Midterm

Math 443/5

6 May 2026

Instructions

As always, your answer will be graded on the quality of presentation as well as the correct answer. To get a good score: write your answer neatly, use complete sentences, and *justify your work*.

- If you are enrolled in MTH 443, choose one of the following two options:
  - Option A: complete Exercises 1. and 2.
  - Option B: complete Exercises 1. and 3.
- If you are enrolled in MTH 543, complete Exercises 1. and 2.

Exercises

1. Let $\alpha = \sqrt{10 + 7\sqrt{2}}$ and $\beta = \sqrt{10 - 7\sqrt{2}}$. Write
   - f for the minimal polynomial for α over $\mathbb{Q}$,
   - K for the splitting field for f over $\mathbb{Q}$, and
   - G for the Galois group of K over $\mathbb{Q}$.

   (a) Compute f.

   (b) Prove that $K = \mathbb{Q}(\alpha)$, and deduce that $|G| = 4$. (Hint: show $\sqrt{2} \in \mathbb{Q}(\alpha)$ and compute $\alpha\beta$.)

   (c) Since
   - G acts transitively on the roots of f and
   - $|G| = 4$,

   there is exactly one element of G that maps α to β—let's call this element σ. Prove

   $$\sigma(\beta) = -\alpha.$$

   (Hint: compute $\sigma\left(\alpha^2\right)$ and use your work from part (b).)

   (d) Prove that G is cyclic.

   (e) By (d), we know G has exactly one subgroup of size two. What is that subgroup's fixed field?

2. Suppose $f \in \mathbb{Q}[x]$ is an irreducible cubic polynomial with exactly one real root. Let K be the splitting field for f and let G be the Galois group for K over $\mathbb{Q}$. Prove that $G \simeq S_3$.

3. Suppose that K/F is a degree-four Galois extension of fields with Galois group G. Prove: if there exist fields E_1, E_2 such that

   $$F \subsetneq E_1 \subsetneq K \qquad \text{and} \qquad F \subsetneq E_2 \subsetneq K \qquad \text{and} \qquad E_1 \neq E_2,$$

   then G is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. (Feel free to use your knowledge that there are exactly two isomorphism classes of groups of size four.)

Extra Credit

A definition

Definition.

We say an integer d is *squarefree* if

$$\text{for all primes } p: \qquad \text{if } p \mid d, \text{ then } p^2 \nmid d.$$

An exercise

Let $d > 1$ be a squarefree integer and consider the equation

$$X^2 - dY^2 = d.$$

Let $(m, n) \in \mathbb{Z}^2$ be any solution to the above equation. Let

- $f(x) = x^4 - 2mx^2 + d \in \mathbb{Q}[x]$,
- K be the splitting field for $f(x)$ over $\mathbb{Q}$, and
- G be the Galois group of K over $\mathbb{Q}$.

1. Prove that $f(x)$ is irreducible.
2. Prove that G is cyclic of size four.