M901-2008 Assignment 8: Due Monday November 24

Instructions: Do any three of the following problems.

(1) Let F be an algebraic closure of a field K. Assume that a field E is Galois over K and cyclic if $E \subseteq F$ and if E is finite over K. [Aside: the point of this problem is to prove (g), which gives a converse to Exercise 5 on Assignment 7. Feel free to ignore steps (a)-(f) if you can prove (g) directly.]

   (a) Prove that every intermediate field L is normal over K. Conclude that any automorphism $\sigma \in \mathrm{Aut}_K F$ restricts to an automorphism $\sigma_L \in \mathrm{Aut}_K L$.

   (b) Let E be an intermediate field, finite over K, let $\sigma \in \mathrm{Aut}_K F$ and assume that $E^\sigma = K$, where E^σ is the set of all elements $e \in E$ with $\sigma(e) = e$. Prove that $G(E/K)$ is generated by σ_E.

   (c) Let E be an intermediate field, let $\sigma \in \mathrm{Aut}_K F$ with $E^\sigma = K$, let $\alpha \in F$, and assume $\sigma(\alpha) = \alpha$. Show that $E \cap K(\alpha) = K$, that $f_{\alpha,E} = f_{\alpha,K}$, and conclude that $[E(\alpha) : E] = [K(\alpha) : K]$.

   (d) Let E be an intermediate field, finite over K, let $\sigma \in \mathrm{Aut}_K F$ with $E^\sigma = K$, let $\alpha \in F$, and assume $\sigma(\alpha) = \alpha$. Prove that $[E : K]$ and $[K(\alpha) : K]$ are relatively prime.

   (e) Let E be an intermediate field, let $\sigma \in \mathrm{Aut}_K F$ with $E^\sigma = K$, let $\alpha \in F$, and assume $\sigma(\alpha) = \alpha$. Given $g \in \mathrm{Aut}_E E(\alpha)$ and $s = \sigma_{E(\alpha)}$, show that $gs = sg$.

   (f) Let E be an intermediate field, let $\sigma \in \mathrm{Aut}_K F$ with $E^\sigma = K$, let $\alpha \in F$, and assume $\sigma(\alpha) = \alpha$. If $r = [K(\alpha) : K]$ and $\sigma^r(a) = a$ for some $a \in E(\alpha)$, prove that $\sigma(a) = a$.

   (g) Prove that there is a K-automorphism μ of F such that $F^\mu = K$.

(2) Find a finite subset S of the complex numbers such that $\mathbf{Q}(S)/\mathbf{Q}$ is a cyclic Galois extension of degree 45.

(3) Let $\Phi_n(x)$ denote the n-th cyclotomic polynomial over the rationals and let ζ_n denote a primitive n-th root of 1.

   (a) Show that $\Phi_{2n}(x) = \Phi_n(-x)$ if $n > 1$ is odd.

   (b) If p is a prime factor of n, show that $\Phi_{pn}(x) = \Phi_n(x^p)$.

(4) Let $\Phi_n(x)$ denote the n-th cyclotomic polynomial over the rationals. You may assume the fact for any n that $x^n - 1 = \Pi_{d|n} \Phi_d(x)$.

   (a) Show that $\Pi_{d|n} \Phi_d(x^m) = \Pi_{d|nm} \Phi_d(x)$.

   (b) If p is prime but does not divide n, show that $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$.

(5) Not every positive integer is a sum of two squares; for example, 3 is not a sum of the squares of any two integers. However, every integer is the sum of two squares modulo any prime p. More generally, let F be any finite field. Show that every element in F is a sum of two squares.