1 Homework 3.

1. Suppose p is a prime number. Prove that $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension and

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_0 \rangle$$

where $\sigma_0 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n},\ \sigma(a) := a^p$.

(**Hint**. Recall that $\mathbb{F}_{p^n}$ is a splitting field of the separable polynomial $x^{p^n} - x$ over $\mathbb{F}_p$, and $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p]$.)

2. Suppose p is a prime number and $\overline{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$. Let $\sigma_0 : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p,\ \sigma_0(x) = x^p$.

   (a) Argue why $\overline{\mathbb{F}}_p/\mathbb{F}_p$ is Galois, and prove that $\sigma_0 \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.

   (b) Prove that $\mathrm{Fix}(\sigma_0^n) =: \mathbb{F}_{p^n}$ is a finite field of order p^n, and $\overline{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.

   (c) Prove that

$$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \simeq \varprojlim(\mathbb{Z}/n\mathbb{Z})$$

   where

$$\varprojlim(\mathbb{Z}/n\mathbb{Z}) := \{(x_n)_n \in \prod_n \mathbb{Z}/n\mathbb{Z} \mid \forall m|n, x_n \equiv x_m \pmod{m}\}.$$

   (d) Prove that $\varprojlim(\mathbb{Z}/n\mathbb{Z})$ is torsion-free.

   (e) Suppose F is a subfield of $\overline{\mathbb{F}}_p$ and $[\overline{\mathbb{F}}_p : F] < \infty$. Prove that $F = \overline{\mathbb{F}}_p$.

(**Hint**. For part (d), suppose $k(x_n)_n = 0$ for some positive integer k; then for every positive integer n, we have $kx_{kn} \equiv 0 \pmod{kn}$. Hence $x_{kn} \equiv 0 \pmod{n}$. Because $x_n \equiv x_{kn} \pmod{n}$, deduce that $x_n \equiv 0 \pmod{n}$. Therefore $(x_n)_n = 0$.)

3. Suppose p is prime and $f \in F[x]$ is a separable irreducible polynomial of degree p. Let E be a splitting field of f over F. Argue why E/F is a Galois extension, and prove that $\mathrm{Gal}(E/F)$ is solvable if and only if for every two distinct zeros α and α' of f in E, $F[\alpha, \alpha'] = E$.

(**Hint**. Use the main theorem of Galois theory and Galois's theorem on solvable subgroups of S_p which act transitively on $[1..p]$.)

4. Suppose p is prime and $f \in \mathbb{Q}[x]$ is an irreducible polynomial of degree p. Suppose f has at least two real zeros and one complex non-real zero. Let $E \subseteq \mathbb{C}$ be a splitting field of f over $\mathbb{Q}$. Prove that $\mathrm{Gal}(E/\mathbb{Q})$ is not solvable.

5. Suppose E is a splitting field of an irreducible separable polynomial $f \in F[x]$ over F. Suppose

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

where α_i's are in E.

   (a) Prove that $\mathrm{Gal}(E/F[\alpha_i])$'s are conjugate of each other as subgroups of $\mathrm{Gal}(E/F)$.

   (b) Prove that if $\mathrm{Gal}(E/F)$ is abelian, then $E = F[\alpha_1]$ and

$$|\mathrm{Gal}(E/F)| = n.$$

(**Hint**. Part (a): argue that $\mathrm{Gal}(E/F)$ acts transitively on $\{\alpha_1, \ldots, \alpha_n\}$ and $G_i := \mathrm{Gal}(E/F[\alpha_i])$ is a stabilizer subgroup of $\mathrm{Gal}(E/F)$ with respect to α_i. For the second part, argue that in general

$$G_1 \cap \cdots \cap G_n = \{\mathrm{id}_E\};$$

in particular, if E/F is an abelian extension, then $G_1 = 1$.)

6. Suppose n is a positive integer and $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$.

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

   (b) Argue why $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ is a Galois extension and prove that $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ can be embedded into $(\mathbb{Z}/n\mathbb{Z})^\times$; in particular it is abelian.

   (c) Prove that $\mathbb{Q}[\sqrt[3]{2}]$ is not a subfield of $\mathbb{Q}[\zeta_n]$ for every n.

(**Hint.** For the second part, notice that for every $\sigma \in \mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ the multiplicative order of $\sigma(\zeta_n)$ is n, and so there exists $k_\sigma \in \mathbb{Z}$ such that $\gcd(k_\sigma, n) = 1$ and $\sigma(\zeta_n) = \zeta_n^{k_\sigma}$. Show that

$$\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma \mapsto k_\sigma + n\mathbb{Z}$$

is an injective group homomorphism.

For the third part, argue that $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ is not a normal extension and get a contradiction using the main theorem of Galois theory.)

7. Suppose $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$, and $\alpha_0 \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$.

   (a) Let $\Sigma_{\alpha_0} := \{F \in \mathrm{Int}(\overline{\mathbb{Q}}/\mathbb{Q}) \mid \alpha_0 \notin F\}$. Prove that Σ_{α_0} has a maximal element with respect to the ordering given by $\subseteq$.

   (b) Suppose F is a maximal element of Σ_{α_0} and $E \in \mathrm{Int}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a finite Galois extension of F. Prove that $\mathrm{Gal}(E/F)$ is cyclic.

   (**Hint**. For part (b), argue that for every $K \in \mathrm{Int}(E/F)$ which is not F, $F[\alpha_0] \subseteq K$. Use the main theorem of Galois theory and deduce that every proper subgroup of $\mathrm{Gal}(E/F)$ is a subgroup of $\mathrm{Gal}(E/F[\alpha_0])$. Deduce that for every $\sigma \in \mathrm{Gal}(E/F) \setminus \mathrm{Gal}(E/F[\alpha_0])$, $\mathrm{Gal}(E/F) = \langle \sigma \rangle$.)

8. Suppose $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$ and $\widehat{\sigma} \in \mathrm{Aut}_{\mathbb{Q}}(\overline{\mathbb{Q}})$. Let $F := \mathrm{Fix}(\widehat{\sigma})$. Suppose $E \in \mathrm{Int}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a finite Galois extension of F. Prove that $\mathrm{Gal}(E/F)$ is cyclic.

   (**Hint**. Argue why the restriction of $\widehat{\sigma}$ to E gives us an F-automorphism σ of E. Argue why $\mathrm{Fix}(\langle \sigma \rangle) = F$, and deduce that $\mathrm{Gal}(E/F) = \langle \sigma \rangle$.)