorization $f(y) = f_1(y)f_2(y)$ in $\mathbb{Q}[y]$, and conversely.) It suffices to show that $f(y)$ has no nontrivial factorization in $\mathbb{Z}[y]$. First, $f(y)$ has no linear factors in $\mathbb{Z}[y]$, otherwise it would have a root in $\mathbb{Z}$ dividing 1; but both $f(1) = -1$ and $f(-1) = 1$ are nonzero, so this cannot happen. If $f(y)$ factors into quadratic factors in $\mathbb{Z}[y]$, then

$$f(y) = y^4 + 3y^2 - 4y - 1 = (y^2 + ay - 1)(y^2 + by + 1)$$

for some $a, b \in \mathbb{Z}$. From the coefficients of y^3 and y, we get $a + b = 3$ and $a - b = -4$. Adding these equations gives $2a = -1$, which is not possible for $a \in \mathbb{Z}$. This contradiction proves that $f(y) \in \mathbb{Q}[y]$ and so $m(x) \in \mathbb{Q}[x]$ is irreducible. So $m(x)$ is the minimal polynomial of α over $\mathbb{Q}$.

(b) I will denote the given expression by $\theta = \sqrt{u} + \sqrt{v + 2\sqrt{w}}$ where

$$u = 11 + 2\sqrt{29}, \qquad v = 16 - 2\sqrt{29}, \qquad w = 55 - 10\sqrt{29}.$$

The fact that $u, v, w \in \mathbb{Q}[\sqrt{29}]$ will be helpful in these calculations. In particular, note that $uw = 25$. My strategy is to show that θ has the same minimal polynomial over $\mathbb{Q}$ as α. Using calculus, we see that $m(x)$ has four real roots, one on each of the intervals $[-7, -6]$, $[-3, -2]$, $[1, 2]$, $[7, 8]$. Numerical estimates show that $\alpha, \theta \in [7, 8]$, so they are both equal to the largest root of $m(x)$. This gives $\alpha = \theta$. Now

$$\begin{aligned}
\theta - \sqrt{u} &= \sqrt{v + 2\sqrt{w}} \\
\theta^2 - 2\theta\sqrt{u} + u &= v + 2\sqrt{w} \\
\theta^2 + u - v &= 2\theta\sqrt{u} + 2\sqrt{w} \\
(\theta^2 + u - v)^2 &= (2\theta\sqrt{u} + 2\sqrt{w})^2 \\
\theta^4 + 2(u-v)\theta^2 + (u-v)^2 &= 4u\theta^2 + 8\theta\sqrt{uw} + 4w \\
\theta^4 + 2(u-v)\theta^2 + (u-v)^2 &= 4u\theta^2 + 40\theta + 4w \\
\theta^4 + [2(u-v) - 4u]\theta^2 - 40\theta + [(u-v)^2 - 4w] &= 0 \\
\theta^4 - 54\theta^2 - 40\theta + 269 &= 0.
\end{aligned}$$

Here we have carefully calculated the coefficients using arithmetic in $\mathbb{Q}[\sqrt{29}]$; and it follows that $\theta = \alpha$ as explained above.

4. From $m(x) = x^3 - 7x^2 + 5x - 3 = (x - \alpha)(x - \beta)(x - \gamma)$ we obtain

$$\alpha + \beta + \gamma = 7, \qquad \alpha\beta + \alpha\gamma + \beta\gamma = 5, \qquad \alpha\beta\gamma = -3.$$

This answers (a) and (b). As for (c), we have

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \alpha\gamma + \beta\gamma) = 7^2 - 2 \cdot 5 = 39.$$

The fact that all these values are rational follows from the fact that each of the expressions is fixed by the Galois group of the polynomial (since permuting α, β, γ does not change them). The fact that they are all integers follows from knowing a little more algebra beyond what we are covering in our course: Not only are α, β, γ *algebraic numbers* (i.e. roots of nonzero polynomials with integer coefficients), they are in fact *algebraic integers* (i.e. roots of *monic* polynomials with integer coefficients).

5. In class, we listed irreducible polynomials of degree $\leqslant 4$ over $\mathbb{F}_2$. One of them is $m(x) = x^4 + x + 1$. This is irreducible since it has factors of degree 1 in $\mathbb{F}_2[x]$ (0,1 are not roots) and it is not divisible by $x^2 + x + 1$ (the only irreducible quadratic). So
$$\mathbb{F}_{16} = \mathbb{F}_2[\alpha] = \{a + b\alpha + c\alpha^2 + d\alpha^3 \ : \ a, b, c, d \in \mathbb{F}_2\}$$
where $\alpha^4 = \alpha + 1$.

6. There are p^2 monic polynomials of degree two, $x^2 + bx + c \in \mathbb{F}_p[x]$, corresponding to the choices of $b, c \in \mathbb{F}_p$. Of these, exactly $\frac{1}{2}p(p+1)$ are reducible polynomials $(x - r)(x - s)$ corresponding to the choices of roots $r, s \in \mathbb{F}_p$, not necessarily distinct. This leaves $p^2 - \frac{1}{2}p(p+1) = \frac{1}{2}(p^2-p)$ irreducible *monic* polynomials of degree two. Multiplying these by any of the $p-1$ nonzero constants gives a total of $\frac{1}{2}p(p-1)^2$ irreducible polynomials of degree two (not necessarily monic).

7. No, $i \notin \mathbb{Q}[\sqrt{-2}]$. Both of the elements $i = \sqrt{-1}$ and $\theta = \sqrt{-2} = i\sqrt{2}$ are quadratic irrational; and they generate quadratic extensions $F_1 = \mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$ and $F_2 = \mathbb{Q}[\theta] = \{a + b\theta : a, b \in \mathbb{Q}\}$ respectively. In both cases, the real elements are just the rationals: $F_1 \cap \mathbb{R} = F_2 \cap \mathbb{R} = \mathbb{Q}$. In particular, neither of the fields contains $\sqrt{2}$. If $i \in F_2$ then $\sqrt{2} = \theta/i \in F_2$, a contradiction.

8. This argument arose in our discussion of straightedge-and-compass constructions. We have a tower of extension fields
$$E_n \supseteq E_{n-1} \supseteq \cdots \supseteq E_2 \supseteq E_1 \supseteq E_0 = \mathbb{Q}$$
where $E_i = E_{i-1}[\sqrt{b_i}]$ for $i = 1, 2, \ldots, n$. Since $\sqrt{b_i}$ is a root of the quadratic polynomial $x^2 - b_i \in E_{i-1}[x]$, we have $[E_i : E_{i-1}] \leqslant 2$. By transitivity of degrees of extensions, $[E_n : \mathbb{Q}] = 2^k$ for some $k \in \{0, 1, 2, \ldots, n\}$. Now consider the element $\beta \in E_n$ defined by $\beta = \sum_{i=1}^{n} a_i\sqrt{b_i}$. Since $E_n \supseteq \mathbb{Q}[\beta] \supseteq \mathbb{Q}$, $[\mathbb{Q}[\beta] : \mathbb{Q}]$ must divide $[E_n : \mathbb{Q}] = 2^k$. However, $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$, so $\beta \neq \alpha$.

9. No, $\mathbb{Q}[\sqrt{3}] \ncong \mathbb{Q}[\sqrt{5}]$ since the polynomial $f(x) = x^2 - 5 \in \mathbb{Q}[x]$ has roots in $\mathbb{Q}[\sqrt{5}]$ but not in $\mathbb{Q}[\sqrt{3}]$.

   If $\sqrt{5} = a + b\sqrt{3}$ for some $a, b \in \mathbb{Q}$, then $5 = a^2 + 2ab\sqrt{3} + 3b^2$ and $2ab\sqrt{3} = 5 - a^2 - 3b^2$. Since $\sqrt{3}$ is irrational, this would require $ab = 0$. But if $b = 0$ then $\sqrt{5} = a \in \mathbb{Q}$, which is impossible. Otherwise $a = 0$ and $\sqrt{5} = b\sqrt{3}$ and $\sqrt{15} = 3b \in \mathbb{Q}$, a final contradiction.

10. Since $f(a) = a^4 + 1 > 0$ for all $a \in \mathbb{R}$, $f(x)$ has no real roots and certainly no rational roots. If it factors as a product of two quadratic factors in $\mathbb{Z}[x]$ then any such factorization must have the form $f(x) = (x^2 + ax + b)(x^2 - ax + b)$ where $a, b \in \mathbb{Z}$ (in order to avoid terms of degree 3). But then $b = \pm 1$ and $2b - a^2 = 0$ so $a^2 = \pm 2$ which has no integer solutions, a contradiction. We conclude that $f(x)$ is irreducible in $\mathbb{Z}[x]$ and also in $\mathbb{Q}[x]$.

Note that $\zeta^4 = -1$ so $\zeta^8 = 1$. We have $\mathbb{Q}[\zeta] \subseteq \mathbb{Q}[\zeta^3] \subseteq \mathbb{Q}[\zeta^9] = \mathbb{Q}[\zeta]$ so $E = \mathbb{Q}[\zeta] = \mathbb{Q}[\zeta^3]$. Similar arguments show $E = \mathbb{Q}[\zeta^5] = \mathbb{Q}[\zeta^7]$. In fact the roots of $f(x)$ are $\zeta, \zeta^3, \zeta^5, \zeta^7$ and so these four roots are conjugates. For $k \in \{1,3,5,7\}$, denote by $\sigma_k : E \to E$ the automorphism which satisfies $\sigma_k(\zeta) = \zeta^k$. Such automorphisms exist since ζ^k $(k = 1,3,5,7)$ are conjugates of ζ. These are all the automorphisms of E since any automorphism $\sigma \in E$ must map $\zeta \mapsto \zeta^k$ for some $k \in \{1,3,5,7\}$, these being all the roots of $f(x)$; and since ζ generates the extension $E \supseteq \mathbb{Q}$, σ must coincide with σ_k. It is easy to see that $G = E = \{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$ is a Klein four-group.

11. (a) F (b) F (c) T (d) F (e) T (f) T (g) T (h) T (i) T (j) T

Comments in #11:

(a) In class we gave an easy counterexample: $f(x) = x^3 - 2 = (x - \alpha)(x - \omega\alpha)(x - \omega^2\alpha)$ whose splitting field $E = \mathbb{Q}[\alpha, \omega]$ has automorphism group $\langle \sigma, \tau \rangle \cong S_3$, the nonabelian group of order six.

(b) As discussed in class, the nontrivial automorphism τ of $\mathbb{Q}[\sqrt{2}]$ is discontinuous. Let $a_1, a_2, a_3, \ldots \in \mathbb{Q}$ be a sequence of rational numbers converging to $\sqrt{2}$; then

$$\lim_{n\to\infty} \tau(a_n) = \lim_{n\to\infty} a_n = \sqrt{2}$$

whereas

$$\tau\Big(\lim_{n\to\infty} a_n\Big) = \sigma\big(\sqrt{2}\big) = -\sqrt{2}.$$

(c) As discussed in class.

(d) The field $\mathbb{R}$ has no nontrivial automorphisms. Observe that $\sqrt{2}$ is a square in $\mathbb{R}$ but $-\sqrt{2}$ is not. (Suppose ϕ is an automorphism of $\mathbb{R}$ satisfying $\phi(\sqrt{2}) = -\sqrt{2}$, and let $a = \sqrt[4]{2} \in \mathbb{R}$. Then $\phi(a)^2 = \phi(a^2) = \phi(\sqrt{2}) = -\sqrt{2} < 0$, which is impossible for $\phi(a) \in \mathbb{R}$.)

(e) For example, the three cube roots of 2 are $\alpha, \omega\alpha, \omega^2\alpha$ where $\alpha = 2^{1/3}$ and ω is a primitive cube root of unity. Since α and $\omega\alpha$ are conjugates, $\mathbb{Q}[\alpha] \cong \mathbb{Q}[\omega\alpha]$. But these fields are distinct since one is a subfield of $\mathbb{R}$, and the other is not.

(f) An example of a proper field extension of $\mathbb{C}$ is $\mathbb{C}(t)$, the field of rational functions of t with complex coefficients. Note however that $\mathbb{C}$ has no proper *finite* extension fields.

(g) Let $E \supseteq \mathbb{Q}$ be an extension field, and let σ be automorphism of E. It is easy to see that $\sigma(a) = a$ for every $a \in \mathbb{Q}$; so by definition of a field automorphism, $\sigma(au + bv) = a\sigma(u) + b\sigma(v)$ for all $a, b \in \mathbb{Q}$; $u, v \in E$.

(h) Similar to #2 on the Sample Test.

(i) $60 = 2^2 \cdot 3 \cdot 5$ where $3 = 2+1$ and $5 = 2^2+1$ are Fermat primes..

(j) Let $E \supseteq \mathbb{Q}$ be a cubic field extension, so that $[E : \mathbb{Q}] = 3$. Suppose that E has three distinct automorphisms ι, σ, σ^2, and consider an element of the form $b = a + \sigma(a) + \sigma^2(a) \in E$ where $a \in E$. Then

$$\sigma(b) = \sigma(a) + \sigma^2(a) + a = b.$$

This implies that $b \in \mathbb{Q}$. (The extension $E \supset \mathbb{Q}$ has no intermediate fields, since it has prime degree 3; so the fixed field of any automorphism is either $\mathbb{Q}$ or E. Since $\sigma \neq \iota$, its fixed field must consist of rational numbers only.)