MATH 322 **Exam 1 – Take Home** Spring 2019

**Name:** ______________________________

**Instructions:** This is the take-home portion of the first exam. Here are my expectations:

- WORK ALONE! You may not collaborate or discuss problems with other students, either in or outside of this class. Also do not discuss with tutors, significant others, parents, kids, etc. If you need clarification on a problem, ask me.
- You may use your notes (including notes from last semester) or the textbook, but only notes you have taken in this class (or in Algebra I) and only the assigned textbook from this class. This is intended only for you to refresh your memory if you forget a definition, not for you to copy proofs (or even the style of proof) from your notes. Alternatively, if you do not remember a definition, send me an email.
- Other than your notes and textbook, do not use any outside sources. In particular, absolutely NO INTERNET (other than our textbook and Canvas).
- This is not a timed exam, and you may take as much time on it as you like. However, I do not intend for you to spend more than 3 hours total working on the exam.
- You should write up all solutions neatly on your own paper and staple this sheet to your solutions. Clearly number each problem, and put the problems in the usual numerical order (no non-identity permutations please).
- As always, you must show all your work to receive credit, and explanations and proofs should be written out in complete English sentences. A page of just equations and calculations will probably receive no credit.
- **Due Monday, February 18.**

Have Fun!

---

(12pts) 1. For each part below, either give an example and explain why the example works, or explain why no example exists.

(a) An ideal $J \subseteq \mathbb{Q}[x]$ and two non-zero elements $a(x), b(x) \in \mathbb{Q}[x]$ such that $(J + a(x))(J + b(x)) = J + 0$.

(b) An algebraic number which cannot be constructed using a compass and straight edge.

(c) A degree 8 field extension $\mathbb{Q}(a, b)$ of $\mathbb{Q}$ for which $b \in \mathbb{Q}(a)$.

(d) A degree 7 field extension $\mathbb{Q}(a, b)$ of $\mathbb{Q}$ for which $b \notin \mathbb{Q}(a)$ and $a \notin \mathbb{Q}(b)$.

(16pts) 2. Consider the polynomial $p(x) = x^4 - 10x^2 + 25x - 5$. Note that $p(x)$ is irreducible (by Eisenstein's criterion).

(a) As we have seen, there is a field extending $\mathbb{Q}$ which *does* contain a root to the polynomial. Let's call the root $\varrho$ and the extension field $E$. We have two ways to represent $E$; one is a quotient ring, the other is as $\mathbb{Q}(\varrho)$. Carefully explain what these two representations look like (that is, what is the general form of elements in the representations). Additionally, give at least two specific examples of elements, what they look like in each representation and how the two representations are related.

(b) Thinking of $E$ as $\mathbb{Q}(\varrho)$, is $\varrho^5 - 7\varrho^3 + 1$ an element of $E$? What element in the quotient ring does this correspond to? Write both representations in a more standard form (with smallest possible exponents). Then explain how this serves as a quick way to find the remainder when $x^5 - 7x^3 + 1$ is divided by $p(x)$.

(c) We know $E$ is actually a field, so every non-zero element has an inverse. What is the inverse of $\varrho^3 - 4\varrho^2 + 6\varrho + 1$? Show all your work and explain why it is easier to complete the computation working with polynomials.

(d) $E$ contains at least one root of $p(x)$, but it might contain more than one root. Explain how we can be sure that $E$ does not contain all the roots of $p(x)$. It might be helpful to graph $p(x)$.

(12pts) 3. Consider the polynomial $p(x) = x^3 - 2 \in \mathbb{Q}[x]$. This has three roots: $\sqrt[3]{2}$, $\sqrt[3]{2}e^{i\pi/3}$, and $\sqrt[3]{2}e^{i2\pi/3}$. To make things easier to write, let's use the Greek letter $\omega$ (omega) to represent $e^{i\pi/3}$ (so the roots are then $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$).

(a) Describe the splitting field $E$ for $p(x)$ and find its degree of $\mathbb{Q}$. Explain how you know its degree is not 3.

(b) Give a basis for the splitting field.

(c) Describe a non-trivial (non-identity) automorphism of the splitting field. You should be able to do this by saying where two particular elements go, but make sure you show where every element of the basis is sent. In particular, where does $\sqrt[3]{2} + \omega$ go under your automorphism?

(d) The polynomial $x^6 - 3x^5 + 6x^4 - 11x^3 + 12x^2 + 3x + 1$ happens to have $\sqrt[3]{2} + \omega$ as a root. Use part (c) to find another root, and explain how you know you are right.

4. Remember that the group $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ is the group of permutations of $\{1, 2, 3\}$. It is also isomorphic to $D_3$, the group of symmetries of a triangle (think of labeling each corner with the numbers $\{1, 2, 3\}$. The field $E$ you found in the previous question has $S_3$ as its Galois group.

(4pts) (a) Which element of $\mathrm{Gal}(E/\mathbb{Q})$ does your automorphism in part (c) of the last question correspond to? Then pick another element from $S_3$ and find the automorphism that corresponds to it.

(6pts) (b) There are other polynomials whose splitting field has $S_3$ as its Galois group. Briefly explain why both of the following polynomials are NOT such polynomials:
$a(x) = x^6 - 2$
$b(x) = x^3 + 1$.

(10bn-pts) 5. Bonus: As we saw in class, there is a correspondence between subgroups of the Galois group and subfields of a splitting field $E$. Illustrate this for the particular $E$ from the last two questions:

(a) Pick a non-trivial intermediate field $F$ (between $\mathbb{Q}$ and $E$) and find $\mathrm{Gal}(E/F)$ (this is the group of automorphisms of $E$ which fix $F$, i.e., the *fixer* of $F$). Which subgroup of $S_3$ is this Galois group isomorphic to?

(b) Pick a non-trivial subgroup $H$ of $S_3$, different from the one you discovered in part (a). Find an intermediate field $F'$ (between $\mathbb{Q}$ and $E$) such that $H \cong \mathrm{Gal}(E/F')$ (that is, find the *fixfield* of $H$).