MATH 322 **Homework 3 Solutions** Due: Wednesday, February 13

Instructions: Carefully write up solutions to the questions below. A solution should consist of both the answer and a careful explanation for why that answer must be correct. Any solutions without an explanation written out in English prose will receive no credit. You are welcome to work together, but write up solutions in your own, individual rules. Also, NO INTERNET!

(4pts) 1. Suppose E is a degree 2 extension of F. Prove that E is the splitting field for some polynomial in $F[x]$.

Solution: If E is a degree 2 extension of F, then $E = F(c)$ where c is the root to some irreducible degree 2 polynomial, $p(x)$. We claim that E is actually the splitting field for $p(x)$. Note that in E, we can factor $p(x)$ as $(x-c)q(x)$ where $q(x)$ is a degree 1 polynomial with coefficients in E. But this means that $q(x)$ has a root in E as well: if $q(x) = ax + b$ then $\frac{b}{a}$ is a root, which is in E because a and b are. Thus E contains all the roots of $p(x)$, as required.

(6pts) 2. Let $p(x)$ be a polynomial of degree n in $F[x]$ for some field F. Prove that there is a splitting field E for $p(x)$ such that $[E : F] \leq n!$. Your proof must use **mathematical induction**! Let $P(n)$ be the statement, "If $p(x)$ has degree n, then there is a splitting field with degree no more than $n!$" and prove $P(n)$ is true for all $n \geq 1$.

Solution: We know that we can always find an extension of F of degree at most n (exactly n if $p(x)$ is irreducible) which contains a root of $p(x)$. In this larger field, we can factor $p(x)$ as $(x-c)q(x)$ where c is the newly adjoined root of $p(x)$. We now know that $q(x)$ has degree $n-1$. Now repeat. To make this rigorous, use induction.

For the base case, it is clear that any polynomial of degree 1 has a splitting field E with $[E : F] \leq 1$, since $E = F$ works. Now assume that the proposition is true for all polynomials of degree k. Consider $p(x)$ of degree $k+1$. Find an extension F_1 of F in which $p(x)$ has a root. Factor $p(x) = (x-c)q(x)$ in $F_1[x]$. We have that $[F_1 : F] \leq k+1$. Now $q(x)$ is a polynomial of degree k, so we can apply our induction hypothesis to conclude that there is a splitting field E for $q(x)$ extending F_1 with $[E : F_1] \leq k!$. But E contains all the roots of $q(x)$, as well as c (the other root of $p(x)$) so E is a splitting field for $p(x)$ extending F. By the tower rule, $[E : F] \leq (k+1)!$.

(8pts) 3. Consider the field $\mathbb{Q}(\sqrt[4]{3}, i)$.

(a) Is this a splitting field for some polynomial in $\mathbb{Q}[x]$? If so, what is the degree of that polynomial?

Solution: Yes, since in this field $x^4 - 3$ factors completely (its roots are $\pm\sqrt[4]{3}$ and $\pm\sqrt[4]{3}i$). So it is the splitting field of a degree 4 polynomial.

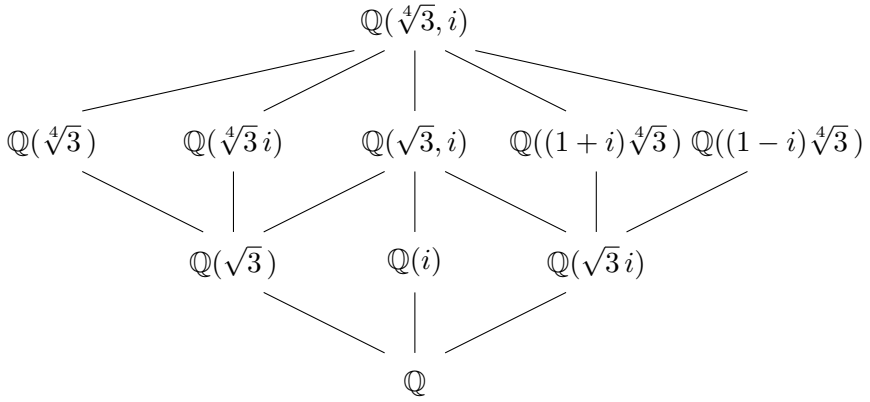
It is also the splitting field of a degree 8 polynomial. We know there is some element α of the field such that $\mathbb{Q}(\alpha)$ is the field. This number will have a degree 8 minimal polynomial, and that polynomial will split completely in the field.

(b) What is the degree $[\mathbb{Q}(\sqrt[4]{3}, i) : \mathbb{Q}]$? Explain how you know.

Solution: This is degree 8. We know that $\mathbb{Q}(\sqrt[4]{3})$ has degree 4 over $\mathbb{Q}$, but that this is only real, so adding i will be more than a degree 1 extension. However, i has minimal polynomial $x^2 + 1$, so it will be a degree 2 extension of $\mathbb{Q}(\sqrt[4]{3})$. Using the tower rule, we get degree 8.

(c) Draw as much of a complete tower diagram as you can describing the fields between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{3}, i)$.

Solution: You don't need to have all of this, but here is the complete tower diagram for this field.



(d) Prove that the fields $\mathbb{Q}(\sqrt[4]{3})$ and $\mathbb{Q}(\sqrt[4]{3}i)$ are isomorphic, but not equal. This might help with the previous parts.

Solution: Since $p(x) = x^4 - 3$ is the minimal polynomial for both $\sqrt[4]{3}$ and $\sqrt[4]{3}i$, we have that both fields are isomorphic to $\mathbb{Q}[x]/\langle p(x)\rangle$, so are therefore isomorphic to each other.

However, the fields are not equal, since the first field contains only real numbers but the second field contains complex numbers.

(12pts) 4. Consider the polynomial $a(x) = x^4 - 10x^2 + 21$ in $\mathbb{Q}[x]$.

(a) Find the splitting field E over $\mathbb{Q}$. Draw a tower diagram including all intermediate fields, and their degrees. Hint: start by factoring $a(x)$.

Solution: The polynomial factors in $\mathbb{Q}[x]$ as $(x^2 - 3)(x^2 - 7)$. Thus a splitting field is $E = \mathbb{Q}(\sqrt{3}, \sqrt{7})$.

(b) Let $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ be different intermediate fields between $\mathbb{Q}$ and E. Explain why there is NOT an isomorphism from $\mathbb{Q}(\alpha)$ to $\mathbb{Q}(\beta)$. In particular, say why no isomorphism can send α to β.

Solution: We have $\alpha = \sqrt{3}$ and $\beta = \sqrt{7}$, for example. Suppose there were an isomorphism between $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{7})$, call it φ. Then $\varphi(\sqrt{3}) = a + b\sqrt{7}$ for some $a, b \in \mathbb{Q}$. But then $\varphi(3) = \varphi(\sqrt{3})\varphi(\sqrt{3}) = a^2 + 2ab\sqrt{7} + b^2 7$. We know though that $\varphi(3) = 3$ since $3 \in \mathbb{Q}$. So this says that

$$3 = a^2 + 2ab\sqrt{7} + 7b^2.$$

Since $\sqrt{7} \notin \mathbb{Q}$ this would mean either $a = 0$ or $b = 0$, but if $a = 0$ then $3/7$ would be a perfect square (it is not) and if $b = 0$ then $3 = a^2$ which is also false. Thus there is no place for $\sqrt{3}$ to go under the isomorphism, so there is no isomorphism.

(c) Describe a non-trivial *automorphism* of E. Explain how you know your example works. Remember, an automorphism is an isomorphism from E to itself (that is, it moves some of the elements of E around, but is still a bijection satisfying the homomorphism property).

Solution: Any automorphism must send roots of irreducible polynomials to roots of the *same* irreducible polynomial. So we could send $\sqrt{3}$ to $-\sqrt{3}$, or $\sqrt{7}$ to $-\sqrt{7}$ (or both). In fact, we know that we can start with either of these and extend to an automorphism of the splitting field. So one automorphism is determined by $\sigma(\sqrt{3}) = -\sqrt{3}$ and $\sigma(\sqrt{7}) = \sqrt{7}$ (the other basis element, $\sqrt{21}$ will have $\sigma(\sqrt{21}) = -\sqrt{21}$ due to the homomorphism property).

(d) Describe the Galois group $\mathrm{Gal}(E : \mathbb{Q})$ for E over $\mathbb{Q}$. Be sure to explicitly say what each element of the group is, as well as say what "standard" group it is isomorphic to.

Solution: The Galois group contains all the automorphisms of E which fix $\mathbb{Q}$. This means that the automorphisms must send roots to irreducible polynomials to other roots of the same irreducible polynomial. We also know that since $[E : \mathbb{Q}] = 4$, the Galois group will contain 4 elements. Let's call the four elements ε, σ, τ, $\sigma\tau$. The identity automorphisms is ε. We will let $\sigma(\sqrt{3}) = -\sqrt{3}$ but $\sigma(\sqrt{7}) = \sqrt{7}$. Analogously, $\tau(\sqrt{7}) = -\sqrt{7}$ but $\tau(\sqrt{3}) = \sqrt{3}$. This completely determines the automorphisms, as it determines the automorphisms on the basis $\{1, \sqrt{3}, \sqrt{7}, \sqrt{21}\}$

The Galois group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, as every element is its own inverse.