Math 111C HW7

Zih-Yu Hsieh

May 27, 2025

1

Question 1 *Let $F \subseteq K \subseteq L$ be field extensions. Prove or disprove the following statements:*

(i) If L/F is Galois, then so is K/F.

(ii) If L/K and K/F are both Galois, then so is L/F.

Pf:

(i) To disprove the first statement, here is a counterexample:

Consider the three fields, $\mathbb{Q} \subseteq \mathbb{Q}(2^{1/3}) \subseteq \mathbb{Q}(2^{1/3},\ \zeta_3)$, where $\zeta_3 = e^{2\pi i/3}$ (a 3^{rd} primitive root of unity).

First, since $\text{char}(\mathbb{Q}) = 0$, $\mathbb{Q}$ is a perfect field, hence any finite extension of $\mathbb{Q}$ is separable. Then, since $\mathbb{Q}(2^{1/3},\ \zeta_3)/\mathbb{Q}$ is a finite extension, it is separable.

Then, if we consider $2^{1/3} \in \mathbb{Q}(2^{1/3},\ \zeta_3)$, since it is a root of $x^3 - 2 \in \mathbb{Q}[x]$ (proven above), while this polynomial satisfies the Eisenstein Criterion for prime $p = 2$, hence $x^3 - 2$ is irreducible over $\mathbb{Q}$. So, because it is both monic and irreducible over $\mathbb{Q}$ while $2^{1/3}$ is a root, then it must be the minimal polynomial of $2^{1/3}$. Now, recall that in **HW 3 Question 4**, we've proven that for any $n \in \mathbb{N}$, $\mathbb{Q}(2^{1/n},\ \zeta_n)$ is a splitting field of $x^n - 2$ (where ζ_n is a primitive n^{th} root of unity), hence $\mathbb{Q}(2^{1/3}, \zeta_3)$ is a splitting field of $x^3 - 2$. Which, since being a normal extension of $\mathbb{Q}$ is equivalent to be a splitting field of some subset of $\mathbb{Q}[x]$, then $\mathbb{Q}(2^{1/3},\ \zeta_3)/\mathbb{Q}$ (as a splitting field of $x^3 - 2$) is a normal extension.

Together with both information above, $\mathbb{Q}(2^{1/3},\ \zeta_3)/\mathbb{Q}$ is both Normal and Separable, hence it is a Galois Extension. Yet, if consider $\mathbb{Q}(2^{1/3})/\mathbb{Q}$, since $2^{1/3} \in \mathbb{Q}(2^{1/3})$ has minimal polynomial $x^3 - 2$ (proven above), while it is clear that $\mathbb{Q}(2^{1/3}) \subsetneq \mathbb{Q}(2^{1/3}, \zeta_3)$, where the larger field here is a splitting field of $x^3 - 2$ contained in $\mathbb{C}$ (since the larger field contains $\zeta_3 \notin \mathbb{R}$, while $\mathbb{Q}(2^{1/3}) \subset \mathbb{R}$). So, as a proper subfield, $\mathbb{Q}(2^{1/3})$ is not a splitting field of $x^3 - 2$. Because it is the minimal polynomial of $2^{1/3} \in \mathbb{Q}(2^{1/3})$, then there is an element with its minimal polynomial not splitting over $\mathbb{Q}(2^{1/3})$, showing that $\mathbb{Q}(2^{1/3})$ is not normal, hence not Galois.

So, given $\mathbb{Q} \subseteq \mathbb{Q}(2^{1/3}) \subseteq \mathbb{Q}(2^{1/3},\ \zeta_3)$, even though $\mathbb{Q}(2^{1/3},\ \zeta_3)/\mathbb{Q}$ is Galois, but $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is not Galois, showing that given $F \subseteq K \subseteq L$, L/F being Galios doesn't imply K/F is Galois.

(ii) For the second statement, consider the counterexample provided by **Question 4** in this HW:

Given the field extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$, which the adjoining element $\sqrt{1+\sqrt{2}}$ satisfies:

$$\left(\sqrt{1+\sqrt{2}}\right)^2 = 1 + \sqrt{2}, \quad \sqrt{2} = \left(\sqrt{1+\sqrt{2}}\right)^2 - 1 \in \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)$$

Hence, this implies that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$.

The first claim is that $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$ is not Galois: From what we've proven in **Question 4** (can check the proof), the minimal polynomial of $\sqrt{1+\sqrt{2}}$ over $\mathbb{Q}$ is x^4-2x^2-1, which has roots $\pm\sqrt{1+\sqrt{2}},\ \pm\sqrt{1-\sqrt{2}} \in \mathbb{C}$. So, if we fix $\mathbb{C}$ as the large algebraically closed field, then the unique splitting field of x^4-2x^2-1 is given by $\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}}) \subset \mathbb{C}$ (Note: $\sqrt{1-\sqrt{2}} \notin \mathbb{R}$). Yet, because $\mathbb{Q}(\sqrt{1+\sqrt{2}}) \subset \mathbb{R}$, then $\mathbb{Q}(\sqrt{1+\sqrt{2}}) \subsetneq \mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}})$, which is not a splitting field of x^4-2x^2-1. Since $\sqrt{1+\sqrt{2}}$ has its minimal polynomial not splitting completely over $\mathbb{Q}(\sqrt{1+\sqrt{2}})$, then $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$ is not normal, hence not Galois.

The second claim is that both $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}(\sqrt{2})$ are degree 2 extensions: Since $\sqrt{2}$ satisfies $(\sqrt{2})^2-2=0$, then it is a root of $x^2-2 \in \mathbb{Q}[x]$; and since this polynomial satisfies the Eisenstein Criterion for prime $p=2$, then it is irreducible. Hence, because x^2-2 is both monic and irreducible, it is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$, which implies the following:

$$\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2-2), \quad [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$$

On the other hand, since x^4-2x^2-1 is said to be the minimal polynomial of $\sqrt{1+\sqrt{2}}$ over $\mathbb{Q}$, then we get the following:

$$\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right) \cong \mathbb{Q}[x]/(x^4-2x^2-1), \quad \left[\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right):\mathbb{Q}\right] = 4$$

Which, by the relations of field extension, we get:

$$4 = \left[\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right):\mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right):\mathbb{Q}(\sqrt{2})\right]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2\left[\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right):\mathbb{Q}(\sqrt{2})\right]$$

$$\implies \left[\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right):\mathbb{Q}(\sqrt{2})\right] = 2$$

So, this shows that both $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}(\sqrt{2})$ are degree 2 extensions.

The final claim is that over a perfect field F, a degree 2 extension is Galois: Since F is perfect, any degree 2 extension (which is finite) is separable. Also, if K/F is the given degree 2 extension, choose any $\alpha \in K \setminus F$, then the list $1, \alpha, \alpha^2$ has 3 elements, which is linearly dependent (since K is a 2-dimensional F-vector space). Hence, WLOG, there exists $b, c \in F$, such that $\alpha^2 + b\alpha + c = 0$. Then, $m_{\alpha,F}(x) \mid x^2+bx+c \in F[x]$, showing that $\deg(m_{\alpha,F}) \leq 2$; on the other hand, since $\alpha \notin F$, then $\deg(m_{\alpha,F}) > 1$, which enforces $\deg(m_{\alpha,F}) = 2$. Because x^2+bx+c is chosen to be monic, we must have $m_{\alpha,F}(x) = x^2+bx+c$ (since their degree matches up, being one others' factor, and are both monic). As a consequence, $F(\alpha) \cong F[x]/(x^2+bx+c)$, which $[F(\alpha):F] = 2$. Furthermore, since $F(\alpha) \subseteq K$, while $[K:F] = 2$, then $F(\alpha)$ as a linear subspace of K has the same dimension with K, showing that $F(\alpha) = K$. Finally, since $\alpha \in K = F(\alpha)$ has its minimal polynomial being degree 2, while α is a root of $m_{\alpha,F}(x)$, which implies that $m_{\alpha,F}(x)$ splits completely over K; now, suppose $K' \subseteq K$ is the splitting field of $m_{\alpha,F}(x)$, then K' must contain all roots of it, showing that $\alpha \in K'$, or $K = F(\alpha) \subseteq K'$, hence we can deduce that $K = K'$, or K is the splitting field of $m_{\alpha,F}(x)$. Since K is a splitting field of some subset of $F[x]$, then it is normal. So, K/F as a degree 2 extension is both separable and normal, which is Galois.

To conclude for the counterexample, since $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$, and $\mathbb{Q}$ is perfect, which implies that its algebraic extension $\mathbb{Q}(\sqrt{2})$ is also perfect (proven in **HW 5 Question 4**), hence $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}(\sqrt{2})$ (which are both degree 2 extensions over a perfect field) by our claims above, are both Galois. However, our first claim shows that $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$ is not Galois. Hence, given $F \subseteq K \subseteq L$, even if K/F and L/K are Galois, it doesn't guarantee that L/F is Galois.

2

Question 2 *Let K/F be a finite extensions. Prove that:*

(a) K/F is normal if and only if K is a splitting field of some polynomial $p(x) \in F[x]$ over F.

(b) K/F is Galois if and only if K is a splitting field of some separable poynomial $p(x) \in F[x]$ over F.

Pf:

Before starting the proof, since K/F is a finite extension, there exists distinct $\alpha_1, ..., \alpha_n \in K$, such that $K = F(\alpha_1, ..., \alpha_n)$. Where, each index $i \in \{1, ..., n\}$ has α_i being algebraic over F, so $m_{\alpha_i,F}(x)$ exists.

(a)$\Longrightarrow$: Suppose K/F is normal, then for every index $i \in \{1, ..., n\}$, the minimal polynomial of α_i, $m_{\alpha_i,F}(x) \in F[x]$ splits completely over K. Which, if define $p(x) \in F[x]$ as follow:

$$p(x) = \prod_{i=1}^{n} m_{\alpha_i,F}(x)$$

then since each polynomial component in the above product splits completely over K, then $p(x)$ also splits completely over K.

Now, it suffices to show that K is a splitting field of $p(x) \in F[x]$: Suppose $F \subseteq K' \subseteq K$, where K' is the splitting field of $p(x)$ contained in K. Then, it implies that K' must necessarily contain all the roots of $p(x)$ in K. Because for each index $i \in \{1, ..., n\}$, the definition of $p(x)$ above shows that $m_{\alpha_i,F}(x) \mid p(x)$, then since $m_{\alpha_i,F}(\alpha_i) = 0$, we must have $p(\alpha_i) = 0$. So, each α_i is a root of $p(x)$. Hence, with K' containing all the roots of $p(x)$ in K, each $\alpha_i \in K'$, showing that $K = F(\alpha_1, ..., \alpha_n) \subseteq K'$. Hence, $K = K'$, or K is a splitting field of $p(x) \in F[x]$.

$\Longleftarrow$: Recall that K/F is normal iff K is a splitting field of some collections of polynomials $A \subseteq F[x]$.

Now, suppose that K/F is a splitting field of $p(x) \in F[x]$, then let $A = \{p(x)\}$, apply the statement from above, we get that K/F is indeed Normal.

(b)$\Longrightarrow$: Suppose K/F is Galois, then it is both a normal and separable extension. As a consequence, for each index $i \in \{1, ..., n\}$, not only $m_{\alpha_i,F}(x) \in F[x] \subseteq K[x]$ splits completely over K, and it necessarily has simple roots.

Now, let $A = \{m_{\alpha_i,F}(x) \mid 1 \leq i \leq n\} \subset F[x]$ (the collection of all α_i's minimal polynomial, which if two α_i, α_j share the same minimal polynomial, it counts only once in A). Which, given any $f(x), g(x) \in A$, since they're both minimal polynomials of some α_i, α_j respectively, then they're both monic and irreducible; which, suppose $f(x), g(x)$ share some roots $\beta \in K$, then being monic and irreducible polynomial, it enforces $f(x), g(x)$ to both be the minimal polynomial of β, or $f(x) = g(x)$. Take the contrapositive, if $f(x) \neq g(x)$, then they share no roots.

Which, let $p(x) \in F[x]$ be defined as follow:

$$p(x) = \prod_{f(x) \in A} f(x)$$

Which, $p(x)$ is the product of distinct polynomials in A.

First, notice that each $f(x) \in A$ splits completely over K (since it is a minimal polynomial of some α_i), then $p(x)$ as the product of them must split completely.

Then, since each $f(x) \in A$ only has simple roots (again since it is a minimal polynomial of some α_i), while for any other $g(x) \in A$ with $g(x) \neq f(x)$, they share no roots, then as product of distinct polynomials in A, $p(x)$ must also have simple roots (suppose β is a root of $p(x)$, it must be a root for some $f(x) \in A$; but then, for any other $g(x) \in A$, since $f(x) \neq g(x)$ implies they share no roots, then $g(\beta) \neq 0$, so β must necessarily have multiplicity 1, since it is a root for only $f(x)$, and $f(x)$ only has simple roots).

The above proves that $p(x) \in F[x]$ is a separable polynomial, while $p(x) \in K[x]$ splits completely, hence it suffices to show that K is indeed a splitting field of $p(x)$: Following from similar methods used in **part (a)**, if $F \subseteq K' \subseteq K$, where K' is the splitting field of $p(x)$ contained in K, then it must contain all roots of $p(x)$; on the other hand, for all $i \in \{1, ..., n\}$, since $m_{\alpha_i,F}(x) \in A$, then $m_{\alpha_i,F}(x) \mid p(x)$, showing that $p(\alpha_i) = 0$. So, α_i is a root of $p(x)$, or $\alpha_i \in K'$. Hence, $K = F(\alpha_1, ..., \alpha_n) \subseteq K'$, showing that $K = K'$.

Therefore, we can conclude that K is a splitting field of $p(x) \in F[x]$, where $p(x)$ is separable.

$\Longleftarrow$: Recall that K/F is Galois iff K is a splitting field of some collections of separable polynomials $A \subseteq F[x]$.

Now, suppose that K/F is a splitting field of $p(x) \in F[x]$ (where $p(x)$ is separable), then let $A = \{p(x)\}$, apply the statement from above, we get that K/F is indeed Galois.

3

Question 3 *Let K/F be "separable" and $K = F(\alpha_1, ..., \alpha_n)$. For a fixed algebraic closure $\overline{F}$ such that $F \subseteq K \subseteq \overline{F}$, suppose that $\phi_1, \phi_2, ..., \phi_m$ are all the F-embeddings from K to $\overline{F}$. Prove that $F(S)$ is a Galois Closure of K/F where $S = \{\phi_i(\alpha_j) \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$.*

Pf:

Let $A = \{m_{\alpha_j,F}(x) \mid 1 \leq j \leq n\} \subset F[x]$.

1. S **contains all roots of all polynomials in** A**:**

First, it is clear that all element in S is a root of some polynomials in A, since any $s \in S$ satisfies $s = \phi_i(\alpha_j)$ for some $1 \leq i \leq m$ and $1 \leq j \leq n$. Which, because $m_{\alpha_j,F}(x) \in F[x]$, all of its coefficients are fixed by ϕ_i (which is an F-embedding), hence $0 = \phi_i(0) = \phi_i(m_{\alpha_j,F}(\alpha_j)) = m_{\alpha_j,F}(\phi_i(\alpha_j))$, showing that $s = \phi_i(\alpha_j)$ is also a root of $m_{\alpha_j,F}(x) \in A$.

Then, for any $m_{\alpha_j,F}(x) \in A$, let $s \in \overline{F}$ be one of its roots, since $m_{\alpha_j,F}(x)$ is assumed to be monic and irreducible over F, then having s being a root, implies that it is also the minimal polynomial of s. Hence, $F(\alpha_j) \cong F[x]/(m_{\alpha_j,F}(x)) \cong F(s)$ via an explicit isomorphism given as follow:

$$\varphi : F(\alpha_j) \tilde{\to} F(s), \quad \forall a_0, a_1, ..., a_n \in F,\ \varphi(a_0 + a_1\alpha_j + ... + a_n\alpha_j^n) = a_0 + a_1 s + ... + a_n s^n$$

Notice that φ fixes all the elements of F, and also $F(s) \subseteq \overline{F}$, so composing with the inclusion map, the new map $\varphi : F(\alpha_j) \to \overline{F}$ is in fact an F-embedding. Since K/F is algebraic, while $F \subseteq F(\alpha_j) \subseteq K$, then this guarantees that $K/F(\alpha_j)$ is algebraic; on the other hand, since $F(\alpha_j) \subseteq K \subseteq \overline{F}$, this ensures that $\overline{F}$ is also an algebraic closure of $F(\alpha_j)$ (since $\overline{F}/F$ is algebraic, so $\overline{F}/F(\alpha_j)$ is also algebraic; then since $\overline{F}$ is algebraically closed, it is an algebraic closure of $F(\alpha_j)$). Hence, as $K/F(\alpha_j)$ is an algebraic extension, the above embedding $\varphi : F(\alpha_j) \to \overline{F}$ can be extended to $\overline{\varphi} : K \to \overline{F}$, with $\overline{\varphi} \mid_{F(\alpha_j)} = \varphi$. Because φ is already an F-embedding, $\overline{\varphi}$ is also an F-embedding. Hence, $\overline{\varphi} = \phi_i$ for some $1 \leq i \leq n$. So, we get that $\phi_i(\alpha_j) = \overline{\varphi}(\alpha_j) = \varphi(\alpha_j) = s$, which shows that $s \in S$.

The above implications show that S must contain (and only contains) all roots of all polynomials in A.

2. $F(S)/F$ **is Galois:**

First, since $K = F(\alpha_1, ..., \alpha_n)$ is assumed to be a separable extension of F, then $\alpha_1, ..., \alpha_n$ must have their minimal polynomials being separable, hence A as a collection of all α_j's minimal polynomial, is a subset of $F[x]$ containing only separable polynomials.

Then, because $S \subset F(S)$ contains all the roots of all polynomials in A, every $f(x) \in A$ splits completely over $F(S)$. Now, suppose $K' \subseteq F(S)$ is the splitting field of the subset A, then K' must contain all roots of all polynomials in A; because S only contains the roots of polynomials in A, this implies that $S \subset K'$, which further implies $F(S) \subseteq K'$, or $F(S) = K'$. Hence, $F(S)$ is a splitting field of A.

Finally, because $F(S)$ is a splitting field of A (which is a collection of separable polynomials), then $F(S)/F$ is a Galois Extension.

3. $F(S)$ **is a Galois Closure of** K**:**

Suppose $K' \subseteq F(S)$ is the Galois Closure of K/F, then since $K = F(\alpha_1, ..., \alpha_n)$, for each index $j \in \{1, ..., n\}$, we must have $m_{\alpha_j,F}(x)$ split completely over K'. Hence, because A collects all $m_{\alpha_j,F}(x)$ (and only contains these polynomials), every polynomial in A splits completely over K'. However, in the previous section, when proving that $F(S)/F$ is a Galois Extension, we've shown that $F(S)$ is a splitting field of A, then since every polynomial in A splits completely over $K' \subseteq F(S)$, this implies that $K' = F(S)$ by the definition of splitting field. Hence, $F(S)$ is a Galois Closure of K/F.

4

Question 4 *Find the Galois Closure of* $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ *over* $\mathbb{Q}$.

Pf:

First, since Galois Closure is a normal extension, every element must have its minimal polynomial over $\mathbb{Q}$ splits completely. Then, $\sqrt{1+\sqrt{2}}$ must also have its minimal polynomial splits completely. Hence, the first goal is to find the minimal polynomial of $\alpha = \sqrt{1+\sqrt{2}}$ over $\mathbb{Q}$. Notice that it satisfies the following:

$$\alpha = \sqrt{1+\sqrt{2}} \implies \alpha^2 = 1+\sqrt{2} \implies \alpha^2 - 1 = \sqrt{2} \implies (\alpha^4 - 2\alpha^2 + 1) = 2 \implies \alpha^4 - 2\alpha^2 - 1 = 0$$

This shows that α is a root of $x^4 - 2x^2 - 1 \in \mathbb{Q}[x]$. Then, to prove that it is irreducible, consider the ring automorphism on $\mathbb{Q}[x]$ by $x \mapsto (x+1)$. Which, we get:

$$x^4 - 2x^2 - 1 \mapsto (x+1)^4 - 2(x+1)^2 - 1$$

$$(x+1)^4 - 2(x+1)^2 - 1 = (x^4 + 4x^3 + 6x^2 + 4x + 1) - 2(x^2 + 2x + 1) - 1 = x^4 + 4x^3 + 4x^2 - 2$$

Notice that after the shift, $(x+1)^4 - 2(x+1)^2 - 1 = x^4 + 4x^3 + 4x^2 - 2$ satisfies the Eisenstien's Criterion for prime $p = 2$, which is irreducible over $\mathbb{Q}$. This implies that $x^4 - 2x^2 - 1$ is also irreducible over $\mathbb{Q}$.

Because $x^4 - 2x^2 - 1 \in \mathbb{Q}[x]$ is monic and irreducible, while $\alpha = \sqrt{1+\sqrt{2}}$ is a root, hence $x^4 - 2x^2 - 1$ is necessarily the minimal polynomial of $\sqrt{1+\sqrt{2}}$ over $\mathbb{Q}$.

Then, since the minimal polynomial of $\sqrt{1+\sqrt{2}}$ over $\mathbb{Q}$ (namely $x^4 - 2x^2 - 1$), should split completely in a Galois Closure, then it must contain a splitting field of $x^4 - 2x^2 - 1$. So, the second goal is to find the roots of $x^4 - 2x^2 - 1$ over $\mathbb{C}$. Let $y = x^2$, then $x^4 - 2x^2 - 1 = y^2 - 2y - 1$. Which, by Quadratic Formula, we get:

$$y = \frac{-(-2) \pm \sqrt{(-2)^2 - 4 \cdot 1 \cdot (-1)}}{2} = \frac{2 \pm \sqrt{8}}{2} = 1 \pm \sqrt{2}$$

Hence, solving for $y = x^2 = 1 \pm \sqrt{2}$ would provide the roots for the polynomial. Which for this equation, $x = \pm\sqrt{1+\sqrt{2}},\ \pm\sqrt{1-\sqrt{2}} \in \mathbb{C}$. Hence, these four distinct roots all satisfy $x^4 - 2x^2 - 1 = 0$, while the polynomial can have at most 4 distinct roots, so these must be all the roots of $x^4 - 2x^2 - 1$.

As a consequence, we get $\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}}) \subset \mathbb{C}$ is the splitting field of $x^4 - 2x^2 - 1$ under $\mathbb{C}$.

Finally, we can show that $\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}})$ is a Galois Closure of $\mathbb{Q}(\sqrt{1+\sqrt{2}})$:

Since $\mathrm{char}(\mathbb{Q}) = 0$, then it is a perfect field, hence $\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}})/\mathbb{Q}$ as a finite extension must be separable. On the other hand, since $\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}})$ is also a splitting field of $x^4 - 2x^2 - 1 \in \mathbb{Q}[x]$, then this enforces $\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}})$ to also be a normal extension. Therefore, $\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}})/\mathbb{Q}$ is a Galois Extension.

Now, suppose $\mathbb{Q}(\sqrt{1+\sqrt{2}}) \subseteq K \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}})$, where K is the Galois Closure of $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ under $\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}})$. Then, since $\sqrt{1+\sqrt{2}} \subseteq K$, its minimal polynomial $x^4 - 2x^2 - 1 \in \mathbb{Q}[x]$ must split completely over K. So, K must contain all the roots of $x^4 - 2x^2 - 1$ in $\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}})$, which is given by $\pm\sqrt{1+\sqrt{2}}$ and $\pm\sqrt{1-\sqrt{2}}$. Hence, this implies that $\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}}) \subseteq K$, or $K = \mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}})$.

Therefore, $\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}})$ is indeed a Galois Closure of $\mathbb{Q}(\sqrt{1+\sqrt{2}})$.

5

Question 5 *Prove that, if K_1/F and K_2/F are Galois, so is $(K_1 \cap K_2)/F$.*

Pf:

First, since by assumption K_2/F is Galois implies it is algebraic, then any $\alpha \in K_2$ is algebraic over F, which is also algebraic over K_1. As a consequence, consider the field $K_1K_2 = K_1(K_2)$: Since each element in K_2 is algebraic over K_1, then $K_1(K_2)/K_1$ is algebraic; together with K_1/F being algebraic (since it is a Galois Extension), then $K_1(K_2)/F$ is also algebraic. So, we can fix an algebraic closure $\overline{F}$ such that $F \subseteq K_1(K_2) \subseteq \overline{F}$, which as sets, the three fields $K_1, K_2, (K_1 \cap K_2) \subseteq \overline{F}$.

Then, since K_1/F and K_2/F are both Galois, then they're separable extensions; hence, every element $\alpha \in (K_1 \cap K_2) \subseteq K_1$ is separable over F, showing that $(K_1 \cap K_2)/F$ is a separable extension.

Now, since K_1/F and K_2/F are both normal (since they're Galois), then any of their element has the minimal polynomial splits completely over the given field itself. Which, for all $\alpha \in (K_1 \cap K_2)$, since $m_{\alpha,F}(x)$ splits completely over K_1 and K_2, it must also split over $K_1(K_2)$; on the other hand, since $K_1[x] \subseteq K_1(K_2)[x]$ and $K_2[x] \subseteq K_1(K_2)[x]$, while all three polynomials rings are UFDs, then the factorization in $K_1[x]$ and $K_2[x]$ must necessarily be the same as the factorization in $K_1(K_2)[x]$. So, for any $\beta \in K_1$ that is a root of $m_{\alpha,F}(x)$, since $(x - \beta) \mid m_{\alpha,F}(x)$ in $K_1[x] \subseteq K_1(K_2)[x]$, then $(x - \beta)$ is one of its irreducible factors; by the unique factorization mentioned, we must have $(x - \beta) \in K_2[x]$, showing that $\beta \in K_2$, or $\beta \in K_1 \cap K_2$.

Which, since $m_{\alpha,F}(x)$ splits completely in $K_1[x]$, which implies that K_1 contains all roots of $m_{\alpha,F}(x)$; then, since all roots of $m_{\alpha,F}(x)$ in K_1 also appears in $K_1 \cap K_2$, then $m_{\alpha,F}(x)$ splits completely over $K_1 \cap K_2$. This proves that $(K_1 \cap K_2)/F$ is a normal extension.

Combining both information above, $(K_1 \cap K_2)/F$ is in fact Galois.