Math 4720/5210 # Homework #6 **Due: Mon., Mar. 25th, 2024**

Important Note: In problems #2 and #3, you are asked to "find" Galois groups.
I will clarify what I mean by this (and help with these problems) in class.

BACKGROUND THEOREMS: Let $\varphi : \mathbb{F} \to \widehat{\mathbb{F}}$ be an isomorphism of fields. This induces an isomorphism $\widetilde{\varphi} : \mathbb{F}[x] \to \widehat{\mathbb{F}}[x]$ of the corresponding polynomial rings (extending φ and sending x to x). Let $f(x) \in \mathbb{F}[x]$ and $\widetilde{\varphi}(f(x)) = \widehat{f}(x) \in \widehat{\mathbb{F}}[x]$.

Theorem #1: Suppose $f(x)$ is irreducible (over $\mathbb{F}$). If α is any root of $f(x)$ and β is any root of $\widehat{f}(x)$, then there exists an isomorphism $\widehat{\varphi} : \mathbb{F}[\alpha] \to \widehat{\mathbb{F}}[\beta]$ extending $\varphi : \mathbb{F} \to \widehat{\mathbb{F}}$ and sending α to β.

Theorem #2: $\mathbb{E}$ be a splitting field for $f(x)$ (over $\mathbb{F}$) and $\widehat{\mathbb{E}}$ is a splitting field for $\widehat{f}(x)$ (over $\widehat{\mathbb{F}}$), then there exists an isomorphism $\widehat{\varphi} : \mathbb{E} \to \widehat{\mathbb{E}}$ extending $\varphi : \mathbb{F} \to \widehat{\mathbb{F}}$.

Theorem #3: If $\widehat{\varphi} : \mathbb{E} \to \widehat{\mathbb{E}}$ is an isomorphism of fields extending $\varphi : \mathbb{F} \to \widehat{\mathbb{F}}$, then for any $\alpha \in \mathbb{E}$ such that $f(\alpha) = 0$ we also have $\widehat{f}(\widehat{\varphi}(\alpha)) = 0$ (i.e., roots map to roots).

#1 Rootin' Around: Let $\mathbb{F}$ be a field, $f(x) \in \mathbb{F}[x]$ (not a constant polynomial), and $\mathbb{E}$ be a splitting field for $f(x)$ over $\mathbb{F}$. In addition, let $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ (we say G is the Galois group of the polynomial $f(x)$).

(a) Suppose that $f(x)$ is irreducible. Show that G acts *transitively* on the roots of $f(x)$ in $\mathbb{E}$.
In particular, given any two roots for $f(x)$, say $\alpha, \beta \in \mathbb{E}$, there exists some $\sigma \in G$ such that $\sigma(\alpha) = \beta$.

(b) Suppose G acts transitively on the roots of $f(x)$ in $\mathbb{E}$. In addition, suppose $f(x)$ has no repeated roots. Show that $f(x)$ is irreducible (over $\mathbb{F}$).
Hint: Suppose that $f(x)$ factors. Explain why G must send roots of a factor to other roots of that same factor. Transitivity of the action will force distinct factors to share a root (why?). This is a problem (why?).

Note: In summary, for separable polynomials, the Galois group of a a polynomial acts transitively on the polynomial's roots if and only if it is an irreducible polynomial (over the base field).

#2 Finding Galois: Let $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. Find the Galois group of $f(x)$ (over $\mathbb{Q}$).

Note: $f(x) = (x - \sqrt{2} - \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} + \sqrt{3})$.
You may find Rotman's Example 20 on page 54 helpful.

Claim: $f(x)$ is irreducible in $\mathbb{Q}[x]$.

proof: By the Rational Root Theorem, the only possible rational roots are ± 1, since $f(\pm 1) = -8 \neq 0$, $f(x)$ has no roots in $\mathbb{Q}$. Thus the only way $f(x)$ could be reducible is if it factors into a product of (irreducible) quadratics. Given $f(x)$ is monic, without loss of generality we can assume the factors are monic. Suppose $f(x) = (x^2+ax+b)(x^2+cx+d)$. Noting the coefficient of x^3 in $f(x)$ is zero, we must have $c = -a$. Finally, noting that the constant term of $f(x)$ is 1, we must either have $b = d = 1$ or $b = d = -1$. Case 1: $f(x) = (x^2 + ax + 1)(x^2 - ax + 1) = x^4 + (2 - a^2)x^2 + 1$ so that $2 - a^2 = -10$ and so $a^2 = 12$ and thus $a \notin \mathbb{Q}$. Case 2: $f(x) = (x^2 + ax - 1)(x^2 - ax - 1) = x^4 + (-2 - a^2) + 1$ so that $-2 - a^2 = -10$ and so $a^2 = 8$ and thus $a \notin \mathbb{Q}$. Therefore, $f(x)$ cannot factor into quadratics in $\mathbb{Q}[x]$. Thus $f(x)$ is irreducible in $\mathbb{Q}[x]$. ■

Suggestive Calculation: $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$, $\sqrt{6}(\sqrt{2} + \sqrt{3}) = 3\sqrt{2} + 2\sqrt{3}$, and $3(\sqrt{2} + \sqrt{3}) - (3\sqrt{2} + 2\sqrt{3}) = \sqrt{3}$.

#3 Roots of Unity: Just remember $\sqrt{1} = 1$.

(a) Find a primitive n^{th}-root of unity when $n = 1, 2, 3, 4, 5,$ and 6. Your final formulas should not involve sines and cosines. For example: $e^{2\pi i/3} = \cos(2\pi/3) + i\sin(2\pi/3)$ is a primitive third root of unity, but an unacceptable (final) answer. You may find Wolfram Alpha helpful as you seek out what numbers like $\cos(2\pi/5)$ are (unless you have more special triangles memorized than I do).

(b) Find the Galois groups of $x^n - 1$ over $\mathbb{Q}$ when $n = 1, 2, 3, 4, 5, 6$ and 7.