Math 121. Homework 9

1. Let p be an *odd* prime. Recall the isomorphism $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}) \simeq (\mathbf{Z}/p^n\mathbf{Z})^\times$.
(i) For any $n \geq 1$, show that there exists a unique subfield $K \subseteq \mathbf{Q}(\zeta_{p^n})$ with degree p^{n-1} over $\mathbf{Q}$ and that $K/\mathbf{Q}$ is Galois with cyclic Galois group. In addition, show that K and $\mathbf{Q}(\zeta_p)$ have trivial intersection (i.e., $\mathbf{Q}$) and have composite $\mathbf{Q}(\zeta_{p^n})$.
(ii) The field $\mathbf{Q}(\zeta_9)$ contains the quadratic field $\mathbf{Q}(\zeta_3) = \mathbf{Q}(\sqrt{-3})$. For $a = \zeta_9 + \zeta_9^{-1} = 2\cos(2\pi/9)$, show that $K = \mathbf{Q}(a)$ is the only other field lying strictly between $\mathbf{Q}(\zeta_9)$ and $\mathbf{Q}$, and that it is Galois of degree 3 over $\mathbf{Q}$.
(iii) Find the minimal polynomial f over $\mathbf{Q}$ for a in (ii), and verify that its discriminant Δ_f is a square in $\mathbf{Q}$ (as it must be, since $\mathrm{Gal}(\mathbf{Q}(a)/\mathbf{Q}) = A_3$).

2. We consider subfields of a fixed choice of $\overline{\mathbf{Q}}$. Recall that for N and d positive integers with $d|N$, the natural diagram of groups (using restriction and reduction along left and right respectively)

$$\begin{array}{ccc} \mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q}) & \simeq & (\mathbf{Z}/N\mathbf{Z})^\times \\ \downarrow & & \downarrow \\ \mathrm{Gal}(\mathbf{Q}(\zeta_d)/\mathbf{Q}) & \simeq & (\mathbf{Z}/d\mathbf{Z})^\times \end{array}$$

commutes, so $\mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q}(\zeta_d)) = \{x \in (\mathbf{Z}/N\mathbf{Z})^\times \mid x \equiv 1 \bmod d\}$.
(i) By working inside $\mathbf{Q}(\zeta_N)$ with $N = nm$ for any positive integers n and m, prove $\mathbf{Q}(\zeta_n) \cap \mathbf{Q}(\zeta_m) = \mathbf{Q}(\zeta_{(n,m)})$ and $\mathbf{Q}(\zeta_n)\mathbf{Q}(\zeta_m) = \mathbf{Q}(\zeta_{[n,m]})$, where $(n,m) = \gcd(n,m)$ and $[n,m] = \mathrm{lcm}(n,m)$.
(ii) Using (i), prove that $\mathbf{Q}(\zeta_n) = \mathbf{Q}(\zeta_m)$ if and only if $n = m$ or one of n or m is odd and the other is twice that (e.g., $\mathbf{Q}(\zeta_{14}) = \mathbf{Q}(\zeta_7)$ since $-\zeta_7$ is a primitive 14th root of unity).

3. Let L/k and F/k be a finite Galois extensions such that there exists a k-embedding $i : L \to F$. Upon choosing such an i, consider the resulting restriction map $i^* : \mathrm{Gal}(F/k) \to \mathrm{Gal}(L/k)$ on Galois groups (using that the action on F by any $\sigma \in \mathrm{Gal}(F/k)$ preserves the subfield $i(L)$ that is Galois over k; we have $\sigma \circ i = i \circ i^*(\sigma)$ on L).

Show that as i varies, the map i^* changes precisely by composition with conjugation by elements of $\mathrm{Gal}(L/k)$. Deduce that i^* is independent of i if and only if $\mathrm{Gal}(L/k)$ is abelian.

4. This exercise proves that an irreducible $f \in \mathbf{Q}[X]$ splitting completely over $\mathbf{R}$ with degree not a power of 2 (e.g., *any* odd degree > 1) is not "solvable in *real* radicals". In particular, even if the roots of such an f (all in $\mathbf{R}$!) are solvable in radicals, any such "radical formula" in $\mathbf{C}$ for the roots must involve non-real complex numbers. (For cubic irreducible $f \in \mathbf{Q}[X]$ with three real roots, this recovers the *casus irreduciblis* that baffled mathematicians in the Middle Ages).

(i) Let p be prime, and k *any* field. Prove $X^p - a$ is *irreducible* in $k[X]$ for $a \in k - k^p$. Hint: check a^d does not have a pth root in k for any integer d not divisible by p. (For composite n you might guess $X^n - a$ is irreducible if $a \notin k^d$ for all $d|n$ with $d > 1$, but this is *false* if $4|n$ and $-4 \notin k^4$ since $X^n + 4c^n = (X^{n/2} + 2c^{n/2})^2 - (2c^{n/4}X^{n/4})^2 = (X^{n/2} - 2c^{n/4}X^{n/4} + 2c^{n/2})(X^{n/2} + 2c^{n/4}X^{n/4} + 2c^{n/2})$.)

(ii) Let k be a field and $L = k(a)$ where $a^n = c \in k^\times$. (Informally, $L = k(c^{1/n})$, but this notation is dangerous when $X^n - c$ is not *irreducible* over k.) Exhibit L/k as a tower $k = k_0 \subset k_1 \subset \cdots \subset k_r = L$ where $k_i = k_{i-1}(a_i)$ with $a_i^{\ell_i} \in k_{i-1}$ for primes $\ell_i | n$.

(iii) In the setup of (ii), assume L does not contain roots of unity other than ± 1 (e.g., any subfield of $\mathbf{R}$). Prove that for any subextension $F \subseteq L$ over k that is Galois over k, $[F : k]$ is a power of 2. Hint: As in Artin's proof of the Fundamental Theorem of Algebra, for a prime $p|[F : k]$ increase k to arrange $[F : k] = p$. Compare F/k with stages in the tower built in (ii) to show $p = 2$.

(iv) Let L/k be a radical tower not containing roots of unity other than ± 1. Show that any subfield F/k that is Galois has degree a power of 2.