Math 111C HW6

Zih-Yu Hsieh

May 22, 2025

1

Question 1 *Let E be a splitting field of $f(x) \in F[x]$ and $G = Aut(E/F)$. Prove that:*

(a) If $f(x)$ is irreducible, then G acts transitively on the set of all roots of $f(x)$, i.e. if α, β are two roots of $f(x)$ in E, there exists $\sigma \in G$ with $\sigma(\alpha) = \beta$.

(b) If $f(x)$ has no repeated roots and G acts transitively on the roots, then $f(x)$ is irreducible.

Pf:

(a) Suppose $f(x) \in F[x]$ is irreducible, then let $a \in F$ be the leading coefficient of $f(x)$ (which $a \neq 0$), then $a^{-1}f(x)$ is a monoic polynomial. For any roots of $f(x)$ in E, denoted as $\alpha, \beta \in E$, since $a^{-1}f(\alpha) = a^{-1}f(\beta) = 0$, while $a^{-1}f(x)$ is an irreducible monic polynomial in $F[x]$, then it must be the minimal polynomial of α and β. Hence, $F(\alpha) \cong F[x]/(a^{-1}f(x)) \cong F(\beta)$, and an explicit isomorphism is given as $\varphi : F(\alpha) \tilde{\to} F(\beta)$ by:

$$\forall a_0, a_1, ..., a_n \in F, \quad \varphi(a_n\alpha^n + ... + a_1\alpha + a_0) = a_n\beta^n + ... + a_1\beta + a_0$$

Now, notice the following information:

- For all $k \in F$, $\varphi(k) = k$ (which φ fixes F, or $\varphi\big|_F = \mathrm{Id}_F$).
- Since E/F is a splitting field of $f(x)$, then E/F is an algebraic extension, hence there exists an algebraic closure $\overline{F}$ of F, such that $F \subseteq E \subseteq \overline{F}$.
- Because $\alpha, \beta \in E$ are roots of $f(x) \in F[x]$, then they're algebraic over F, hence $F(\alpha), F(\beta)$ are algebraic extensions of F, with $F(\alpha), F(\beta) \subseteq E$. With the fact that E/F is algebraic and $F \subseteq F(\alpha) \subseteq E$, then $E/F(\alpha)$ is also an algebraic extension.
- Because $F \subseteq F(\alpha) \subseteq \overline{F}$, while $\overline{F}/F$ is an algebraic extension, then $\overline{F}/F(\alpha)$ is an algebraic extension; since $\overline{F}$ is itself algebraically closed, it is also an algebraic closure of $F(\alpha)$.

So, composing the inclusion $F(\beta) \hookrightarrow \overline{F}$, the isomorphism $\varphi : F(\alpha) \tilde{\to} F(\beta)$ can be extended to an embedding $\varphi : F(\alpha) \to \overline{F}$, which is also an F-embedding (since φ fixes F). Furthermore, since $E/F(\alpha)$ is an algebraic extension, while $F(\alpha)$ is embedded into $\overline{F}$ (its own algebraic closure also), then such embedding $\varphi : F(\alpha) \to \overline{F}$ can be extended to an embedding $\sigma : E \to \overline{F}$, such that $\sigma\big|_{F(\alpha)} = \varphi$. So, $\sigma\big|_F = \varphi\big|_F = \mathrm{Id}_F$.

Then, the final step is to claim that $\sigma(E) = E$, or $\sigma \in \mathrm{Aut}(E/F)$ after restricting the codomain.

Since $f(x) \in F[x]$, while σ fixes F, then after extending the F-embedding $\sigma : E \to \overline{F}$ to a canonical ring homomorphism $\overline{\sigma} : E[x] \to \overline{F}[x]$ (which $\overline{\sigma}(a) = \sigma(a)$ and $\overline{\sigma}(x) = x$ for all $a \in E$, so this map is injective), then $\overline{\sigma}(f(x)) = f(x)$ (since all of its coefficients are in F, while σ fixes F). So, since $\sigma(E) \cong E$, while $\overline{\sigma}$ preserves $f(x)$, then $\sigma(E)$ is also a splitting field of $f(x)$ under $\overline{F}$. However, since $\overline{F}$ is chosen in a way such that $E \subseteq \overline{F}$, then because a splitting field of a polynomial $f(x) \in F[x]$ is unique when chosen a larger algebraic extension of F such that f splits completely, then $E, \sigma(E) \subseteq \overline{F}$ while both being a splitting field of $f(x)$ implies that $E = \sigma(E)$, hence restricting the codomain of σ to the range, we get that $\sigma : E \tilde{\to} E$, which $\sigma \in \mathrm{Aut}(E)$. Finally, since we've proven that $\sigma \big|_F = \mathrm{Id}_F$, then $\sigma \in \mathrm{Aut}(E/F) = G$.

Hence, because $\sigma \in G$, while $\sigma \big|_{F(\alpha)} = \varphi$, and $\varphi(\alpha) = \beta$ based on the setup, then $\sigma(\alpha) = \beta$. So, this proves that G acts transitively on the set of all roots of $f(x)$.

(b) Suppose $f(x)$ has no repeated roots, while G acts transitively on the roots, then for any two roots of $f(x)$, denote as $\alpha, \beta \in E$, there exists $\sigma \in G = \mathrm{Aut}(E/F)$, such that $\sigma(\alpha) = \beta$. Then, since $F(\alpha), F(\beta) \subseteq E$ are finite extensions of F, let $\varphi = \sigma \big|_{F(\alpha)}$, then we get the following:

$$\forall a_0, a_1, ..., a_n \in F, \quad \varphi(a_0 + a_1\alpha + ... + a_n\alpha^n) = \sigma(a_0 + a_1\alpha + ... + a_n\alpha^n) = a_0 + a_1\beta + ... + a_n\beta^n$$

This proves that $\varphi(F(\alpha)) = F(\beta)$ (since choice of $a_0, a_1, ..., a_n \in F$ are arbitrary), so after restricting the codomain, $\varphi : F(\alpha) \tilde{\to} F(\beta)$ is in fact an isomorphism.

Now, consider the minimal polynomials $m_{\alpha,F}(x), m_{\beta,F}(x) \in F[x]$: First, since $m_{\alpha,F}(\alpha) = 0$, while all of its coefficients are in F, then we get:

$$\varphi(0) = \varphi(m_{\alpha,F}(\alpha)) = m_{\alpha,F}(\beta) = 0$$

So, this implies that $m_{\beta,F}(x) \mid m_{\alpha,F}(x)$ (since β is a root of $m_{\alpha,F}(x)$). Then, because both $m_{\alpha,F}(x)$ and $m_{\beta,F}(x)$ are irreducible in $F[x]$, then $m_{\beta,F}(x) \mid m_{\alpha,F}(x)$ implies that $m_{\alpha,F}(x) = k \cdot m_{\beta,F}(x)$, where $k \in (F[x])^\times = F^\times$; but since both polynomials are monic, then $k = 1$. So, $m_{\beta,F}(x) = m_{\alpha,F}(x)$. This implies that all roots of $f(x)$ must have the same minimal polynomial. Hence, WLOG, let $m(x) \in F[x]$ be the minimal polynomial of all roots of $f(x)$ in E.

Finally, since all roots of $f(x)$ has minimal polynomial $m(x) \in F[x]$, then $m(x) \mid f(x)$, so $\deg(m) \leq \deg(f)$; on the other hand, since E is a splitting field of f, while f is assumed to have no repeated roots, then let $n = \deg(f)$, it implies that there are n distinct roots of f in E. Since they're all having $m(x)$ as the minimal polynomial, they're all roots of $m(x)$, so m has at least n distinct roots, showing that $\deg(m) \geq n = \deg(f)$. So, this enforces $\deg(m) = \deg(f)$. And, because $m(x) \mid f(x)$, then $f(x) = k \cdot m(x)$ for some $k \in F^\times$. Which, since $m(x) \in F[x]$ is irreducible (because it's a minimal polynomial of some elements in E), then $f(x)$ as a nonzero constant multiple of $m(x)$ is also irreducible. This finishes the proof.

2

Question 2 *In each part, find the degree of the extension K/F.*

(a) Splitting field $K \subseteq \mathbb{C}$ of $f(x) = x^4 - 4$ over $F = \mathbb{Q}$.

(b) Splitting field $K \subseteq \mathbb{C}$ of $f(x) = x^6 - 2$ over $F = \mathbb{Q}$.

(c) Splitting field K of $f(x) = x^{10} - 2$ over $F = \mathbb{F}_5$.

Pf:

(a) Notice that $\sqrt{2}, -\sqrt{2}, \sqrt{2}i, -\sqrt{2}i \in \mathbb{C}$ all satisfies $x^4 = 4$, so they're all the roots of $x^4 - 4 \in \mathbb{Q}[x]$ over $\mathbb{C}$. Hence, the splitting field of $x^4 - 4 \in \mathbb{Q}[x]$ is $K = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{2}i, -\sqrt{2}i)$.

Now, notice that $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$; on the other hand, since $\sqrt{2}i \in K$, then $i = \frac{\sqrt{2}i}{\sqrt{2}} \in K$, which indicates that the field $\mathbb{Q}(\sqrt{2}, i) \subseteq K$.

Furthermore, since $\sqrt{2}, -\sqrt{2}, \sqrt{2}i, -\sqrt{2}i$ can all be generated by $\sqrt{2}$ and i, then we can also deduce that $K = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{2}i, -\sqrt{2}i) \subseteq \mathbb{Q}(\sqrt{2}, i)$. So, we can conclude that $K = \mathbb{Q}(\sqrt{2}, i)$.

Then, consider the relation $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq K = \mathbb{Q}(\sqrt{2}, i)$: Since $\sqrt{2} \notin \mathbb{Q}$, and it satisfies $(\sqrt{2})^2 - 2 = 0$, then it is a root of $x^2 - 2 \in \mathbb{Q}[x]$. Since this polynomial satisfies Eisenstein Criterion for prime $p = 2$, it is irreducible; and since it is also monic, while $\sqrt{2}$ is its root, then $x^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$. Hence, $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$, which indicates that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Also, If consider $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2})(i)$, since $i \notin \mathbb{Q}(\sqrt{2})$, while i satisfies $(i)^2 + 1 = 0$, then it is a root of $x^2 + 1 \in \mathbb{Q}[x]$. Which, since this polynomial has no roots in $\mathbb{Q}(\sqrt{2})$ (since all $q \in \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ has $q^2 > 0$, so no q satisfies $q^2 = -1$, or $q^2 + 1 = 0$), then it is irreducible over $\mathbb{Q}(\sqrt{2})$. Together with the fact that $x^2 + 1$ is monic, it is the minimal polynomial of i over $\mathbb{Q}(\sqrt{2})$. So, $\mathbb{Q}(\sqrt{2})(i) \cong \mathbb{Q}(\sqrt{2})[x]/(x^2 + 1)$, which indicates that $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$.

Finally, with the above two degrees of field extension, we get:

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

(b) Notice that for all integer $0 \leq k \leq 5$ (6 distinct entries), we have $2^{1/6} e^{2\pi i \cdot k/6} \in \mathbb{C}$ satisfies the equation $(2^{1/6} e^{2\pi i \cdot k/6})^6 - 2 = 0$. Then, since these are all distinct (6 distinct roots), while $x^6 - 2 \in \mathbb{Q}[x]$ can have at most 6 distinct roots, then these must be all the roots of $x^6 - 2$ over $\mathbb{C}$. Which, since K is the splitting field of $x^6 - 2$, it is precisely the field obtained by $\mathbb{Q}$ adjoining all the above roots.

Now, since $2^{1/6}, 2^{1/6} \cdot e^{2\pi i/6} \in K$, then let $\zeta_6 = e^{2\pi i/6}$, we get that $\zeta_6 = \frac{2^{1/6} \cdot e^{2\pi i/6}}{2^{1/6}} \in K$. Hence, the field $\mathbb{Q}(2^{1/6}, \zeta_6) \subseteq K$. On the other hand, each root of $x^6 - 2$ over $\mathbb{C}$ is in the form $2^{1/6} \cdot e^{2\pi i \cdot k/6} = 2^{1/6} \cdot \zeta_6^k$ for some integer $0 \leq k \leq 5$, this shows that each root $2^{1/6} \cdot e^{2\pi i \cdot k/6} \in \mathbb{Q}(2^{1/6}, \zeta_6)$, hence $K \subseteq \mathbb{Q}(2^{1/6}, \zeta_6)$, which together with the previous inclusion shows that $K = \mathbb{Q}(2^{1/6}, \zeta_6)$.

Then, consider the relation $\mathbb{Q} \subseteq \mathbb{Q}(2^{1/6}) \subseteq K = \mathbb{Q}(2^{1/6}, \zeta_6)$: First, since $2^{1/6} \notin \mathbb{Q}$ is a root of $x^6 - 2 \in \mathbb{Q}[x]$, and this polynomial satisfies the Eisenstein Criterion for prime $p = 2$, then it is irreducible; together with the fact that it is monic, then it must be the minimal polynomial of $2^{1/6}$ over $\mathbb{Q}$. Hence, $\mathbb{Q}(2^{1/6}) \cong \mathbb{Q}[x]/(x^6 - 2)$, showing that $[\mathbb{Q}(2^{1/6}) : \mathbb{Q}] = 6$.

Also, if consider the $\mathbb{Q}(2^{1/6},\zeta_6)=\mathbb{Q}(2^{1/6})(\zeta_6)$, since $\zeta_6\notin\mathbb{R}$, while $\mathbb{Q}(2^{1/6})\subset\mathbb{R}$, then ζ_6 must have its minimal polynomial with degree ≥ 2; on the other hand, given the polynomial $x^2-x+1\in\mathbb{Q}(2^{1/6})[x]$, using quadratic formula, we get the roots are given by:

$$\alpha=\frac{-(-1)\pm\sqrt{(-1)^2-4\cdot 1\cdot 1}}{2\cdot 1}=\frac{1\pm\sqrt{-3}}{2}$$

Which, since $\zeta_6=e^{2\pi i/6}=\frac{1+\sqrt{3}}{2}$, then ζ_6 is a root of x^2-x+1. Then, let $m(x)\in\mathbb{Q}(2^{1/6})[x]$ be the minimal polynomial of ζ_6 over $\mathbb{Q}(2^{1/6})$, ζ_6 being a root of x^2-x+1 implies $m(x)\mid(x^2-x+1)$, which $\deg(m)\leq 2$; on the other hand, we know $m(x)$ is proven to have degree ≥ 2, this enforces $\deg(m)=2$. Which, $m(x)$ divides x^2-x+1, thw two polynomials are both degree 2, while x^2-x+1 is monic, indicates that $m(x)=x^2-x+1$. So, $\mathbb{Q}(2^{1/6})(\zeta_6)\cong\mathbb{Q}(2^{1/6})[x]/(m(x))=\mathbb{Q}(2^{1/6})[x]/(x^2-x+1)$, which shows that $[\mathbb{Q}(2^{1/6},\zeta_6):\mathbb{Q}(2^{1/6})]=2$.

Finally, combine all the degree of extensions from above, we get:

$$[K:\mathbb{Q}]=[\mathbb{Q}(2^{1/6},\zeta_6):\mathbb{Q}(2^{1/6})]\cdot[\mathbb{Q}(2^{1/6}):\mathbb{Q}]=2\cdot 6=12$$

(c) Given $f(x)=x^{10}-2$ over $\mathbb{F}_5$. Notice that within $\mathbb{F}_5$, the following equality is true:

$$2^5=(2^2)^2\cdot 2=4^2\cdot 2=(16\mod 5)\cdot 2=1\cdot 2=2$$

Hence, with the fact that $\mathbb{F}_5[x]$ has characteristic 5, using Frobenius Endomorphism, we get:

$$x^{10}-2=(x^2)^5-2^5=(x^2-2)^5$$

Hence, all the roots of $x^{10}-2$ are precisely the roots of x^2-2, which K as a splitting field of $x^{10}-2$, is the same field as $\mathbb{F}_5$ adjoining the roots of $x^{10}-2$ that's within K, which is the same as $\mathbb{F}_5$ adjoining the roots of x^2-2, so it is also a splitting field of x^2-2. Hence, it suffices to show the degree of any splitting field K of x^2-2 as a field extension of $\mathbb{F}_5$.

Now, notice that within $\mathbb{F}_5$, $0^2=0$, $1^2=1$, $2^2=4$, $3^2=(9\mod 5)=4$, and $4^2=(16\mod 5)=1$. So, since no element in $\mathbb{F}_5$ satisfies $x^2=2$, then $x^2-2\in\mathbb{F}_5[x]$ has no roots in $\mathbb{F}_5$, showing that it is irreducible over $\mathbb{F}_5$. This shows that the splitting field $K\neq\mathbb{F}_5$, which $[K:\mathbb{F}_5]\geq 2$.

Then, since the field extension $K'=\mathbb{F}_5[x]/(x^2-2)$ contains a root of $x^2-2\in\mathbb{F}_5[x]\subset K'[x]$, namely the element $\theta=\overline{x}\in K'$ (and $[K':\mathbb{F}_5]=2$). Then, x^2-2 has a linear factor in $K'[x]$, showing that it splits completely over K'. So, if consider the splitting field of x^2-2, $K''\subseteq K'$, then we know $[K'':\mathbb{F}_5]\leq[K':\mathbb{F}_5]=2$.

Which, since all splitting fields of $x^2-2\in\mathbb{F}_5[x]$ are all isomorphic, then $K\cong K''$, which shows that $[K:\mathbb{F}_5]=[K'':\mathbb{F}_5]\leq 2$. Which, with both inequalities of $[K:\mathbb{F}_5]$ above, we can conclude the following:

$$[K:\mathbb{F}_5]=2$$

3

Question 3 *Let L be the splitting field of $f(x) = x^3 + x + 1$ over $\mathbb{Q}$ contained in $\mathbb{C}$. Prove that $Aut(L/\mathbb{Q}) \cong S_3$.*

Pf:

First, we'll get some information about the roots of $f(x)$: Since it is a cubic polynomial, it must have at least a real root; On the other hand, as a real differentiable function, its derivative is $3x^2+1$, which is always positive, this indicates that $f(x)$ is strictly increasing on the whole domain $\mathbb{R}$, which is injective. Therefore, it can have at most 1 real root. This indicates that f has a real root (denoted as $\alpha \in \mathbb{R}$), while the other two roots must be complex roots, and being the conjugate of each other (denoted as $\beta, \overline{\beta} \in \mathbb{C}$). Which, $L = \mathbb{Q}(\alpha, \beta, \overline{\beta})$ (since the splitting field of $f(x)$ is the same as adjoining the roots to the base field).

Notice that for any $\sigma \in \text{Aut}(L/\mathbb{Q})$, it is purely determined by the permutation of the three roots of $f(x)$: Suppose $k \in \{\alpha, \beta, \overline{\beta}\}$ (a root of $f(x)$), then since σ fixes coefficients $\mathbb{Q}$ while $f(x) \in \mathbb{Q}[x]$, then $0 = \sigma(0) = \sigma(f(k)) = f(\sigma(k))$, which shows that $\sigma(k)$ is a root of $f(x)$. On the other hand,if $k \in L$ satisfies $f(\sigma(k)) = 0$, then by similar reasoning, $\sigma(f(k)) = 0$, implying that $f(k) = 0$ (since σ is an automorphism), then k is a root of $f(x)$. So, σ can only send roots of $f(x)$ to roots of $f(x)$, and since σ is bijective, it in fact forms a permutation of the 3 roots of $f(x)$. On the other hand, since $L = \mathbb{Q}(\alpha, \beta, \overline{\beta})$, then the automorphism σ is purely determined by where the three roots go.

So, if we define the map $\text{Aut}(L/\mathbb{Q}) \to S_3$, by associating $\{\alpha, \beta, \overline{\beta}\}$ with $\{1, 2, 3\}$ in order, and $\sigma \mapsto \tau \in S_3$ iff σ permutes $\{\alpha, \beta, \overline{\beta}\}$ in the same way as τ acts on $\{1, 2, 3\}$ in the associated order. Then, this map is injective, because if two automorphisms σ_1, σ_2 permute the roots $\{\alpha, \beta, \overline{\beta}\}$ in the same way, since any automorphism in $\text{Aut}(L/\mathbb{Q})$ is purely determined on how they permute the given three roots, then $\sigma_1 = \sigma_2$. So, this shows that $\text{Aut}(L/\mathbb{Q})$ can be identified as a subgroup of S_3 (since the composition of two automorphisms acts on the roots in the same way of composing their associated permutations in S_3).

Then, notice that the conjugation map $\mathbb{C} \to \mathbb{C}$ when restricting to L is certainly a field automorphism of L, since it is an injective map (that is a field automorphism of $\mathbb{C}$), while for every finite $\mathbb{Q}$-combination of the finite products of $\alpha, \beta, \overline{\beta}$, the conjugation only affects each term of α, β, and $\overline{\beta}$. However, $\overline{\alpha} = \alpha$, while β and $\overline{\beta}$ are conjugates of each other, then for any $k \in L$, since it is a finite $\mathbb{Q}$-combination of products of $\alpha, \beta, \overline{\beta}$, then the conjugation maps k into L (since it acts on each individual $\alpha, \beta, \overline{\beta}$, which their conjugation is closed under L).

Based on the given order of the roots $\{\alpha, \beta, \overline{\beta}\}$, the conjugation map can be identified as the transposition $(2\ 3) \in S_3$. Which, since $(2\ 3)$ has order 2, then 2 divides $|\text{Aut}(L/\mathbb{Q})|$.

Also, from **Question 1** in this HW, we know because $f(x) = x^3 + x + 1$ has no roots in $\mathbb{Q}$ (based on rational root theorem, the only rational roots are ± 1, but none of them are the roots of $f(x)$, so $f(x)$ is a degree 3 polynomial with no roots, showing that it is irreducible over $\mathbb{Q}$), then because L is a splitting field of $f(x) \in \mathbb{Q}[x]$, then $\text{Aut}(L/\mathbb{Q})$ acts transitively on the set of roots $\{\alpha, \beta, \overline{\beta}\}$, so there exists $\sigma \in \text{Aut}(L/\mathbb{Q})$, such that $\sigma(\alpha) = \beta$. There are two scenarios:

1. If $\sigma(\beta) = \alpha$, then $\sigma(\overline{\beta}) = \overline{\beta}$. This indicates that σ only permutes α and β, which with the order of the roots identified as $\{\alpha, \beta, \overline{\beta}\}$, σ corresponds to the transposition $(1\ 2) \in S_3$. Then, since there exists an automorphism that corresponds to $(2\ 3)$ (namely the conjugation map), based on the following relationship, we get:
$$(1\ 2) \circ (2\ 3) \circ (1\ 2) = (1\ 2) \circ (1\ 3\ 2) = (1\ 3)$$

This indicates that we get automorphisms in $\mathrm{Aut}(L/\mathbb{Q})$ that corresponds to $(1\ 2),\ (2\ 3),\ (1\ 3) \in S_3$ respectively. Hence, with all three transpositions, it generates S_3. This indicates that $\mathrm{Aut}(L/\mathbb{Q}) \cong S_3$.

2. If $\sigma(\beta) = \overline{\beta}$ instead, then since σ doesn't fix any roots $\{\alpha, \beta, \overline{\beta}\}$, then it corresponds to a 3-cycle in S_3. So, σ must have order 3, showing that 3 divides $|\mathrm{Aut}(L/\mathbb{Q})|$. But, together with the fact that 2 divides $|\mathrm{Aut}(L/\mathbb{Q})|$, then 6 divides $|\mathrm{Aut}(L/\mathbb{Q})|$, showing that $|\mathrm{Aut}(L/\mathbb{Q})| \geq 6$. However, since there exists an injection from $|\mathrm{Aut}(L/\mathbb{Q})|$ into S_3 while $|S_3| = 6$, then $|\mathrm{Aut}(L/\mathbb{Q})| \leq 6$. With these two facts, $|\mathrm{Aut}(L/\mathbb{Q})| = 6$, and since $\mathrm{Aut}(L/\mathbb{Q})$ can be identified as a subgroup of S_3, the order of $\mathrm{Aut}(L/\mathbb{Q})$ and S_3 match implies that $\mathrm{Aut}(L/\mathbb{Q}) \cong S_3$.

In either case, we'll eventually derive the fact that $\mathrm{Aut}(L/\mathbb{Q}) \cong S_3$, which finishes the proof.

4

Question 4 *Calculate the splitting field of* $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$.

Pf:

First, since $0^3 + 0 + 1 = 1 \neq 0$, and $1^3 + 1 + 1 = 1 + 1 + 1 = 1 \neq 0$, then $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ has no roots in $\mathbb{F}_2$. Because it is a degree 3 polynomial, having no roots implies that it is irreducible over $\mathbb{F}_2$.

Now, consider the field $K = \mathbb{F}_2[x]/(x^3 + x + 1)$: Taken $\theta = \overline{x} \neq 0$, then it satisfies $\overline{x}^3 + \overline{x} + 1 = \overline{x^3 + x + 1} = 0$. Hence, for the same polynomial $f(y) = y^3 + y + 1 \in \mathbb{F}_2[y] \subset K[y]$, the element $\theta \in K$ is a root. This implies that $(y - \theta) \in K[x]$ is a linear factor of $f(y)$, so there exists $\alpha, \beta \in K$, such that the following factorization holds:

$$f(y) = y^3 + y + 1 = (y - \theta)(y^2 + \alpha y + \beta) = y^3 + (-\theta + \alpha)y^2 + (-\theta\alpha + \beta)y + (-\theta)\beta$$

Which, solving for coefficients, the constant coefficient is $1 = (-\theta)\beta = \theta\beta$, which indicates that $\beta = \theta^{-1} \in K$. Going deeper, we know that the following equation holds:

$$\theta^3 + \theta + 1 = \overline{x}^3 + \overline{x} + 1 = \overline{x^3 + x + 1} = 0, \implies \theta^3 + \theta = -1 = 1$$

$$\implies \theta(\theta^2 + 1) = 1 \implies \theta^{-1} = \theta^2 + 1$$

So, we can conclude that $\beta = \theta^2 + 1 \in K$.

On the other hand, if solving for the coefficient of y^2, we get that $0 = (-\theta) + \alpha$, which $\alpha = \theta$.

Hence, the first factorization is given by:

$$f(y) = y^3 + y + 1 = (y - \theta)(y^2 + \alpha y + \beta) = (y - \theta)(y^2 + \theta y + (\theta^2 + 1))$$

Now, consider the element $\theta^2 \in K$: If we plug it into the polynomial $y^2 + \theta y + (\theta^2 + 1) \in K[x]$, we get:

$$(\theta^2)^2 + \theta \cdot \theta^2 + (\theta^2 + 1) = \theta^3 \cdot \theta + \theta^3 \cdot 1 + (\theta + 1)^2 = \theta^3(\theta + 1) + (\theta + 1)^2 = (\theta^3 + \theta + 1)(\theta + 1) = 0$$

(Note: the second equality is true with $(\theta^2 + 1) = (\theta + 1)^2$ is because $K/\mathbb{F}_2$ is a characteristic-2 field, and the last equality is true since θ is a root of $y^3 + y + 1 \in K[x]$).

This shows that $\theta^2 \in K$ is a root of $y^2 + \theta y + (\theta^2 + 1) \in K[x]$, hence $(y - \theta^2)$ is a linear factor of it, which there exists $\gamma \in K$, such that the following holds:

$$y^2 + \theta y + (\theta^2 + 1) = (y - \theta^2)(y - \gamma)$$

So, within K, $f(y) = y^3 + y + 1$ can be factored as:

$$f(y) = y^3 + y + 1 = (y - \theta)(y + \theta y + (\theta^2 + 1)) = (y - \theta)(y - \theta^2)(y - \gamma)$$

Hence, $f(y)$ splits completely over K.

Finally, let $K' \subseteq K$ be the splitting field of $f(y)$ under K. Then, let $\alpha \in K'$ be the root of $f(y)$, we know $\mathbb{F}_2(\alpha) \subseteq K'$, which since $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ is proven to be irreducible, while being monic, then $f(\alpha) = 0$ implies that $f(x)$ is the minimal polynomial of α over $\mathbb{F}_2$. Hence, $\mathbb{F}_2(\alpha) \cong \mathbb{F}_2[x]/(x^3 + x + 1)$, which shows that $[F(\alpha) : \mathbb{F}_2] = 3$. However, since $K = \mathbb{F}_2[x]/(x^3 + x + 1)$, then $[K : \mathbb{F}_2] = 3$. So, since $\mathbb{F}_2(\alpha) \subseteq K' \subseteq K$, this enforces $\mathbb{F}_2(\alpha) = K$ (since they have the same dimension with base field $\mathbb{F}_2$), which further enforces $K' = K$. So, $K = \mathbb{F}_2[x]/(x^3 + x + 1)$ is a splitting field of $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$.

5

Question 5 *Let $f(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree 3. Prove that $f(x)$ is irreducible over $\mathbb{F}_{p^5}$.*

Pf:

Since $|\mathbb{F}_{p^5}| = p^5$, then as a field extension of $\mathbb{F}_p$, we must have $[\mathbb{F}_{p^5} : \mathbb{F}_p] = 5$ (Note: Given any finite extension $K/\mathbb{F}_p$, if $[K : \mathbb{F}_p] = k \in \mathbb{N}$, then the number of elements $|K| = p^k$).

Now, given $f(x) \in \mathbb{F}_p[x]$ that is irreducible with degree 3, we'll prove by contradiction that it is irreducible over $\mathbb{F}_{p^5}$. Suppose the contrary that it is reducible over $\mathbb{F}_{p^5}$, then since it is degree 3, being reducible in $\mathbb{F}_{p^5}$ implies there exists a root in $\mathbb{F}_{p^5}$.

Let $\alpha \in \mathbb{F}_{p^5}$ be a root of $f(x)$, then since $f(x) \in \mathbb{F}_p[x]$ is irreducible, and WLOG can assume it is monic (by multiplying by a^{-1}, where a is the leading coefficient of f), so we can treat $f(x)$ as the minimal polynomial of α over $\mathbb{F}_p$. Hence, $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^5}$.

However, since $f(x)$ has degree 3, then $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = 3$ based on the fact that $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p(\alpha)$; however, since $\mathbb{F}_p \subseteq \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^5}$, while $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ and $\mathbb{F}_{p^5}/\mathbb{F}_p$ are proven to be finite extensions from above, then we get the following:

$$5 = [\mathbb{F}_{p^5} : \mathbb{F}_p] = [\mathbb{F}_{p^5} : \mathbb{F}_p(\alpha)] \cdot [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_{p^5} : \mathbb{F}_p(\alpha)] \cdot 3$$

This indicates that $3 \mid 5$, yet this is a contradiction since 3 and 5 are coprime. So, our assumption is false, $f(x)$ must be irreducible over $\mathbb{F}_{p^5}$.