MODERN ALGEBRA II SPRING 2019:
THIRTEENTH PROBLEM SET

1. Let \( A_1 \) be the element \( a + b\sqrt{2} + c(\sqrt{2})^2 \in \mathbb{Q}(\sqrt{2}) \). Viewing \( \mathbb{Q}(\sqrt{2}) \) as a subfield of its splitting field \( \mathbb{Q}(\sqrt{2}, \omega) \) (where \( \omega \neq 1 \) satisfies \( \omega^3 = 1 \), show that, if \( \sigma \in \text{Gal}(\mathbb{Q}(\sqrt{2}, \omega)/\mathbb{Q}) \), then \( \sigma(A_1) \) is either \( A_1 \), \( A_2 \), or \( A_3 \), where

\[
A_1 = a + b\sqrt{2} + c(\sqrt{2})^2;
A_2 = a + b\omega\sqrt{2} + c\omega^2(\sqrt{2})^2;
A_3 = a + b\omega^2\sqrt{2} + c\omega(\sqrt{2})^2.
\]

More generally, if \( \sigma \in \text{Gal}(\mathbb{Q}(\sqrt{2}, \omega)/\mathbb{Q}) \), then \( \sigma \) permutes the \( A_i \). Conclude that \( A_1A_2A_3 \) is left fixed by every \( \sigma \in \text{Gal}(\mathbb{Q}(\sqrt{2}, \omega)/\mathbb{Q}) \), and hence (by the main theorem of Galois theory), \( A_1A_2A_3 \in \mathbb{Q} \). Can \( A_1A_2A_3 \) ever be 0? In fact, argue that \( A_1A_2A_3 = 0 \iff a = b = c = 0 \). Evaluate \( A_1A_2A_3 \) in terms of \( a, b, c \). Where have we seen this expression before? Setting \( D = A_1A_2A_3 \in \mathbb{Q} \), use Galois theory to see without any computation that \( A_2A_3/D \in \mathbb{Q}(\sqrt{2}) \) and that it is an explicit inverse for \( A_1 \).

2. Let \( f(x) \in \mathbb{Q}[x] \) be an irreducible cubic polynomial with exactly one real root. Let \( E \) be the splitting field of \( f(x) \).

(i) Argue that \( E \) has an automorphism of order 2 given by complex conjugation, so that the Galois group of \( E \) over \( \mathbb{Q} \) has an element of order 2. Using this fact alone, can the Galois group of \( E \) over \( \mathbb{Q} \) be equal to \( A_3 \)?

(ii) Show (without using (i)) that \( E \) has degree 6 over \( \mathbb{Q} \). (Let \( \alpha \) be a real root of \( f(x) \). What is \( [\mathbb{Q}(\alpha) : \mathbb{Q}] \)? Can \( \mathbb{Q}(\alpha) \) be a splitting field for \( f(x) \)? Why or why not? Show that \( [E : \mathbb{Q}(\alpha)] = 2 \).)

3. Let \( F \) be a field of characteristic zero, and let \( E \) be a normal extension of \( F \) with Galois group isomorphic to \( S_3 \). Show that \( E \) is the splitting field of an irreducible cubic polynomial. (Hint: use Galois theory to find a subfield \( K \) of \( E \) such that \( [K : F] = 3 \). Can \( K \) be a normal extension of \( F \)? Now argue that \( K = F(\alpha) \) for some \( \alpha \in E \) which is a root of an irreducible polynomial \( f(x) \) of degree 3 over \( F \), and conclude that \( E \) is the splitting field of \( f(x) \).)
4. Let $\zeta = \zeta_5$ be the 5th root of unity $e^{2\pi i/5}$, and consider the field $\mathbb{Q}(\zeta)$.

(i) Show that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$.

(ii) Galois theory predicts that there is exactly one quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta)$. To find this extension, let $\alpha = \zeta + \zeta^{-1} = \zeta + \zeta^4 = \zeta + \bar{\zeta}$, where the bar denotes complex conjugation. Show that $\alpha$ satisfies the quadratic equation $\alpha^2 + \alpha - 1 = 0$ (recall that $\zeta$ satisfies the equation $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$), and hence $\alpha = \frac{-1 \pm \sqrt{5}}{2}$. To determine the sign, use $\zeta = e^{2\pi i/5}$ to see that $\alpha = 2 \cos(2\pi/5)$. What is the sign of $\cos(2\pi/5)$? Conclude that $\alpha = \frac{-1 + \sqrt{5}}{2}$. (Pure thought alone cannot determine the sign of the square root: in fact, by Galois theory, there is no way to distinguish algebraically between, say, $\zeta$ and $\zeta^a$, where $1 \leq a \leq 4$, and hence between $\zeta + \zeta^{-1}$ and $\zeta^a + \zeta^{-a}$. Taking $a = 1$ or $a = 4$ gives $\alpha$; the other choice of the square root comes from taking $a = 2$ or $3$ and hence from $\zeta^2 + \zeta^3$.)

(iii) The field $\mathbb{Q}(\zeta)$ is a degree two extension of $\mathbb{Q}(\alpha)$. Show that

$$\zeta^2 - \alpha \zeta + 1 = 0,$$

and express $\zeta$ in terms of $\alpha$ by using the quadratic formula.

(iii) Now let $\zeta = \zeta_7$ be the 7th root of unity $e^{2\pi i/7}$, and consider the field $\mathbb{Q}(\zeta)$. Then $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^*$ and has two proper nontrivial subgroups of orders 3 and 2 respectively: $\langle 2 \rangle$ and $\{\pm 1\} = \langle 6 \rangle$. Galois theory predicts that the degree six extension $\mathbb{Q}(\zeta)$ has exactly one subfield which is a quadratic extension of $\mathbb{Q}$ and one subfield which is a cubic extension of $\mathbb{Q}$. Using the equation $\zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$, show that $\alpha = \zeta + \zeta^2 + \zeta^4$ satisfies the quadratic equation $\alpha^2 + \alpha + 2 = 0$, and hence $\alpha = \frac{-1 \pm \sqrt{-7}}{2}$. To find the cubic extension, let $\beta = \zeta + \zeta^{-1}$. By computing $\beta^2$, $\beta^2 - 2$, and $(\beta^2 - 2)\beta$, show that $\beta$ is the root of a cubic polynomial in $\mathbb{Q}[x]$ and determine this polynomial explicitly.