Math 494, Homework 9: due April 1

(1) For $n \in \mathbb{N}$, define $\phi(n)$ to be the cardinality of $(\mathbb{Z}/n\mathbb{Z})^*$, i.e., the number of integers k with $1 \le k \le n$ for which $\gcd(k,n) = 1$. For each prime power q and each positive integer d dividing $q-1$, express the number of order-d elements of $\mathbb{F}_q^*$ as a value of ϕ. Deduce from this a positive lower bound on the number of monic irreducible degree-n polynomials in $\mathbb{F}_q[x]$ (express the lower bound in terms of a value of ϕ).

(2) Let q be a prime power with $q \equiv 1 \pmod 4$, and let $f(X)$ and $g(X)$ be distinct monic irreducible polynomials in $\mathbb{F}_q[X]$. Show that the image of $f(X)$ in $\mathbb{F}_q[X]/(g(X))$ is a square if and only if the image of $g(X)$ in $\mathbb{F}_q[X]/(f(X))$ is a square.
(I will post hints on piazza.)

(3) Let N/K be a Galois extension, and let L be a field with $K \subseteq L \subseteq N$. Let H be the set of all elements $h \in \mathrm{Gal}(N/K)$ such that $h(L) = L$. Show that H is the normalizer of $\mathrm{Gal}(N/L)$ in $\mathrm{Gal}(N/K)$.
Note that the condition $h(L) = L$ says h preserves L as a set, which is a different assertion than saying that h fixes every element of L. That is, it says h fixes L setwise but not necessarily pointwise.

(4) Determine all n for which a regular n-gon can be constructed using straightedge and compass.

(5) Fill in the missing details in the following sketch of a proof that $\mathbb{C}$ is algebraically closed. Note that the only non-algebraic ingredient is the intermediate value theorem on $\mathbb{R}$.
Let $M/\mathbb{C}$ be any finite extension, and let N be the normal closure of $M/\mathbb{R}$. Show (easily) that $N/\mathbb{R}$ is Galois. Let H be a Sylow 2-subgroup of $G := \mathrm{Gal}(N/\mathbb{R})$, and put $L := N^H$. Show that $[L : \mathbb{R}]$ is odd. Then use the intermediate value theorem to show that $[L : \mathbb{R}]$ cannot be greater than 1. Conclude that $G = H$, so that $[N : \mathbb{R}]$ is a power of 2. Now $N/\mathbb{C}$ is Galois with Galois group being a 2-group. Deduce that if $N \ne \mathbb{C}$ then there is a field K with $\mathbb{C} < K \le N$ and $[K : \mathbb{C}] = 2$. Then obtain a contradiction by showing directly that there is no degree-2 extension $K/\mathbb{C}$.

(6) Problems 7.1, 7.2, 7.3, 7.6 from chapter 16 of Artin *(in 7.1, assume that a, b, ab are all nonsquares in F, and that F does not have characteristic 2).*