MATH 322 **Exam 1 – Take Home** Spring 2020

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, Canvas, and an online calculator such as Wolfram alpha).
- Time-frame: The extended time on this take-home is meant to give you some flexibility for when you work on it. You are welcome to look at the exam and think about it as much as you like, but please limit yourself to no more than 3 hours active work time. You can break up these 3 hours over multiple days, and use time between work sessions to study other problems (including studying for the in-class portion). This is meant not only to be fair to your classmates, but also to be fair and respectful of your own time.
- You should write up all solutions neatly in the space provided. If you need extra room, attach additional paper and clearly label your work.
- 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 Wednesday, February 26.**

Have Fun!

By signing below, I certify that the work on this take-home exam is solely my own, that I did not receive assistance from anyone other than my instructor, and did not use resources other than my own notes and the course textbook.

Signature: ______________________________ Date: ________________

(6pts) 1. Suppose $a(x)$ is a polynomial of degree 5 in $\mathbb{Q}[x]$ that has $\sqrt[3]{6}$ as a root. Prove that $a(x)$ is NOT irreducible. Your proof should use ideals and facts about ideals in $\mathbb{Q}[x]$.

(16pts) 2. Consider the polynomial $p(x) = x^4 - 10x^2 + 25x - 5$. Note that $p(x)$ is irreducible (by Eisenstein's criterion). As we have seen, there is a field extending $\mathbb{Q}$ which *does* contain a root to the polynomial. Let's call the root ϱ and the extension field E. We have two ways to represent E; one is a quotient ring, the other is as $\mathbb{Q}(\varrho)$.

(a) 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 $p(x)$.

Continuing from the previous page...

(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: $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, and $\sqrt[3]{2}\omega^2$ where $\omega = e^{i2\pi/3}$. We saw in class that the splitting field $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ had Galois group $G(E/\mathbb{Q})$ isomorphic to S_3.

(a) Give a basis for the splitting field.

(b) One of the elements of the Galois group can be described as

$$\sigma = \begin{pmatrix} \sqrt[3]{2} & \omega \\ \sqrt[3]{2}\omega & \omega^2 \end{pmatrix}.$$

Say where σ sends each element of the basis for E. Also, what is $\sigma(\sqrt[3]{2} + \omega)$?

(c) 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 the elements of the Galois group to find all the roots of the polynomial and explain why you are correct.

(8pts) 4. There are other polynomials whose splitting field has S_3 as its Galois group. Briefly explain why neither of the following polynomials are such polynomials:
$a(x) = x^6 - 2$

$b(x) = x^3 + 1.$

(8pts) 5. Consider the polynomial $p(x) = x^7 - 1$. One of the roots of this polynomial is $\alpha = e^{i2\pi/7}$. Let E be the splitting field for $p(x)$.

(a) What is $[\mathbb{Q}(\alpha) : \mathbb{Q}]$? Is $\mathbb{Q}(\alpha) = E$? Hint: you might want to write down the other roots of $p(x)$, and maybe even enter $p(x)$ into Wolfram alpha.

(b) The Galois group $G(E/Q)$ is isomorphic to $\mathbb{Z}_6$, but it is probably easier to think of this as $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ where the operation is multiplication mod 7 (we also called this $U(7)$). Illustrate that this makes sense by describing two elements of the Galois group and saying which elements of $\mathbb{Z}_7^*$ they correspond to. Then perform the group operation on the pair of elements in both contexts.

(10bn-pts) 6. 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 question:

(a) Pick a non-trivial intermediate field F (between $\mathbb{Q}$ and E) and find $G(E/F)$ (this is the group of automorphisms of E which fix F, i.e., the *fixer* of F). Which subgroup of $\mathbb{Z}_7^*$ is this Galois group isomorphic to?

(b) Pick a non-trivial subgroup H of Z_7^*, different from the one you discovered in part (a). Find an intermediate field F' (between $\mathbb{Q}$ and E) such that $H \cong G(E/F')$ (that is, find the *fixfield* of H).