E. Dummit's Math 5111 ~ Algebra 1, Fall 2020 ~ Homework 5, due Fri Oct 16th.

Justify all responses with proof and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. You may use results from earlier parts of problems in later parts, even if you were unable to solve the earlier parts.

---

1. Recall that we have shown that a regular n-gon can be constructed with straightedge and compass if and only if the length $\cos(2\pi/n)$ can be constructed with straightedge and compass.

   (a) Show that $\cos(2\pi/5) = \dfrac{\sqrt{5}-1}{4}$, and deduce that the regular 5-gon is constructible with straightedge and compass. [Hint: Observe that $\cos(4\pi/5) = \cos(6\pi/5)$ and then use cosine identities to obtain a cubic equation satisfied by $\alpha = \cos(2\pi/5)$.]

   (b) Show that the regular 9-gon is not constructible with straightedge and compass.

   (c) Show that the minimal polynomial of $\cos(2\pi/7)$ over $\mathbb{Q}$ is $m(x) = 8x^3 + 4x^2 - 4x - 1$. Deduce that the regular 7-gon is not constructible with straightedge and compass.

---

2. Let K be the splitting field of $x^4 - 2$ over $\mathbb{Q}$.

   (a) Show that $K = \mathbb{Q}(2^{1/4}, i)$ and determine $[K : \mathbb{Q}]$.

   (b) Show that $x^4 - 2$ is irreducible over $\mathbb{Q}(i)$.

---

3. Let $f(x) = x^6 + 3$, let α be any root of f inside $\mathbb{C}$, and set $E = \mathbb{Q}(\alpha)$.

   (a) Find $[E : \mathbb{Q}]$.

   (b) Show that E contains $\zeta_6 = e^{2\pi i/6}$.

   (c) Show that f splits completely over E, and that in fact E is the splitting field of f.

---

4. Let p be a prime, $q(x) \in \mathbb{F}_p[x]$, and let K be the splitting field of $q(x)$.

   (a) If $a \in \mathbb{F}_p$, show that $a^p = a$, and then conclude that $q(x^p) = q(x)^p$.

   (b) Show that the Frobenius map $\varphi_p(x) = x^p$ permutes the set of roots of $q(x)$.

---

5. Let p be a prime, n be a positive integer, and $\zeta_{p^n} = e^{2\pi i/p^n}$ denote a primitive p^nth root of unity. In class, we proved that the polynomial $\dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ was irreducible over $\mathbb{Q}$ and used it to deduce that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. The goal of this problem is to extend this argument to higher prime powers.

   (a) If n is a positive integer divisible by p but not by p^2, prove that the polynomial $q(x) = \dfrac{x^{p^n} - 1}{x^{p^{n-1}} - 1} = x^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + \cdots + x^{p^{n-1}} + 1$ is irreducible over $\mathbb{Q}$. [Hint: Use Eisenstein's criterion on $q(x+1)$. Try working with the fraction form of $q(x)$ over $\mathbb{F}_p$.]

   (b) Show that $[\mathbb{Q}(\zeta_{p^n}) : \mathbb{Q}] = p^{n-1}(p-1)$ for any positive integer n.

---

6. Prove that the following are equivalent (suggestion: show that (a)-(d) are equivalent, and then do the others):

   (a) Every nonconstant polynomial in $F[x]$ has a root in F.
   (b) Every nonconstant polynomial in $F[x]$ splits completely in F.
   (c) If K/F is an algebraic extension, then $K = F$.
   (d) If K/F is a finite-degree extension, then $K = F$.
   (e) F is the algebraic closure of some field E.
   (f) Two polynomials in $F[x]$ are relatively prime if and only if they have no common roots in F.
   (g) For any positive integer n, every linear transformation $T : F^n \to F^n$ has at least one nonzero eigenvector in F^n.
