Feedback

HOMEWORK 2 SOLUTIONS

February 4, 2019

Dummit and Foote Chapter 13 Selected Exercises

§13.1 # 1 Show that $p(x) = x^3 + 9x + 6$ is irreducible in $\mathbb{Q}[x]$. Let θ be a root of $p(x)$. Find the inverse of $1 + \theta$ in $\mathbb{Q}(\theta)$.

Solution: Note that as 3 is prime and divides 9 and 6, but $3^2 = 9$ does not divide 6, $p(x)$ is irreducible by Eisenstein.

If θ is a root of $p(x)$, then $\mathbb{Q}(\theta)$ has as a basis $1, \theta, \theta^2$ (because $p(x)$ is degree 3). So, let β be the inverse of $1 + \theta$ in $\mathbb{Q}(\theta)$. Then if $\beta = b_0 + b_1\theta + b_2\theta^2$,

$$\begin{aligned} 1 &= (1+\theta)(\beta) \\ &= (1+\theta)(b_0 + b_1\theta + b_2\theta^2) \\ &= b_0 + b_1\theta + b_2\theta^2 + b_0\theta + b_1\theta^2 + b_2\theta^3 \\ &= (b_0) + (b_1 + b_0)\theta + (b_2 + b_1)\theta^2 + b_2\theta^3. \end{aligned}$$

However, as $p(\theta) = 0$, we have that $\theta^3 = -9\theta - 6$, so we have that

$$1 = (b_0 - 6b_2) + (b_1 + b_0 - 9b_2)\theta + (b_2 + b_1)\theta^2.$$

This becomes the set of equations

$$\begin{aligned} 1 &= b_0 - 6b_2 \\ 0 &= b_0 + b_1 - 9b_2 \\ 0 &= b_1 + b_2, \end{aligned}$$

which has solution

$$b_0 = \frac{1}{4}, \qquad b_1 = -\frac{5}{2}, \qquad b_2 = \frac{5}{2}.$$

So, $1 + \theta$ has inverse

$$1 + \theta = \frac{1}{4} - \frac{5}{2}\theta + \frac{5}{2}\theta^2 \quad ✓$$

in $\mathbb{Q}(\theta)$.

§13.1 # 2 Show that $x^3 - 2x - 2$ is irreducible over $\mathbb{Q}$ and let θ be a root. Compute $(1+\theta)(1+\theta+\theta^2)$ and $\frac{1+\theta}{1+\theta+\theta^2}$ in $\mathbb{Q}(\theta)$.

Solution: Note that as 2 divides -2, but $2^2 = 4$ does not divide -2, $x^3 - 2x - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion.

Note that as θ is a root of $x^3 - 2x - 2$, we have that $\theta^3 - 2\theta - 2 = 0$, so $\theta^3 = 2\theta + 2$. So,

$$(1+\theta)(1+\theta+\theta^2) = 1 + 2\theta + 2\theta^2 + \theta^3 = 1 + 2\theta + 2\theta^2 + 2\theta + 2 = 3 + 4\theta + 2\theta^2. \quad ✓$$

Next, let $\beta = b_0 + b_1\theta + b_2\theta^2$ be the inverse of $1 + \theta + \theta^2$ in $\mathbb{Q}(\theta)$. Then

$$\begin{aligned} 1 &= (1+\theta+\theta^2)(b_0 + b_1\theta + b_2\theta^2) \\ &= b_0 + (b_0 + b_1)\theta + (b_2 + b_1 + b_0)\theta^2 + (b_1 + b_2)\theta^3 + b_2\theta^4 \\ &= (b_0 + 2b_1 + 2b_2) + (b_0 + 3b_1 + 4b_2)\theta + (b_0 + b_1 + 3b_2)\theta^2, \end{aligned}$$

which gives rise to the system of equations

$$
\begin{aligned}
1 &= b_0 + 2b_1 + 2b_2 \\
0 &= b_0 + 3b_1 + 4b_2 \\
0 &= b_0 + b_1 + 3b_2.
\end{aligned}
$$

This has solution

$$b_0 = -\frac{1}{3}, \qquad b_1 = \frac{1}{3}, \qquad b_2 = -\frac{2}{3},$$???

so the inverse of $1 + \theta + \theta^2$ is

$$-\frac{1}{3} + \frac{1}{3}\theta - \frac{2}{3}\theta^2.$$

5/3 $\frac{1}{3}$ ✓   Redo.

Thus,

$$
\begin{aligned}
\frac{1+\theta}{1+\theta+\theta^2} &= (1+\theta)\left(-\frac{1}{3} + \frac{1}{3}\theta - \frac{2}{3}\theta^2\right) \\
&= \frac{1}{3}(-1 - \theta^2 - 2\theta^3) \\
&= -\frac{1}{3}(5 + 4\theta + \theta^2).
\end{aligned}
$$

No

$-\frac{2}{3}$ ✓

product =

$$\boxed{-\frac{1}{3}x^2 + \frac{2}{3}x + \frac{1}{3}}$$

§13.2 # 3 Determine the minimal polynomial over $\mathbb{Q}$ for the element $1 + i$.

Solution: Note that $(1+i)^2 = 2i$, so

$$(1+i)^2 - 2(1+i) + 2 = 0,$$

which gives us a polynomial $p(x) = x^2 - 2x + 2$ with $p(1+i) = 0$. However, by Eisenstein's criterion, $x^2 - 2x + 2$ is irreducible, so $p(x)$ is the minimal polynomial over $\mathbb{Q}$ for $1 + i$.

§13.2 # 4 Determine the degree over $\mathbb{Q}$ of $2 + \sqrt{3}$ and $1 + \sqrt[3]{2} + \sqrt[3]{4}$.

Solution: Note that $(2 + \sqrt{3})^2 = 7 + 4\sqrt{3}$, so

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

and $2 + \sqrt{3}$ is a root of $p(x) = x^2 - 4x + 1$. Moreover,

$$p(x+1) = (x+1)^2 - 4(x+1) + 1 = x^2 - 2x - 2$$

is irreducible by Eisenstein, so $p(x)$ is also irreducible, and is the minimal polynomial for $2 + \sqrt{3}$. Thus, $2 + \sqrt{3}$ is degree 2 over $\mathbb{Q}$.

Next, note that

$$(1 + \sqrt[3]{2} + \sqrt[3]{4})^2 = 5 + 4(2^{1/3}) + 3(2^{2/3})$$

and

$$(1 + \sqrt[3]{2} + \sqrt[3]{4})^3 = 19 + 15(2^{1/3}) + 12(2^{2/3}),$$

so $1 + \sqrt[3]{2} + \sqrt[3]{4}$ is a root of $p(x) = x^3 - 3x^2 - 3x - 1$. Moreover,

$$p(x-1) = x^3 - 6x - 3,$$

which is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 3$. Thus, $p(x)$ is the minimal polynomial for $1 + \sqrt[3]{2} + \sqrt[3]{4}$.

Once $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, then $(\sqrt{2}+\sqrt{3})-\sqrt{2} = \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

§13.2 # 7 Prove that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ [one inclusion is obvious, for the other consider $(\sqrt{2}+\sqrt{3})^2$, etc.]. Conclude that $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = 4$. Find an irreducible polynomial satisfied by $\sqrt{2}+\sqrt{3}$.

Proof. Clearly, $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$, so $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$. On the other hand, note that $(\sqrt{2}+\sqrt{3})^2 = 6+2\sqrt{6}$ and $(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2}+9\sqrt{3}$. ✓

So, $(\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3}) = 2\sqrt{2}$, which implies that $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Moreover, $(\sqrt{2}+\sqrt{3})^3 - 11(\sqrt{2}+\sqrt{3}) = -2\sqrt{3}$, so $\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ as well. Thus, $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Therefore, $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Or.

Note that $(\sqrt{2}+\sqrt{3})^4 = (5+2\sqrt{6})^2 = 49+20\sqrt{6}$, so if $p(x) = x^4 - x^2 + 1$, then $p(\sqrt{2}+\sqrt{3}) = 0$. Note that $p(x)$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$, so $p(x)$ is irreducible in $\mathbb{Q}[x]$ as well, demonstrating both an irreducible polynomial satisfied by $\sqrt{2}+\sqrt{3}$ and that $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = 4$. ✓ □

§13.2 # 11 (a) Let $\sqrt{3+4i}$ denote the square root of the complex number $3+4i$ that lies in the first quadrant and let $\sqrt{3-4i}$ denote the square roote of $3-4i$ that lies in the fourth quadrant. Prove that $[\mathbb{Q}(\sqrt{3+4i}+\sqrt{3-4i}] = 1$.

(b) Determine the degree of the extension $\mathbb{Q}\left(\sqrt{1+\sqrt{-3}}+\sqrt{1-\sqrt{-3}}\right)$ over $\mathbb{Q}$.

* We will talk about these in class.

Proof. (a) We will show that the element $\sqrt{3+4i}+\sqrt{3-4i}$ is in fact rational, which implies the desired result.

This involves a number of algebraic manipulations of $(\sqrt{3+4i}+\sqrt{3-4i})^2$, which are presented below:

$$\begin{aligned}(\sqrt{3+4i}+\sqrt{3-4i})^2 &= (3+4i)+2\sqrt{3+4i}\sqrt{3-4i}+(3-4i)\\ &= 6+2\sqrt{(3+4i)(3-4i)}\\ &= 6+2\sqrt{9+16}\\ &= 6+2\sqrt{25}\\ &= 16,\end{aligned}$$

✓

which implies that $\sqrt{3+4i}+\sqrt{3-4i} = \pm 4$, and as such is a rational number. Thus, $[\mathbb{Q}(\sqrt{3+4i}+\sqrt{3-4i}):\mathbb{Q}] = 1$.

(b) Note that

$$\begin{aligned}(\sqrt{1+\sqrt{-3}}+\sqrt{1-\sqrt{3}})^2 &= (1+\sqrt{-3})+2\sqrt{(1-\sqrt{3})(1+\sqrt{3})}+(1-\sqrt{3})\\ &= 2+2\sqrt{1+3}\\ &= 6,\end{aligned}$$

✓ good

so $\sqrt{1+\sqrt{-3}}+\sqrt{1-\sqrt{-3}} = \sqrt{6}$. This satisfies the minimal polynomial x^2-6, which is irreducible by Eisenstein with $p=3$, and thus $[\mathbb{Q}(\sqrt{1+\sqrt{-3}}+\sqrt{1-\sqrt{-3}}:\mathbb{Q}] = 2$.

□

13.2.12 Suppose the degree of the extension K/F is a prime p. Show that any subfield E of K containing F is either K or F.

✓

Proof. (Thomas) Suppose E is a subfield of K containing F. Then $p = [K:F] = [K:E][E:F]$ and since p is prime, either $[K:E] = p$ and $[E:F] = 1$ or vice versa. If $[K:E] = p$ then $[E:F] = 1$ and $E = F$. If $[K:E] = 1$ then $K = E$. □

13.2.13 Suppose $F = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_i^2 \in \mathbb{Q}$ for $i = 1, 2, \ldots, n$. Prove that $2^{\frac{1}{3}} \notin F$.

Proof. (Thomas) Suppose for the sake of contradiction that $2^{\frac{1}{3}} \in F$. Then $3 = [\mathbb{Q}(2^{\frac{1}{3}}) : \mathbb{Q}] \big| [F : \mathbb{Q}]$. Note that $[F : \mathbb{Q}] = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}(\alpha_1, \ldots, \alpha_{n-1})][\mathbb{Q}(\alpha_1, \ldots, \alpha_{n-1}) : \mathbb{Q}(\alpha_1, \ldots, \alpha_{n-2})] \ldots [\mathbb{Q}(\alpha_1) : \mathbb{Q}]$. Since each $\alpha_i^2 \in \mathbb{Q}$, we have $[\mathbb{Q}(\alpha_1, \ldots, \alpha_i) : \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})] \big| 2$ for each i so $[F : \mathbb{Q}] \big| 2^l$ for some $l \in \mathbb{Z}$. But this is a contradiction, since $3 \big| [F : \mathbb{Q}]$ then implies $3 | 2^l$. Thus $2^{\frac{1}{3}} \notin F$. ✓ □

13.2.14 Prove that if $[F(\alpha) : F]$ is odd then $F(\alpha) = F(\alpha^2)$.

Proof. (Thomas) Suppose $[F(\alpha) : F]$ is odd. Note that $F(\alpha^2)$ is a subfield of $F(\alpha)$ so $[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$. Note that α is a root of the polynomial $x^2 - \alpha^2 \in F(\alpha^2)[x]$ which has degree 2 so $[F(\alpha) : F(\alpha^2)] \big| 2$. But since $[F(\alpha) : F]$ is odd we see that $[F(\alpha) : F(\alpha^2)] = 1$ so $F(\alpha) = F(\alpha^2)$. ✓ Nice. □

13.2.18 Let k be a field and let $k(x)$ be the field of rational functions in x with coefficients from k. Let $t \in k(x)$ be the rational function $\frac{P(x)}{Q(x)}$ with relatively prime polynomials $P(x), Q(x) \in k[x]$, with $Q(x) \neq 0$. Then $k(x)$ is an extension of $k(t)$ and to compute its degree it is neccesary to compute the minimal polynomial with coefficients in $k(t)$ satisfied by x.

(a) Show that the polynomial $P(X) - tQ(X)$ in the variable X and coefficients in $k(t)$ is irreducible in $k(t)$ and has x as a root. [By Guass' Lemma this polynomial is irreducible in $(k(t))[X]$ if and only if it is irreducible in $(k[t])[X]$. Then note that $(k[t])[X] = (k[X])[t]$.]

Proof. (Thomas) Define $Z(X) = P(X) - tQ(X)$ and note that in $(k[X])[t]$ the polynomial $Z(X)$ is linear and is thus irreducible. Since $(k[X])[t] = (k[t])[X]$, we note that $Z(X)$ is also irreducible in $(k[t])[X]$. Then by Gauss' Lemma $Z(X)$ is also irreducible in $(k(t))[X]$ as desired. Finally, note that $Z(x) = P(x) - tQ(x) = P(x) - \frac{P(x)}{Q(x)}Q(x) = P(x) - P(x) = 0$ and x is a root of $Z(X)$. □ ✓

(b) Show that the degree of $P(X) - tQ(X)$ as a polynomial in X with coefficients in $k(t)$ is the maximum of the degrees of $P(x)$ and $Q(x)$.

Proof. (Thomas) Define $Z(X) = P(X) - tQ(X)$ and note that $Z(X) \in (k(t))[X]$ but $P(X), Q(X) \in k[X]$. Then the coefficients in $P(X), Q(X)$ are from k so the coefficients in $P(X)$ and $tQ(X)$ cannot cancel. Then noting that in $(k(t))[X]$, $P(X) - tQ(X)$ is a sum of polynomials the degree of $Z(X)$ is simply the maximum of the degrees of $Q(X), P(X)$ as desired. □ ✓ ✓

(c) Show that $[k(x) : k(t)] = [k(x) : k(\frac{P(x)}{Q(x)})] = \max(\ \deg P(x),\ \deg Q(x)\ )$.

Proof. (Thomas) Note that $\big(k(t)\big)(x) = k(x)$ since $t \in k(x)$ and $k(x)$ is a field. Then since $Z(X) = P(X) - tQ(X)$ is irreducible over $k(t)$ with x as a root, $Z(X) = m_{x,k(t)}(X)$ and $[\big(k(t)\big)(x) : k(t)] = [k(x) : k(t)] = deg(m_{x,k(t)}(X))$ which is the maximum of the degrees of $Q(X), P(X)$. □ Nice.

13.2.19 Let K be an extension of F of degree n.

(a) For any $\alpha \in K$ prove that α acting by left multiplication on K is an F-linear transformation of K.

?

Proof. (Thomas) Choose $\alpha \in K$ and define $\phi : K \to K$ by $\phi(k) = \alpha k$ and let $a, b \in F$ and $A, B \in K$. Observe that $\phi(aA + bB) = \alpha(aA + bB) = \alpha ab + \alpha bB = a\alpha A + b\alpha B = a\phi(A) + b\phi(B) \in K$ so left multiplication by α is an F-linear transformation on K. □

No. or Rather only .5 of a proof. What about $\psi(fk) = f\psi(k)$ for $f \in F$, $k \in K$?

(b) Prove that K is isomorphic to a subring of the ring of $n \times n$ matrices over F, so the ring of $n \times n$ matrices over F contains an isomorphic copy of *every* extension of F of degree $\leq n$.

Proof. (Thomas) Let $k \in K$. Since multiplication by α is a linear transformation, there exists a matrix $M_\alpha \in M_n(K)$ such that αk is the ~~same transformation~~ as $M_\alpha k$. Then define $\psi : K \to M_n(K)$ by $\psi(k) \mapsto M_k$. Noting that linear transformation have unique matrix representations (and vice versa) we see that ψ is well defined and a bijection.

Not a good choice of language. A matrix represents a l.t. wrt some basis $\mathcal{B}$.

Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for K. Then note that for any $\gamma \in K$, $M_\gamma = \left(\gamma\alpha_1 \,\middle|\, \ldots \,\middle|\, \gamma\alpha_n\right)$.

Let $a, b \in K$ and note that $\psi(a+b) = M_{a+b} = \left((a+b)\alpha_1 \,\middle|\, \ldots \,\middle|\, (a+b)\alpha_n\right) = \left(a\alpha_1 \,\middle|\, \ldots \,\middle|\, a\alpha_n\right) + \left(b\alpha_1 \,\middle|\, \ldots \,\middle|\, b\alpha_n\right) = M_a + M_b = \psi(a) + \psi(b)$.

Further, note that $\psi(ab) = M_{ab} = \left(ab\alpha_1 \,\middle|\, \ldots \,\middle|\, ab\alpha_n\right) = \left(a\alpha_1 \,\middle|\, \ldots \,\middle|\, a\alpha_n\right)\left(b\alpha_1 \,\middle|\, \ldots \,\middle|\, b\alpha_n\right) = M_a M_b = \psi(a)\psi(b)$.

Then we see that ψ is a bijective ring homomorphism and is thus an isomorphism from $K \to \psi(M_n(K))$. ✓ □

13.2.20 Show that if the matrix of the linear transformation "multiplication by α" considered in the previous exercise is A then α is a root of the characteristic polynomial for A. This gives an effective procedure for determining an equation of degree n satisfied by an element α in an extension of F of degree n. Use this proceedure to obtain the monic polynomial of degree 3 satisfied by $2^{\frac{1}{3}}$ and by $1 + 2^{\frac{1}{3}} + 4^{\frac{1}{3}}$.

✓ Cayley - Hamilton

Proof. (Thomas) Note that by the Caley-Hamilton theorem A satisfies its own characteristic polynomial. Then since $\alpha \mapsto A$ by an isomorphism we see that α must satisfy the same polynomial. ✓

Consider $K = \mathbb{Q}(2^{\frac{1}{3}})$ with basis $\{1, 2^{1/3}, 2^{2/3}\}$.

Letting $\alpha = 2^{\frac{1}{3}}$, we obtain $M_\alpha = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. Note that M_α has the characteristic equation $x^3 - 2 = 0$ and that $2^{1/3}$ satisfies this equation. Then $x^3 - 2$ is the monic polynomial of degree 3 satisfied by $2^{\frac{1}{3}}$. ✓

Letting $\alpha = 1 + 2^{\frac{1}{3}} + 4^{1/3} = 1 + 2^{\frac{1}{3}} + 2^{\frac{2}{3}}$, we obtain $M_\alpha = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}$. Note that M_α has the characteristic equation $x^3 - 3x^2 - 3x - 1 = 0$ and that $1 + 2^{1/3} + 2^{2/3}$ satisfies this equation. Then $x^3 - 3x^2 - 3x - 1$ is the monic polynomial of degree 3 satisfied by $1 + 2^{\frac{1}{3}} + 4^{1/3}$. □

✓

Good.