MATH 7752 Homework 7

James Harbour

March 25, 2022

Problem 1

(a): Consider the field $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Prove that $[K : \mathbb{Q}] = 4$.

Proof. As $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$, it follows that $[K : \mathbb{Q}(\sqrt{2})] \leq 2$. We claim that $\sqrt{3} \notin Q(\sqrt{2})$. Suppose, for the sake of contradiction, that $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Then there exist $a, b \in \mathbb{Q}$ such that $a + b\sqrt{2} = \sqrt{3}$. So $3 = a^2 + 2ab\sqrt{2} + 2b^2$, whence a or b is 0 as otherwise this would imply that $\sqrt{2}$ is rational which is absurd. If both are zero, the $3 = 0$ which is absurd, so at least one of them is nonzero. If $a = 0, b \neq 0$, then $3 = 2b^2$, which is absurd as 3 is odd. If $b = 0, a \neq 0$, then $3 = a^2$ whence $a = \pm\sqrt{3}$ which is absurd as $a \in \mathbb{Q}$.

Thus, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, so $[K : \mathbb{Q}(\sqrt{2})] = 2$ whence

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$$

□

(b): Let $L = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Show that $L = K$.

Proof. Clearly $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, so it suffices to prove the reverse inclusion. Let $\alpha = \sqrt{2} + \sqrt{3}$. By rationalizing, we find that $\frac{1}{\alpha} = \sqrt{3} - \sqrt{2}$ whence $\sqrt{2} = \alpha - \frac{1}{\sqrt{\alpha}} \in \mathbb{Q}(\alpha)$ and $\sqrt{3} = \alpha + \frac{1}{\sqrt{\alpha}} \in \mathbb{Q}(\alpha)$, so $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\alpha)$. □

Problem 2

Let $S = \{n_1, \ldots, n_r\}$ be a finite set of positive integers with $n_i \geq 2$. For each $j \in \{1, \ldots, r\}$ let $\mathbb{Q}_j = \mathbb{Q}(\sqrt{n_1}, \ldots, \sqrt{n_j})$. Moreover, set $\mathbb{Q}_0 = \mathbb{Q}$.

(a): Prove that $[\mathbb{Q}_r : \mathbb{Q}] = 2^m$ for some integer $0 \leq m \leq r$. Moreover, show that the following set spans $\mathbb{Q}_r$ over $\mathbb{Q}$,

$$P(S) = \{1\} \cup \{\sqrt{n} : n \text{ is a product of distinct elements from } S\}.$$

Proof. For all i, as $\sqrt{n_i}^2 - n_i = 0$, it follows that $\mu_{n_i, Q_{i-1}} | x^2 - n_i$ so $[Q_i : Q_{i-1}] \in \{1, 2\}$. Thus,

$$[Q_r : Q] = [Q_r : Q_{r-1}] \cdots [Q_1 : Q_0] = 2^m$$

for some $m \leq r$. As $\sqrt{S} := \{\sqrt{n} : n \in S\} \subseteq P(S)$ and every element of $\sqrt{S}$ is algebraic over Q, $\mathbb{Q}_r = Q(P(S)) = Q[P(S)]$ as desired. □

(b): Prove that $[\mathbb{Q}_r : \mathbb{Q}] < 2^r$ if and only if n_1 is a complete square, or there exists $2 \leq j \leq r$ such that $\sqrt{n_j} = \alpha + \beta\sqrt{n_{j-1}}$, for some $\alpha, \beta \in \mathbb{Q}_{j-2}$.

Proof.
$\underline{\Longrightarrow}$: Suppose that $[\mathbb{Q}_r : \mathbb{Q}] < 2^r$. If n_1 is not a complete square, then $[Q_1 : Q_0] = 2$ whence there is at least one $j \in \{2, \dots, r\}$ such that $[\mathbb{Q}_j : \mathbb{Q}_{j-1}] = 1$. Then $\sqrt{n_j} \in \mathbb{Q}_{j-1} = \mathbb{Q}_{j-2}(\sqrt{n_{j-1}}) = \mathbb{Q}_{j-2}[\sqrt{n_{j-1}}]$, so there exist $a, b \in Q_{j-2}$ such that $\sqrt{n_j} = a + b\sqrt{n_{j-1}}$.

$\underline{\Longleftarrow}$: If n_1 is a complete square then $[\mathbb{Q}_1 : \mathbb{Q}_0] = 1$ whence $[\mathbb{Q}_r : \mathbb{Q}] \leq 2^{r-1} < 2^r$, so suppose that n_1 is not a complete square and that there exists $2 \leq j \leq r$ such that $\sqrt{n_j} = \alpha + \beta\sqrt{n_{j-1}}$, for some $\alpha, \beta \in \mathbb{Q}_{j-2}$. Then $\sqrt{n_j} \in \mathbb{Q}_{j-2}[\sqrt{n_{j-1}}] = \mathbb{Q}_{j-2}(\sqrt{n_{j-1}}) = \mathbb{Q}_{j-1}$, whence $[\mathbb{Q}_j : \mathbb{Q}_{j-1}] = 1$ and thus $[\mathbb{Q}_r : \mathbb{Q}] \leq 2^{r-1} < 2^r$. □

(c): Suppose that the integers $n_1, \dots, n_r$ are square-free and pairwise relatively prime. Prove that $[\mathbb{Q}_r : \mathbb{Q}] = 2^r$. Conclude that the extension $L = \mathbb{Q}(T)$, where $T = \{\sqrt{n} : n \in \mathbb{N}, n \text{ square free}\}$ is an infinite algebraic extension of $\mathbb{Q}$.

Problem 3

Let F be a field and α an algebraic element of odd degree over F (i.e. the degree $[F(\alpha) : F]$ is odd). Show that $F(\alpha^2) = F(\alpha)$.

Proof. Note that we have a tower of field extensions $F \subseteq F(\alpha^2) \subseteq F(\alpha)$. As α is a root of $x^2 - \alpha^2 \in F(\alpha^2)[x]$, it follows that $\mu_{\alpha, F(\alpha^2)} | x^2 - \alpha^2$ and thus $[F(\alpha) : F(\alpha^2)] \leq 2$. Suppose, for the sake of contradiction, that $F(\alpha^2) \neq F(\alpha)$. Then $[F(\alpha) : F(\alpha^2)] = 2$, whence $[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F] = 2[F(\alpha^2) : F]$ is even, contradiction the assumption that α has odd degree over F. □

Problem 4

Let K/F be an algebraic extension.

(a): Let $F \subset R \subset K$ where R is a subring of K. Prove that R must be a subfield.

Proof. Let $\alpha \in R \setminus \{0\}$. Then as K/F is algebraic and $\alpha \in K$, so α is algebraic over F. Hence, $F(\alpha) = F[\alpha] \subseteq R$, whence $\alpha^{-1} \in R$, so R is a field. □

(b): Show that (a) would be false if we dropped the assumption that K/F is algebraic.

Proof. Suppose that K/F is not algebraic. Take $\alpha \in K \setminus \{0\}$ transcendental over F. Then $F[\alpha]$ is a subring of K. We claim that $\frac{1}{\alpha} \notin F[\alpha]$. Suppose, for the sake of contradiction, that $\frac{1}{\alpha} \in F[\alpha]$. Then there exist $b_0, \cdots, b_n \in F$ such that $f(x) = b_n x^n + \cdots + b_0 \in F[x]$ has $f(\frac{1}{\alpha}) = 0$. Then

$$0 = \alpha^n \cdot f\left(\frac{1}{\alpha}\right) = \sum_{k=0}^{n} b_k \alpha^{n-k}$$

whence α is algebraic over F, contradicting that α is transcendental over F. □

Problem 5

Let K/F be a finite field extension, $n = [K : F]$, and fix some basis $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ of K over F. For any $\alpha \in K$ define $T_\alpha : K \to K$ by $\beta \mapsto \alpha\beta$. Note that $T_\alpha \in \mathrm{End}_F(K)$. Let $A_\alpha = [T_\alpha]_\Omega \in M_n(F)$ be the matrix of T_α with respect to Ω.

(a): Prove that the map $K \xrightarrow{\rho} M_n(F)$ given by $\alpha \mapsto A_\alpha$ is an injective ring homomorphism.

Proof. Note that, if $\alpha, \beta \in K$, then $(T_\alpha T_\beta)(\gamma) = T_\alpha(\beta\gamma) = \alpha\beta\gamma = T_{\alpha\beta}(\gamma)$ and $(T_\alpha + T_\beta)(\gamma) = T_\alpha(\gamma) + T_\beta(\gamma) = (\alpha + \beta)\gamma = T_{\alpha+\beta}(\gamma)$ for all $\gamma \in K$, so $T_\alpha T_\beta = T_{\alpha\beta}$ and $T_\alpha + T_\beta = T_{\alpha+\beta}$. Thus

$$\begin{aligned} A_\alpha A_\beta &= [T_\alpha]_\Omega [T_\beta]_\Omega = [T_\alpha T_\beta]_\Omega = [T_{\alpha\beta}]_\Omega = A_{\alpha\beta} \\ A_\alpha + A_\beta &= [T_\alpha]_\Omega + [T_\beta]_\Omega = [T_\alpha + T_\beta]_\Omega = [T_{\alpha+\beta}]_\Omega = A_{\alpha+\beta}, \end{aligned}$$

so the map $\alpha \mapsto A_\alpha$ is a ring homomorhpism. As $\ker(\rho) \subseteq K$ is an ideal of the field K, it follows that $\ker(\rho) \in \{0, K\}$. Thus, it suffices to show that ρ is nonzero, whence it would follow that $\ker(\rho) \neq K$ and thus $\ker(\rho) = 0$. To see this, note that $1 \neq 0$ in K and $\rho(1) = [T_1]_\Omega = [id_K]_\Omega \neq 0$ as $id_K(\alpha_i) = \alpha_i \neq 0$. □

(b): Prove that the minimal polynomial of α over F and the minimal polynomial of A_α coincide.

Proof. Let $\mu_\alpha = \sum_{k=0}^{s} c_k x^k \in F[x]$ be the minimal polynomial of α over F. Let $\{e_1, \cdots, e_n\}$ be the standard basis for F^n. On one hand, note that for $1 \leq i \leq n$,

$$\mu_\alpha(A_\alpha)(e_i) = \left(\sum_{k=0}^{s} c_k A_\alpha^k\right)(e_i) = \sum_{k=0}^{s} c_k [T_\alpha^k(\alpha_i)] = \sum_{k=0}^{s} c_k \alpha^k \alpha_i = \mu_\alpha(\alpha)\alpha_i = 0$$

whence $\mu_\alpha(A_\alpha) = 0$. Thus $\mu_\alpha \in \mathrm{Ann}(A_\alpha)$.

On the other hand, suppose that $f(x) \in \mathrm{Ann}(A_\alpha)$. Observe that, for $\beta \in K$

$$f(T_\alpha)(\beta) = \left(\sum_{k=0}^{s} b_k T_\alpha^k\right)(\beta) = \sum_{k=0}^{s} b_k \alpha^k \beta = T_{f\alpha}(\beta),$$

so $f(T_\alpha) = T_{f(\alpha)}$. Then

$$0 = f(A_\alpha) = \sum_{k=0}^{s} b_k [T_\alpha]_\Omega^k = \left[\sum_{k=0}^{s} b_k T_\alpha^k\right] = [f(T_\alpha)]_\Omega = [T_{f(\alpha)}]_\Omega = A_{f(\alpha)} = \rho(f(\alpha)),$$

whence by injectivity of ρ, $f(\alpha) = 0$, i.e. $f(x) \in (\mu_\alpha)$.

Thus $(\mu_\alpha) = \mathrm{Ann}(A_\alpha)$, so by uniqueness of the monic generators for each of these ideals, the minimal polynomial for α over F and the minimal polynomial of A_α coincide. □

Problem 6

Let K/F be an extension of fields and let $F \subseteq K_1 \subseteq K$ and $F \subseteq K_2 \subseteq K$ be two subextensions of K/F. The *compositum* of K_1 and K_2 is the smallest subfield of K that contains both K_1 and K_2. **Notation:** We denote the compositum by K_1K_2.

(a): Consider the F-algebra $K_1 \otimes_F K_2$. Show that there exists a unique F-algebra homomorphism $\Phi : K_1 \otimes_F K_2 \to K_1K_2$ such that $\Phi(a \otimes b) = ab$. Conclude that $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$.

Proof. Define a map $\varphi : K_1 \times K_2 \to K_1K_2$ by $\varphi(a, b) = ab$. This map is clearly F-bilinear and $\varphi(ac, bd) = acbd = abcd = \varphi(a, b)\varphi(c, d)$, so there exists a unique F-algebra homomorphism $\Phi : K_1 \otimes_F K_2 \to K_1K_2$ such that $\Phi(a \otimes b) = ab$.
If either K_1 or K_2 is infinite degree over F, then the inequality is trivially true, so assume $[K_1 : F], [K_2 : F] < +\infty$. Then, by rank nullity theorem,

$$[K_1K_2 : F] = \dim_F(K_1K_2) \leq \dim_F(K_1 \otimes K_2) = \dim_F(K_1)\dim_F(K_2) = [K_1 : F][K_2 : F].$$

$\square$

(b): Assuming that K_1, K_2 are finite degree extensions over F, show that $K_1 \otimes_F K_2$ is a field if and only if the above $\leq$ becomes an equality.
(c): Suppose that $K_1 \cap K_2 \neq F$. Prove that $K_1 \otimes_F K_2$ is not a field.