Exam 1 – Take Home

MATH 322 **Solutions** Spring 2019

(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 $(J + a(x))(J + b(x)) = J + 0$.

> **Solution:** We could have $p(x) = (x^2 - 3)(x^2 - 5)$ and $J = \langle p(x) \rangle$. Then $a(x) = x^2 - 3$ and $b(x) = x^2 - 5$ are both non-zero elements of $\mathbb{Q}[x]$ (in fact, $J + a(x) \neq 0$ and $J + b(x) \neq 0$) but $J + p(x) = J + 0$. This particular example shows that $\mathbb{Q}[x]/J$ is not an integral domain.

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

> **Solution:** For example, $a = \sqrt[3]{2}$ is such a number. It is algebraic since it is the root of $x^3 - 2$, but not constructible since it is not in a degree 2^k extension of $\mathbb{Q}$.

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

> **Solution:** For example, $\mathbb{Q}(\sqrt[8]{3}, \sqrt{3}) = \mathbb{Q}(\sqrt[4]{3})$ has degree 8 over $\mathbb{Q}$ since $\sqrt[8]{3}$ has minimum polynomial $x^8 - 3$ (which is irreducible by Eisenstein's criterion).

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

> **Solution:** Impossible. Suppose $\mathbb{Q}(a, b)$ had degree 7 over $\mathbb{Q}$. Then since $[\mathbb{Q}(a, b) : \mathbb{Q}] = [\mathbb{Q}(a, b) : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}]$, and 7 is prime, we have that either $[\mathbb{Q}(a, b) : \mathbb{Q}(a)] = 1$ or $[\mathbb{Q}(a) : \mathbb{Q}] = 1$. In the first case, this says that $\mathbb{Q}(a, b) = \mathbb{Q}(a)$ (in which case the extension is simple), in the second case this says that $\mathbb{Q}(a, b) = \mathbb{Q}(b)$ (again simple) since $\mathbb{Q}(a) = \mathbb{Q}$.

(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 ϱ and the extension field E. We have two ways to represent E; one is a quotient ring, the other is as $\mathbb{Q}(\varrho)$. 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.

(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: $\sqrt[3]{2}$, $\sqrt[3]{2}e^{i2\pi/3}$, and $\sqrt[3]{2}e^{i4\pi/3}$. To make things easier to write, let's use the Greek letter ω (omega) to represent

$e^{i2\pi/3}$ (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 over $\mathbb{Q}$. Explain how you know its degree is not 3.

> **Solution:** $E = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega)$, which has degree 6 over $\mathbb{Q}$. We know the degree is not 3 since the degree 3 extension $\mathbb{Q}(\sqrt[3]{2})$ only contains real numbers, so cannot contain the other two roots of the polynomial.

(b) 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 $x^3 - 1 = (x-1)(x^2+x+1)$.

(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?

> **Solution:** We can send $\sqrt[3]{2}$ to itself and ω to ω^2 (complex conjugation). Or we could send $\sqrt[3]{2}$ to $\sqrt[3]{2}\omega$ and either send ω to itself or its conjugate. There are 5 choices for the automorphism (plus the trivial makes 6).
> 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 $\sqrt[3]{2}\omega - \omega - 1$.

(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.

> **Solution:** Another root would be whatever the image of $\sqrt[3]{2} + \omega$ is under the automorphism found in (c). This is because E is the splitting field for this polynomial as well, so any automorphism of E must send this root to another root.

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.

> **Solution:** You have some choices here. I would say that (123) corresponds to the automorphism that send $\sqrt[3]{2}$ to $\sqrt[3]{2}\omega$ and ω to itself. Take (23) to be the automorphism that just sends ω to its conjugate. The remaining ones can be found by composition.

(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:
$a(x) = x^6 - 2$
$b(x) = x^3 + 1$.

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

(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?

Solution: If we pick the intermediate field $\mathbb{Q}(\sqrt[3]{2})$, then this will correspond to one of the 2-element subgroups of S_3, such as $\{(1), (23)\}$. If you pick $\mathbb{Q}(\omega)$, then we would look for a 3-element subgroup: $\{(1), (123), (132)\}$.

(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).

Solution: Pick the other one from the solution to the previous problem. Note that there are three subgroups of size 2 that you could pick, each corresponding to a different fixfield of degree 3, but there is only one subgroup of size 2.