University of Wyoming

Math 4520—Fall 2025

Algebra III

Fields

Department of Mathematics

# Solutions to the Test

November, 2025

1. (a) Divide the equation $\alpha^4 - 16\alpha^2 + 4 = 0$ by $4\alpha^4$ to obtain $\frac{1}{4} - 4\left(\frac{1}{\alpha}\right)^2 + \left(\frac{1}{\alpha}\right)^4 = 0$. The minimal polynomial of $\frac{1}{\alpha}$ over $\mathbb{Q}$ is $x^4 - 4x^2 + \frac{1}{4}$. (Any factorization of this polynomial is equivalent to a factorization of the original $m(x)$. Our new polynomial can't be reducible, because the original $m(x)$ was irreducible.)

   (b) $x^2 - 16x + 4$

   (c) $m(x) = x^4 - 16x^2 + 4$

2. We discussed the extension $\mathbb{Q}[\zeta] \supset \mathbb{Q}$ at length in class, where $\zeta$ is a primitive ninth root of unity.

   (a) No; for example $\zeta^7 + \zeta^4 + \zeta = 0$ and $\zeta^8 + \zeta^5 + \zeta^2 = 0$. These are obtained directly from the relation $f(\zeta) = \zeta^6 + \zeta^3 + 1 = 0$. Each of the three sets $\{1, \zeta^3, \zeta^6\}$, $\{\zeta, \zeta^4, \zeta^7\}$, and $\{\zeta^2, \zeta^5, \zeta^8\}$ forms the vertices of an equilateral triangle centered at 0.

   (b) $[E : \mathbb{Q}] = 6$ equals the degree of the minimal polynomial $f(x)$. Here $\{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$ is a basis for the extension $E \supset \mathbb{Q}$.

   (c) As pointed out in class (using De Moivre's relation), $\alpha = \zeta + \zeta^{-1} = \zeta + \zeta^8$.

   (d) In class, we found the minimal polynomial to be $x^3 - 3x + 1$. Recall that $\alpha = \zeta + \zeta^{-1}$ so $\alpha^3 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} = 3\alpha + \zeta^3 + \zeta^6 = 3\alpha - 1$, so $\alpha^3 - 3\alpha + 1 = 0$.

   (e) $[F : \mathbb{Q}] = 3$ equals the degree of the minimal polynomial in (d). Here $\{1, \alpha, \alpha^2\}$ is a basis for the extension $F \supset \mathbb{Q}$.

   (f) The three roots are $\alpha = \zeta + \zeta^8 = 2\cos\frac{2\pi}{9}$, $\zeta^2 + \zeta^7 = 2\cos\frac{4\pi}{9}$, and $\zeta^4 + \zeta^5 = 2\cos\frac{8\pi}{9}$.

3. (a) Since $\mathbb{Q}[2\alpha+1] = \mathbb{Q}[\alpha] = E$, this extension has degree 9.

   (b) Consider $F = \mathbb{Q}[\alpha^2] \subseteq E$. Since $E = F[\alpha]$ where $\alpha$ is a root of $f(x) = x^2 - \alpha^2 \in F[x]$, we have $[E : F] = 1$ or $2$ according as $\alpha \in F$ or $\alpha \notin F$. The latter possibility cannot occur, otherwise $9 = [E : \mathbb{Q}] = [E : F][F : \mathbb{Q}] = 2[F : \mathbb{Q}]$, which is impossible. So $E = F$ which has degree 9 over $\mathbb{Q}$.

   (c) This is very similar to (b), but in this case the extension has degree either 3 or 9 and it is impossible to say with certainty which value is correct. Consider $F = \mathbb{Q}[\alpha^3] \subseteq E$. We have $E = F[\alpha]$ where $\alpha$ is a root of $f(x) = x^3 - \alpha^3 \in F[x]$. If $\alpha \in F$ then $F = E$ has degree 9 over $\mathbb{Q}$. Otherwise $\alpha \notin F$ and $[E : F] = [F : \mathbb{Q}] = 3$. As an example of the latter case, consider $\alpha = 2^{1/9}$ so that $\alpha^3 = 2^{1/3}$.

4. $\left[\begin{smallmatrix}2&1\\3&4\end{smallmatrix}\middle|\begin{smallmatrix}4\\1\end{smallmatrix}\right] \sim \left[\begin{smallmatrix}1&4\\3&4\end{smallmatrix}\middle|\begin{smallmatrix}2\\1\end{smallmatrix}\right] \sim \left[\begin{smallmatrix}1&4\\0&6\end{smallmatrix}\middle|\begin{smallmatrix}2\\2\end{smallmatrix}\right] \sim \left[\begin{smallmatrix}1&4\\0&1\end{smallmatrix}\middle|\begin{smallmatrix}2\\5\end{smallmatrix}\right] \sim \left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\middle|\begin{smallmatrix}3\\5\end{smallmatrix}\right]$.

   The unique solution is $(x, y) = (3, 5)$. *Check*: $2{\cdot}3 + 5 = 4$; $3{\cdot}3 + 4{\cdot}5 = 1$.

5. All 3 roots of $m(x) = x^3 + x + 1$ are found in the field $E$. They are found to be $\theta$, $\theta^2$, and $\theta^4$. Of course we were given that $\theta$ is a root of $m(x)$; and the others are checked using the table, and the fact that $\theta^7 = 1$:

$$m(\theta^2) = \theta^6 + \theta^2 + 1 = (1{+}\theta^2) + \theta^2 + 1 = 0;$$
$$m(\theta^4) = \theta^{12} + \theta^4 + 1 = \theta^5 + \theta^4 + 1 = (1{+}\theta{+}\theta^2) + (\theta{+}\theta^2) + 1 = 0.$$

   And there is a faster way to see this, starting with $m(\theta) = 0$, then squaring both sides, then squaring again. This approach will make more sense after we have discussed field automorphisms. . .

6. (a) T (b) F (c) F (d) F (e) T (f) T (g) F (h) F (i) F (j) F

   Some comments and explanations, provided for your benefit only (not required for answering #6):

   (a) Every subfield of $\mathbb{C}$ contains $\mathbb{Q}$.
   (b) Since $[\mathbb{Q}[2^{1/3}] : \mathbb{Q}] = 3$ is not divisible by $[\mathbb{Q}[2^{1/2}] : \mathbb{Q}] = 2$, $\mathbb{Q}[2^{1/2}]$ cannot be a subfield of $\mathbb{Q}[2^{1/3}]$ (by the transitivity of degrees of field extensions).
   (c) As indicated in class, every number field (finite extension of $\mathbb{Q}$) has only finitely many subfields.
   (d) The transcendental number $\pi$ lies in the subfield $\mathbb{Q}(\pi) \subset \mathbb{R}$ which is not a finite extension of $\mathbb{Q}$. If $[\mathbb{Q}(\pi) : \mathbb{Q}] = n < \infty$, then $1, \pi, \pi^2, \ldots, \pi^n$ would be linearly dependent over $\mathbb{Q}$, forcing $\pi$ to be the root of a nonzero polynomial of degree at most $n$ with rational coefficients, a contradiction.
   (e) Given $\alpha \in \mathbb{C}$, the polynomial $x^2 - \alpha \in \mathbb{C}[x]$ has a root by the Fundamental Theorem of Algebra.
   (f) If $\alpha \in \mathbb{Q}[\beta]$, then $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\beta]$. If $\beta \in \mathbb{Q}[\alpha]$, then $\mathbb{Q}[\beta] \subseteq \mathbb{Q}[\alpha]$. Combine these two conclusions.
   (g) This sounds too much like AI slop. Assuming $\alpha \in \mathbb{C}$ even has a minimal polynomial $m(x)$, then by definition, $\alpha$ is algebraic. Saying that $m(x)$ is irreducible in $\mathbb{Q}[x]$ is redundant. And saying that $m(x)$ has no real roots is irrelevant (well, it says that $m(x)$ must have even degree, but this has no bearing on the question: a total non sequitur).
   (h) Again, this sounds like AI slop. (And I sound like I am on a rant, sorry.) The ring of $2 \times 2$ real matrices is not even commutative, and it has zero divisors.
   (i) The set $\mathbb{A}$ consisting of all elements $\alpha \in \mathbb{C}$ which are algebraic over $\mathbb{Q}$, is a subfield (which we have introduced in class) of degree $[\mathbb{A} : \mathbb{Q}] = \infty$.
   (j) Every irreducible polynomial in $\mathbb{R}[x]$ has degree 1 or 2. This is a corollary of the Fundamental Theorem of Algebra; see the handout on Complex Numbers for details.