Homework 10 **Math 5591H**

Due by Tuesday, April 9

14.2.10. Let $f = x^8 - 3 \in \mathbb{Q}[x]$.

(a) Find the degrees and all the conjugates of $\alpha = \sqrt[8]{3} \in \mathbb{R}$ and of $\omega = e^{2\pi i/8}$. Determine whether the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is normal and whether $\mathbb{Q}(\omega)/\mathbb{Q}$ is normal.

(b) Find the splitting field K of f and find its degree.

(c) Find the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. (*Hint:* Explain why α and ω can be sent by elements of G to any of their conjugates independently, and why every element of G is defined by its action on α and ω. Name the elements of G and find the multiplication rule of G.)

14.2.13. Prove that if the Galois group of the splitting field of a cubic over $\mathbb{Q}$ is cyclic of order 3 then all roots of the cubic are real. (*Hint:* Consider the complex conjugation.)

14.2.14. Let $K = \mathbb{Q}\big(\sqrt{2+\sqrt{2}}\big)$; prove that $K/\mathbb{Q}$ is a Galois extension and that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_4$.

14.3.8. Determine the splitting field and the Galois group of the polynomial $f(x) = x^p - x - a \in \mathbb{F}_p[x]$, where $a \in \mathbb{F}_p \setminus \{0\}$. (*Hint:* Let α be a root of f; prove that any nontrivial automorphism of $\mathbb{F}_p(\alpha)$ has order p.)

Cf. 14.2.3. Let $f = (x^2-2)(x^2-3)(x^2-5) \in \mathbb{Q}[x]$; find the splitting field K of f and $\mathrm{Gal}(f/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q})$. List all 16 subgroups of G and for every subgroup $H \leq G$ find the subfield $\mathrm{Fix}(H)$ of K.

14.5.10. Prove that $\sqrt[3]{2}$ is not contained in any cyclotomic field. (*Hint:* What is the Galois group of $x^3 - 2$? What is the Galois group of a cyclotomic extension?)

A1. Prove that there are no biquadratic extensions of finite fields. (*Hint:* What is the Galois group of a biquadratic extension? What is the Galois group of a finite extension of a finite field?)

A2. Let K/F be a Galois extension, let $G = \mathrm{Gal}(K/F)$. For every prime p and every $r \in \mathbb{N}$ such that $p^r \,\big|\, |G|$, prove that there is a subfield L of K with $[K : L] = p^r$. (*Hint:* Recall Sylow.)