MAT 612 **HW #7** Name ______________________________
04/17/10, due Friday 04/23/10, 5 pm
25 points

For these problems, use the Fundamental Theorem of Galois Theory (which we are in the midst of proving in class): if E is Galois over F with $|E : F| < \infty$, then subgroups of $G = \text{Gal}(E, F)$ are in one-to-one correspondence with fields K with $F \subseteq K \subseteq E$, and $|E : K| = |\,\text{Gal}(E, K)|$. Moreover, $H = \text{Gal}(E, K)$ is normal in G if and only if K is Galois over F, in which case $G/H \cong \text{Gal}(K, F)$.
In addition, you may use the following results (which will be proved in the course of proving the "FTGT"): if $\text{char}(F) = 0$ then E is Galois over F if and only if E is a splitting field of some polynomial in $F[x]$. In this case, every irreducible $f \in F[x]$ splits over E, and G acts transitively on its roots.

1. Find a splitting field $E \subseteq \mathbb{C}$ of the polynomial $f(x) = x^4 - 4$ over $\mathbb{Q}$. Identify the Galois group, and find $\alpha \in E$ such that $E = \mathbb{Q}[\alpha]$. (α is called a *primitive element* for the extension.)

2. Let $\omega = e^{2\pi i/n}$.

   (a) Show that $E = \mathbb{Q}[\omega]$ is a splitting field for the polynomial $f(x) = x^n - 1$, hence E is Galois over $\mathbb{Q}$.

   (b) Let $f(x) = \prod_{(k,n)=1}(x - \omega^k)$. Show $f \in \mathbb{Q}[x]$. (In fact $f(x)$ is irreducible over $\mathbb{Q}$.)

   (c) Show that $\mathbb{Q}[\omega^k] = \mathbb{Q}[\omega]$ if $(k, n) = 1$, use this to prove that $\text{Gal}(E, \mathbb{Q})$ is isomorphic to the group $U(\mathbb{Z}_n)$ of units in $\mathbb{Z}_n$. You may use the fact that $f(x)$ is irreducible, without proof.

   (d) By analyzing the group $U(\mathbb{Z}_{17})$, show that $e^{2\pi i/17}$ is constructible by compass and straightedge. (Hence the 17-gon is constructible; the same is true for any prime number of the form $n = 2^m + 1$; if $2^m + 1$ is prime, m must be a power of 2.)

   (e) By analyzing the group $U(\mathbb{Z}_{18})$, prove that $e^{2\pi i/18}$ is not constructible by compass and straightedge. (Since $e^{2\pi i/6}$ is constructible, this shows that angles cannot be trisected.)

   (f) Using part (b), find the minimal polynomial of ω over $\mathbb{Q}$ for $n = 3, 4, 5$, and 6.

   (g) $m_\omega^{\mathbb{Q}}(x)$ is called the n^{th} *cyclotomic polynomial*, denoted Φ_n. Find the degree of Φ_n.

   (h) Let $\omega = e^{2\pi i/8}$. Identify explicitly all fields F such that $\mathbb{Q} \subseteq F \subseteq E$ with $|F : \mathbb{Q}| = 2$.

3. (a) Suppose $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial of odd degree n, and not all roots of f are real. Show that the Galois group of f has order strictly greater than n. Here, the Galois group of a polynomial $f \in F[x]$ is, by definition, the Galois group of a splitting field of f over F. (Hint: Complex conjugation is an automorphism of $\mathbb{C}$; show that it must send a splitting field of f in $\mathbb{C}$ to itself.)

   (b) Identify the Galois group of a cubic polynomial in $\mathbb{Q}[x]$ that has only one real root.