Name: ______________________________ Problem 1: ____________ /25

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

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

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

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

(a). $\alpha = \frac{1}{1+\sqrt{7}} = \frac{\sqrt{7}-1}{\sqrt{7}-1}\,\frac{1}{\sqrt{7}+1} = \frac{1}{6}(-1+1\cdot\sqrt{7})$. $F = E\cdot 1 \oplus E\cdot\sqrt{7}$, basis $\mathcal{B} = (1, \sqrt{7})$.

$L_\alpha : F \to F$, $\beta \mapsto \alpha\beta$, $A_\alpha := [L_\alpha]_{\mathcal{B},\mathcal{B}} = \begin{array}{c c} & \begin{array}{cc} 1 & \sqrt{7} \end{array} \\ \begin{array}{c} 1 \\ \sqrt{7} \end{array} & \begin{bmatrix} -\frac{1}{6} & \frac{7}{6} \\ +\frac{1}{6} & -\frac{1}{6} \end{bmatrix} \end{array}$, $c_{A_\alpha}(X) = \begin{vmatrix} X+\frac{1}{6} & -\frac{7}{6} \\ -\frac{1}{6} & X+\frac{1}{6} \end{vmatrix} = (X+\frac{1}{6})^2 - \frac{7}{36}$

$[E(\alpha):E] \neq 1$ & divides $[F:E] = 2 =$ prime. Hence $\boxed{[E(\alpha):E] = 2}$. So $c_A(X)$ $=$ minimal poly $\boxed{m_\alpha(X) = X^2 + \frac{1}{3}X - \frac{1}{6}}$. (Also $-6X^2 m_\alpha(\frac{1}{X}) = X^2 - 2X - 6$ is irred. by Eisenstein)

(b) $F = E\cdot 1 \oplus E\cdot\sqrt[3]{2} \oplus E(\sqrt[3]{2})^2$, basis $\mathcal{B} = (1, \sqrt[3]{2}, (\sqrt[3]{2})^2)$. $L_\alpha : F \to F$, $\beta \mapsto \alpha\beta$

$A_\alpha := [L_\alpha]_{\mathcal{B},\mathcal{B}} = \begin{array}{c c} & \begin{array}{ccc} 1 & \sqrt[3]{2} & (\sqrt[3]{2})^2 \end{array} \\ \begin{array}{c} 1 \\ \sqrt[3]{2} \\ (\sqrt[3]{2})^2 \end{array} & \begin{bmatrix} 1 & 3 & -3 \\ -1 & 1 & 3 \\ 1 & -1 & 1 \end{bmatrix} \end{array}$, $c_A(X) = \begin{vmatrix} X-1 & -3 & 3 \\ 1 & X-1 & -3 \\ -1 & 1 & X-1 \end{vmatrix}$

$\searrow\searrow\searrow = (X-1)^3 \cancel{+} 9 + 3$, $\swarrow\swarrow\swarrow = +9(X-1)$, $c_A(X) = \boxed{(X-1)^3 + 9(X-1) + 6 \\ = X^3 - 3X^2 + 12X - 4}$ $\leftarrow$ Irred. by Eisenstein.

$[E(\alpha):E] \neq 1$ & divides $[F:E] = 3 =$ prime.
Hence $\boxed{[E(\alpha):E] = 3}$. So $m_\alpha(X) = c_A(X)$ (or use Eisenstein to see $c_A(X+1)$ is irred.)

(c) $F = E\cdot 1 \oplus E\cdot t$, basis $\mathcal{B} = (1, t)$, $A_\alpha = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$, $c_A(X) = \begin{vmatrix} X-1 & 1 \\ -1 & X-1 \end{vmatrix} = (X-1)^2 + 1$ $= \boxed{X^2 + X + 1}$

Since $[E(\alpha):E] \neq 1$ & $[E(\alpha):E]$ divides $[F:E] = 2 =$ prime, $\boxed{[E(\alpha):E] = 2}$ (or use that $c_A(X)$ has no root in E).

Name: ______________________ **Problem 2:** __________ /35

Problem 2(35 points) Let E be a field of characteristic $\neq 2$. Recall that for elements $D_1, D_2 \in E^\times$ 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 σ_1 and σ_2 of F fixing E and such that

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

(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 gen'd 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, E-basis for F is $\mathcal{B} = (1, \sqrt{D_1}, \sqrt{D_2}, \sqrt{D_1D_2})$. With $\sigma(1) := 1$ & $\sigma(\sqrt{D_1D_2}) := \sigma(\sqrt{D_1})\cdot\sigma(\sqrt{D_2})$, the only E-algebra relations, $\sigma(b_ib_j) - \sigma(b_i)\sigma(b_j) = 0$, left to check are $\sigma(D_1 \cdot 1) = \sigma(\sqrt{D_1})\sigma(\sqrt{D_1})$ & $\sigma(D_2 \cdot 1) = \sigma(\sqrt{D_2})\cdot\sigma(\sqrt{D_2})$, i.e. $\sigma(\sqrt{D_i})$ is a root of $x^2 - D_i$. Since $-\sqrt{D_1}$ is a root of $x^2 - D_1$ & since $-\sqrt{D_2}$ is a root of $x^2 - D_2$, this is true. So σ_1 & σ_2 extend to E-alg. isomorphisms of F. (One can also use univ. property of root algebras or fund. thm. of Galois thy).

(b) $$[\sigma_1]_{\mathcal{B},\mathcal{B}} = \begin{array}{c} 1 \\ \sqrt{D_1} \\ \sqrt{D_2} \\ \sqrt{D_1D_2} \end{array}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}, \quad [\sigma_2]_{\mathcal{B},\mathcal{B}} = \begin{array}{c} 1 \\ \sqrt{D_1} \\ \sqrt{D_2} \\ \sqrt{D_1D_2} \end{array}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}, \quad [\sigma_1\sigma_2]_{\mathcal{B},\mathcal{B}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$
$$\begin{array}{cccc} 1 & \sqrt{D_1} & \sqrt{D_2} & \sqrt{D_1D_2} \end{array} \qquad \begin{array}{cccc} 1 & \sqrt{D_1} & \sqrt{D_2} & \sqrt{D_1D_2} \end{array}$$

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

$\underline{\text{char} \neq 2}$ ↗

$$\mathrm{Ker}([\sigma_2] - Id) = \mathrm{Ker}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -2 \end{bmatrix} = \mathrm{Span}(1, \sqrt{D_1}) = \boxed{E[\sqrt{D_1}] \leftarrow \text{Fixed field of } \sigma_2}$$

$\underline{\text{char} \neq 2}$ ↗

char $\neq 2$

(b) contd. $\mathrm{Ker}([\sigma_1\sigma_2] - Id) = \mathrm{Ker}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \mathrm{Span}(1, \sqrt{D_1D_2}) = \boxed{E[\sqrt{D_1D_2}] \leftarrow \text{Fixed field of } \sigma_1\sigma_2}$

Fixed field of $\{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$ = intersection of these three subspaces

$= \mathrm{Span}(1) = \boxed{E \leftarrow \text{fixed field of } \{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}}$

(c) $[F:E] = \#\mathcal{B} = \#(1, \sqrt{D_1}, \sqrt{D_2}, \sqrt{D_1D_2}) = \underline{\underline{4}}$

& $\#\{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\} = \underline{\underline{4}}$. Since $E = F^{\{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}}$

& $[F:E] = \#\{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$, by definition F/E is a Galois extension with Galois group $\{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$.

Name: ________________________ **Problem 3:** __________ /40

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 $\sqrt{b} = \alpha^2 - a$ 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 α 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.

(a). Let $\alpha = s + t\cdot\sqrt{u}$ be in $L[\sqrt{u}]$ w/ $\alpha^2 = v = v\cdot 1 + 0\cdot\sqrt{u}$. Since $\alpha^2 = (s^2 + ut^2) + 2st\sqrt{u}$, $2st$ equals 0. Since char $\neq 2$, $s = 0$ or $t = 0$. $\underline{s=0}$. $v = ut^2$ so $\boxed{v/u \text{ is a square in } L}$

$\underline{t=0}$. $v = s^2$ so $\boxed{v \text{ is a square in } L}$

(b) $[E[\sqrt{b}] : E] = 2$, so $E[\sqrt{b}]$ is $E[\sqrt{D_1}]$, $E[\sqrt{D_2}]$ or $E[\sqrt{D_1 D_2}]$ (by Fund. Thm. of Gal. thy, these are the only fields in F w/ deg = 2)

So, up to square factors, $D_1 = b$, $D_2 = b$ or $D_1 D_2 = b$.

Up to permutation & square factors, may assume $D_1 = b$.

Then $F = E[\sqrt{D_1}, \sqrt{D_2}] = E[\sqrt{b}, \sqrt{c}]$ for $c = D_2$ non-square & bc non-square.

(Can also do this by considering $[E[\sqrt{b}, \sqrt{D_1}] : E]$, $[E[\sqrt{b}, \sqrt{D_2}] : E]$ & $[E[\sqrt{b}, \sqrt{D_1 D_2}] : E]$,

(c) For $L = E[\sqrt{b}]$ & $L[\sqrt{u}] = L[\sqrt{c}] = F$, every root of $a+\sqrt{b}$ in $L[\sqrt{u}]$ is of the form w or $w\sqrt{u}$ for some w in L. By hypothesis $a+\sqrt{b}$ is not a square in L. So the root is of the form $w\sqrt{u}$. Since every w in $E[\sqrt{b}]$ is of the form $s+t\sqrt{b}$ & since $\sqrt{u}$ equals $\sqrt{c}$,

$$\alpha = (s+t\sqrt{b})\sqrt{c} = \boxed{s\sqrt{c} + t\sqrt{bc}}.$$

(d) $\begin{cases} \alpha = s\sqrt{c} + t\sqrt{bc} \\ \sigma_1\alpha = -s\sqrt{c} - t\sqrt{bc} \\ \sigma_2\alpha = +s\sqrt{c} - t\sqrt{bc} \\ \sigma_1\sigma_2\alpha = -s\sqrt{c} + t\sqrt{bc} \end{cases} \Rightarrow \alpha\cdot\sigma_1\alpha\cdot\sigma_2\alpha\cdot\sigma_1\sigma_2\alpha = \left((s\sqrt{c}+t\sqrt{bc})(s\sqrt{c}-t\sqrt{bc})\right)^2$

$$= (s^2c - t^2bc)^2$$

= square of an element, $s^2c - t^2bc$, which is in E.

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

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

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