Problem 1 (25 points) In each of the following cases, for the given finite extension \( F/E \) and the given element \( a \in F \), find the degree of \( a \) over \( E \) and find the minimal polynomial of \( a \) over \( E \).

(a) (5 points) \( E = \mathbb{Q} \), \( F = \mathbb{Q}[\sqrt{7}] \), \( a = \frac{1}{1 + \sqrt{7}} \).

(b) (10 points) \( E = \mathbb{Q} \), \( F = \mathbb{Q}[\sqrt{3}] \), \( a = 1 - \sqrt{3} + (\sqrt{3})^2 \).

(c) (10 points) \( E = \mathbb{F}_3 \), \( F = \mathbb{F}_3[t]/(t^2 + 1) \), \( a = t + 1 \).

\[
\alpha = \frac{1}{1 + \sqrt{7}} = \frac{\sqrt{7} - 1}{\sqrt{7} - 1} = \frac{1}{6} (-1 + \sqrt{7}) \quad F = \mathbb{E} \oplus \mathbb{E}\sqrt{7}, \text{ basis } \mathcal{B} = (1, \sqrt{7}). \\
L_\alpha : F \rightarrow F, \quad A_\alpha := [L_\alpha]_{\mathcal{B} \mathcal{B}} = \begin{bmatrix} 1 & -\frac{1}{6} & -\frac{7}{6} \\ \sqrt{7} & \frac{7}{6} & \frac{1}{6} \end{bmatrix}, \quad c_\alpha(x) = \begin{vmatrix} x + \frac{1}{6} & -\frac{7}{6} \\ -\frac{1}{6} & x + \frac{1}{6} \end{vmatrix} = \left( x + \frac{1}{6} \right)^2 - \frac{7}{36} \\
\left[ E(\alpha) : E \right] \neq 1 \text{ & divides } [F : E] = 2 = \text{ prime. Hence } \left[ E(\alpha) : E \right] = 2. \text{ So } c_\alpha(x) \text{ is minimal poly of } \alpha \text{ over } E. \]

\[
(b) F = \mathbb{E} \oplus \mathbb{E}\sqrt{2} \oplus \mathbb{E}(\sqrt{2})^2, \text{ basis } \mathcal{B} = (1, \sqrt{2}, (\sqrt{2})^2). \\
L_\alpha : F \rightarrow F, \quad A_\alpha := [L_\alpha]_{\mathcal{B} \mathcal{B}} = \begin{bmatrix} 1 & 3 & -3 \\ \sqrt{2} & -1 & 1 \\ (\sqrt{2})^2 & 1 & -1 \end{bmatrix}, \quad c_\alpha(x) = \begin{vmatrix} x - 1 & -3 & 3 \\ 1 & x - 1 & -3 \\ -1 & 1 & x - 1 \end{vmatrix} = (x - 1)^2 \oplus 9(x - 1) + 1 \\
\left[ E(\alpha) : E \right] \neq 1 \text{ & divides } [F : E] = 3 = \text{ prime. Hence } \left[ E(\alpha) : E \right] = 3. \text{ So } c_\alpha(x) = c_\alpha(x) (\text{or use Eisenstein to see } c_\alpha(x+1) \text{ is irreducible.})
\]

\[
(c) F = \mathbb{E} \oplus \mathbb{E} \cdot t, \text{ basis } \mathcal{B} = (1, t), \quad A_\alpha := \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, \quad c_\alpha(x) = \begin{vmatrix} x - 1 & 1 \\ -1 & x - 1 \end{vmatrix} = (x - 1)^2 + 1 \\
\left[ E(\alpha) : E \right] \neq 1 \text{ & } [E(\alpha) : E] \neq 2 = \text{ prime.} \]

Since \( [E(\alpha) : E] = 2 \) divides \( [F : E] = 2 \), \( [E(\alpha) : E] = 2 \) (or use that \( c_\alpha(x) \) has no root in \( E \)).
Problem 2 (35 points) Let $E$ be a field of characteristic $\neq 2$. Recall that for elements $D_1, D_2 \in E^*$ such that $D_1, D_2$ and $D_1D_2$ are all non-squares, the field extension $F = E[\sqrt{D_1}, \sqrt{D_2}]$ is called a biquadratic extension.

(a) (10 points) Prove that there are unique automorphisms $\sigma_1$ and $\sigma_2$ of $F$ fixing $E$ and such that

$$\sigma_1 : \begin{cases} \sqrt{D_1} & \mapsto -\sqrt{D_1} \\ \sqrt{D_2} & \mapsto \sqrt{D_2} \end{cases} \quad \sigma_2 : \begin{cases} \sqrt{D_1} & \mapsto \sqrt{D_1} \\ \sqrt{D_2} & \mapsto -\sqrt{D_2} \end{cases}$$

(b) (15 points) Find the fixed subfields of each of the following four groups of automorphisms of $F$: $\{1, \sigma_1\}$, $\{1, \sigma_2\}$, $\{1, \sigma_1\sigma_2\}$ and $\{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$.

(c) (10 points) Prove that $F/E$ is a Galois extension with Galois group $\{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$ (you may cite any of the theorems from lecture or the book, but please clearly state any theorem you use).

(a) Since $F$ is good over $E$ by $\sqrt{D_1}, \sqrt{D_2}$, every $E$-alg. automorphism is uniquely determined by its values on $\sqrt{D_1}$ & $\sqrt{D_2}$, $\sigma(\sqrt{D_1})$ & $\sigma(\sqrt{D_2})$.

A basis for $F$ is $\{(1, \sqrt{D_1}, \sqrt{D_2}, \sqrt{D_1D_2})\}$. With $\sigma(1) = 1$ & $\sigma(\sqrt{D_1D_2}) = \sigma(\sqrt{D_1}).\sigma(\sqrt{D_2})$, the only $E$-algebra relations, $\sigma(b_i b_j)\sigma(b_i b_k) = 0$, left to check are $\sigma(D_1 \cdot 1) = \sigma(\sqrt{D_1})\sigma(\sqrt{D_1}) = \sigma(\sqrt{D_1})$, i.e. $\sigma(\sqrt{D_1})$ is a root of $x^2 - D_1$. Since $-\sqrt{D_1}$ is a root of $x^2 - D_1$, & since $-\sqrt{D_1}$ is a root of $x^2 - D_2$, this is true. So $\sigma_1$ & $\sigma_2$ extend to $E$-alg. isomorphisms of $F$. (One can also use univ. property of root algebras or frv. thm. of Galois thm).

(b) $[\sigma_1]_{E, F} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $[\sigma_2]_{E, F} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $[\sigma_1 \sigma_2]_{E, F} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$.

Ker $[\sigma_1 - I] = \text{Ker} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix} = \text{Span} (1, \sqrt{D_2}) = E[\sqrt{D_2}] \subset \text{Fixed field of } \sigma_1$

Ker $[\sigma_2 - I] = \text{Ker} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix} = \text{Span}(1, \sqrt{D_1}) = E[\sqrt{D_1}] \subset \text{Fixed field of } \sigma_2$
(b) cont'd. \( \ker \left( \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} - I_4 \right) = \ker \left[ \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \right] = \text{Span}(1, \sqrt{D_2}) = \left[ \mathbb{E}[\sqrt{D_2}] \right] \text{ fixed field of } \sqrt{D_2} \)

Fixed field of \( \{1, \sqrt{D_2}, \sqrt{D_2}, \sqrt{D_2} \} = \text{intersection of these three subspaces} \)

\[ = \text{Span}(1) = \left[ \mathbb{E} \right] \text{ fixed field of } \{1, \sqrt{D_2}, \sqrt{D_2}, \sqrt{D_2} \} \]

(c) \[ [F : E] = \#(\mathbb{B}) = \#(1, \sqrt{D_2}, \sqrt{D_2}, \sqrt{D_2}) = 4 \]

\[ \mathbb{B} \neq \{1, \sqrt{D_2}, \sqrt{D_2}, \sqrt{D_2} \} = 4. \text{ Since } \mathbb{E} = F \{1, \sqrt{D_2}, \sqrt{D_2}, \sqrt{D_2} \} \]

\[ [F : E] = \#(1, \sqrt{D_2}, \sqrt{D_2}, \sqrt{D_2}) \text{ by definition } \]

a Galois extension with Galois group \( \{1, \sqrt{D_2}, \sqrt{D_2}, \sqrt{D_2} \}. \]
Problem 3 (40 points) You may use the previous problem to solve this problem (even if you did not solve every part of the previous problem). Let $F/E$ be a biquadratic extension, let $a, b \in E$ be elements such that $b$ is a non-square element and such that $a + \sqrt{b}$ is not a square in $E[\sqrt{b}]$. Assume that $F$ contains $\alpha = \sqrt{a + \sqrt{b}}$, i.e., suppose that the polynomial $(y^2 - a)^2 - b \in E[y]$ has a linear factor in $F$.

(a) (10 points) Let $L$ be any field of characteristic $\neq 2$, let $u$ be a non-square element in $L$, and let $v$ in $L$ be an element which has a square root in $L[\sqrt{u}]$. Prove that there exists an element $w$ in $L$ such that the square root is either of the form $w$ or $w\sqrt{u}$. In particular, either $v$ or $v/u$ is a square in $L$.

(b) (10 points) For the element $\sqrt{b} = a^2 - a$ in $F$, use Problem 2 to identify the possibilities for the subfield $E[\sqrt{b}]$ of $F$. Using (a) if necessary, conclude that $F$ is of the form $E[\sqrt{b}, \sqrt{c}]$ where $c$ is an element of $E$ such that $c$ and $bc$ are both non-squares.

(c) (10 points) Next set $L$ to be $E[\sqrt{b}]$, set $u$ to be $c$ and set $v$ to be $a + \sqrt{b}$. Conclude that $\alpha$ is of the form $s\sqrt{c} + t\sqrt{bc}$ for $s, t$ in $E$.

(d) Finally, use (c) to compute that the product $\alpha \sigma_1(\alpha)\sigma_2(\alpha)\sigma_1\sigma_2(\alpha)$ is a square in $E$. Since also there is a factorization,

$$(y^2 - a)^2 - b = (y - \alpha)(y - \sigma_1\alpha)(y - \sigma_2\alpha)(y - \sigma_1\sigma_2\alpha),$$

conclude that $a^2 - b$ is a square in $E$. Thus $E[\sqrt{a + \sqrt{b}}]$ is a biquadratic extension of $E$ only if $a^2 - b$ is a square in $E$.

Extra Credit. (5 points) Prove the converse: if $b$ is a non-square, if $a + \sqrt{b}$ in $E[\sqrt{b}]$ is a non-square, and if $a^2 - b$ is a square in $E$, prove that $E[\sqrt{a + \sqrt{b}}]$ is a biquadratic extension of $E$.
(c) For \( L = \mathbb{E} \sqrt{D} \) & \( L[\sqrt{w}] = L[\sqrt{c}] = F \), every root of \( a + \sqrt{b} \) in \( L[\sqrt{w}] \) is of the form \( w \) or \( w\sqrt{w} \) for some \( w \) in \( L \). By hypothesis \( a + \sqrt{b} \) is not a square in \( L \). So the root is of the form \( w\sqrt{w} \). Since every \( w \) in \( \mathbb{E} \sqrt{D} \) is of the form \( s + t\sqrt{D} \) & since \( \sqrt{w} \) equals \( \sqrt{c} \),

\[ \alpha = (s + t\sqrt{D})\sqrt{c} = \sqrt{s^2 + tsbc}. \]

\( \sigma \alpha = \begin{cases} \sigma \alpha = -s\sqrt{c} + t\sqrt{bc} \\ \sigma \alpha = -s\sqrt{c} - t\sqrt{bc} \\ \sigma \alpha = s\sqrt{c} - t\sqrt{bc} \\ \sigma \alpha = s\sqrt{c} + t\sqrt{bc} \end{cases} \]

\( \sigma \alpha \cdot \sigma \alpha \cdot \sigma \alpha \cdot \sigma \alpha = (s\sqrt{c} + t\sqrt{bc})(s\sqrt{c} - t\sqrt{bc})^2 \)

\[ = (s^2 - t^2bc)^2 \]

= square of an element, \( s^2 + t^2bc \) which is in \( E \).

And \( (y^2 - a)^2 - b = y^4 - 2ay^2 + (a^2 - b) \). So \( a^2 - b = (s^2 - t^2bc)^2 \) is the square of an element in \( E \).

\( \overline{E.C.} \) If \( a^2 - b \) equals \( w^2 \), set \( c = \frac{a + w}{2} \) (or \( \frac{a - w}{2} \)).

Then \( (1 + \frac{1}{2c} \sqrt{b})\sqrt{c} \) is a square root of \( a + \sqrt{b} \) in \( \mathbb{E}[\sqrt{b}, \sqrt{c}] \).