Math 494, Homework 8: due Mar 25

(1) Determine all primitive elements for the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. (This means: name all γ such that $\mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$).

(2) A field K is called *perfect* if every finite extension L/K is separable. Show that K is perfect if and only if one of these holds:
   (1) K has characteristic 0, or
   (2) K has characteristic p with $p > 0$, and also every element of K has a p-th root in K.

(3) Let p be prime, let $L := \mathbb{F}_p(X, Y)$ be the field of rational functions in two variables, and put $K := \mathbb{F}_p(X^p, Y^p)$. It was shown in piazza that $L \neq K(z)$ for any $z \in L$ ("A splitting field which is not the splitting field of an irreducible polynomial"). Determine $[L : K]$, and exhibit infinitely many distinct fields F such that $K \subset F \subset L$ *(don't just cite problem 4 for this, instead you should name the fields F here).*

(4) Let L/K be a finite-degree field extension, where K is infinite. Show that L can be written as $K(\alpha)$ for some $\alpha \in L$ if and only if there exist only finitely many fields F with $K \subset F \subset L$.
(I will post hints for this on piazza.)

(5) Let n be a positive integer and put $\zeta := e^{2\pi i/n}$, so that ζ is a primitive n-th root of unity in $\mathbb{C}$. Show that $\Phi_n(X) := \prod_i (X - \zeta^i)$ is in $\mathbb{Q}[X]$, where the product runs over all $i \in \mathbb{Z}$ such that $\gcd(i, n) = 1$ and $1 \leq i \leq n$. Under the assumption that $\Phi_n(X)$ is irreducible in $\mathbb{Q}[X]$, name all automorphisms of $\mathbb{Q}(\zeta)$, and name a familiar group which is isomorphic to the group of all such automorphisms.

(6) In the notation of the above problem, fill in the following sketch of a proof that $\Phi_n(X)$ is irreducible in $\mathbb{Q}[X]$: first show that $X^n - 1 = \prod_{d|n} \Phi_d(X)$ (where the product is over all positive integers d which divide n), and deduce that $\Phi_n(X) \in \mathbb{Z}[X]$. Let ζ be any primitive n-th root of unity in $\mathbb{C}$, and let $f(X)$ be the minimal polynomial of ζ over $\mathbb{Q}$. For any prime p which doesn't divide n, let $f_p(X)$ be the minimal polynomial of ζ^p over $\mathbb{Q}$. We want to show that $f(X) = f_p(X)$. Show that both $f(X)$ and $f_p(X)$ are in $\mathbb{Z}[X]$, and that if $f(X) \neq f_p(X)$ then $f(X) \cdot f_p(X)$ divides $X^n - 1$ in $\mathbb{Z}[X]$. Then show that this yields an impossible situation when we reduce mod p. Thus the set of roots of $f(X)$ is preserved by p-th powering, and hence by m-th powering for any m coprime to n. Conclude that $f(X) = \Phi_n(X)$, so that $\Phi_n(X)$ is irreducible in $\mathbb{Q}[X]$.