MODERN ALGEBRA II SPRING 2013: TWELFTH PROBLEM SET

1. Consider the field $\mathbb{Q}(\sqrt[3]{2},\omega)$, with $\omega = \frac{1}{2}(-1+\sqrt{-3})$. By our work in class, we have seen that $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}) \cong S_3$. In fact, if $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \omega\sqrt[3]{2}$, $\alpha_3 = \omega^2\sqrt[3]{2}$, then $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$ permutes $\alpha_1, \alpha_2, \alpha_3$, and any permutation corresponds to some element of the Galois group. Moreover, the subgroups of S_3 are $\{1\}$, $\langle(123)\rangle$, $\langle(23)\rangle$, $\langle(13)\rangle$, $\langle(12)\rangle$, and S_3.

   (i) Let $\rho \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$ be the unique element such that $\rho(\omega) = \omega$ and $\rho(\sqrt[3]{2}) = \omega\sqrt[3]{2}$. Thus ρ corresponds to the permutation (123). Guess the fixed field $\mathbb{Q}(\sqrt[3]{2},\omega)^\rho = \mathbb{Q}(\sqrt[3]{2},\omega)^{\langle\rho\rangle}$ and prove that your guess is correct. (Hint: Clearly $\mathbb{Q}(\omega) \leq \mathbb{Q}(\sqrt[3]{2},\omega)^{\langle\rho\rangle}$. By counting degrees, the only possibilities are $\mathbb{Q}(\sqrt[3]{2},\omega)^{\langle\rho\rangle} = \mathbb{Q}(\omega)$ or $\mathbb{Q}(\sqrt[3]{2},\omega)^{\langle\rho\rangle} = \mathbb{Q}(\sqrt[3]{2},\omega)$. Why is the second alternative not possible?)

   (ii) Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$ be complex conjugation. Thus σ corresponds to the permutation (23). Identify the fixed field $\mathbb{Q}(\sqrt[3]{2},\omega)^\sigma = \mathbb{Q}(\sqrt[3]{2},\omega)^{\langle\sigma\rangle}$ and prove that your identification is correct.

   (iii) For the remaining proper subgroups $H_1 = \langle(12)\rangle$ and $H_2 = \langle(13)\rangle$ of S_3, viewing H_1 and H_2 as subgroups of $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$, identify the corresponding fixed fields $\mathbb{Q}(\sqrt[3]{2},\omega)^{H_1}$ and $\mathbb{Q}(\sqrt[3]{2},\omega)^{H_2}$.

2. Consider the field $\mathbb{Q}(\sqrt[4]{2},i)$. By our work in class, we have seen that $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q})$ has order 8. In fact, if $\beta_1 = \sqrt[4]{2}$, $\beta_2 = i\sqrt[4]{2}$, $\beta_3 = -\sqrt[4]{2}$, $\beta_4 = -i\sqrt[4]{2}$, then $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q})$ permutes $\beta_1, \beta_2, \beta_3$, β_4 and the permutations (1234) and (24) correspond to elements of the Galois group. Hence $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q}) \cong D_4$. Moreover, the following are among the subgroups of D_4: $\langle(1234)\rangle$ $\langle(13)(24)\rangle$, $\langle(24)\rangle$, $\langle(13)\rangle$.

   (i) Suppose that $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q})$ corresponds to the permutation $(13)(24)$. Show that $\sigma(\sqrt{2}) = \sqrt{2}$ and that $\sigma(i) = i$. Conclude that $\mathbb{Q}(\sqrt[4]{2},i)^\sigma = \mathbb{Q}(\sqrt[4]{2},i)^{\langle\sigma\rangle} = \mathbb{Q}(\sqrt{2},i)$.

   (ii) Let $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q})$ be complex conjugation. Thus τ corresponds to the permutation (24). Identify the fixed field $\mathbb{Q}(\sqrt[4]{2},i)^\tau = \mathbb{Q}(\sqrt[4]{2},i)^{\langle\tau\rangle}$.

   (iii) Let $\rho \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q})$ correspond to the permutation (13). Show that $\mathbb{Q}(i\sqrt[4]{2})$ is contained in the fixed field $\mathbb{Q}(\sqrt[4]{2},i)^\rho = \mathbb{Q}(\sqrt[4]{2},i)^{\langle\rho\rangle}$ and then argue that $\mathbb{Q}(i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2},i)^{\langle\rho\rangle}$.

(iv) For the subgroup $H = \langle(1234)\rangle$, argue that $\mathbb{Q}(i)$ is contained in $\mathbb{Q}(\sqrt[4]{2}, i)^H$ by showing that the element of $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ corresponding to (1234) fixes i.

3. (Cyclotomic extensions.) Let F be a field of characteristic zero and let $n \in \mathbb{N}$.

   (i) Show that the polynomial $x^n - 1$ has no multiple roots in any extension field E of F.

   (ii) Let E be a splitting field for $x^n - 1$ over F. Show that E contains n distinct roots of $x^n - 1$, called the n^{th} *roots of unity*, and that the set of all such is a cyclic subgroup of E^*. A generator ζ is called a *primitive* n^{th} root of unity. Show that $E = F(\zeta)$ for ζ any primitive n^{th} root of unity. For $F = \mathbb{Q}$, we write ζ_n for the choice $\zeta = e^{2\pi i/n}$. Note that ζ^i is well-defined for $i \in \mathbb{Z}/n\mathbb{Z}$ and that
   $$x^n - 1 = \prod_{i=0}^{n-1}(x - \zeta^i) = \prod_{i \in \mathbb{Z}/n\mathbb{Z}}(x - \zeta^i).$$

   (iii) Let E and ζ be as above. Show that E is a normal extension of F. Let $\sigma \in \mathrm{Gal}(E/F)$. Show that $\sigma(\zeta) = \zeta^i$ for a unique $i \in (\mathbb{Z}/n\mathbb{Z})^*$. The main point here is to show that i must be relatively prime to n, i.e. that the order of $\sigma(\zeta)$ is n. Finally show that the function
   $$\sigma \in \mathrm{Gal}(E/F) \mapsto i \in (\mathbb{Z}/n\mathbb{Z})^*,$$
   where $\sigma(\zeta) = \zeta^i$, defines an injective homomorphism from $\mathrm{Gal}(E/F)$ to $(\mathbb{Z}/n\mathbb{Z})^*$. In particular, $\mathrm{Gal}(E/F)$ is abelian.

   (iv) We have seen that, for $F = \mathbb{Q}$ and $n = p$ a prime number, $\Phi_p(x) = (x^p - 1)/(x - 1) \in \mathbb{Q}[x]$ and $\Phi_p(x)$ is irreducible, by the Eisenstein criterion. Using this fact, show that $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$, which is cyclic of order $p - 1$.

   (Note: In fact, one can show that the polynomial
   $$\Phi_n(x) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^*}(x - \zeta^i)$$
   has coefficients in $\mathbb{Q}$ and is always irreducible in $\mathbb{Q}[x]$. It then follows that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$.)