1. Let E_n be the splitting field of $x^n - 1$ over $\mathbb{Q}$.

(a) Prove that $E_n = \mathbb{Q}[\zeta_n]$ where $\zeta_n = e^{\frac{2\pi i}{n}}$.

(b) Prove that, if $\sigma \in \mathrm{Aut}(E_n)$, then the multiplicative order of $\sigma(\zeta_n)$ is n and conclude that

$$\sigma(\zeta_n) = \zeta_n^i$$

where $\gcd(i, n) = 1$.

(c) Let $G = \{ i \in (\mathbb{Z}/n\mathbb{Z})^\times \mid \exists\, \sigma_i \in \mathrm{Aut}(E_n) : \sigma_i(\zeta_n) = \zeta_n^i \}$.

(Here $(\mathbb{Z}/n\mathbb{Z})^\times$ is the group of units of $\mathbb{Z}/n\mathbb{Z}$.)

Prove that G is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ and

$$\mathrm{Aut}(E_n) \simeq G.$$

(d) Let $\Phi_n(x) := \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^i)$. Prove that

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x).$$

(e) Prove that $\Phi_n(x) \in \mathbb{Z}[x]$. (Hint: By induction and using d.) Conclude that $m_{\zeta, \mathbb{Q}}(x) \in \mathbb{Z}[x]$ if $\mathrm{Ord}(\zeta) = n$.

(f) Prove that $m_{\zeta,\mathbb{Q}}(x) = m_{\zeta^p,\mathbb{Q}}(x)$ if p is a prime and $p \nmid n$ and $\operatorname{ord}(\zeta) = n$.

(Hint. Let $f(x) = m_{\zeta,\mathbb{Q}}(x)$ and $g(x) = m_{\zeta^p,\mathbb{Q}}(x)$. Then $g(x^p) = f(x) \cdot h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Hence $\bar{g}(x)^p = \bar{f}(x) \cdot \bar{h}(x)$ in $\mathbb{F}_p[x]$ which implies that $\bar{f}(x) \cdot \bar{g}(x) \mid x^n - 1$ is NOT square-free. Get a contradiction as $\gcd(nx^{n-1}, x^n - 1) = 1$ in $\mathbb{F}_p[x]$.)

(g) Prove that $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \phi(n)$ (Euler's ϕ-function) and $\operatorname{Aut}(\mathbb{Q}[\zeta_n]) \simeq \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$.

2. Let F be an extension of $\mathbb{Q}[\zeta_n]$. Prove that for any $a \in F^\times$ let $\sqrt[n]{a}$ be a solution of $x^n - a = 0$ (in the algebraic closure of F.)

(a) Prove that $F[\sqrt[n]{a}]/F$ is Galois.

(b) Prove that $\operatorname{Aut}(F[\sqrt[n]{a}]/F) \hookrightarrow \mu_n = \langle \zeta_n \rangle \simeq \mathbb{Z}/n\mathbb{Z}$.

(Hint. $\forall \sigma \in \operatorname{Aut}(F[\sqrt[n]{a}]/F)$ $\exists \zeta_\sigma \in \mu_n$ s.t.

$$\sigma(\sqrt[n]{a}) = \zeta_\sigma \sqrt[n]{a}.$$

Prove that $\sigma \longmapsto \zeta_\sigma$ is a group homomorphism.)

Conclude that $\mathrm{Aut}(F[\sqrt[n]{a}]/F)$ is a cyclic group.

© Prove that

$$F[\sqrt[n]{a}] = F[\sqrt[n]{b}] \iff aF^{\times n} = bF^{\times n}.$$

(Hint: ($\Rightarrow$) if $\langle\sigma\rangle = \mathrm{Aut}(F[\sqrt[n]{a}]/F)$, then

$\mathrm{Ord}(\sigma(\sqrt[n]{a})/\sqrt[n]{a}) = \mathrm{ord}(\sigma)$. This implies

$$\sigma\left(\sqrt[n]{a}/\sqrt[n]{b}^{\,i}\right) = \sqrt[n]{a}/\sqrt[n]{b}^{\,i}$$

for some i.)

3. Let F be a field; assume $\mathrm{char}(F) \neq 2$; $D_i \in F^\times$.

ⓐ Prove that $F[\sqrt{D_1}, \ldots, \sqrt{D_n}]/F$ is Galois.

ⓑ Let $D \in F^\times$. If $\sqrt{D} \in F[\sqrt{D_1}, \ldots, \sqrt{D_n}]$, then

$$DF^{\times 2} \in \langle D_1F^{\times 2}, \ldots, D_nF^{\times 2}\rangle \subseteq F^\times/F^{\times 2}.$$

(Hint. First observe that after dropping some of D_i, if necessary, we can assume

$$|\langle D_1F^{\times 2}, \ldots, D_nF^{\times 2}\rangle| = 2^n.$$

Second use induction hypothesis to show that

$$[F[\sqrt{D_1},\dots,\sqrt{D_n}]:F]=2^n$$

and conclude $Gal(F[\sqrt{D_1},\dots,\sqrt{D_n}]/F)\simeq \underbrace{\mathbb{Z}/2\mathbb{Z}\times\cdots\times\mathbb{Z}/2\mathbb{Z}}_{n \text{ copies}}$

Third. using the fundamental theorem of Galois theory show that any degree 2 extension of F which is a subfield of $F[\sqrt{D_1},\dots,\sqrt{D_n}]$ is of the form

$$F[\sqrt{\prod_{i\in I} D_i}]$$

where I is a non-empty subset of $\{1,\dots,n\}$.

Forth. Finish it using last week's problem:

$$F[\sqrt{D}]=F[\sqrt{\prod_{i\in I} D_i}] \iff DF^{\times 2}=\prod_{i\in I} D_i F^{\times 2}.)$$

(c) Prove that $Gal(F[\sqrt{D_1},\dots,\sqrt{D_n}]/F)\simeq \langle D_1F^{\times 2},\dots,D_nF^{\times 2}\rangle$.

(d) Prove that $F[\sqrt{D_1}+\cdots+\sqrt{D_n}]=F[\sqrt{D_1},\dots,\sqrt{D_n}]$ if $|\langle D_1F^{\times 2},\dots,D_nF^{\times 2}\rangle|=2^n$. In particular,

$F[\sqrt{D_1}+\cdots+\sqrt{D_n}]/F$ is Galois.

4. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p, where p is prime. Assume f has exactly two non-real roots. Let E be the splitting field of $f(x)$ over $\mathbb{Q}$. Prove that

$$\mathrm{Gal}(E/\mathbb{Q}) \simeq S_p.$$

(Hint. Let $\alpha_1, \alpha_2, \dots, \alpha_p$ be the set of roots of f in $\mathbb{C}$. First observe that $\mathrm{Gal}(E/\mathbb{Q}) \hookrightarrow$ group of permutations of $\{\alpha_1, \dots, \alpha_p\} \simeq S_p$.

Second $G \subseteq S_p$ has a cycle of length p:

$$(i_1, i_2, \dots, i_p).$$

Third $\exists\ i \neq j : (i, j) \in G$.

Fourth $\langle (1, 2, \dots, p), (1, j) \rangle = S_p$.)

[You can use the forth step without proof. Here is a way to prove it:

① $\sigma\ (i, j)\ \sigma^{-1} = (\sigma(i), \sigma(j))$

② $(1, k)(1, i)(1, k) = (k, i)$ if $k \neq i$.

③ $(i_1, i_2)(i_2, i_3) \cdots (i_{n-1}, i_n) = (i_1, \ldots, i_n)$ if

$|\{i_1, \ldots, i_n\}| = n$.

①, ②, ③ $\Rightarrow$ $\langle (1,2), (1,3), \ldots, (1,n) \rangle = S_n$.

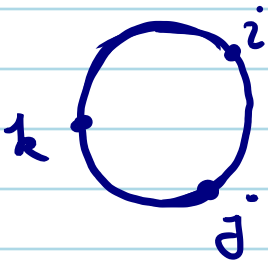
④ Let $G = \langle (1,2,\ldots,n), (i_0, j_0) \rangle$. Then

$(i,j) \in G$ if $|i-j| = |i_0 - j_0|$

(Let's say m is G-admissible if $m \equiv i-j \pmod n$ and $(i,j) \in G$.)

⑤ Considering $(i,j)(j,k)(i,j) = (i,k)$ when $|\{i,j,k\}| = 3$

Show that the set of G-admissible elements of $\mathbb{Z}/n\mathbb{Z}$ is a group. So if $n = p$ is prime, any element of $\mathbb{Z}/p\mathbb{Z}$ is G-admissible. And conclude $G = S_p$.]



5. Let E be the splitting field of

ⓐ $m_{\alpha, \mathbb{Q}}(x)$ over $\mathbb{Q}$ where $\alpha = \sqrt{2+\sqrt{2}}$

ⓑ $x^p - 2$ over $\mathbb{Q}$ where p is an odd prime

Find $[E : \mathbb{Q}]$ and discribe $\mathrm{Gal}(E/\mathbb{Q})$ in each case.