49) [D-F] 14.4 #1 (10 points). Determine the Galois closure of \( \mathbb{Q}(\sqrt{1+\sqrt{2}}) \) over \( \mathbb{Q} \).

Let \( F/\mathbb{Q} \) be any finite extension. By the primitive element theorem \( F = \mathbb{Q}(\alpha) \) for some \( \alpha \in F \subset \mathbb{C} \). Let \( f(X) \in \mathbb{Q}[X] \) be the irreducible polynomial of \( \alpha \) over \( \mathbb{Q} \). Let \( L \subset \mathbb{C} \) be the splitting field of \( f(X) \) over \( \mathbb{Q} \). Clearly \( F \subset L \) is Galois. Moreover if \( K/\mathbb{Q} \) is any Galois extension with \( F \subset K \subset \mathbb{C} \), then \( L \subset K \) (because any irreducible polynomial over a field \( k \) which has a root in a Galois extension of \( k \) is separable and splits completely in the Galois extension). Thus the Galois closure of \( F \) is the splitting field of \( f(X) \). In the present problem \( \alpha = \sqrt{1+\sqrt{2}} \) and \( f(X) = X^4 - 2X^2 - 1 \), thus the Galois closure of \( \mathbb{Q}(\alpha) \) is \( \mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}}) \).

50) [D-F] 14.4 #2 (10 points). Find a primitive generator for \( F = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \).

Consider \( \alpha = a\sqrt{2} + b\sqrt{3} + c\sqrt{5} \in F \) with \( a, b, c \in \mathbb{Q} \setminus \{0\} \). We recall from Problem 40) of HW 9 that \( F/\mathbb{Q} \) is Galois with the eight automorphisms of \( F/\mathbb{Q} \) being \( (\sqrt{2}, \sqrt{3}, \sqrt{5}) \mapsto (\pm\sqrt{2}, \pm\sqrt{3}, \pm\sqrt{5}) \). Thus \( \alpha \) has eight Galois conjugates. We also recall that in a Galois extension \( K/k \), the number of Galois conjugates of any \( \alpha \in K \) is \( [\text{Gal}(K/k) : \text{Gal}(K/k(\alpha))] = [k(\alpha) : k] \). In the present problem this shows that \( \mathbb{Q}(\alpha)/\mathbb{Q} \) is a degree eight extension and hence \( \mathbb{Q}(\alpha) = F \). In other words \( \alpha \) is a primitive generator. Any other \( \alpha \) which has eight Galois conjugates will also work.

51 [D-F], 14.7 #3 (5 points). State and prove a necessary and sufficient condition on \( \alpha, \beta \in F \) so that \( F(\sqrt{\alpha}) = F(\sqrt{\beta}) \) assuming \( \text{char}(F) \neq 2 \). Use this to determine if \( \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\sqrt{1+\sqrt{2}}) \).

\( F(\sqrt{\alpha}) = F(\sqrt{\beta}) \iff [F(\sqrt{\alpha}, \sqrt{\beta}) : F] = 2 \iff \alpha\beta \text{ is a square in } F \) (by problem 27 of HW7). Letting \( F = \mathbb{Q}(\sqrt{2}) \), \( \alpha = -1 \) and \( \beta = 1 - \sqrt{2} \), we see that \( \alpha\beta = -1 + \sqrt{2} \) is not a square in \( F \) (because squares in \( F \) are of the form \( a^2 + 2b^2 + 2ab\sqrt{2} \) where \( a, b \in \mathbb{Q} \)) and hence \( \mathbb{Q}(i, \sqrt{2}) \neq \mathbb{Q}(\sqrt{1+\sqrt{2}}) \).

51 [D-F], 14.7 #12 (5 points). Let \( L \) be the Galois closure of the finite extension \( \mathbb{Q}(\alpha)/\mathbb{Q} \). For any prime \( p \) dividing the order of \( \text{Gal}(L/\mathbb{Q}) \) prove that there is a subfield \( F \subset L \) with \( [L : F] = p \).
and \( L = F(\alpha) \).

Since \( p \) divides \( |G| \) where \( G = \text{Gal}(L/\mathbb{Q}) \), there exist subgroups \( H < G \) of order \( p \), and hence fields \( \mathbb{Q} \subset F \subset L \) with \( [L : F] = p \). We will show that \( F \) can be chosen such that \( \alpha \notin F \), so that \( F(\alpha) \) will necessarily equal \( L \). We give two proofs for why \( F \) can be chosen such that \( \alpha \notin F \).

a) If \( \alpha \in F \) for all \( F/\mathbb{Q} \) with \( [L : F] = p \), we see that \( E := \cap_{\sigma \in G} \sigma F \) contains \( \mathbb{Q}(\alpha) \). We observe that \( \sigma E = E \) for all \( \sigma \in G \). We recall that every \( \tau \in \text{Aut}(\mathbb{Q}/\mathbb{Q}) \) is an extension of a \( \sigma \in G \). Thus \( \tau E = E \) for all \( \tau \in \text{Aut}(\mathbb{Q}/\mathbb{Q}) \), and thus \( E/\mathbb{Q} \) satisfies the definition of a finite normal extension. It is automatically separable since \( \text{char}(\mathbb{Q}) = 0 \). Thus \( E/\mathbb{Q} \) is Galois and contains \( \mathbb{Q}(\alpha) \), therefore \( L = E \), but this contradicts \( [L : E] \geq [L : F] = p \).

b) If \( f(X) \in \mathbb{Q}[X] \) is the irreducible polynomial for \( \alpha \) over \( \mathbb{Q} \), then as observed in the solution to Problem 49) above, \( L/\mathbb{Q} \) is the splitting field of \( f(X) \). We recall that \( G \) acts transitively on the \( d = [\mathbb{Q}(\alpha) : \mathbb{Q}] \) roots \( \{\alpha_1, \ldots, \alpha_d\} \) of \( f(X) \) in \( L \). Now, there exists an \( \alpha_i \notin F \), because otherwise \( F = L \) contradicting \( [L : F] = p \). We pick a \( g \in G \) such that \( g(\alpha_i) = \alpha \), and observe that \( F' := g(F) \) satisfies \( \alpha \notin F' \) and \( [L : F'] = p \).

53 [D-F], 14.8 #4 (10 points). We verify directly that the given quintic \( f(X) \) has \( \alpha \) as a root where \( \alpha = \xi + \xi^{-1}, \xi = \xi_{11} \). Since \( \alpha \) clearly has five Galois conjugates in the cyclotomic field \( \mathbb{Q}(\xi) \), we see that the minimal polynomial for \( \alpha \) over \( \mathbb{Q} \) is a quintic and hence must be \( f(X) \). Since \( \mathbb{Q}(\xi)/\mathbb{Q} \) is an abelian extension, we know that \( \mathbb{Q}(\alpha)/\mathbb{Q} \) is a Galois extension of degree five, and hence \( f(X) \) splits completely in \( \mathbb{Q}(\alpha) \). Thus \( \mathbb{Q}(\alpha)/\mathbb{Q} \) is the splitting field of \( f(X) \) and \( \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \mathbb{Z}/5\mathbb{Z} \).