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 $0, 1, 4$.)

By the way, we independently verify that the minimal polynomial given for α is also irreducible, in the same way: its discriminant is $2^2 - 4{\cdot}3 = 2$ which is a nonsquare in F.

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 $\mathbb{Q}$.

Remarks: It turned out I didn't require the relation $\alpha^2 = \theta^2 + 2\theta + 4$. If I did, then I would have used the fact that $1, \alpha, \alpha^2, \alpha^3$ are four elements in an extension $\mathbb{Q}[\theta] \supset \mathbb{Q}$ of degree 3 (with basis $1, \theta, \theta^2$) so they are linearly dependent over $\mathbb{Q}$. At this point we would have solved for α^3 as a linear combination of $1, \alpha, \alpha^2$. We would have obtained the same answer as above.

3. Following the hint, observe that $m(x) = x^3 - 2 \in F[x]$ is irreducible (the only cubes in F are $\{0, 1, 6\}$) so $\mathbb{F}_{343} = F[\alpha]$ where α is a root of $m(x)$. To find a 3×3 matrix $A \in F^{3\times3}$ having the same minimal polynomial as α, use a companion matrix of $m(x)$ as we did earlier in the semester, say

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{bmatrix}$$

so

$$R = F[A] = \{a + bA + cA^2 \;:\; a, b, c \in F\} = \left\{ \begin{bmatrix} a & b & c \\ 2c & a & b \\ 2b & 2c & a \end{bmatrix} \;:\; a, b, c \in F \right\}.$$

4. 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 $\alpha^4 = \alpha + 1$.

5. (a) Let α be a root of $m(x)$ in an extension field $E \supset F$ of degree p, so that $E \cong \mathbb{F}_q$ where $q = p^p$. So $\sigma(\alpha) = \alpha^p = \alpha - 1$, using the fact that α is a root of $m(x)$. Repeatedly applying σ gives $\sigma^j(\alpha) = \alpha - j$ for $j = 0, 1, 2, \ldots, p-1 \in E$. These are all roots of $m(x)$ since σ is an automorphism of E.

   Alternatively, one could write the roots as $\alpha, \alpha+1, \alpha+2, \ldots, \alpha+p-1$. (Or $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{p-1}}$, but that would not be simplified.)

   (b) The automorphism σ permutes the p roots of $m(x)$ in a cycle of length p as
$$\alpha \mapsto \alpha-1 \mapsto \alpha-2 \mapsto \cdots \mapsto \alpha-p+1 \mapsto \alpha.$$

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

   If $\sqrt{3} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$, then $3 = a^2 + 2ab\sqrt{2} + 2b^2$ and $2ab\sqrt{2} = 3 - a^2 - 2b^2$. Since $\sqrt{2}$ is irrational, this would require $ab = 0$. But if $b = 0$ then $\sqrt{3} = a \in \mathbb{Q}$, which is impossible. Otherwise $a = 0$ and $\sqrt{3} = b\sqrt{2}$ and $\sqrt{6} = 2b \in \mathbb{Q}$, a final contradiction.

7. (a) $f(t) = \frac{t}{4}\left(1 - \frac{t^2}{4}\right)^{-1} = \frac{t}{4} + \frac{t^3}{16} + \frac{t^5}{64} + \frac{t^7}{256} + \frac{t^9}{1024} + \cdots$.
   You know several other ways to expand the series (using Taylor series, partial fractions, recursively solving for coefficients, etc., any of which would give the same answer) but since this is simply a geometric series, there is a clear shortest approach.

   (b) $e^x = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \frac{x^5}{120} + \cdots \in E$ is not a rational function.

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

Comments in #8:

(a) Recall that if $E \supseteq F$ is any field extension, the fields E and F have the same characteristic.

(b) As discussed in class, the nontrivial automorphism σ 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
$$\lim_{n\to\infty} \sigma(a_n) = \lim_{n\to\infty} a_n = \sqrt{2}$$
whereas

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

(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 in $\mathbb{R}$.)

(e) Let $\alpha = \pi^2$; then α is transcendental over $\mathbb{Q}$, so $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\pi)$ via an isomorphism $\mathbb{Q}(\alpha) \to \mathbb{Q}(\pi)$ mapping $\alpha \mapsto \pi$. However, $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\pi)$; in fact, $[\mathbb{Q}(\pi) : \mathbb{Q}(\alpha)] = 2$. (Recall that if α and β are transcendental over $\mathbb{Q}$, then $\mathbb{Q}(\alpha) \cong \mathbb{Q}(t) \cong \mathbb{Q}(\beta)$.)

(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 #9 on Practice Problems 1.

(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.)