Name: ______________________________ **Problem 1:** ____________ /25

Problem 1(45 points) Let $\sqrt{5}$ be the positive, real root of $x^2 - 5$. Let ϵ be the automorphism of $\mathbb{Q}(\sqrt{5})$ sending $\sqrt{5}$ to $-\sqrt{5}$. Let t be $5 + 2\sqrt{5}$ and let $u := \sqrt{5 + 2\sqrt{5}}$ be the positive, real root of $x^2 - t$.

(a)(5 points) Prove that u is algebraic over $\mathbb{Q}$ and find its minimal polynomial $m_{u,\mathbb{Q}}(x)$.

(b)(5 points) Compute $t\epsilon(t)$ as an element in $\mathbb{Q}$.

(c)(10 points) Prove that $\mathbb{Q}(u)$ contains a root v of $x^2 - \epsilon(t)$.

(d)(5 points) Explain why $\mathbb{Q}(u)$ is the splitting field of $m_{u,\mathbb{Q}}(x)$.

(e)(10 points) Let σ be the automorphism of $\mathbb{Q}(u)$ sending u to a root v of $x^2 - \epsilon(t)$. Compute $\sigma(\sqrt{5})$ and use this to compute $\sigma(v)$.

(f)(10 points) Find the order of σ and use this to identify $\mathrm{Aut}(\mathbb{Q}(u)/\mathbb{Q})$.

(a) $u^2 - 5 = 2\sqrt{5}$, $(u^2-5)^2 = 20$, $\underline{u^4 - 10u^2 + 5 = 0}$. So u is algebraic. By Eisenstein, $m_{u,\mathbb{Q}}(X) = X^4 - 10X^2 + 5$ is irreducible, thus the minimal polynomial of u.

(b) $t = 5 + 2\sqrt{5}$, $\varepsilon(t) = 5 - 2\sqrt{5}$, $t \cdot \varepsilon(t) = (5+2\sqrt{5})(5-2\sqrt{5}) = 5^2 - (2\sqrt{5})^2 = 25 - 20 = \boxed{5}$

(c) $\varepsilon(t) = \frac{5}{t} = \frac{(\sqrt{5})^2}{u^2} = \left(\frac{\sqrt{5}}{u}\right)^2$. So $\boxed{v = \frac{\sqrt{5}}{u}}$ is one root of $X^2 - \varepsilon(t)$ (& $-v$ is the 2^{nd} root).

$\mathbb{Q}(u)$ contains $\sqrt{5}$ since $\sqrt{5} = \frac{u^2-5}{2}$. So $\mathbb{Q}(u)$ contains $v = \frac{\sqrt{5}}{u}$.

(d) $\mathbb{Q}(u)$ contains the four roots $u, -u, v = \frac{\sqrt{5}}{u} = \frac{u}{2} - \frac{5}{2u}$ & $-v$.

(e) $\sigma(u) = v = \frac{\sqrt{5}}{u}$, $\sqrt{5} = \frac{u^2-5}{2} \Rightarrow \sigma(\sqrt{5}) = \frac{\sigma(u)^2 - 5}{2} = \frac{v^2-5}{2}$
$= \frac{\varepsilon(t) - 5}{2} = \frac{(5-2\sqrt{5})-5}{2} = \boxed{-\sqrt{5}}$. So $\sigma(v) = \frac{\sigma(\sqrt{5})}{\sigma(u)} = \frac{-\sqrt{5}}{\sqrt{5}/u} = \boxed{-u}$.

(f) $\sigma: \begin{cases} u \to v \\ -u \to -v \\ v \to -u \\ -v \to u \end{cases} \longleftrightarrow \underset{u\ v\ -u\ -v}{(1 3 2 4)}$ has order $\boxed{4}$. And $\#\mathrm{Aut}(\mathbb{Q}(u)/\mathbb{Q}) = [\mathbb{Q}(u) : \mathbb{Q}]$
$= \deg m_{u,\mathbb{Q}}(X) = 4$. So $\mathrm{Aut}\left(\mathbb{Q}(u)/\mathbb{Q}\right) \cong \mathbb{Z}/4\mathbb{Z}$.

Name: ____________________ **Problem 2:** __________ /25

Problem 2(25 points) Let F be a field of characteristic 0 which contains a primitive n^{th} root of unity, ζ_n. Recall that every Galois extension E/F with order n cyclic Galois group, $\text{Aut}(E/F) = \langle\sigma\rangle \cong \mathbb{Z}/n\mathbb{Z}$, is of the form $F(t)$ where t in E is a root of an irreducible polynomial $x^n - a$ in $E[x]$ and satisfying $\sigma(t) = \zeta_n t$.

Let u be a nonzero element of E such that $b := u^n$ is in F. Prove that there exists an integer $r = 0, \ldots, n-1$ such that b/a^r is an n^{th} power in F, i.e., $b/a^r = c^n$ for some nonzero c in F. Conclude that $((F^\times)^n \cap E^\times)/(E^\times)^n$ is the cyclic subgroup generated by $\overline{a}$. (This subgroup of $E^\times/(E^\times)^n$ characterizes the cyclic extension F/E up to isomorphism.)

Hint. What are generators of the eigenspaces of the F-linear transformation σ of E? What are the Galois conjugates of u? What does this imply about $\sigma(u)$ and t^r?

One eigenvector is t with eigenvalue ζ_n; $\sigma(t) = \zeta_n(t)$. Since E is a field, each power t^r, $r=0,\ldots,n-1$, is nonzero. Since σ is a field homomorphism, $\sigma(t^r) = \sigma(t)^r = (\zeta_n t)^r = \zeta_n^r t^r$. Hence t^r is an eigenvector with ~~eigenvaltue~~ eigenvalue ζ_n^r. Since ζ_n is a primitive n^{th} root of 1, $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$ are all distinct. So $F\cdot 1, F\cdot t, F\cdot t^2, \ldots, F\cdot t^{n-1}$ are n distinct eigenspaces. Since $[F:E] = \deg(x^n - a) = n$, these eigenspaces diagonalize σ.

Every Galois conjugate of u is a root of $x^n - b$. The roots of $x^n - b$ are precisely the n distinct elements $\zeta_n^r u$ (note, I do not claim these are all Galois conjugates). So $\sigma(u)$ is of the form $\zeta_n^r u$ for some $r = 0, \ldots, n-1$. But t^r spans the ζ_n^r-eigenspace. Hence $u = c\cdot t^r$ for $c \in F^\times$. Thus $b = u^n = (c\cdot t^r)^n = c^n a^r$, i.e., $b/a^r = c^n$.

Therefore $\frac{(F^\times)^n \cap E^\times}{(E^\times)^n}$ equals $\{\overline{1}, \overline{a}, \ldots, \overline{a}^{n-1}\} = \langle \overline{a} \rangle$.

Name: ______________________ **Problem 3:** __________ /30

Problem 3(30 points) Let F be a field and let $f(x)$ be a monic polynomial in $F[x]$ such that $f(x)$ factors into a product of monic linear polynomials in some finite, Galois extension K of F, i.e.,

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i).$$

The *discriminant* of $f(x)$ is defined to be

$$\mathrm{Disc}(f) := \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2} \prod_{i \ne j} (\alpha_i - \alpha_j).$$

The element $\mathrm{Disc}(f)$ is invariant under $\mathrm{Aut}(K/F)$, hence is an element of F. (Discriminants were discussed in Tuesday's lecture, but the following problem requires none of the results proved in that lecture.)

(a)(10 points) If $f(x)$ equals $(x - \theta)g(x)$, prove that $\mathrm{Disc}(f)$ equals $(g(\theta))^2\mathrm{Disc}(g)$. Assuming $f(x)$ is separable, conclude that $\mathrm{Disc}(g)$ is a square if and only if $\mathrm{Disc}(f)$ is a square.

(b)(5 points) For quadratic polynomials, the explicit formula for the discriminant is

$$g(x) = x^2 - a_1x + a_2, \quad \mathrm{Disc}(g) = a_1^2 - 4a_2.$$

Assuming $\mathrm{char}(F)$ is $\ne 2$, prove that a quadratic polynomial $g(x)$ factors into linear polynomials in F if and only if $\mathrm{Disc}(g)$ is a square in F.

(c)(10 points) Finally, let E be a field with $\mathrm{char}(E) \ne 2, 3$. Let $f(x)$ be a monic, irreducible, separable, cubic polynomial in $E[x]$. Let $F = E[t]/\langle f(t) \rangle$ be a root field of $f(x)$, and let θ be a root of $f(x)$ in F so that $f(x) = (x - \theta)g(x)$ in $F[x]$. If $\mathrm{Disc}(f)$ is a square in E, prove that F is a splitting field for $f(x)$.

(d)(5 points) Let $f(x)$ and F/E be as above. When $\mathrm{Disc}(f)$ is a square in E, what is the Galois group $\mathrm{Aut}(F/E)$?

(a) $g(x)$ factors as $\prod_{i=1}^{n}(x-\alpha_i)$. So $f(x)$ factors as $(x-\theta)(x-\alpha_1)\cdots(x-\alpha_n)$. So $\mathrm{Disc}(f) = (\theta-\alpha_1)^2\cdots(\theta-\alpha_n)^2 \cdot \prod_{i<j}(\alpha_i-\alpha_j)^2$. But $(\theta-\alpha_1)\cdots(\theta-\alpha_n)$ equals $g(\theta)$ & $\prod_{i<j}(\alpha_i-\alpha_j)^2$ equals $\mathrm{Disc}(g)$. So $\mathrm{Disc}(f) = [g(\theta)]^2\,\mathrm{Disc}(g)$. If f is separable, then $g(\theta) \neq 0$. So $\mathrm{Disc}(f)$ is a square if & only if $\mathrm{Disc}(g)$ is a square.

(b) $x^2 - a_1 x + a_2 = (x - \frac{a_1}{2})^2 - \frac{\mathrm{Disc}(g)}{2^2}$. If there exists a root θ, then $\mathrm{Disc}(g) = (2\theta - a_1)^2$ is a square. And if $\mathrm{Disc}(g)$ is a square, δ^2, then $\theta_1 = \frac{a_1}{2} + \frac{\delta}{2}$, $\theta_2 = \frac{a_1}{2} - \frac{\delta}{2}$ are roots of $g(x)$.
(Note this fails if $\mathrm{char}(F) = 2$: $x^2 + x + 1$ is irreducible over $\mathbb{F}_2$ but $\mathrm{Disc} = 1 = 1^2$.)

(c) If $\mathrm{Disc}(f)$ is a square in E, then it is a square in F. Then by (a), $\mathrm{Disc}(g)$ is a square in F. So by (b), $g(x)$ factors in F. Hence $f(x)$ factors into linear polynomials in F, i.e., F is a splitting field. (I guess $\mathrm{char}(E) \neq 3$ was unnecessary.)

(d) Since $[F:E] = \deg(f)$ equals 3, $\#\mathrm{Aut}(F/E)$ equals 3. Thus $\mathrm{Aut}(F/E) \cong \mathbb{Z}/3\mathbb{Z}$.