Lior Silberman's Math 422/501: Problem Set 7 (due 6/11/2020)

Galois theory

1. Let L/K be a finite Galois extension. Let $K \subset M_1, M_2 \subset L$ be two intermediate fields. Show that the following are equivalent:
   (1) M_1/K and M_2/K are isomorphic extensions.
   (2) There exists $\sigma \in \mathrm{Gal}(L:K)$ such that $\sigma(M_1) = M_2$.
   (3) $\mathrm{Gal}(L:M_i)$ are conjugate subgroups of $\mathrm{Gal}(L:K)$.

2. (V-extensions) Let K have characteristic different from 2.
   (a) Suppose L/K is normal, separable, with Galois group $C_2 \times C_2$. Show that $L = K(\alpha,\beta)$ with $\alpha^2, \beta^2 \in K$.
   (b) Suppose $a, b \in K$ are such that none of a, b, ab is a square in K. Show that $\mathrm{Gal}(K(\sqrt{a},\sqrt{b}):K) \simeq C_2 \times C_2$.

3. (The generalized quaternion group). Let G be a non-commutative group of order 8. Show that either $G \simeq D_8 = C_2 \ltimes C_4$ or $G \simeq Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2,\ i^4 = 1,\ ij = k,\ ji = i^2 k \rangle$ (the elememt $i^2 = j^2 = k^2$ is usually denoted -1 so the elements of the group are $\{\pm 1, \pm i, \pm j, \pm k\}$.

**4. Let $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$.
   (a) Show that $[\mathbb{Q}(\alpha):\mathbb{Q}] = 8$ and that this extension is normal.
   (b) Show that $\mathrm{Gal}(\mathbb{Q}(\alpha):\mathbb{Q}) \simeq Q_8$.

The fundamental theorem of algebra

5. (Preliminaries)
   (a) Show that every finite extension of $\mathbb{R}$ has even order.
   (b) Show that every quadratic extension of $\mathbb{R}$ is isomorphic to $\mathbb{C}$.

6. (Punch-line)
   (a) Let $F:\mathbb{R}$ be a finite extension. Show that $[F:\mathbb{R}]$ is a power of 2.
   Hint: Consider the 2-Sylow subgroup of the Galois group of the normal closure.
   (b) Show that every proper algebraic extension of $\mathbb{R}$ contains $\mathbb{C}$.
   (c) Show that every proper extension of $\mathbb{C}$ contains a quadratic extension of $\mathbb{C}$.
   (d) Show that $\mathbb{C}:\mathbb{R}$ is an algebraic closure.

Example: Cyclotomic fields

PRAC For practice (but not for submission)

(a) Show that $x^n - 1 \in \mathbb{Q}[x]$ has n distinct roots.

(b) Write μ_n for the set of roots of this polynomial. Show that it forms a cyclic group of order n.

DEF μ_n is called the *group of roots of unity of order [dividing] n*. A root of unity $\zeta \in \mu_n$ is called *primitive* if it is a generator, that is if it has order exactly n. We write ζ_n for a primitive root of unity of order n, for example $e^{\frac{2\pi i}{n}} \in \mathbb{C}$ (by problem 6(a) the choice doesn't matter). For the purpose of the problem set we also write $P_n \subset \mu_n$ for the set of primitive roots of unity of order n. The polynomial $\Phi_n(x) = \prod_{\zeta \in P_n}(x - \zeta)$ is called the nth *cyclotomic polynomial*. The field $\mathbb{Q}(\zeta_n)$ is called the nth *cyclotomic field*.

(c) Show that $\prod_{d|n} \Phi_d(x) = x^n - 1$. We'll later show that this is the factorization of $x^n - 1$ into irreducibles in $\mathbb{Q}[x]$.

6. Let ζ_n be a primitive nth root of unity.

(a) Show that $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$.

(b) Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$. For $\sigma \in G$ show there is a unique $j \in (\mathbb{Z}/n\mathbb{Z})^\times$ so that $\sigma(\zeta_n) = \zeta_n^{j(\sigma)}$ and that $j \colon G \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an injective homomorphism (we'll later show that this map is an isomorphism).

(c) Show that $\Phi_n(x) \in \mathbb{Q}[x]$ and that the degree of Φ_n is exactly $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.

7. (prime power and prime order) Fix an odd prime p and let $r \geq 1$.

(a) Show that $\Phi_{p^r}(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1}$ and that this polynomial is irreducible.

(b) Show that $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}) \simeq (\mathbb{Z}/p^r\mathbb{Z})^\times$.

RMK Parts (a),(b) hold for $p = 2$ as well.

(c) Show that $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q})$ is cyclic.

(d) Show that $\mathbb{Q}(\zeta_p)$ has a unique subfield K so that $[K : \mathbb{Q}] = 2$.

(e) Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p) : \mathbb{Q})$. Show that there is a unique non-trivial homomorphism $\chi \colon G \to \{\pm 1\}$.

(f) Let $g = \sum_{\sigma \in G} \chi(\sigma)\sigma(\zeta_p)$ (the "Gauss sum"). Show that $g \in K$ and that $g^2 \in \mathbb{Q}$.

(*g) Show that $g^2 = (-1)^{\frac{p-1}{2}} p$, hence that $K = \mathbb{Q}(g)$.