Homework 5 Key

15.2.1) Let α be a complex root of the polynomial x^3-3x+4. Then $\alpha^2+\alpha+1 \neq 0$, so $\alpha^2+\alpha+1$ is invertible with inverse $a+b\alpha+c\alpha^2$ for $a, b, c \in \mathbb{Q}$. Thus

$$1 = (1+\alpha+\alpha^2)(a+b\alpha+c\alpha^2).$$

Expanding the right side and using the relation $\alpha^3 = 3\alpha - 4$, we get

$$1 = (a-4b-4c) + (a+4b-c)\alpha + (a+b+4c)\alpha^2,$$

and since $1, \alpha, \alpha^2$ are linearly independent over $\mathbb{Q}$, we get the system

$$\begin{aligned} a-4b-4c &= 1 \\ a+4b-c &= 0 \\ a+b+4c &= 0. \end{aligned}$$

Solving this, we get $(a, b, c) = \left(\frac{17}{49}, -\frac{5}{49}, -\frac{3}{49}\right)$. Thus

$$(1+\alpha+\alpha^2)^{-1} = \frac{17}{49} - \frac{5}{49}\alpha - \frac{3}{49}\alpha^2.$$

15.2.2) Let $f(x) = \sum_{k=0}^{n}(-1)^{n-k}a_k x^k$ with $a_n = 1$ be an irreducible polynomial over F with α a root of f in an extension field K. Then α is nonzero, and we must have $a_0 \neq 0$ since f is irreducible. Thus

$$\sum_{k=0}^{n}(-1)^{n-k}a_k\alpha^k = 0,$$

so subtracting $(-1)^n a_0$, we get

$$\alpha\left(\sum_{k=0}^{n-1}(-1)^{n+1-k}a_{k+1}\alpha^k\right) = (-1)^{n+1}a_0.$$

Dividing by $(-1)^{n+1}a_0$, we have

$$\alpha\left(\sum_{k=0}^{n-1}(-1)^k\frac{a_{k+1}}{a_0}\alpha^k\right) = 1,$$

so

$$\alpha^{-1} = \left(\sum_{k=0}^{n-1}(-1)^k\frac{a_{k+1}}{a_0}\alpha^k\right).$$

15.3.2) We have $f(x) \equiv x^4 + x + 1 \pmod 2$ which is irreducible in $\mathbb{F}_2[x]$, so f is irreducible in $\mathbb{Q}[x]$. Then letting α be a root of f, α has degree 4 over $\mathbb{Q}$. Notice that $\sqrt[3]{2}$ is a root of $x^3 - 2$ as a polynomial in $\mathbb{Q}(\alpha)[x]$, and thus $\sqrt[3]{2}$ has degree $1, 2$, or 3 over $\mathbb{Q}(\alpha)$. We have

$$[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}(\alpha)] \leq 4 \cdot 3 = 12,$$

which implies that $4 \mid [\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}]$ and $[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}] \leq 12$, so $[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}] \in \{1, 4, 8, 12\}$. Moreover, we have

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

so $3 \mid [\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}]$ as well, which forces $[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}] = 12$, and thus $[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 4$. Then the degree of α over $\mathbb{Q}(\sqrt[3]{2})$ is 4, so f is irreducible over $\mathbb{Q}(\sqrt[3]{2})$.

15.3.8) The algebraic numbers form a field, so are closed under addition and multiplication. Then

$$(\alpha+\beta)^2 - 4\alpha\beta = (\alpha-\beta)^2$$

is an algebraic number. If γ^2 is a algebraic number, then γ is algebraic as well, because γ^2 is a root of a polynomial $f(x)$, so γ is a root of the polynomial $f(x^2)$. Thus $\alpha - \beta$ is algebraic, so

$$\frac{(\alpha+\beta)+(\alpha-\beta)}{2} = \alpha$$

is algebraic, and then $(\alpha+\beta) - \alpha = \beta$ is algebraic as well.

15.3.9) Let $a := \deg f$ and $b := \deg g$. Then

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\beta)][\mathbb{Q}(\beta):\mathbb{Q}],$$

so

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = a\cdot[K(\beta):K] = b\cdot[L(\alpha):L].$$

Then $f(x)$ is irreducible in $L[x]$ iff α has degree a over L iff $[L(\alpha):L]=a$ iff $[K(\beta):K]=b$ iff β has degree b over K iff $g(x)$ is irreducible in $K[x]$.

15.4.1) Let $\gamma = 1 + \alpha^2$. Then since $\alpha^3 - \alpha = 1$, we have

$$(\gamma - 1)(\gamma - 2)^2 = (\alpha^2)(\alpha^2 - 1)^2 = (\alpha^3 - \alpha)^2 = 1,$$

so γ is a root of $(x-1)(x-2)^2 - 1 = x^3 - 5x^2 + 8x - 5$. This polynomial is irreducible over $\mathbb{Q}$ because it has no rational roots by the rational root test, and a cubic with no rational roots is irreducible.

15.4.2) Let $\alpha = \sqrt{3} + \sqrt{5}$.

(a) The elements $1, \sqrt{3}, \sqrt{5}, \sqrt{15}$ form a basis for $\mathbb{Q}(\sqrt{3}+\sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$, so α has degree 4 over $\mathbb{Q}$. Since $\alpha^2 = 8 + 2\sqrt{15}$ and $\alpha^4 = 124 + 32\sqrt{15}$, we get that α is a root of the irreducible polynomial $x^4 - 16x^2 + 4$.

(b) Notice that α is a root of $x^2 - 2\sqrt{5}x + 2$, which is irreducible over $\mathbb{Q}(\sqrt{5})$, because otherwise $\sqrt{3} + \sqrt{5} \in \mathbb{Q}(\sqrt{5})$.

(c) Notice that $1, \sqrt{3}, \sqrt{5}, \sqrt{10}$ are linearly independent over $\mathbb{Q}(\sqrt{10})$, so α has degree 4 over $\mathbb{Q}(\sqrt{10})$. Thus the same polynomial from part (a) is irreducible over $\mathbb{Q}(\sqrt{10})$ with α a root.

(d) Notice that α is a root of $x^2 - (8 + 2\sqrt{15})$, which is irreducible over $\mathbb{Q}(\sqrt{15})$, because otherwise $\sqrt{3} + \sqrt{5} \in \mathbb{Q}(\sqrt{15})$.