1 Let $\alpha = \sqrt{2+\sqrt{2}}$.

(a) Compute the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

(b) Prove that $\mathbb{Q}(\alpha) \supseteq \mathbb{Q}$ is a Galois extension.

(c) Prove that the Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ is a cyclic group.

(d) Use the Fundamental Theorem of Galois Theory to draw the lattice of intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\alpha)$.

2 On HW 9, you proved that the splitting field for $x^4 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\zeta)$, where $\zeta^4 = -1$. You also showed that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$.

(a) Prove that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is isomorphic to the Klein 4-group.

(b) Use the Fundamental Theorem of Galois Theory to draw the lattice of intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\zeta)$.

3 Recall that, if p is a prime number, the pth **cyclotomic polynomial** is

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + x^2 + \cdots + x^{p-1}.$$

We now define a cyclotomic polynomial $\Phi_n(x) \in \mathbb{Q}[x]$ for every positive integer n. Set $\Phi_1(x) = x - 1$. If $n > 1$, then we inductively define $\Phi_n(x)$ so that

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

where the product is over all divisors d of n. That is, we are assuming (by induction) that the cyclotomic polynomials $\Phi_d(x)$ for all *proper* divisors $d < n$ have already been defined, and so the only unknown in the above equation is $\Phi_n(x)$.

(a) Check that this inductive definition is consistent with the original definition of $\Phi_p(x)$ for p prime.

(b) Use this definition to compute $\Phi_8(x)$, $\Phi_{10}(x)$, and $\Phi_{12}(x)$.

(c) Show that

$$n = \sum_{d|n} \phi(d),$$

where ϕ denotes the Euler totient function. [HINT: Count the number of integers $k \in \{1, \ldots, n\}$ such that $\gcd(k, n) = \frac{n}{d}$.]

(d) Prove that $\Phi_n(x)$ has degree $\phi(n)$.

4 Let $\Phi_n(x) \in \mathbb{Q}[x]$ be the nth cyclotomic polynomial, as defined in the previous problem.
Recall that ζ is an n**th root of unity** if $\zeta^n = 1$, and ζ is a **primitive** n**th root of unity** if additionally $\zeta^i \neq 1$ for $1 \leq i < n$.

(a) Show that ζ is an nth root of unity if and only if ζ is a root of $x^n - 1$, and ζ is a primitive nth root of unity if and only if ζ is a root of $\Phi_n(x)$.

(b) Show that, for any odd positive integer n, $\Phi_{2n}(x) = \Phi_n(-x)$. [HINT: If ζ is a primitive nth root of 1, show that $-\zeta$ is also a root of unity. What is its order?]

(c) Let ζ be a primitive nth root of unity. Prove that $\mathbb{Q}(\zeta)$ is the splitting field of $x^n - 1$. (The field $\mathbb{Q}(\zeta)$ is called the n**th cyclotomic field**.)

5 Let n be a positive integer, and let $U_n = (\mathbb{Z}/n\mathbb{Z})^\times$ be the group of units in the ring $\mathbb{Z}/n\mathbb{Z}$. That is,

$$U_n = \{\overline{k} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(k, n) = 1\}.$$

(You considered this group on HW 11 in MA 361.)

Let ζ be a primitive nth root of unity.

(a) Use the fact that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ (a result due to Gauss and Dedekind) to show that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is a group of order $\phi(n)$.

(b) Prove that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong U_n$.

[HINT: Any automorphism of $\mathbb{Q}(\zeta)$ is determined by where it maps ζ. Show that there is an automorphism $\sigma_k \colon \zeta \mapsto \zeta^k$ if and only if $\gcd(k, n) = 1$.]