

Math 500: //DRAFT ONLY// HW 10 due Friday, April 25, 2025.

Webpage: <http://dunfield.info/500>

Office hours: Wednesdays 1:30-2:30pm and Thursdays 2:00-3:00pm; additional times possible by appointment.

1. Let K/F be an extension of degree n .
 - (a) For $\alpha \in K$, prove that multiplication by α defines an F -linear transformation $T_\alpha: K \rightarrow K$.
 - (b) Prove that K is isomorphic to a subring of $M_{n \times n}(F)$.
 - (c) Prove that the minimal polynomial $m_{\alpha, F}(x)$ is the same as the minimal polynomial of the linear transformation T_α . Note: Thus α satisfies the characteristic polynomial of T_α . This can be used to help find minimal polynomials.

Thus, the ring of $n \times n$ matrices contains every degree n extension over F as a subring, up to isomorphism.

2. Determine the splitting field and its degree over \mathbb{Q} for $x^4 + 2$.
3. Determine the splitting field and its degree over \mathbb{Q} for $x^4 + x^2 + 1$.
4. Let $\phi: \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ be the Frobenius map. Determine the minimal polynomial and the rational canonical form of ϕ as an \mathbb{F}_p -linear map on the n -dimensional vector space \mathbb{F}_{p^n} .
5. A field element ζ is a root of unity if $\zeta^n = 1$ for some $n > 0$. Prove that if K is a finite extension of \mathbb{Q} then it contains only finitely many roots of unity.
6. Let $\zeta = e^{2\pi i/8}$. Show that $\sqrt{2} \in K = \mathbb{Q}(\zeta)$. Then determine the minimal polynomial of ζ over $F = \mathbb{Q}(\sqrt{2})$, and use this to describe all field homomorphisms $\phi: \mathbb{Q}(\zeta) \rightarrow \mathbb{C}$ such that $\phi|_F = \text{id}_F$.
7. Recall that $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{2} + \sqrt{3}$. Show that L/\mathbb{Q} is a splitting field of $f = x^4 - 10x^2 + 1$, and describe how $G = \text{Aut}(L/\mathbb{Q})$ permutes the roots of f .
8. Let $\zeta = e^{2\pi i/12}$ be a primitive 12th root of unity.
 - (a) Prove that ζ is a zero of the polynomial $f = x^4 - x^2 + 1$, and that the other zeros are $\zeta^5, \zeta^7, \zeta^{11}$.
 - (b) Show that $\zeta \notin \mathbb{Q}(\zeta^2)$.
 - (c) Prove that f is irreducible over \mathbb{Q} , and that it is the minimal polynomial of ζ over \mathbb{Q} .
 - (d) Prove that $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a splitting field of f .
9. Let ζ be as in the previous problem. Show that $G := \text{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$.

Credit: Problems 6-9 by Charles Rezk, rest from Dummit and Foote.