MODERN ALGEBRA II SPRING 2013: THIRTEENTH PROBLEM SET

1. Let F be a field of characteristic zero, let $f(x) \in F[x]$ be an **irreducible** polynomial of degree n, and let E be a splitting field of $f(x)$, with roots $\alpha_1, \dots, \alpha_n \in E$.

   (i) We have seen that, if $G = \mathrm{Gal}(E/F)$, then n divides the order of G and the order of G divides $n!$. Give another proof of the fact that n divides the order of G as follows: use the fact that $\#(\mathrm{Gal}(E/F)) = [E : F]$ and that $E = F(\alpha_1, \dots, \alpha_n)$, and consider the sequence of extensions

   $$F \leq F(\alpha_1) \leq E.$$

   (ii) Does G always necessarily contain an element of order exactly n? (Consider the case $F = \mathbb{Q}$ and $f(x) = x^4 - 10x^2 + 1$.)

2. Let A_1 be the element $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{2})$. Viewing $\mathbb{Q}(\sqrt[3]{2})$ as a subfield of its splitting field $\mathbb{Q}(\sqrt[3]{2}, \omega)$ (where $\omega = e^{2\pi i/3}$ satisfies $\omega^3 = 1$ and hence $\omega^4 = \omega$), show that, if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$, then $\sigma(A_1)$ is either A_1, A_2, or A_3, where

   $$\begin{aligned} A_1 &= a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2; \\ A_2 &= a + b\omega\sqrt[3]{2} + c\omega^2(\sqrt[3]{2})^2; \\ A_3 &= a + b\omega^2\sqrt[3]{2} + c\omega(\sqrt[3]{2})^2. \end{aligned}$$

   More generally, if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$, then σ permutes the A_i. Conclude that $A_1A_2A_3$ is left fixed by every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$, 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 $D = A_1A_2A_3 = 0 \iff a = b = c = 0$. Evaluate $D = A_1A_2A_3$ in terms of a, b, c. Where have we seen this expression before? Finally, use the formula $A_1^{-1} = D^{-1}(A_2A_3)$ to find an explicit formula for A_1^{-1}.

3. 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 α 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 $[E : \mathbb{Q}(\alpha)] = 2$.)

4. 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 $f(x)$.)

5. Let F be a field of characteristic zero containing all of the cube roots of unity and let ω be a generator of this group. Suppose that E is a normal extension of F whose Galois group is cyclic of order 3, and let σ be a generator for $\mathrm{Gal}(E/F)$. Suppose that $\beta \in E$ is nonzero and that $\sigma(\beta) = \omega\beta$, i.e. that β is an eigenvector for σ with eigenvalue ω. Conclude that (i) $\beta \notin F$; (ii) $\beta^3 \in F$; (iii) $E = F(\beta)$. Thus, under the assumption that we can find a $\beta \neq 0$ such that $\sigma(\beta) = \omega\beta$, E is obtained from F by adding a cube root.

   (In fact, using a little linear algebra, it is not hard to show that σ in fact always has an eigenvector with eigenvalue ω. Hence, under the above assumptions, $E = F(\sqrt[3]{a})$ for some $a \in F$.)

6. Let $\zeta = \zeta_5$ be the 5^{th} 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 α satisfies the quadratic equation $\alpha^2 + \alpha - 1 = 0$ (recall that ζ satisfies the equation $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$), and hence $\alpha = \dfrac{-1 \pm \sqrt{5}}{2}$. 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 $\alpha = \dfrac{-1 + \sqrt{5}}{2}$. (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, ζ and ζ^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 α; 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 ζ in terms of radicals.

(iii) Now let $\zeta = \zeta_7$ be the 7^{th} root of unity $e^{2\pi i/7}$, and consider the field $\mathbb{Q}(\zeta)$. 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 $\alpha = \dfrac{-1 \pm \sqrt{-7}}{2}$. To find the cubic extension, let $\beta = \zeta + \zeta^{-1}$. By computing β^2, $\beta^2 - 2$, and $(\beta^2 - 2)\beta$, show that β is the root of a cubic polynomial in $\mathbb{Q}[x]$ and determine this polynomial explicitly.