Your Name Goes Here

Dartmouth College
Mathematics 81/111 — Homework 6

1. Let K be the splitting field over $\mathbb{Q}$ of $f(x) = (x^2 - 2)(x^2 - 3)(x^2 - 5)$.
   (a) Characterize the Galois group $\mathrm{Gal}(K/\mathbb{Q})$, i.e., describe the elements and the isomorphism class of the group.
   (b) Determine all the intermediate fields F, with $\mathbb{Q} \subseteq F \subseteq K$, and their degrees.
   (c) Prove that $\xi = \sqrt{2} + \sqrt{3} + \sqrt{5}$ is a primitive element for the extension. Hint: Do this in a Galois way, that is, do not try to compute the degree of ξ over $\mathbb{Q}$.

2. Let p be a prime, and K the splitting field of $x^p - 2$ over $\mathbb{Q}$.
   (a) Characterize the elements of the Galois group of $K/\mathbb{Q}$ ensuring of course that the maps you write down are indeed automorphisms.
   (b) Show that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the group of matrices $\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right)$, where $u, v \in \mathbb{F}_p$, $u \neq 0$.

3. Let ϕ be the Euler totient function, which we can define by $\phi(1) = 1$ and for $n \geq 2$, $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$. We know by the Chinese Remainder Theorem, if $m, n \geq 2$ are relatively prime integers then $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ as rings, so their unit groups are also isomorphic: $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Thus the Euler function satisfies $\phi(mn) = \phi(m)\phi(n)$ when $\gcd(m, n) = 1$.
   (a) Show that for any two positive integers m, n we have $\phi(m)\phi(n) = \phi([m, n])\phi((m, n))$ where $[m, n]$ denotes the lcm of m, n and (m, n) denotes their gcd.
   (b) Show that composite of the cyclotomic fields $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$ is the cyclotomic field $Q(\zeta_\ell)$ where $\ell = [m, n]$.
   (c) Using the above and some Galois theory, show that $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d)$, where $d = (m, n)$. In case we have not quite gotten there, Theorem VI.1.12 should be useful.

4. Let L/K be a finite extension of fields. Let $[L : K]_s$, the separable degree of L/K, denote the number of distinct embeddings of L/K into an algebraic closure $\overline{K}$. Let $L_s = \{\alpha \in L \mid \alpha \text{ is separable over } K\}$. We are going to explore inseparability a bit more. You could find most of this in V.6 of Lang, but since we did not do it in class, it is worth your time to work through this exercise on your own.

   If L/K is separable, we know that $L = L_s$, so let's assume that L/K is not separable. Let $\sigma : L_s/K \to \overline{K}$ be an embedding. Characterize all the extensions of σ to an embedding of $L/K \to \overline{K}$. Use this to show that $[L : K]_s = [L_s : K]$.

(assignment continued on next page)

5. Let L/K be a finite separable extension of fields with $[L : K] = n$, and let $\widehat{L}$ be the normal (i.e., Galois) closure of L. We have shown in class that $[\widehat{L} : K] \leq n!$. Now establish the sharper result that $[\widehat{L} : K] \mid n!$. Hint: If we let $G = \mathrm{Gal}(\widehat{L}/K)$, the result would follow (why?) by showing the existence of an injective homomorphism $\varphi : G \to S_n$.