Exam 1 – Take Home
Solutions

MATH 322 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 $\mathbb{Q}[x]$.

Solution: Consider the ideal J of all polynomials that have $\sqrt[3]{6}$ as a root. This really is an ideal (for example, it is the kernel of the evaluation homomorphism $\sigma_{\sqrt[3]{6}}$ which evaluates a given polynomial at $\sqrt[3]{6}$).

The ideal is an ideal of the ring $F[x]$, so is principle. In other words, $J = \langle p(x) \rangle$ for some polynomial $p(x)$. But $p(x)$ must be equal to $x^3 - 6$ as this polynomial is irreducible an has $\sqrt[3]{6}$ as a root (if it wasn't, then $x^3 - 6$ would be a multiple of $p(x)$, which is impossible since $x^3 - 6$ is irreducible).

Thus every polynomial in J is a multiple of $x^3 - 6$, so in particular there cannot be any degree 4 or greater polynomial in J which is irreducible. Thus $a(x)$ is not irreducible.

(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.

Solution: The representation $\mathbb{Q}(\varrho)$ is the set of all elements of the form $a + b\varrho + c\varrho^2 + d\varrho^3$ where $a, b, c, d \in \mathbb{Q}$. We know that we don't need a ϱ^4 term because the degree of the field extension over $\mathbb{Q}$ is 4, as ϱ is the root to an irreducible degree 4 polynomial.

The other representation is the quotient ring $\mathbb{Q}[x]/\langle p(x)\rangle$, in which elements are cosets $\langle p(x)\rangle + a(x)$ for all polynomials $a(x) \in \mathbb{Q}[x]$. But by the division algorithm we can always pull out multiples of $p(x)$ for any $a(x)$ with degree greater than 3, so we can assume $a(x)$ has degree at most 3.

These two representations are isomorphic by the evaluation map that evaluates the polynomial $a(x)$ at ϱ. For example, in $\mathbb{Q}(\varrho)$ the element $3 + 2\varrho - \varrho^2 + 7\varrho^3$ corresponds to the coset $\langle p(x)\rangle + 3 + 2x - x^2 + 7x^3$. Or going the other way, the coset $\langle p(x)\rangle + 5 + 4x^3$ corresponds to the element $5 + 4\varrho^4$.

(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 $p(x)$.

Solution: From the fact that ϱ is a root of $p(x)$ we have that $\varrho^4 = 10\varrho^2 - 25\varrho + 5$. Of course $\varrho^5 = \varrho \cdot \varrho^4$. Thus the element we have here is

$$\varrho(10\varrho^2 - 25\varrho + 5) - 7\varrho^3 + 1 = 3\varrho^3 - 25\varrho^2 + 5\varrho + 1$$

In the quotient ring this is

$$\langle p(x)\rangle + 3x^3 - 25x^2 + 5x + 1$$

What does this have to do with divisions and remainders? Well $x^5 - 7x^3 + 1 \in \langle p(x)\rangle + 3x^3 - 25x^2 + 5x + 1$ is saying that after dividing $x^5 - 7x^3 + 1$ by $p(x)$ you are left with a remainder of $3x^3 - 25x^2 + 5x + 1$. But we got this remainder not be actually dividing, but by plugging in $10x^2 - 25x + 5$ in for x^4.

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.

Solution: We will find the inverse of the coset $\langle p(x)\rangle + x^3 - 4x^2 + 6x + 1$ in $\mathbb{Q}[x]/\langle p(x)\rangle$. Using long division, we get $p(x) = (x+4)(x^3 - 4x^2 + 6x + 1) - 9$. Thus

$$1 = \frac{1}{9}p(x) + \left(\frac{-1}{9}x - \frac{4}{9}\right)(x^3 - 4x^2 + 6x + 1).$$

In other words, $1 \in \langle p(x)\rangle + \left(\frac{-1}{9}x - \frac{4}{9}\right)(x^3 - 4x^2 + 6x + 1)$ so $(\langle p(x)\rangle + \left(\frac{-1}{9}x - \frac{4}{9}\right))(\langle p(x)\rangle + (x^3 - 4x^2 + 6x + 1) = \langle p(x)\rangle + 1$.
Transferring back to E, we find that the inverse of $\varrho^3 - 4\varrho^2 + 6\varrho + 1$ is $\frac{-1}{9}\varrho - \frac{4}{9}$.

(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 $p(x)$.

Solution: If you graph $p(x)$ you see that there are two real roots, so there must be 2 complex roots as well. If ϱ is a real root, there is no way to get the complex root from this in $\mathbb{Q}(\varrho)$. Of course we don't know which root ϱ is, but it doesn't matter: if ϱ' is a different root of $p(x)$ then $\mathbb{Q}(\varrho) \cong \mathbb{Q}(\varrho')$ since they are both isomorphic to the same quotient ring.

(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.

Solution: A basis is $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2, \omega, \sqrt[3]{2}\omega, \sqrt[3]{2}^2\omega\}$. Note that ω is a root of the degree 2 polynomial $x^2 + x + 1$ since $x^3 - 1 = (x-1)(x^2+x+1)$.

(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 $\sigma(\sqrt[3]{2} + \omega)$?

Solution: If we send $\sqrt[3]{2}$ to $\sqrt[3]{2}\omega$ and ω to its conjugate, we would send $\sqrt[3]{2} + \omega$ to $\sqrt[3]{2}\omega + \omega^2$. Since $\omega^2 = -\omega - 1$ this becomes $\sqrt[3]{2}\omega - \omega - 1$.

(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.

Solution: The other roots will be the images of this number under each automorphism. So for example, another one will be $\sqrt[3]{2}\omega + \omega^2$.

(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:
$a(x) = x^6 - 2$

Solution: $a(x)$ has a spitting field of too high a degree: $\mathbb{Q}(\sqrt[6]{2})$ is a degree 6 extension, but there are also complex roots that this does not include, so the degree must be higher.

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

Solution: $b(x)$ has a splitting field of degree 2, since $x^3 + 1 = (x + 1)(x^2 - x + 1)$.

(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.

Solution: The polynomial factors as $(x-1)(x^6+x^5+\cdots+x+1)$, and α is a root of the degree 6 part. This means $[\mathbb{Q}(\alpha) : \mathbb{Q})] = 6$. The other five roots are all powers of α, so in fact $\mathbb{Q}(\alpha)$ contains all the roots, so it is the splitting field.

(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.

Solution: Each automorphism in the Galois group is determined by where it sends α. Let $\sigma_2(\alpha) = \alpha^2$ and $\sigma_3(\alpha) = \alpha^3$ (this is okay, since the roots of the minimal polynomial for α are $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$). Now if we perform the group operation (composition) on these, we get $\sigma_2 \circ \sigma_3(\alpha) = \sigma_2(\alpha^3) = (\alpha^3)^2 = \alpha^6$.
The corresponding calculation in $\mathbb{Z}_7^*$ is $2 \cdot 3 = 6$.

(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?

Solution: Consider $F = \mathbb{Q}(\alpha + \alpha^6)$. This is certainly a subfield of E and has the property that complex conjugation fixes every element (since α and α^6 are complex conjugates). Thus fixer of F is $\{\sigma_1, \sigma_6\}$.

(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).

Solution: Let $H = \{1, 2, 4\}$, or in terms of automorphisms, $\{\sigma_1, \sigma_2, \sigma_4\}$. What elements of E do these fix? Well, $\sigma_2(\alpha) = \alpha^2$ and $\sigma_2(\alpha^2) = \alpha^4$ and $\sigma_2(\alpha^4) = \alpha$. So if we consider the element $\alpha + \alpha^2 + \alpha^4$ we notice that σ_2 fixes it. It is easy to see that σ_4 also fixes it. Thus the fixfield of H will be $F' = \mathbb{Q}(\alpha + \alpha^2 + \alpha^4)$.

We can say a little more. Since the index of H in G is $[G : H] = 6/3 = 2$, we know that the degree of F' over $\mathbb{Q}$ will be $[F' : \mathbb{Q}] = 2$. This in turn tell us that the number $\alpha + \alpha^2 + \alpha^4$ is the root of a degree 2 polynomial.