Exam 1 – In Class

MATH 322 **Solutions** February 18, 2019

Name: _____

Instructions: Answer each of the following questions, and make sure you SHOW ALL YOUR WORK! Answers without supporting work will be counted as incorrect. When asked to explain or prove your answers, use complete English sentences.

(12pts) 1. Suppose α is a real number such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. What does this tell you about...

(a) ...the number α in terms of polynomials? Be as specific as possible.

Solution: That there is a degree 3 polynomial $p(x)$ that has α as a root.

(b) ...about the field $\mathbb{Q}(\alpha)$? What does the field look like (i.e., what does a basis look like)?

Solution: A basis is $\{1, \alpha, \alpha^2\}$ (has size 3). Every element in the field can be written $a + b\alpha + c\alpha^2$ for $a, b, c \in \mathbb{Q}$.

(c) ...about the Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$, if you know also that $\mathbb{Q}(\alpha)$ is a splitting field? (You should say what sorts of things and how many of them are in the Galois group.)

Solution: The Galois group will contain three elements, each an automorphism of $\mathbb{Q}(\alpha)$ that leaves $\mathbb{Q}$ fixed. In other words, $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \mathbb{Z}_3$.

(d) ...about whether it is possible to construct a line segment of length α using a compass and straight edge? Briefly explain.

Solution: α will NOT be a constructible number, since constructible numbers must exist in a field extension of $\mathbb{Q}$ that is degree 2^k for some k.

(12pts) 2. For each item below, say whether the statement is TRUE or FALSE and justify your answer. If the statement is true, briefly explain why; if the statement is false, give a counterexample with brief explanation.

(a) Every algebraic number is constructible.

Solution: False. For example, $\sqrt[3]{2}$ is algebraic (since it is the root of the polynomial $x^3 - 2$) but not constructible (since it does not live in a degree 2^k extension of $\mathbb{Q}$).

(b) If α is an algebraic number, then $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/\langle p(x)\rangle$ for some polynomial $p(x)$.

Solution: True. $p(x)$ will be the minimal polynomial for α. The isomorphism is given by the FHT, via the evaluation homomorphism (evaluating at α).

(c) If $\mathbb{Q}(\alpha)$ is a degree 2 extension of $\mathbb{Q}$, then then $\alpha = \sqrt{c}$ for some $c \in \mathbb{Q}$.

Solution: False. For example, the polynomial $x^2 - 3x + 6$ is irreducible. Let α be a root, so $\mathbb{Q}(\alpha)$ is a degree 2 extension of $\mathbb{Q}$. However, if $\alpha = \sqrt{c}$, then since $\alpha^2 = 3\alpha - 6$ we would have $c = 9c - 36\alpha + 36$ which would say that $\alpha = \frac{8c+36}{36}$ which would make α rational.

(d) If $p(\alpha) = 0$, then $\mathbb{Q}(\alpha)$ is the splitting field for $p(x)$.

Solution: False. $p(x) = x^3 - 2$ has three roots, but $\mathbb{Q}(\sqrt[3]{2})$ does not contain all the roots of $p(x)$, so is not the splitting field for it.

(12pts) 3. Consider the field $E = \mathbb{Q}(\sqrt{5} + \sqrt[3]{7})$ and its subfields. In each part below, find the degree of the field extension and explain how you know you are correct.

(a) $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}]$.

Solution: The degree is 2, since $\sqrt{5}$ has minimum polynomial $x^2 - 5$ (irreducible by Eisenstein's criterion).

(b) $[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}]$.

Solution: The degree is 3, as $\sqrt[3]{7}$ is the root of the irreducible polynomial $x^3 - 7$.

(c) $[E : \mathbb{Q}(\sqrt{5})]$. Hint: Use the fact that E contains both $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt[3]{7})$.

Solution: The degree must be 3, since the degree of E over $\mathbb{Q}$ will be 6 (see below). We cannot have the degree be 1, because that would mean that $\sqrt[3]{7}$ was already in $\mathbb{Q}(\sqrt{5})$, but that would mean the degree of $\mathbb{Q}(\sqrt[3]{7})$ over $\mathbb{Q}$ would be at most 2 (it is not). The degree cannot be 2 either, because that would make $[E : \mathbb{Q}]$ at most 4, but it needs to be a multiple of 3 since E is an extension of $\mathbb{Q}(\sqrt[3]{7})$.

(d) $[E : \mathbb{Q}]$.

Solution: Since $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt[3]{7})$ are both subfields of E, the degree of E must be a multiple of both 2 and 3, so at a minimum, must be 6. But $E \subseteq \mathbb{Q}(\sqrt{5}, \sqrt[3]{7})$ which definitely has degree 6, so the degree of E over $\mathbb{Q}$ is indeed 6.

(4pts) 4. Use the previous question to prove that $x^6 - 15x^4 - 14x^3 + 75x^2 - 210x - 76$ is irreducible. Hint: the polynomial has $\sqrt{5} + \sqrt[3]{7}$ as a root.

Solution: Call the polynomial $p(x)$. Since $\sqrt{5} + \sqrt[3]{7}$ is a root of $p(x)$, we know that the minimum polynomial for $\sqrt{5} + \sqrt[3]{7}$ must have degree *at most* 6. But above we saw that the degree of E over $\mathbb{Q}$ was actually 6, so $p(x)$ must be the minimum polynomial for $\sqrt{5} + \sqrt[3]{7}$, and as such be irreducible.

5. Let $p(x) = (x^2 - 5)(x^3 - 7)$, and let E be the splitting field of $p(x)$.

(5pts) (a) Prove that there is no automorphism of E which sends $\sqrt{5}$ to $\sqrt[3]{7}$. Show specifically what goes wrong using the homomorphism property.

Solution: If there were such an automorphism, say φ, then

$$5 = \varphi(5) = \varphi(\sqrt{5}\sqrt{5}) = \varphi(\sqrt{5})\varphi\sqrt{5} = \sqrt[3]{7}^2$$

which is clearly false.

(5pts) (b) Give an example of a non-trivial automorphism of E and briefly explain how you know your example works.

Solution: We just need to send roots of irreducible polynomials to roots of other irreducible polynomials. So let $\sigma : E \to E$ be be such that $\sigma(\sqrt{5}) = -\sqrt{5}$ and $\sigma(\sqrt[3]{7}) = \sqrt[3]{7}$. This is enough, since a basis for E is $\{1, \sqrt{5}, \sqrt[3]{7}, \sqrt{5}\sqrt[3]{7}, \sqrt[3]{7}^2, \sqrt{5}\sqrt[3]{7}^2\}$, so saying where $\sqrt{5}$ and $\sqrt[3]{7}$ to is enough to specify the automorphism on every element, using the homomorphism property.

(5bn-pts) (c) Bonus: Could $\mathrm{Gal}(E/\mathbb{Q})$ be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$? Explain.

Solution: No. The problem is the splitting field for $p(x)$ is not degree 6, since $p(x)$ has non-real roots, but $\mathbb{Q}(\sqrt{5}, \sqrt[3]{7})$, already of degree 6, has only real number elements.