Math 111C HW8

Zih-Yu Hsieh

June 6, 2025

1

Question 1 *Show that every finite separable extension K/F has only finitely many sub-extensions.*

Pf:

Since K/F is a finite separable extension, there exists $\alpha_1, ..., \alpha_n \in K$, such that $F(\alpha_1, ..., \alpha_n) = K$ (and all α_i are separable over F by definition).

Which, fix $\overline{F}$ such that $K \subseteq \overline{F}$, and take $A = \{m_{\alpha_1,F}(x), ..., m_{\alpha_n,F}(x)\} \subset F[x]$. Consider $L \subseteq \overline{F}$ to be the splitting field of A, then since each polynomial in A must split completely over L, it must necessarily contain all the roots of all polynomials in A; on the other hand, since each $\alpha_i \in K \subseteq \overline{F}$ is a root of $m_{\alpha_i,F}(x) \in A$, then $\alpha_i \in L$, hence $K = F(\alpha_1, ..., \alpha_n) \subseteq L$.

Now, because each α_i is separable, then $m_{\alpha_i,F}(x) \in A$ is also a separable polynomial, hence A is consists of separable polynomials. Then, because L is a splitting field of A, then L/F is in fact a finite Galois Extension. Hence, $|\mathrm{Gal}(L/F)| = [L : F] < \infty$.

Which, based on **Galois Correspondance** of finite Galois Extension, any subfield $F \subseteq E \subseteq L$ corresponds to a unique subgroup $H \leq \mathrm{Gal}(L/F)$ (where $E = L^H$). Then, for any sub-extension of K, given as E (where $F \subseteq E \subseteq K \subseteq L$), we know E corresponds to a unique subgroup $H \leq \mathrm{Gal}(L/F)$. Then, since $\mathrm{Gal}(L/F)$ is proven to be finite, there are only finitely many subgroups. Hence, this implies that K/F can only have finitely many sub-extensions, since each distinct sub-extension must correspond to a unique subgroup of $\mathrm{Gal}(L/F)$ (which has only finitely many distinct subgroups).

So, we concluded that K/F (as a finite separable extension), must have only finitely many sub-extensions.

2

Question 2 *Let $L \subseteq \mathbb{C}$ be the splitting field of $f(x) = x^3 - 3x + 1$ over $\mathbb{Q}$. Let $\alpha, \beta, \gamma \in L$ be roots of $f(x)$.*

(a) Calculate $Gal(L/\mathbb{Q})$ as a group of permutations of $\{\alpha, \beta, \gamma\}$.

(b) Is there an automorphism of L that acts on $\{\alpha, \beta, \gamma\}$ as the transposition (α, β)?

*(**Hint:-** For a polynomial $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ with roots $\alpha, \beta, \gamma \in \mathbb{C}$, the discriminant of $f(x)$, D is defined as*

$$D = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2$$

It is known that $D = 18abc + a^2b^2 - 4b^3 - 4a^3c - 27c^2$).

Pf:

Before starting the question, we'll try to understand the relations between the roots, and some implications we could make: Since $f(x)$ (for the discriminant calculation) has $a = 0$, $b = -3$, and $c = 1$, then we get $D = -4(-3)^3 - 27 \cdot 1^2 = 27 \cdot 4 - 27 = 81 > 0$. This implies that $f(x)$ has three distinct real roots. And, based on Rational Root Theorem, $f(x)$ only has possible rational roots ± 1, and since these are not the actual roots (by plugging in $f(x)$), then $f(x)$ has no rational roots. Also, because $f(x)$ has degree 3, then it is irreducible over $\mathbb{Q}$.

Notice that $L = \mathbb{Q}(\alpha, \beta, \gamma)$ (since L is the splitting field of $f(x)$, which is generated by the roots of $f(x)$). Also, based on **Vieta's Formula**, the x^2 coefficient satisfies $0 = -(\alpha + \beta + \gamma)$, and the constant coefficient $1 = \alpha\beta\gamma$. So, in terms of α, β satisfies the following formula:

$$\gamma = -\alpha - \beta, \quad \alpha\beta\gamma = \alpha\beta(-\alpha - \beta) = 1 \implies \alpha\beta^2 + \alpha^2\beta + 1 = 0 \tag{1}$$

Hence, β satisfies the equation $\alpha x^2 + \alpha^2 x + 1 = 0$, which is a root of $\alpha x^2 + \alpha^2 x + 1 \in \mathbb{C}[x]$ (similar logic can be applied to γ). Hence, by quadratic formula, we get the following relation:

$$\beta, \gamma = \frac{-\alpha^2 \pm \sqrt{(\alpha^2)^2 - 4\alpha}}{2\alpha} = -\frac{\alpha}{2} \pm \sqrt{\frac{\alpha^2}{4} - \frac{1}{\alpha}} \tag{2}$$

WLOG, assume β is the root with positive sign. Notice that this implies $L = \mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}\left(\alpha, \sqrt{\frac{\alpha^2}{4} - \frac{1}{\alpha}}\right)$ (since β, γ can be created by combinations of α and $\sqrt{\frac{\alpha^2}{4} - \frac{1}{\alpha}}$, while conversely $\sqrt{\frac{\alpha^2}{4} - \frac{1}{\alpha}}$ can also be created by β, γ). Also, we get the following relations:

$$\begin{cases} \alpha - \beta = \frac{3\alpha}{2} - \sqrt{\frac{\alpha^2}{4} - \frac{1}{\alpha}} \\ \beta - \gamma = 2\sqrt{\frac{\alpha^2}{4} - \frac{1}{\alpha}} \\ \gamma - \alpha = -\frac{3\alpha}{2} - \sqrt{\frac{\alpha^2}{4} - \frac{1}{\alpha}} \end{cases} \tag{3}$$

Hence, without considering the "usual" square root in $\mathbb{R}$, define $\sqrt{D} := (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$, we get:

$$\begin{aligned} \sqrt{D} &= \left(\frac{3\alpha}{2} - \sqrt{\frac{\alpha^2}{4} - \frac{1}{\alpha}}\right)\left(2\sqrt{\frac{\alpha^2}{4} - \frac{1}{\alpha}}\right)\left(-\frac{3\alpha}{2} - \sqrt{\frac{\alpha^2}{4} - \frac{1}{\alpha}}\right) \\ &= \left(\frac{9\alpha^2}{4} - \left(\frac{\alpha^2}{4} - \frac{1}{\alpha}\right)\right) 2\sqrt{\frac{\alpha^2}{4} - \frac{1}{\alpha}} = \left(4\alpha^2 + \frac{1}{\alpha}\right)\sqrt{\frac{\alpha^2}{4} - \frac{1}{\alpha}} \end{aligned} \tag{4}$$

Which, because $\sqrt{D}$ can be created by α and $\sqrt{\frac{\alpha^2}{4}-\frac{1}{\alpha}}$, $\sqrt{D} \in \mathbb{Q}\left(\alpha, \sqrt{\frac{\alpha^2}{4}-\frac{1}{\alpha}}\right) = L$; also, because $D = 81 \neq 0$, so $\sqrt{D} \neq 0$, which shows that $4\alpha^2 + \frac{1}{\alpha} \neq 0$. Hence, $\sqrt{\frac{\alpha^2}{4}-\frac{1}{\alpha}} = \sqrt{D}\left(4\alpha^2+\frac{1}{\alpha}\right)^{-1} \in \mathbb{Q}(\alpha, \sqrt{D})$. These two relations show that $L = \mathbb{Q}\left(\alpha, \sqrt{\frac{\alpha^2}{4}-\frac{1}{\alpha}}\right) = \mathbb{Q}(\alpha, \sqrt{D})$.

As a consequence, since $D = 81$ for $f(x)$ in this problem, then $\sqrt{D} = \pm 9 \in \mathbb{Q}$ (Note: this $\sqrt{D}$ is what we've defined above, not the actual square root of $\mathbb{R}$; hence, depending on the arrangement of the roots, $\sqrt{D}$ could be positive or negative). Hence, $L = \mathbb{Q}(\alpha, \sqrt{D}) = \mathbb{Q}(\alpha)$. On the other hand, because α is a root of $f(x) = x^3 - 3x + 1$, which has proven to be irreducible initially (and monic), then $L = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f(x))$, showing that $[L : \mathbb{Q}] = [\mathbb{Q}[x]/(f(x)) : \mathbb{Q}] = \deg(f(x)) = 3$. Hence, $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 3$.

(a) First, since for any $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ fixes all elements of $\mathbb{Q}$, then for all $k \in L$ and the fact that $f(x) \in \mathbb{Q}[x]$, we have $\sigma(f(k)) = f(\sigma(k))$. Hence, any $k \in \{\alpha, \beta, \gamma\}$ (the roots of $f(x)$), we must have $0 = \sigma(f(k)) = f(\sigma(k))$, showing that $\sigma(k) = 0$. Therefore, $\sigma(k)$ is again a root of $f(x)$, showing that $\sigma(k) \in \{\alpha, \beta, \gamma\}$.

This shows that σ can only send roots of $f(x)$ to roots of $f(x)$, hence it acts on the set $\{\alpha, \beta, \gamma\}$ as a permutation; also, because $L\mathbb{Q}(\alpha, \beta, \gamma)$, then the structure of σ is solely determined by its action on $\{\alpha, \beta, \gamma\}$. Hence, σ can be identified by a unique permutation in S_3, and therefore $\mathrm{Gal}(L/\mathbb{Q}) \cong H \leq S_3$ for some subgroup H.

However, initially we've determined that $|\mathrm{Gal}(L/\mathbb{Q})| = 3$, which shows that $|H| = 3$. Then, because S_3 (with $|S_3| = 6$) only has one subgroup with order $\frac{6}{2} = 3$, namely A_3 (the collection of all 3-cycles together with identity in this case), then we must have $\mathrm{Gal}(L/\mathbb{Q}) \cong H = A_3$.

(b) In **part (a)** we've identified that $\mathrm{Gal}(L/\mathbb{Q}) \cong A_3 \leq S_3$, which shows that every element being the identity or a 3-cycle, hence there has no transpositions at all. Therefore, as a consequence there is no automorphism in $\mathrm{Gal}(L/\mathbb{Q})$ that acts as a transposition (α, β) on $\{\alpha, \beta, \gamma\}$.

3

Question 3 *Repeat the above question with $f(x) = x^3 - 4x + 1$.*

Pf:

For this problem, we'll try a different approach (as a practice). For $f(x)$ in the question, to calculate discriminant, we have $a = 0,\ b = -4$, and $c = 1$. Hence, we get $D = -4(-4)^3 - 27 \cdot 1^2 = 256 - 27 = 229$, this indicates that $f(x)$ has three distinct real roots (which we'll use the same notation $\{\alpha, \beta, \gamma\}$). Notice that by Rational Root Theorem, the only possible rational roots of $f(x)$ are ± 1; but, none of these values are actual roots of $f(x)$ (by manual check), hence $f(x)$ has no rational roots. Since it's with degree 3, then $f(x)$ is in fact irreducible over $\mathbb{Q}$.

Now, define $\sqrt{D} := (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$, since $L = \mathbb{Q}(\alpha, \beta, \gamma)$, then we have $\sqrt{D} \in L$, or $\mathbb{Q}(\sqrt{D}) \subseteq L$. Which, because $D = 229$, then $\sqrt{D} = \pm\sqrt{229} \notin \mathbb{Q}$; which, because $\sqrt{D}$ is a root of $x^2 - 229 \in \mathbb{Q}[x]$, and this polynomial has no roots in $\mathbb{Q}$, then it is irreducible over $\mathbb{Q}$. Hence, $x^2 - 229$ (which is monic) is the minimal polynomial of $\sqrt{D}$ over $\mathbb{Q}$, so we get that $\mathbb{Q}(\sqrt{D}) \cong \mathbb{Q}[x]/(x^2 - 229)$, showing that $[\mathbb{Q}(\sqrt{D}) : \mathbb{Q}] = 2$. As a consequence, because $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{D}) \subseteq L$, then $[L : \mathbb{Q}]$ is divisible by 2.

On the other hand, we also know that $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq L$, and α is a root of $f(x)$ while $f(x)$ is irreducible and monic over $\mathbb{Q}$, hence it is the minimal polynomial of α. Hence, $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f(x))$, showing that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f(x)) = 3$. This also implies that $[L : \mathbb{Q}]$ is divisible by 3, hence $[L : \mathbb{Q}]$ is divisible by 6.

(a) Again, since $L = \mathbb{Q}(\alpha, \beta, \gamma)$, then any $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ is purely determined by its action on $\{\alpha, \beta, \gamma\}$; also, since for any $k \in L$, because $f(x) \in \mathbb{Q}[x]$ (which has coefficients fixed by σ), then $\sigma(f(k)) = f(\sigma(k))$. Hence, for any root $k \in \{\alpha, \beta, \gamma\}$, we must have $0 = \sigma(f(k)) = f(\sigma(k))$, showing that $\sigma(k)$ is also a root of $f(x)$, or $\sigma(k) \in \{\alpha, \beta, \gamma\}$. Hence, σ acts on the three roots as a permutation, showing that $\mathrm{Gal}(L/\mathbb{Q})$ has a permutation action on the three roots. So, $\mathrm{Gal}(L/\mathbb{Q}) \cong H \leq S_3$ (since it acts as a permutation of a 3-element set, it can be characterized by a subgroup of S_3).

    Now, based on the subgroup relation, $[L : \mathbb{Q}] = |\mathrm{Gal}(L/\mathbb{Q})| \leq |S_3| = 6$; also, because we've proven beforehand that 6 divides $[L : \mathbb{Q}]$, shiwhc shows that $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] \geq 6$. So, $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 6$, which enforces $\mathrm{Gal}(L/\mathbb{Q}) \cong H = S_3$ (since the only subgroup of S_3 with order 6 is S_3 itself).

(b) Because in **part (a)**, $\mathrm{Gal}(L/\mathbb{Q})$ is proven to have a permutation action on $\{\alpha, \beta, \gamma\}$ and is isomorphic to S_3 as groups, then there exists automorphism that acts as a transposition (α, β).

4

Question 4 *Let $L \subseteq \mathbb{C}$ be the splitting field of $f(x) = (x^2-2)(x^2-3)$ over $\mathbb{Q}$.*

(a) Show that $L = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ and $[L:\mathbb{Q}] = 4$.

(b) Find Gal$(L/\mathbb{Q})$ as a group of permutations of the roots of f.

(c) Which elements of your ansewr to (b) belong to the subgroup Gal$(L/\mathbb{Q}(\sqrt{6}))$?

Pf:

First, $f(x) = (x^2-2)(x^2-3)$ over $\mathbb{C}$ can be factored as $(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3})$, hence the roots are $\pm\sqrt{2}, \pm\sqrt{3}$. This indicates that the splitting field $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(a) First, it is clear that $\sqrt{2}+\sqrt{3} \in L = \mathbb{Q}(\sqrt{2},\sqrt{3})$, hence $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq L$; on the other hand, this element satisfies the below relation:

$$(\sqrt{3}+\sqrt{2})(\sqrt{3}-\sqrt{2}) = 3-2 = 1 \implies \sqrt{3}-\sqrt{2} = \frac{1}{\sqrt{2}+\sqrt{3}} \tag{5}$$

Hence, $\sqrt{3}-\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Then, $\sqrt{3} = \frac{1}{2}((\sqrt{3}+\sqrt{2})+(\sqrt{3}-\sqrt{2})) \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, which also implies that $\sqrt{2} = (\sqrt{2}+\sqrt{3}) - \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Hence, $L = \mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$, which proves that $L = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Now, to consider the degree, we'll use the relation $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq L = \mathbb{Q}(\sqrt{2},\sqrt{3})$: Since $\sqrt{2}$ has minimal polynomial $x^2-2 \in \mathbb{Q}[x]$, then $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$.

Now, consider the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$: Since it satisfies x^2-3, then the minimal polynomial must divide x^2-3; then, to prove that x^2-3 is the minimal polynomial, we'll show that x^2-3 has no roots in $\mathbb{Q}(\sqrt{2})$.

Suppose the contrary that it has roots in $\mathbb{Q}(\sqrt{2})$, then for some $a, b \in \mathbb{Q}$, $(a+b\sqrt{2})$ satisfies $(a+b\sqrt{2})^2 - 3 = 0$, or $(a^2+2b^2) + 2ab\sqrt{2} = 3 = 3 + 0\cdot\sqrt{2}$.Since $1, \sqrt{2}$ forms a basis of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, this equation implies that $2ab = 0$, which $a = 0$ or $b = 0$. Yet, if $b = 0$, we have $a^2 = 3$, or $a = \pm\sqrt{3} \in \mathbb{Q}$, which violates the fact that $\sqrt{3}$ is irrational; on the other hand, if $a = 0$, we have $(b\sqrt{2})^2 = 2b^2 = 3$. Since $b = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$, $q \neq 0$, and $\gcd(p,q) = 1$, then the equation implies $2\frac{p^2}{q^2} = 3$, showing that $2p^2 = 3q^2$.

Then, this implies $2 \mid 3q^2$, and while $2 \nmid 3$, we must have $2 \mid q^2$, or $2 \mid q$, hence $q = 2k$ for some $k \in \mathbb{Z}$; now, we have $2p^2 = 3q^2 = 3(2k)^2$, then $p^2 = 3 \cdot 2k^2$, showing that $2 \mid p^2$, or $2 \mid p$. Then, we get that 2 is a common factor of p and q, yet this violates the assumption that $\gcd(p,q) = 1$, so we reach a contradiction. So, the assumption is false, showing that x^2-3 has no roots over $\mathbb{Q}(\sqrt{2})$, hence it is irreducible over x^2-3.

As a consequence, since x^2-3 is monic, while $\sqrt{3}$ is a root of it, it is the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$, showing that $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2})[x]/(x^2-3)$, hence $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})] = 2$.

Together with the initial degree of $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$, we get the following:

$$[L:\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2\cdot 2 = 4 \tag{6}$$

(b) From the degree derive in **part (a)**, we know $|\text{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] = 4$. Then, since $4 = 2^2$ (which the group has order prime square), then not only Gal$(L/\mathbb{Q})$ is abelian, we know it is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Now, we'll consider $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}) \subseteq L$ respectively:

- First, since $[L:\mathbb{Q}] = 4$ and $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$, then we must have $[L:\mathbb{Q}(\sqrt{2})] = 2$. Hence, $|\text{Gal}(L/\mathbb{Q}(\sqrt{2}))| = [L:\mathbb{Q}(\sqrt{2})] = 2$, showing that $\text{Gal}(L/\mathbb{Q}(\sqrt{2})) \cong \mathbb{Z}_2$. Which, Since $L = \mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$ (and we know this is isomorphic to $\mathbb{Q}(\sqrt{2})[x]/(x^2-3)$ with the map $\overline{x} \mapsto \sqrt{3}$ based on the relation proven in **part (a)**), hence, since $\mathbb{Q}(\sqrt{2})[x]/(x^2-3)$ has an automorphism given by $\overline{x} \mapsto -\overline{x}$ (which fixes all elements in $\mathbb{Q}(\sqrt{2})$), as a consequence, this means it has a corresponding automorphism $\sigma \in \text{Gal}(L/\mathbb{Q}(\sqrt{2}))$ that is characterized by $\sigma(\sqrt{3}) = \sigma(-\sqrt{3})$.
- Then, using similar logic, we know $[L:\mathbb{Q}] = 4$ and $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2$, showing that $[L:\mathbb{Q}(\sqrt{3})] = 2$ also, so $|\text{Gal}(L/\mathbb{Q}(\sqrt{3}))| = [L:\mathbb{Q}(\sqrt{3})] = 2$, showing that $\text{Gal}(L/\mathbb{Q}(\sqrt{3})) \cong \mathbb{Z}_2$. Again, since $L = \mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt{2})$, $L/\mathbb{Q}(\sqrt{3})$ is a degree 2 extension implies that $\sqrt{2}$ has the minimal polynomial over $\mathbb{Q}(\sqrt{3})$ being degree 2; then, because it is a root of x^2-2 while this polynomial is monic and with degree 2, then x^2-2 must be the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}(\sqrt{3})$. Hence, $L = \mathbb{Q}(\sqrt{3})(\sqrt{2}) \cong \mathbb{Q}(\sqrt{3})[x]/(x^2-2)$. Notice that $\mathbb{Q}(\sqrt{3})[x]/(x^2-2)$ again has an automorphism given by $\overline{x} \mapsto -\overline{x}$ that fixes $\mathbb{Q}(\sqrt{3})$, while the field has an isomorphism to L given by $\overline{x} \mapsto \sqrt{2}$, then under suitable compositions, we get that there exists an automorphism $\psi \in \text{Gal}(L/\mathbb{Q}(\sqrt{3}))$ that satisfies $\psi(\sqrt{2}) = -\sqrt{2}$.

From the aobve, we have two automorphisms acting on the set of roots $\{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}\}$.

$\sigma \in \text{Aut}(L/\mathbb{Q}(\sqrt{2}))$ fixes $\sqrt{2}, -\sqrt{2}$, while acting as a transposition $(\sqrt{3}, -\sqrt{3})$; on the other hand, $\psi \in \text{Aut}(L/\mathbb{Q}(\sqrt{3}))$ fixes $\sqrt{3}, -\sqrt{3}$, while acting as a transposition $(\sqrt{2}, -\sqrt{2})$.

Now, if composition the two together, we get that $\psi \circ \sigma \in \text{Gal}(L/\mathbb{Q})$ is characterized by the composition of transpositions $(\sqrt{2}, -\sqrt{2})(\sqrt{3}, -\sqrt{3})$ (which is an order 2 permutation, since it is composed by two disjoint transpositions, which both have order 2).

Then, notice that σ, ψ, $\psi \circ \sigma$, $\text{Id}_L \in \text{Gal}(L/\mathbb{Q})$ all represents different elements (since they each correspond to a different permutation), together with the fact that $|\text{Gal}(L/\mathbb{Q})| = 4$, these must be all the elements.

On the other hand, notice that none of the element has order 4 (since σ, ψ are both transpositions, while $\psi \circ \sigma$ has order 2, since it is a composition of two disjoint transpositions), then this implies that $\text{Gal}(L/\mathbb{Q}) = \{\text{Id}_L, \sigma, \psi, \psi \circ \sigma\}$ cannot be isomorphic to $\mathbb{Z}_4$. Then, we must have $\text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(c) Finally, since $\sqrt{6} = \sqrt{2} \cdot \sqrt{3} \in L$, and it satisfies $(\sqrt{6})^2 - 6 = 0$, hence it is a root of $x^2 - 6 \in \mathbb{Q}[x]$. However, since this polynomial is irreducible and monic (because the roots $\pm\sqrt{6} \notin \mathbb{Q}$, so as a degree 2 polynomial with no roots in $\mathbb{Q}$, it is irreducible), it is the minimal polynomial of $\sqrt{6}$. Then, we have $\mathbb{Q}(\sqrt{6}) \cong \mathbb{Q}[x]/(x^2-6)$, hence $[\mathbb{Q}(\sqrt{6}):\mathbb{Q}] = 2$. As a consequence, $[L:\mathbb{Q}(\sqrt{6})] = 2$, showing that $|\text{Gal}(L/\mathbb{Q}(\sqrt{6}))| = [L:\mathbb{Q}(\sqrt{6})] = 2$.

Now, we know $\text{Id}_L \in \text{Gal}(L/\mathbb{Q}(\sqrt{6}))$; also, if consider $\psi \circ \sigma \in \text{Gal}(L/\mathbb{Q})$, we know it acts on the roots as composition of disjoint transpositions $(\sqrt{2}, -\sqrt{2})(\sqrt{3}, -\sqrt{3})$. Then, if plug in $\sqrt{6}$, we get:

$$\psi \circ \sigma(\sqrt{6}) = \psi \circ \sigma(\sqrt{2}) \cdot \psi \circ \sigma(\sqrt{3}) = (-\sqrt{2})(-\sqrt{3}) = \sqrt{6} \tag{7}$$

Then, because $\psi \circ \sigma$ fixes the generator $\sqrt{6}$ of $\mathbb{Q}(\sqrt{6})$, then $\psi \circ \sigma$ fixes $\mathbb{Q}(\sqrt{6})$. Hence, it belongs to $\text{Gal}(L/\mathbb{Q}(\sqrt{6}))$.

Which, because it is a group of order 2, and we have the above two distinct elements, then $\text{Gal}(L/\mathbb{Q}(\sqrt{6})) = \{\text{Id}_L, \psi \circ \sigma\}$ (corresponds to $\{e, (\sqrt{2}, -\sqrt{2})(\sqrt{3}, -\sqrt{3})\}$ as sets of permutations).

5

Question 5 *The Galois group of a polynomial $f(x)$ over a perfect field F is defined as $Gal(K/F)$ where K is a splitting field of $f(x)$. Find the Galois groups of x^6-1 over $\mathbb{F}_5$, $\mathbb{F}_{5^2}$, and $\mathbb{F}_{5^3}$.*

Pf:

1. Relations of the 6^{th} Roots of Unity in Arbitrary Field:

Before starting, just based on factorization, we know $x^6-1=(x^3-1)(x^3+1)=(x-1)(x^2+x+1)(x+1)(x^2-x+1)$. So, the splitting field of x^6-1 is the same as the splitting field of (x^2+x+1) and (x^2-x+1).

Also, the roots of the two polynomials above are also related: Let α be a root of x^2-x+1 (so $\alpha\neq 0$, since 0 is not a root of x^2-x+1), then if consider α^{-1}, we get the following relationship:

$$\alpha^2\neq 0,\quad \alpha^2(\alpha^{-2}-\alpha^{-1}+1)=1-\alpha+\alpha^2=0\implies \alpha^{-2}-\alpha^{-1}+1=0 \tag{8}$$

Hence, α^{-1} is also a root of x^2-x+1. Notice that $\alpha^{-1}\neq\alpha$, since if they're the same (which $\alpha^{-1}=\alpha\implies\alpha^2=1$), then we must have $\alpha=\pm 1$; but since ± 1 are not the roots of x^2-x+1, it'll form a contradiction. So, the roots of x^2-x+1 are α,α^{-1}.

On the other hand, if consider $-\alpha$, notice that it satisfies the following equation:

$$(-\alpha)^2+(-\alpha)+1=\alpha^2-\alpha+1=0 \tag{9}$$

Hence, $-\alpha$ is a root of x^2+x+1. On the other hand, if consider $-\alpha^{-1}$, we also get the following:

$$\alpha^2((-\alpha^{-1})^2+(-\alpha^{-1})+1)=\alpha^2(\alpha^{-2}-\alpha^{-1}+1)=1-\alpha+\alpha^2=0\implies(-\alpha^{-1})^2+(-\alpha^{-1})+1=0 \tag{10}$$

So, this implies that $-\alpha^{-1}$ is also a root of x^2+x+1. Beforehand, we alreay know $\alpha^{-1}\neq\alpha$, hence $-\alpha^{-1}\neq-\alpha$. So, the roots of x^2+x+1 is then given by $-\alpha,-\alpha^{-1}$.

As a conclusion, the splitting field of x^2-x+1 (regardless of the base field) automatically contains all the roots of x^2+x+1, hence it forms a splitting field of x^6-1 (since the potential nonlinear factors $(x^2-x+1),(x^2+x+1)$ all splits completely over the splitting field of x^2-x+1, and it cannot have any smaller fields with this property). So, for the below sections, we'll directly consider the splitting field of x^2-x+1.

2. Galois Group of x^6-1 over $\mathbb{F}_5$:

Given x^2-x+1 over $\mathbb{F}_5$, the following are the results if we plug in the elements:

$$\begin{cases}0^2-0+1=1\neq 0\\ 1^2-1+1=1\neq 0\\ 2^2-2+1=4-2+1=3\neq 0\\ 3^2-3+1=(9\mod 5)-3+1=4-3+1=2\neq 0\\ 4^2-4+1=(16\mod 5)-4+1=1-4+1=(-2\mod 5)=3\neq 0\end{cases} \tag{11}$$

Hence, since x^2-x+1 is a degree 2 polynomial with no roots in $\mathbb{F}_5$, it is irreducible over $\mathbb{F}_5$. Then, its splitting field can be obtained through $K=\mathbb{F}_5[x]/(x^2-x+1)$ (since this is the smallest field containing the root of $x^2 - x + 1$, and because it's degree 2, it automatically contains all the possible roots). Hence, $K/\mathbb{F}_5$ is a splitting field of $x^2 - x + 1$, hence a splitting field of $x^6 - 1$.

Which, because $[K : \mathbb{F}_5] = \deg(x^2 - x + 1) = 2$, then as a consequence, $|\text{Gal}(K/\mathbb{F}_5)| = [K : \mathbb{F}_5] = 2$, showing that $\text{Gal}(K/\mathbb{F}_5) \cong \mathbb{Z}_2$. So, the Galois Group of $x^6 - 1$ over $\mathbb{F}_5$ is $\mathbb{Z}_2$.

3. Galois Group of $x^6 - 1$ over $\mathbb{F}_{5^2}$:

Recall that $\mathbb{F}_{5^2}$ is obtained by considering a splitting field of $x^{5^2} - x \in \mathbb{F}_5[x]$. Which, this polynomial has the following factorization:

$$x^{5^2} - x = x(x^{24} - 1) = x(x^{12} - 1)(x^{12} + 1) = x(x^6 - 1)(x^6 + 1)(x^{12} + 1) \tag{12}$$

Then, since $x^{5^2} - x$ splits completely over $\mathbb{F}_{5^2}$, as a liner factor of it, $x^6 - 1$ must also split completely over $\mathbb{F}_{5^2}$. Since this is the base field, then $x^6 - 1$ has splitting field $\mathbb{F}_{5^2}$ over the base field that's also the same. Hence, its galois group $\text{Gal}(\mathbb{F}_{5^2}/\mathbb{F}_{5^2}) = \{\text{Id}_{\mathbb{F}_{5^2}}\}$, which is a trivial group.

4. Galois Group of $x^6 - 1$ over $\mathbb{F}_{5^3}$:

First, we need to find the splitting field of $x^2 - x + 1$ over $\mathbb{F}_{5^3}$, and we'll claim that it doesn't have a root in $\mathbb{F}_{5^2}$ (which as a consequence it doesn't split over $\mathbb{F}_{5^3}$ since it is a degree 2 polynomial).

Suppose the contrary that $x^2 - x + 1$ has roots in $\mathbb{F}_{5^3}$, since we know the prime field of $\mathbb{F}_{5^3}$ is $\mathbb{F}_5$, and $x^2 - x + 1$ doesn't have any root in $\mathbb{F}_5$, then let $\alpha \in \mathbb{F}_{5^3}$ be a root of $x^2 - x + 1 \in \mathbb{F}_5[x]$, we know $\mathbb{F}_5(\alpha) \subseteq \mathbb{F}_{5^3}$. However, since $x^2 - x + 1$ is proven to be irreducible over $\mathbb{F}_5$ in **section 2** of this question, with it being monic and α being its root, it is a minimal polynomial of α. Hence, $\mathbb{F}_5(\alpha) \cong \mathbb{F}_5[x]/(x^2 - x + 1)$, showing that $[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = 2$. But, since we know $[\mathbb{F}_{5^3} : \mathbb{F}_5] = 3$, and $\mathbb{F}_5 \subseteq \mathbb{F}_5(\alpha) \subseteq \mathbb{F}_{5^3}$, then we must have $[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = 2 \mid 3 = [\mathbb{F}_{5^3} : \mathbb{F}_5]$, which is a contradiction.

Therefore, our assumption is false, $x^2 - x + 1$ cannot have a root in $\mathbb{F}_{5^3}$, which further implies that it is irreducible over $\mathbb{F}_{5^3}$. Now, consider $K = \mathbb{F}_{5^3}[x]/(x^2 - x + 1)$, it is the smallest field extension of $\mathbb{F}_{5^3}$ containing the roots of $x^2 - x + 1$, which forms a splitting field of it. Hence, $[K : \mathbb{F}_{5^3}] = \deg(x^2 - x + 1) = 2$. As a consequence, since it is also a splitting field of $x^6 - 1$, then the galois group of $x^6 - 1$ has $|\text{Gal}(K/\mathbb{F}_{5^3})| = [K : \mathbb{F}_{5^3}] = 2$, showing that $\text{Gal}(K/\mathbb{F}_{5^3}) \cong \mathbb{Z}_2$.