Math 121 Homework 2 Solutions

- Section 13.2 # 16,18,19,21
- Section 13.4 # 1,2,3,4

Problem 13.2 #16. Let K/F be an algebraic extension and let R be a ring contained in K that contains F. Prove that R is a subfield of K containing F.

We will give two proofs. The first is more explicit, but the second contains important ideas that underlie the Theorems in Section 3.1.

First Solution. Let $t \in R$, $t \neq 0$. We must show that t is invertible in R. Since t is algebraic over F, it satisfies a polynomial equation $f(t) = 0$,

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0, \qquad a_i \in F.$$

We may assume that this polynomial is irreducible, and so it is not divisible by x. This means that $a_0 \neq 0$. Since R contains F, a_0 is invertible in R, and so

$$t(-a_0^{-1}a_n t^{n-1} + \ldots + a_0^{-1}a_1) = 1.$$

This means that $t^{-1} = -a_0^{-1}a_n t^{n-1} + \ldots + a_0^{-1}a_1 \in R.a_0 \neq 0$. Since R contains F, a_0 is invertible in R, and so

$$t(-a_0^{-1}a_n t^{n-1} + \ldots + a_0^{-1}a_1) = 1.$$

This means that $t^{-1} = -a_0^{-1}a_n t^{n-1} + \ldots + a_0^{-1}a_1 \in R$.

Second Solution. Let $t \in R$, $t \neq 0$. We give an alternate proof show that t is invertible in R. It is sufficient to show that t is contained in a subfield of K that is contained in R. Consider the ring homomorphism $\varepsilon_t : F[x] \longrightarrow R$ that is evaluation at t: thus $\varepsilon_t(g(x)) = g(t)$. The image of this homomorphism is an integral domain, and so its kernel $\mathfrak{p}$ is a prime ideal of $F[x]$. The ideal $\mathfrak{p}$ is nonzero because t is algebraic, and if $f(x)$ is a polynomial it satisfies, then $f(x) \in \mathfrak{p}$. Since a nonzero prime ideal of a principal ideal domain is maximal, $\mathfrak{p}$ is a maximal ideal. Therefore $F[x]/\mathfrak{p}$ is a field. By the First Isomorphism Theorem for Rings (Theorem 7 in Chapter 7 of Dummit and Foote, page 243), $F[x]/\mathfrak{p}$ is isomorphic to the image of ε_t, which is therefore a subfield of K. The image of ε_t contains $t = \varepsilon_t(x)$, and so we are done.

Problem 13.2 #19. Let K be an extension of F of degree n.

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

(b) Prove that K is isomorphic to a subfield of the ring $\mathrm{Mat}_n(F)$ of $n \times n$ integers over F. Thus $\mathrm{Mat}_n(F)$ contains a copy of *every* extension of F of degree $\leqslant n$.

Solution. Part (a) is obvious. Indeed, define $M_\alpha : K \longrightarrow K$ to be the map $M_\alpha(x) = \alpha x$. Then certainly $M_\alpha(x+y) = M_\alpha(x) + M_\alpha(y)$ and $M_\alpha(cx) = cM_\alpha(x)$ for $c \in F$, so M_α is a linear transformation.

Review of relevant Linear Algebra. If V is an F-vector space, let $\mathrm{End}_F(V)$ be the space of F-linear transformations of V. (Linear transformations are also called *vector space endomorphisms*, hence the notation End_F.)

Proposition 1. *If V is an n-dimensional vector space then* $\mathrm{End}_F(V) \cong \mathrm{Mat}_n(F)$.

Proof. Choose a basis $v_1, \cdots, v_n$ of V. If $T : V \longrightarrow V$ is a linear transformation, let M_T be the $n \times n$ matrix (t_{ij}) whose entries are defined by the equation

$$T(v_j) = \sum_i t_{ij} v_i.$$

Then $T \longmapsto M_T$ is a ring homomorphism. Indeed, let us check that $M_{TU} = M_T \cdot M_U$ (matrix multiplication). Write $M_U = (u_{ij})$ so that $U(v_j) = \sum u_{ij} v_i$. Then

$$TU(v_j) = T\left(\sum_k u_{kj} v_k\right) = \sum_k u_{kj} T(v_k) = \sum_k \sum_i u_{kj} t_{ik} v_i.$$

Therefore the i,j-th entry in M_{TU} is $\sum_k t_{ik} u_{kj}$, proving that $M_{TU} = M_T M_U$. We have defined a ring homomorphism $T \longmapsto M_T$ from $\mathrm{End}_F(V)$ to $\mathrm{Mat}_n(F)$. It is easy to see that it is bijective. □

Now we discuss (b). The map $\alpha \longmapsto M_\alpha$ is a ring homomorphism $K \longrightarrow \mathrm{End}(V) \cong \mathrm{Mat}_n(F)$. It is injective since if α is in then kernel, then M_α is the zero map, so $\alpha = M_\alpha(1) = 0$. This proves that $\mathrm{Mat}_n(F)$ contains a copy of K. But we are asked to show that it contains a copy of every extension of F of degree $\leqslant n$. So we have to consider what happens if $[K : F]$ is strictly $< n$. Let $d = [K : F]$. Then we embed K into $\mathrm{Mat}_d(F)$ as before, then embed $\mathrm{Mat}_d(F)$ into $\mathrm{Mat}_n(F)$ by sending a $d \times d$ block X to the matrix

$$\begin{pmatrix} X & \\ & I_{n-d} \end{pmatrix},$$

where I_{n-d} is the $(n-d) \times (n-d)$ identity matrix.

Problem 13.2 #21. Let $K = \mathbb{Q}\left(\sqrt{D}\right)$ for some squarefree integer D. Let $\alpha = a + b\sqrt{D}$ be an element of K. Use the basis $1, \sqrt{D}$ for K as a vector space over $\mathbb{Q}$ and show that the matrix of the linear transformation "multiplication by α" on K consdiered in the previous matrices has the matrix $\begin{pmatrix} a & bD \\ b & a \end{pmatrix}$. Show directly that the map $a + b\sqrt{D} \mapsto \begin{pmatrix} a & bD \\ b & a \end{pmatrix}$ is an isomorphism of K with a subfield of the ring of 2×2 matrices with coefficients in $\mathbb{Q}$.

Solution. Let $T_\alpha : K \longrightarrow K$ be the linear transformation of the multiplication by α map, so $T_\alpha(v) = \alpha v$ for $v \in K$. We identify K as a vector space with $\mathbb{Q}^2$ by the map sending $x + y\sqrt{D}$ to the column vector $\begin{pmatrix} x \\ y \end{pmatrix}$ for $x, y \in \mathbb{Q}$. With this identification

$$T\begin{pmatrix} 1 \\ 0 \end{pmatrix} = T(1) = a + b\sqrt{D} = \begin{pmatrix} a \\ b \end{pmatrix}$$

$$T\begin{pmatrix} 0 \\ 1 \end{pmatrix} = T\left(\sqrt{D}\right) = \left(a + b\sqrt{D}\right)\sqrt{D} = bD + a\sqrt{D} = \begin{pmatrix} bD \\ a \end{pmatrix}.$$

Since

$$\begin{pmatrix} a & bD \\ b & a \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}, \qquad \begin{pmatrix} a & bD \\ b & a \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} bD \\ a \end{pmatrix}$$

we see that with respect to this basis, T is represented by the matrix $\begin{pmatrix} a & bD \\ b & a \end{pmatrix}$.

Now let us check that the map $\theta : K \longrightarrow \mathrm{Mat}_2(\mathbb{Q})$ defined by

$$\theta\left(a + b\sqrt{D}\right) = \begin{pmatrix} a & bD \\ b & a \end{pmatrix}$$

is a ring homomorphism. We can prove that $\theta(\alpha\beta) = \theta(\alpha)\theta(\beta)$ in two ways.

First method: direct computation. Let $\alpha = a + b\sqrt{D}$, $\beta = c + d\sqrt{D}$ so $\alpha\beta = (ac + Dbd) + (ad + bc)\sqrt{D}$. Note that

$$\begin{pmatrix} a & bD \\ b & a \end{pmatrix}\begin{pmatrix} c & dD \\ d & c \end{pmatrix} = \begin{pmatrix} ac + Dbd & (ad + bc)D \\ ad + bc & ac + Dbd \end{pmatrix},$$

that is $\theta(\alpha)\theta(\beta) = \theta(\alpha\beta)$.

Second method: Since $T_\alpha T_\beta(v) = \alpha\beta v = T_{\alpha\beta}(v)$, the matrix of $T_{\alpha\beta}$ with respect to the basis $1, \sqrt{D}$ must be the product of the matrices of T_α and T_β, that is, $\theta(\alpha\beta) = \theta(\alpha)\theta(\beta)$.

It is easy to see that $\theta(\alpha + \beta) = \theta(\alpha) + \theta(\beta)$ and $\theta(1) = I_{\mathbb{C}^2}$ (the identity matrix) so θ is a ring homomorphism. It is injective since K is a field, so it is an isomorphism onto its image.

Problem 13.4 #1. Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 - 2$.

Solution. Let $\alpha = \sqrt[4]{2}$ be the positive real fourth root of 2. We will prove that the splitting field K of $x^4 - 2$ is $\mathbb{Q}(\alpha, i)$ and that it has degree 8 over $\mathbb{Q}$.

The polynomial $x^4 - 2$ is irreducible over $\mathbb{Z}$ by Eisenstein's criterion (By Proposition 13 on page 309 of Dummit and Foote) and then over $\mathbb{Q}$ by Gauss' Lemma (Proposition 5 on page 303).

By Proposition 13 on page 309 of Dummit and Foote it is irreducible in the polynomial ring $\mathbb{Z}[x]$. (Take P to be the prime ideal (3) of $\mathbb{Z}$.) But it follows from Gauss' Lemma (Proposition 5 on page 303) that if it can be factored in $\mathbb{Q}[x]$ then it can be factored in $\mathbb{Z}[x]$, which it can't be, so it is irreducible in $\mathbb{Q}[x]$.

The roots of $x^4 - 2 = 0$ are $\alpha, i\alpha, -\alpha, -i\alpha$ since $1, i, -1, -i$ are the fourth roots of unity. Since the splitting field K of $x^4 - 2$ over $\mathbb{Q}$ is the field generated by all the roots of the polynomial, we see that $K = \mathbb{Q}(\alpha, i\alpha, -\alpha, -i\alpha)$. The last two roots $-\alpha$ and $-i\alpha$ are obviously redundant, so $K = \mathbb{Q}(\alpha, i\alpha)$. This equals $\mathbb{Q}(\alpha, i)$. Indeed, both generators α and $i\alpha$ of K are clearly in $\mathbb{Q}(\alpha, i)$, so $\mathbb{Q}(\alpha, i\alpha) \subseteq \mathbb{Q}(\alpha, i)$. On the other hand, both generators α and $i = i\alpha/\alpha$ of $\mathbb{Q}(\alpha, i)$ are in $\mathbb{Q}(\alpha, i\alpha)$ and so $\mathbb{Q}(\alpha, i\alpha) = \mathbb{Q}(\alpha, i)$.

To prove that $[K : \mathbb{Q}] = 4$, we note that $[K : \mathbb{Q}] = [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$. The degree $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ because α is a root of an irreducible polynomial $x^4 - 2$ over $\mathbb{Q}$. We claim that $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$. Indeed, this is obtained by adjoining a root i of a

polynomial x^2+1 of degree 2 over $\mathbb{Q}(\alpha)$. So it is sufficient to show that this polynomial is irreducible over $\mathbb{Q}(\alpha)$. If not, since it has degree 2, it would have a root in $\mathbb{Q}(\alpha)$. (See Proposition 10 on page 308 of Dummit and Foote.) However the possible i and $-i$ are not in $\mathbb{Q}(\alpha)$ since $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, so this cannot happen. We see that $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$, so $[K : \mathbb{Q}] = [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$.

Problem 13.4 #2. Determine the splitting field and its degree over $\mathbb{Q}$ for x^4+2.

Solution. We will prove that the splitting field for this polynomial x^4+2 is the *same field* $K = \mathbb{Q}(\alpha, i)$ as in the previous problem #1, where as before $\alpha = 2^{1/4}$.

Let $\beta = \varepsilon\alpha$, where $\varepsilon = e^{2\pi i/8}$ is a primitive 8-th root of unity. The roots of the polynomial $x^4+2=0$ are $\beta, i\beta, -\beta, -i\beta$. So the splitting field is $\mathbb{Q}(\beta, i\beta) = \mathbb{Q}(\beta, i)$.

But we will show that $\mathbb{Q}(\beta, i) = \mathbb{Q}(\alpha, i)$. First note that

$$\varepsilon = e^{2\pi i/4} = \frac{1}{\sqrt{2}}(1+i) = \frac{1}{\alpha^2}(1+i), \qquad \beta = \varepsilon\alpha = \frac{1}{\alpha}(1+i).$$

This shows that $\beta \in \mathbb{Q}(\alpha, i)$, and obviously $i \in \mathbb{Q}(\alpha, i)$ so $\mathbb{Q}(\beta, i) \subseteq \mathbb{Q}(\alpha, i)$. On the other hand we may rewrite the last identity

$$\alpha = \frac{1}{\beta}(1+i),$$

and obviously $i \in \mathbb{Q}(\beta, i)$, so $\mathbb{Q}(\alpha, i) = \mathbb{Q}(\beta, i)$. We have proven that the splitting fields of the two polynomials x^4-2 and x^4+2 are the same.

Problem 13.4 # 3. *Determine the splitting field of* x^4+x^2+1, and its degree over $\mathbb{Q}$.

Solution. This polynomial factors as $x^4+x^2+1 = (x^2+x+1)(x^2-x+1)$. Moreover if α is a root of x^2+x+1 then $-\alpha$ is a root of x^2-x+1, so the roots of x^4+x^2+1 are precisely the roots ρ and ρ^2 of x^2+x+1, where $\rho = e^{2\pi i/3}$, together with their negatives $-\rho$ and $-\rho^2$. So the splitting field is just $\mathbb{Q}(\rho)$, which has degree 2 over $\mathbb{Q}$. This completes the solution of the problem.

Here is a line of reasoning that might lead you to guess that this polynomial is reducible and divisible by x^2+x+1. We begin by noticing that the roots of x^4+x^2+1 are sixth roots of unity. One way to see this is to notice that α is a root of x^4+x^2+1 if and only if α^2 is a root of x^2+x+1, and since $x^3-1 = (x-1)(x^2+x+1)$, these are cube roots of unity; so α must be a sixth root of unity. Since a cube root of unity is also a sixth root of unity, we might guess that the cube roots of unity, which are the roots of x^2+x+1 are also sixth roots of unity, suggesting that x^4+x^2+1 should be divisible by x^2+x+1.

Problem 13.4 #5. Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$. (Use Theorems 8 and 27.)

Before proceeding to the solution, a couple of remarks about splitting fields. First, a remark about the definition of the splitting field K of a polynomial f. We may assume that f is monic, but we do not assume that it is irreducible. As we will explain, the definition

(Dummit and Foote, page 536) is equivalent to asserting that $K = F(\alpha_1, \cdots, \alpha_n)$, where α_i are the roots of f in K, and that

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i). \tag{1}$$

Indeed, by definition f factors into linear factors in K, so we must have (1). The definition also assumes that f does not factor into linear factors over any proper subfield of K. This is equivalent to assuming that K is the field $F(\alpha_1, \cdots, \alpha_n)$ generate by the roots α_i. Indeed, letting $K' = F(\alpha_1, \cdots, \alpha_n)$, the factorization (1) is valid in $K'[x]$ and so K' may not be proper, that is, $K = K'$.

Dummit and Foote (on page 536) define the splitting field of a polynomial, but then in the definition of a normal extension (on page 537) they talk about the splitting field of a *collection* of polynomials. Indeed, if the collection is a finite set, $f_1, \cdots, f_n$, then it is obvious from the definition that the splitting field of this collection of polynomials is the same as the splitting field of the single polynomial $f_1 \cdots f_n$. The more general language of the definition of a normal extension is only needed for extension that are algebraic, but infinite, such as $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}, \cdots\right)$, which is a splitting field for an infinite collection of polynomials. Since we can't multiply an infinite number of polynomials together, the more general notion is needed. In problem 13.4, the field extension is assumed to be finite, so we will interpret *splitting field* to mean the splitting field of a polynomial.

Solution. First suppose that $K = F(\alpha_1, \cdots, \alpha_n)$ is the splitting field over F, and let $g \in F[x]$ be another polynomial that has a β root in K. The problem assumes that g is irreducible over F and asks for us to show that g splits in K. So let $L \supseteq K$ be a splitting field over K for

$$g(x) = \prod_{i=1}^{m} (x - \beta_i). \tag{2}$$

Thus

$$L = K(\beta_1, \cdots, \beta_m) = F(\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_m).$$

Since $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_m$ are the roots of fg, we see that L is also a splitting field over F for fg. Since β is one of the roots of g, we order them so that $\beta = \beta_1$. We have $\beta_1 \in K$ want to show that the other $\beta_i \in K$.

Since $\beta = \beta_1$ and β_i are roots of the same irreducible polynomial g, by Theorem 8 (page 519) there exists a homomorphism $\varphi : F(\beta) \longrightarrow F(\beta_i)$ such that φ is the identity map on F, and $\varphi(\beta) = \beta_i$. Now we apply Theorem 27 (page 541) using this φ and the polynomial fg to deduce that φ can be extended to a homomorphism $\varphi : L \longrightarrow L$.

We will now show that $\varphi(K) = K$. Indeed, φ takes the polynomial f to itself (since it is the indentity on F and $f \in F[X]$), so it permutes the roots of F, therefore

$$\varphi K = F(\varphi(\alpha_1), \cdots, \varphi(\alpha_n)) = K.$$

Since $\beta \in K$ it follows that $\beta_i \in \varphi(\beta) \in K$.

We have shown that all the roots β_i of g are in K, so g splits into linear factors in K.

We also need to prove the other direction: if every irreducible polynomial with a root in K splits completely in K, then K is a splitting field. We note that since K/F is finite, $K = F(\alpha_1, \cdots, \alpha_n)$ for some $\alpha_i \in K$, and each α_i is algebraic over F. Let f_i be the irreducible polynomial in $F[X]$ that is satisfied by f_i, then all roots of f_i are in K, by assumption. Now let $f = f_1 \cdots f_n$. Then K contains all roots of f, and is generated by these roots, so K is a splitting field over F.