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 $\sigma(\alpha^2)$ 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.

Solutions

1. (a) Note that

$$(x-\alpha)(x+\alpha)(x-\beta)(x+\beta) = \left(x^2-(10+7\sqrt{2})\right)\left(x^2-(10-7\sqrt{2})\right) = x^4-20x^2+2,$$

which is irreducible by Eisenstein's Criterion at the prime two. Hence, we see $f(x) = x^4-20x^2+2$.

(b) Since $\frac{\alpha^2-10}{7} = \sqrt{2}$, we see $\sqrt{2} \in \mathbb{Q}(\alpha)$; and since $\alpha\beta = \sqrt{2}$, we see that $\beta = \frac{\sqrt{2}}{\alpha} \in \mathbb{Q}(\alpha)$. So we conclude $K = \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha)$.

(c) Since $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(K)$, we note that

$$10+7\sigma\left(\sqrt{2}\right) = \sigma\left(10+7\sqrt{2}\right) = \sigma\left(\alpha^2\right) = \sigma(\alpha)^2 = \beta^2 = 10-7\sqrt{2},$$

which tells us that $\sigma\left(\sqrt{2}\right) = -\sqrt{2}$. Thus, using part (b), we see that

$$\sigma(\beta) = \sigma\left(\frac{\sqrt{2}}{\alpha}\right) = \frac{\sigma\left(\sqrt{2}\right)}{\sigma(\alpha)} = \frac{-\sqrt{2}}{\beta} = -\alpha.$$

(d) Since $\sigma(\alpha) = \beta \neq \alpha$, we know that σ is not the identity in G. And we can use (c) to see that

$$\sigma^2(\alpha) = (\sigma\circ\sigma)(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\beta) = -\alpha \neq \alpha,$$

so σ^2 is *also* not the identity in G. But by (b), we know that $|G| = 4$, so the order of σ is either 1, 2, or 4. We have ruled out the first two possibilities, so we conclude that the order of σ is 4. In particular, the group G is cyclic.

(e) Since

- $[K:\mathbb{Q}] = 4$ by our work in (b),
- $\sqrt{2} \in K$ by our work in (b),
- $\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right] = 2$, and
- G has precisely one nontrivial subgroup by (d),

we know that $\mathbb{Q}\left(\sqrt{2}\right)$ is a nontrivial subextension of $K/\mathbb{Q}$, which—by the Fundamental Theorem of Galois Theory—must be the fixed field of the only nontrivial subgroup of G.

2. Let α be a real root of f, so $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$. But $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, so that $K \supsetneq \mathbb{Q}(\alpha)$ because K contains the nonreal roots of f. Thus, we see that $[K:\mathbb{Q}] > 3$. But we know that G is isomorphic to a subgroup of S_3. Since $|S_3| = 6$, we know by Lagrange's Theorem that G is isomorphic to S_3.

3. If G were cyclic, it would precisely three subgroups. So then by the Fundamental Theorem of Galois Theory, this would imply that the extension K/F has precisely three subextensions. But our hypothesis is that K/F has at least four subextensions! Thus, we conclude that G is not cyclic. There is only one other isomorphism class of groups of size four, so we deduce that G is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$.

Extra credit

Remark. We could do this problem exactly like Exercise 1. by writing

$$f(x) = \left(x - \sqrt{m+n\sqrt{d}}\right)\left(x + \sqrt{m+n\sqrt{d}}\right)\left(x - \sqrt{m-n\sqrt{d}}\right)\left(x - \sqrt{m-n\sqrt{d}}\right),$$

letting $\alpha = \sqrt{m+n\sqrt{d}}$ and $\beta = \sqrt{m-n\sqrt{d}}$, then noting things like $\alpha\beta = \sqrt{d}$, etc. Below is a different method, just for fun.

1. Since $d > 1$ it is divisible by at least one prime p. But we know $m^2 = d(1+n^2)$, so the fact that p is prime tells us $p \mid m$. By definition of squarefree, we know $p^2 \nmid d$, so we conclude that $f(x)$ is irreducible by Eisenstein's Criterion.

2. Since $d > 1$, we see $m \neq 0$ and $n \neq 0$. Let α be any root of $f(x)$, so that $\alpha^4 - 2m\alpha^2 + d = 0$. (And $\alpha \neq 0$ since $d > 1$.) Thus we may remark:

   - $\left(\frac{\alpha^2-m}{n\alpha}\right)^2 = \frac{\alpha^4-2m\alpha^2+m^2}{n^2\alpha^2} = \frac{-d+m^2}{n^2\alpha^2} = \frac{dn^2}{n^2\alpha^2} = \frac{d}{\alpha^2}$ by our hypothesis on (m,n) and
   - $-\alpha^2 - \frac{d}{\alpha^2} = \frac{-\alpha^4-d}{\alpha^2} = \frac{-2m\alpha^2}{\alpha^2} = -2m$ by the definition of α.

   Use these remarks to compute

$$\begin{aligned}
(x-\alpha)(x+\alpha)\left(x - \frac{\alpha^2-m}{n\alpha}\right)\left(x + \frac{\alpha^2-m}{n\alpha}\right) &= (x^2-\alpha^2)\left(x^2 - \left(\frac{\alpha^2-m}{n\alpha}\right)^2\right) \\
&= (x^2-\alpha^2)\left(x^2 - \frac{d}{\alpha^2}\right) && \text{(by our first remark)} \\
&= x^4 + \left(-\alpha^2 - \frac{d}{\alpha^2}\right)x^2 + d \\
&= f(x) && \text{(by our second remark),}
\end{aligned}$$

   so we see that $K = \mathbb{Q}(\alpha)$, and $|G| = [K:\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}] = 4$.

   Now, as in Exercise 1., since

   - G acts transitively on the roots of f and
   - $|G| = 4$,

   there is exactly one automorphism in G that maps α to $\frac{\alpha^2-m}{n\alpha}$—let's call this automorphism σ. And we compute, using our earlier remarks:

$$\begin{aligned}
\sigma^2(\alpha) = (\sigma\circ\sigma)(\alpha) = \sigma(\sigma(\alpha)) = \sigma\left(\frac{\alpha^2-m}{n\alpha}\right) &= \frac{\sigma(\alpha)^2 - m}{n\sigma(\alpha)} \\
&= \frac{\frac{d}{\alpha^2} - m}{n\left(\frac{\alpha^2-m}{n\alpha}\right)} && \text{(by our first remark)} \\
&= \frac{(2m-\alpha^2)-m}{\frac{\alpha^2-m}{\alpha}} && \text{(by our second remark)} \\
&= \frac{m-\alpha^2}{\frac{\alpha^2-m}{\alpha}} \\
&= -\alpha \\
&\neq \alpha,
\end{aligned}$$

   Thus, since the order of σ is neither 1 nor 2, and $|G| = 4$, we conclude that G is cyclic of size four.