1 Homework 4.

1. Suppose $p > 4$ is prime. Prove that $f(x) := x^p - 4x + 2$ is not solvable by radicals.

   (**Hint.** Prove that f is irreducible, and it has at least two real zeros and one non-real complex zero. Suppose E is a splitting field of f over $\mathbb{Q}$, and show that $\mathrm{Gal}(E/\mathbb{Q})$ cannot be solvable.)

2. Suppose F is a field of characteristic zero, $f \in F[x]$ is irreducible, and E is a splitting field of f over F. Suppose

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

   for α_i's in E. Let

   $$\Delta_f := \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j),$$

   and $D_f := \Delta_f^2$. Let $G_{f,F}$ be subgroup of the symmetric group of $\{\alpha_1, \ldots, \alpha_n\}$ which is given by the Galois group $\mathrm{Gal}(E/F)$.

   (a) Prove that $D_f \in F$.

   (b) Prove that $\Delta_f \in F$ if and only if $G_{f,F}$ is a subgroup of the alternating subgroup.

   (**Hint**. Show that for every $\sigma \in \mathrm{Gal}(E/F)$, $\sigma(D_f) = D_f$. To show the second part, argue that $\sigma(\Delta_f) = \mathrm{sign}(\sigma)\Delta_f$ for every $\sigma \in \mathrm{Gal}(E/F)$.)

   (**Remark.** D_f is called the discriminant of f, and it can be expressed as polynomial in terms of the coefficients of f. Find the discriminant of $x^3 - px + q$. This can be very useful to find out what the Galois group of an irreducible cubic polynomial is.)

3. Suppose F is a field, $L := F(x_1, \ldots, x_n)$ is the field of fractions of $F[x_1, \ldots, x_n]$. For $\sigma \in S_n$ and $f \in L$, let $T_\sigma(f) = f(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$.

   (a) Prove that $T : S_n \to \mathrm{Aut}_F(L)$, $(T(\sigma))(f) := T_\sigma(f)$ is an injective group homomorphism.

(b) Let $K := \mathrm{Fix}(T(S_n))$. Elements of K are called *symmetric functions*. Let

$$(t - x_1) \cdots (t - x_n) = t^n - s_1 t^{n-1} + s_2 t^{n-2} - \cdots + (-1)^n s_n.$$

Let $E := F(s_1, \ldots, s_n)$. Prove that L is a splitting field of

$$t^n - s_1 t^{n-1} + \cdots + (-1)^n s_n$$

over E. Deduce that $[L : E] \leq n!$.

(c) Prove that $K = E$.

(d) For $f \in L$, let $G(f) := \{\sigma \in S_n \mid T_\sigma(f) = f\}$. Prove that

$$\mathrm{Fix}(T(G(f))) = K[f].$$

(e) Prove that $G(f) \subseteq G(g)$ for $f, g \in L$ if and only if there is $\theta \in K[t]$ such that $g = \theta(f)$.

(**Hint.** For part (c), notice that $[L : K] = |S_n|$, $E \subseteq K$, and $[L : E] \leq n!$. For part (d), observe that $\mathrm{Gal}(L/K)$ can be identified with S_n, and using the main Galois correspondence, $\mathrm{Gal}(L/K[f])$ gets identified with $G(f)$.)

(**Remark.** This result is known as *Lagrange's Rational Function Theorem*, and Lagrange proved this result before Galois theory was developed. Along the way, he proved some results about permutation groups, which later got generalized to what we call Lagrange's theorem in group theory!)

4. Suppose F is a field of characteristic zero and $\overline{F}$ is an algebraic closure of F. Let

$$F^{\mathrm{ab}} := \{\alpha \in F \mid F[\alpha]/F \text{ is Galois}, \mathrm{Gal}(F[\alpha]/F) \text{ is abelian}\}.$$

(a) Prove that F^{ab}/F is Galois.

(b) $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ is abelian.

(c) If E/F is a finite Galois extension and $\mathrm{Gal}(E/F)$ is abelian, then $E \subseteq F^{\mathrm{ab}}$.

(**Hint.** For part (a), argue that for every $\alpha \in F^{\mathrm{ab}}$, $F[\alpha]$ is a splitting field of $m_{\alpha,F}$ over F. Deduce that for $\alpha, \beta \in F^{\mathrm{ab}}$, $F[\alpha,\beta]$ is a splitting field of $m_{\alpha,F}m_{\beta,F}$ over F. Hence, $F[\alpha,\beta]/F$ is a normal extension. Argue why the restriction maps give us an embedding

$$\mathrm{Gal}(F[\alpha,\beta]/F) \to \mathrm{Gal}(F[\alpha]/F) \times \mathrm{Gal}(F[\beta]/F).$$

Deduce that $\mathrm{Gal}(F[\alpha,\beta]/F)$ is an abelian group. Use this to obtain that for every $E \in \mathrm{Int}(F[\alpha,\beta]/F)$, E/F is Galois and $\mathrm{Gal}(E/F)$ is abelian. Conclude that $\alpha \pm \beta, \alpha\beta^{\pm 1}$ are in F^{ab}. Therefore, F^{ab} is a subfield of $\overline{F}$. Argue that for every $\alpha \in F^{\mathrm{ab}}$ and every $\sigma \in \mathrm{Gal}(\overline{F}/F)$, $\sigma(\alpha) \in F[\alpha]$ and $F[\sigma(\alpha)] = F[\alpha]$. Deduce that F^{ab}/F is a normal extension. Argue why the restriction maps give us an embedding

$$\mathrm{Gal}(F^{\mathrm{ab}}/F) \to \prod_{\alpha \in F^{\mathrm{ab}}} \mathrm{Gal}(F[\alpha]/F),$$

and deduce that $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ is abelian. For the last part, use the primitive element theorem.)

5. Prove that $\mathbb{Q}[\cos(2\pi/n)]/\mathbb{Q}$ is a Galois extension, and

$$\mathrm{Gal}(\mathbb{Q}[\cos(2\pi/n)]/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}/\pm 1.$$

(**Hint.** Argue why $[\mathbb{Q}[\zeta_n] : \mathbb{Q}[\cos(2\pi/n)]] = 2$. Notice that the complex conjugation gives us an element $\tau \in \mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ and $\mathbb{Q}[\cos(2\pi/n)] \subseteq \mathrm{Fix}(\tau)$; deduce that $\mathbb{Q}[\cos(2\pi/n)] = \mathrm{Fix}(\tau)$. Use the concrete isomorphism $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}$ and the main theorem of Galois theory to finish the proof.)

6. Suppose F is a field of characteristic zero and there exists $\zeta \in F$ such that the multiplicative order of ζ is n. Let $\overline{F}$ be an algebraic closure of F. For $a \in F$, let $\sqrt[n]{a} \in \overline{F}$ be a zero of $x^n - a$.

   (a) Prove that
   $$\mathrm{Gal}(F[\sqrt[n]{a}]/F) \simeq \langle a(F^{\times})^n \rangle,$$
   where the right hand side is a cyclic subgroup of $F^{\times}/(F^{\times})^n$.

   (b) Prove that for every $a_1, a_2 \in F^{\times}$, we have $F[\sqrt[n]{a_1}] = F[\sqrt[n]{a_2}]$ if and only if $\langle a_1(F^{\times})^n \rangle = \langle a_2(F^{\times})^n \rangle$.

(**Hint**. For part (a), recall that $\mathrm{Gal}(F[\sqrt[n]{a}]/F)$ is cyclic. Assume it is generated by σ_0. Let $\zeta := \frac{\sigma_0(\sqrt[n]{a})}{\sqrt[n]{a}}$. Notice that

$$\begin{aligned}\sigma_0^d = \mathrm{id} \Leftrightarrow \sigma_0^d(\sqrt[n]{a}) = \sqrt[n]{a} \Leftrightarrow \zeta^d = 1 \\ \Leftrightarrow \sigma_0(\sqrt[n]{a}^d) = \sqrt[n]{a}^d \Leftrightarrow \sqrt[n]{a}^d \in F^\times \\ \Leftrightarrow a^d \in (F^\times)^n.\end{aligned}$$

For part (b), ($\Leftarrow$) is easy. For ($\Rightarrow$), let

$$f_{a_i} : \mathrm{Gal}(F[\sqrt[n]{a_i}]/F) \to \langle\zeta\rangle, \quad f_{a_i}(\sigma) := \frac{\sigma(\sqrt[n]{a_i})}{\sqrt[n]{a_i}}.$$

Notice that f_{a_i}'s are injective group homomorphisms, and the cyclic group $\langle\zeta\rangle$ has a unique subgroup of order $[F[\sqrt[n]{a_i}] : F]$. Hence

$$\mathrm{Im}(f_{a_1}) = \mathrm{Im}(f_{a_2}).$$

Suppose $\mathrm{Gal}(F[\sqrt[n]{a_i}]/F)$ is generated by σ_0; then

$$\langle\frac{\sigma_0(\sqrt[n]{a_1})}{\sqrt[n]{a_1}}\rangle = \mathrm{Im}(f_{a_1}) = \mathrm{Im}(f_{a_2}) = \langle\frac{\sigma_0(\sqrt[n]{a_2})}{\sqrt[n]{a_2}}\rangle.$$

Deduce that there exists an integer i such that

$$\begin{aligned}\left(\frac{\sigma_0(\sqrt[n]{a_1})}{\sqrt[n]{a_1}}\right)^i = \frac{\sigma_0(\sqrt[n]{a_2})}{\sqrt[n]{a_2}} \Rightarrow \sigma_0\left(\frac{\sqrt[n]{a_1}^i}{\sqrt[n]{a_2}}\right) = \frac{\sqrt[n]{a_1}^i}{\sqrt[n]{a_2}} \\ \Rightarrow \frac{\sqrt[n]{a_1}^i}{\sqrt[n]{a_2}} \in F^\times \Rightarrow a_1^i(F^\times)^n = a_2(F^\times)^n.\end{aligned}$$

This means $\langle a_2(F^\times)^n\rangle \subseteq \langle a_1(F^\times)^n\rangle$. By symmetry, claim follows.)

(**Remark**. This result is part of Kummer's theory. Using Hilbert's theorem 90, we get a bijection between the set of cyclic extension of F whose index divides n and cyclic subgroups of $F^\times/(F^\times)^n$.)

7. (Make sure that you know what this problem is and how you can solve it, but you do not need to write and submit your solution) Suppose F is a field of characteristic 0, $\overline{F}$ is an algebraic closure of F, and $F^\times$ has an element ζ_n with multiplicative order n. Let $\mathrm{Int}_{\mathrm{ab},n}(\overline{F}/F)$ be the set of E's in $\mathrm{Int}(\overline{F}/F)$ such that (1) E/F is a finite abelian extension, and (2) for all

$\sigma \in \mathrm{Gal}(E/F)$, we have $\sigma^n = \mathrm{id}$. Let $\mathrm{Sub}_{\mathrm{f}}(F^\times/(F^\times)^n)$ be the set of finite subgroups of $F^\times/(F^\times)^n$. Let

$$\Lambda : \mathrm{Sub}_{\mathrm{f}}(F^\times/(F^\times)^n) \to \mathrm{Int}_{\mathrm{ab},n}(\overline{F}/F), \quad \Lambda(\overline{A}) := F[\sqrt[n]{a} \mid a(F^\times)^n \in \overline{A}],$$

and

$$\Delta : \mathrm{Int}_{\mathrm{ab},n}(\overline{F}/F) \to \mathrm{Sub}_{\mathrm{f}}(F^\times/(F^\times)^n), \quad \Delta(E) := ((E^\times)^n \cap F^\times)/(F^\times)^n.$$

Convince yourself that these are well-defined functions (besides $\Delta(E)$ being finite, you show this as part of this problem), and

$$\Lambda(\Delta(E)) \subseteq E \quad \text{and} \quad \overline{A} \subseteq \Delta(\Lambda(\overline{A})).$$

(a) Suppose $E \in \mathrm{Int}_{\mathrm{ab},n}(\overline{F}/F)$. Prove that there exist positive integers $d_1, \ldots, d_m$ and $a_1, \ldots, a_m \in F^\times$ such that the following holds.

i. $\mathrm{Gal}(E/F) \simeq \prod_{i=1}^m \mathbb{Z}/d_i\mathbb{Z}$ and $d_i | n$. Suppose $\sigma_1, \ldots, \sigma_m \in \mathrm{Gal}(E/F)$ such that $|\langle \sigma_i \rangle| = d_i$ and

$$\mathrm{Gal}(E/F) = \bigoplus_{i=1}^m \langle \sigma_i \rangle.$$

ii. For $1 \le i \le m$, let $F_i := \mathrm{Fix}(\bigoplus_{j \ne i} \langle \sigma_j \rangle)$. Then $\mathrm{Gal}(F_i/F)$ is a cyclic group of order d_i and generated by the restriction of σ_i.

iii. For $1 \le i \le m$, $F_i = F[\sqrt[d_i]{a_i}]$ and $|\langle a_i(F^\times)^n \rangle| = d_i$.

iv. $E = F[\sqrt[d_1]{a_1}, \ldots, \sqrt[d_m]{a_m}]$, and

v. $E = \Lambda(\langle a_1^{n/d_1}(F^\times)^n, \ldots, a_m^{n/d_m}(F^\times)^n \rangle)$; and so Λ is surjective.

(b) For $E \in \mathrm{Int}_{\mathrm{ab},n}(\overline{F}/F)$, let

$$f_E : \mathrm{Gal}(E/F) \times \Delta(E) \to \langle \zeta_n \rangle, \quad f_E(\sigma, a(F^\times)^n) := \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}.$$

Convince yourself that f_E is well-defined. Prove that f_E is a group homomorphism with respect to each component separately. (Sometimes, we say bilinear.)

(c) Use part (a), and prove that if $\sigma \in \mathrm{Gal}(E/F)$ is not identity, then for some $\overline{a}$, we have $f_E(\sigma, \overline{a}) \neq 1$.

(d) Prove that if $\overline{a} \in \Delta(E)$ is not 1, then for some $\sigma \in \mathrm{Gal}(E/F)$, we have $f_E(\sigma, \overline{a}) \neq 1$.

(e) By part (b), deduce that the following are group homomorphisms, and use parts (c) and (d) to show these are injective group homomorphisms:

$$\widehat{f}_G : \mathrm{Gal}(E/F) \to \mathrm{Hom}(\Delta(E), \langle \zeta_n \rangle), \quad (\widehat{f}_G(\sigma))(\overline{a}) = f_E(\sigma, \overline{a})$$

and

$$\widehat{f}_\Delta : \Delta(E) \to \mathrm{Hom}(\mathrm{Gal}(E/F), \langle \zeta_n \rangle), \quad (\widehat{f}_\Delta(\overline{a}))(\sigma) = f_E(\sigma, \overline{a});$$

in particular, $|\Delta(E)| < \infty$.

(f) Prove that if A is a finite abelian group and $na = 0$ for every $a \in A$, then $\mathrm{Hom}(A, \mathbb{Z}/n\mathbb{Z}) \simeq A$. Use this to deduce that

$$\mathrm{Hom}(\mathrm{Gal}(E/F), \langle \zeta_n \rangle) \simeq \mathrm{Gal}(E/F) \quad \text{and} \quad \mathrm{Hom}(\Delta(E), \langle \zeta_n \rangle) \simeq \Delta(E).$$

(g) Use parts (e) and (f) to show $\mathrm{Gal}(E/F) \simeq \Delta(E)$.

(h) Prove that Λ and Δ are inverse of each other.

(**Hint**. For the last part, notice that

$$\Delta(E) \subseteq \Delta(\Lambda(\Delta(E))) \subseteq \Delta(E),$$

and

$$\Lambda(\overline{A}) \subseteq \Lambda(\Delta(\Lambda(\overline{A}))) \subseteq \Lambda(\overline{A}).$$

Because Λ is surjective, by the above equalities deduce that $\Lambda \circ \Delta = \mathrm{id}$. Next, to show $\Delta \circ \Lambda = \mathrm{id}$ use proof by contradiction; this means for some $\overline{A}$, we have $\overline{A} \subsetneq \Delta(\Lambda(\overline{A}))$. Then there exists a non-trivial homomorphism $\chi : \Delta(\Lambda(\overline{A})) \to \langle \zeta_n \rangle$ such that $\overline{A} \subseteq \ker \chi$. Deduce that there exists a non-trivial $\sigma \in \mathrm{Gal}(\Lambda(\overline{A})/F)$ such that $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}$ for every $a \in A$. Argue why this is a contradiction.)

(**Remark**. This is the Abelian case of the Kummer theory. The function f_E is called the Kummer pairing. Roughly, the class field theory gives us similar results in the absence of roots of unity, and Langlands gave a program for finding such a correspondence for non-abelian extensions.)