Homework 3, Math 5032, Due Feb 11th

1. Let $f(x) \in K[x]$ be an irreducible polynomial over K, a subfield of $\mathbb{R}$. Asuume that it has a non-real root of absolute value 1. Then show that if $\alpha \in \mathbb{C}$ is any root of f so is α^{-1} and deduce that the degree of f is even. (Hint: If $\omega \in \mathbb{C}$ with $\mid \omega \mid= 1$ then $\omega^{-1} = \overline{\omega}$, the complex conjugate)

2. Show that in any finite extension of $\mathbb{Q}$ there are atmost finitely many roots of unity.

3. Below are some interesting applications of the cyclotomic polynomial.

   (a) Show that for any prime number p, $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$.

   (b) If p is a prime and $r \geq 1$ an integer, show that $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$.

   (c) If n is an integer which is not divisble by p and $r \geq 1$, show that $\Phi_{p^r n}(X) = \frac{\Phi_n(X^{p^r})}{\Phi_n(X^{p^{r-1}})}$.

   (d) Let ω be a primitive n^{th} root of unity and let $K = \mathbb{Q}(\omega)$ where $n \geq 2$. Show that if n is the power of a prime, then $N_{K/\mathbb{Q}}(1-\omega) = p$ and if n has at least two disitinct prime factors, then $N_{K/\mathbb{Q}}(1-\omega) = 1$.

   (e) Let $0 \neq a \in \mathbb{Z}$ and p a prime and n a positive integer not divisible by n. Prove that p divides $\Phi_n(a)$ if and only if a has period n in $(\mathbb{Z}/p\mathbb{Z})^*$.

   (f) With the same hypothesis as above, prove that p divides $\Phi_n(a)$ for some $a \in \mathbb{Z}$ if and only if $p \equiv 1 \bmod n$. Deduce that there are infinitely many primes of the form $1 \bmod n$. (This is a special case of Dirichlet's Theorem, which states that for any two positive integers a, b with $\gcd(a, b) = 1$, there exists infinitley many primes in the arithmetical progression $\{a + nb\}, n \in \mathbb{N}$.)

   (g) Let G be any finite abelian group. Then we know that $G \cong \oplus_{i=1}^{n} G_i$ where G_is are cyclic groups. Show that there exists distinct primes $p_1, \ldots, p_n$ so that if $N = p_1 \cdot p_2 \cdots p_n$, then $(\mathbb{Z}/N\mathbb{Z})^*$ surjects onto G. Deduce that there exists a finte Galois extension K of $\mathbb{Q}$, $K \subset \mathbb{Q}(\omega)$ where ω is a primitive N^{th} root of 1 and the Galois group of K over $\mathbb{Q}$ is G.