Assignment-1B

Galois Theory

Trishan Mondal

§ Problem 1

Problem. Determine the automorphism of the extension $\mathbb{Q}(\sqrt[4]{2})$ over $\mathbb{Q}(\sqrt{2})$. Give proper justifications.

Proof. We claim that $m_{\sqrt[4]{2},\mathbb{Q}(\sqrt{2})} = x^2 - \sqrt{2}$. To prove this, observe that $\sqrt[4]{2}$ is a root of $x^2 - \sqrt{2}$. Thus, it suffices to show that $x^2 - \sqrt{2}$ is irreducible over $\mathbb{Q}(\sqrt{2})$. Assuming the contrary would imply that it factors into linear terms over $\mathbb{Q}(\sqrt{2})$, leading to a contradiction. Therefore, $m_{\sqrt[4]{2},\mathbb{Q}(\sqrt{2})} = x^2 - \sqrt{2}$.

Since $x^2 - \sqrt{2} = (x - \sqrt[4]{2})(x + \sqrt[4]{2})$, we conclude that $\mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[4]{2})$ is the splitting field of $x^2 - \sqrt{2}$. To compute the group $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2}) \mid \mathbb{Q}(\sqrt{2}))$, we can focus on where the generator $\sqrt[4]{2}$ is mapped. Let $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2}) \mid \mathbb{Q}(\sqrt{2}))$. Since $\sigma(\sqrt[4]{2})$ must be a root of $x^2 - \sqrt{2}$, we have $\sigma(\sqrt{2}) = \pm\sqrt[4]{2}$. This implies that the order of the group $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2}) \mid \mathbb{Q}(\sqrt{2}))$ is at most 2. By the Isomorphism Extension Theorem, we can find σ such that $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$ and $\sigma(\sqrt{2}) = -\sqrt[4]{2}$. Hence, $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2}) \mid \mathbb{Q}(\sqrt{2})) \cong \mathbb{Z}/2\mathbb{Z}$. ■

§ Problem 2

Problem. (a) Prove that any $\sigma \in \mathrm{Aut}(\mathbb{R} \mid \mathbb{Q})$ takes squares to squares and takes positive real numbers to positive real numbers.

(b) Prove that any $\sigma \in \mathrm{Aut}(\mathbb{R} \mid \mathbb{Q})$ is, thus, order preserving, i.e., if $a < b$, then $\sigma(a) < \sigma(b)$ for every $a, b \in \mathbb{R}$

(c) Prove that $-\frac{1}{m} < a - b < \frac{1}{m}$ implies $-\frac{1}{m} < \sigma(a) - \sigma(b) < \frac{1}{m}$. Hence prove that σ is a continuous map on $\mathbb{R}$.

(d) Prove that any continuous map on $\mathbb{R}$ which is identity on $\mathbb{Q}$ is the identity map, hence Aut $(\mathbb{R} \mid \mathbb{Q})$ is the trivial group.

Proof. **(a)** For any $\sigma \in \mathrm{Aut}(\mathbb{R} \mid \mathbb{Q})$, we have $\sigma(x^2) = \sigma(x)^2$, which implies that σ maps squares to squares. Take any positive real number $a > 0$, then $\sigma(a) = (\sigma(\sqrt{a}))^2 \geq 0$. Since σ is an automorphism and its kernel is $\{0\}$, we conclude that $\sigma(a) > 0$ for all $a > 0$.

(b) If $a < b$, then $b - a > 0$, and consequently, $0 < \sigma(b - a) = \sigma(b) - \sigma(a)$. This shows that σ is order-preserving.

(c) Observe that $\sigma(1) = 1$ as $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$. We also have, $\sigma\left(\frac{1}{m}\right) = \frac{1}{m}$. Now, let $-\frac{1}{m} < a - b < \frac{1}{m}$. Using part (b), we find:

$$-\frac{1}{m} = \sigma\left(-\frac{1}{m}\right) < \sigma(a) - \sigma(b) < \sigma\left(\frac{1}{m}\right) = \frac{1}{m}.$$

for any $\varepsilon > 0$, we can find $n_0 \in \mathbb{N}$ such that $\frac{1}{n} < \varepsilon$ for all $n \geq n_0$. Take $\delta = \frac{1}{n_0}$. Then, for all $|x - y| < \delta$, using the result above, we have $|\sigma(y) - \sigma(x)| < \varepsilon$. Thus, σ is uniformly continuous.

(d) Consider a continuous function $f : \mathbb{R} \to \mathbb{R}$ such that $f|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. For $x \in \mathbb{R} \setminus \mathbb{Q}$, there exists a sequence of rational numbers $\{r_n\}_{n \in \mathbb{N}} \subseteq \mathbb{Q}$ converging to x. Therefore, we have:

$$f(x) = f\left(\lim_{n\to\infty} r_n\right) = \lim_{n\to\infty} f(r_n) = \lim_{n\to\infty} r_n = x.$$

This shows that $f = \mathrm{id}_{\mathbb{R}}$. Consequently, if $\sigma \in \mathrm{Aut}(\mathbb{R} \mid \mathbb{Q})$, then, as shown in part (c), σ is continuous and equal to the identity on the rational numbers. Therefore, $\sigma = \mathrm{id}_{\mathbb{R}}$. Thus, Aut $(\mathbb{R} \mid \mathbb{Q})$ is the trivial group. ■

§ Problem 3

Problem. actor the polynomial $x^4 - 2$ into irreducible factors over each of the fields $\mathbb{Q}, \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, i), \mathbb{Q}(\sqrt[4]{2}), \mathbb{Q}(\sqrt[4]{2}, i)$, where $\sqrt[4]{2}$ is the positive real fourth root of 2.

Solution. Let's analyze the irreducibility of the polynomial $x^4 - 2$ over various fields:

- **Over $\mathbb{Q}$:** By Eisenstein's criteria for the prime $p = 2$, we can conclude that $x^4 - 2$ is irreducible over $\mathbb{Z}$. Since $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, by Gauss' Lemma, we deduce that $x^4 - 2$ is irreducible over $\mathbb{Q}$.
- **Over $\mathbb{Q}(\sqrt{2})$:** We factor $x^4 - 2$ as $(x^2 - \sqrt{2})(x^2 + \sqrt{2})$. We've previously established that $x^2 - \sqrt{2}$ is irreducible over $\mathbb{Q}(\sqrt{2})$. Additionally, since $a^2 + \sqrt{2} > 0$ for all $a \in \mathbb{R}$ (which includes $\mathbb{Q}(\sqrt{2})$), we can infer that $x^2 + \sqrt{2}$ does not split into linear factors over $\mathbb{Q}(\sqrt{2})$. Thus, $x^2 + \sqrt{2}$ is also irreducible over $\mathbb{Q}(\sqrt{2})$.
- **Over $\mathbb{Q}(\sqrt{2}, i)$:** We can observe that $x^4 - 2$ factors as $(x^2 - \sqrt{2})(x^2 + \sqrt{2})$ over $\mathbb{Q}(\sqrt{2}, i)$.
- **Over $\mathbb{Q}(\sqrt[4]{2})$:** We claim that $x^4 - 2$ factors as $(x^2 + \sqrt{2})(x - \sqrt[4]{2})(x + \sqrt[4]{2})$ over $\mathbb{Q}(\sqrt[4]{2})$. To establish this, it suffices to show that $x^2 + \sqrt{2}$ is irreducible over $\mathbb{Q}(\sqrt[4]{2})$. For any real number a, we have $a^2 + \sqrt{2} > 0$, ensuring that $x^2 + \sqrt{2}$ cannot be factored into linear terms over $\mathbb{Q}(\sqrt[4]{2})$, which is a subset of $\mathbb{R}$. Thus, $x^2 + \sqrt{2}$ remains irreducible over $\mathbb{Q}(\sqrt[4]{2})$.
- **Over $\mathbb{Q}(\sqrt[4]{2}, i)$:** We observe that $x^4 - 2$ splits into linear factors over $\mathbb{Q}(\sqrt[4]{2}, i)$ as $x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}i)(x + \sqrt[4]{2}i)$. ■

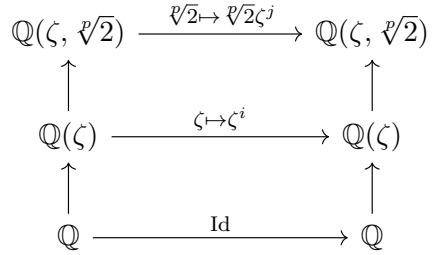
§ Problem 4

Problem. Let p be a prime. Determine the elements of the Galois group of $x^p - 2$ over $\mathbb{Q}$. Prove that this Galois group is isomorphic to the group of matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where $a, b \in \mathbb{F}_p, a \neq 0$, a subgroup of $GL_2(\mathbb{F}_p)$.

Proof. We assert that the splitting field of $x^p - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[p]{2}, \zeta)$, where ζ is a primitive p-th root of unity. All the roots of $x^p - 2$ are contained in the set $\left\{\sqrt[p]{2}\zeta^i \mid i = 0, 1, \ldots, p-1\right\}$, smallest field containg this set is by definition$\mathbb{Q}(\sqrt[p]{2}, \zeta)$. Consequently, $F = \mathbb{Q}(\sqrt[p]{2}, \zeta)$, solidifying it as the splitting field of $x^p - 2$ and thereby a normal extension. By **Eisenstein's criteria**, $x^p - 2$ is irreducible over $\mathbb{Z}$, and **Gauss' Lemma** implies that it's irreducible over $\mathbb{Q}$. As any irreducible polynomial over a characteristic-zero field is separable, $\mathbb{Q}(\sqrt[p]{2}, \zeta)$ is both normal and separable, establishing it as a Galois extension.

Note that $\left|\mathrm{Gal}(\mathbb{Q}(\sqrt[p]{2}, \zeta)/\mathbb{Q})\right| = [\mathbb{Q}(\sqrt[p]{2}, \zeta) : \mathbb{Q}] = p(p-1)$. Any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[p]{2}, \zeta) \mid \mathbb{Q})$ is defined by its action on the generators $\sqrt[p]{2}$ and ζ. Thus $\sigma(\sqrt[p]{2})$ must be a root of $x^p - 2$, we have $\sigma(\sqrt[p]{2}) \in \left\{\sqrt[p]{2}\zeta^i \mid i = 0, 1, \ldots, p-1\right\}$. Additionally, $\sigma(\zeta)$ must be a root of $\min_{\zeta,\mathbb{Q}}(x) = \sum_{i=0}^{p-1} x^i$, implying $\sigma(\zeta) = \zeta^a$ for some $a \in 1, 2, \ldots, p-1$.

We'll now show that there exist σ_{ij} such that $\sigma_{ij}(\sqrt[p]{2}) = \sqrt[p]{2}\zeta^j$ and $\sigma_{ij}(\zeta) = \zeta^i$, where $i \in \mathbb{F}_p^\times$ and $j \in \mathbb{F}_p$. By the Isomorphism Extension Theorem, there exists an extension σ_a of $\mathrm{Id}_{\mathbb{Q}}$ such that $\sigma_a(\zeta) = \zeta^a$. Using the same theorem again, there exists an extension σ_{ab} of σ_a such that $\sigma_{ab}(\sqrt[p]{2}) = \sqrt[p]{2}\zeta^b$.



Now we will show, the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt[p]{2}, \zeta)/\mathbb{Q})$ is isomorphic to the group $G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \right\}$, which is a subgroup of $GL_2(\mathbb{F}_p)$. We define a mapping φ as:

$$\varphi : \mathrm{Gal}(\mathbb{Q}(\sqrt[p]{2}, \zeta) \mid \mathbb{Q}) \to G, \quad \sigma_{ij} \mapsto \begin{pmatrix} i & j \\ 0 & 1 \end{pmatrix}$$

It can be shown that φ is a group homomorphism, surjective, and has $\ker(\varphi) = \mathrm{id}_{\mathbb{Q}}$, implying its injectiveness. Therefore, φ is an isomorphism, and we conclude that $\mathrm{Gal}(\mathbb{Q}(\sqrt[p]{2}, \zeta) \mid \mathbb{Q})$ is isomorphic to G. ■

§ Problem 5

Problem. Suppose that K is a Galois extension of F of degree p^n for some prime p and some $n \geq 1$. Show there are Galois extensions of F contained in K of degrees p and p^{n-1}.

Proof. Let $G = \mathrm{Gal}(K/F)$ be the Galois group of the extension K/F. Since K/F is a Galois extension of degree p^n, we have $|G| = p^n$. Now, let's consider the subgroups of G. By Lagrange's theorem, the order of any subgroup of G must divide the order of G, which is p^n. Since p is prime, the possible orders of subgroups are $1, p, p^2, \ldots, p^n$.

We are interested in finding Galois extensions of F contained in K. Each subgroup of G corresponds to a field fixed by that subgroup. Now, we want to find subgroups H such that $\mathcal{F}(H)/F$ has a certain degree. We are looking for two subgroups with degrees p and p^{n-1}, respectively.

- **Normal subgroup of degree p:** Consider the center of group G, $Z(G)$. By the class equation we can notice, order of $Z(G)$ must be divisable by p. Since it is a subgroup of a p-group it must have order p^r for some $1 \leq r \leq n$, it has a sub group H_1 of order p and $H_1 \in Z(G)$, i.e. $H_1 \trianglelefteq G$. The extension $\mathcal{F}(H_1)|_F$ is Galois and it has degree p^{n-1} by the **Galois correspondence theorem**.
- **Normal subgroup of degree p^{n-1}:** We have noticed $H_1 \trianglelefteq G$, G/H_1 is also a p-group it also have a normal subgroup of order p call it H_2/H_1. By fourth isomorphism theorem we can say $H_2 \trianglelefteq G$ and it has order p^2. Continuing this way we can get a subgroup $H \trianglelefteq G$ of order p^{n-1}. The extension $\mathcal{F}(H)|_F$ is Galois and it has degree p. ■

§ Problem 6

Problem. Show that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a cyclic extension of degree 4 over $\mathbb{Q}$.

Proof. We assert that minimal polynomial of $\sqrt{2+\sqrt{2}}$ over $\mathbb{Q}$ to be $x^4 - 4x^2 + 2$. Notably, $\sqrt{2+\sqrt{2}}$ is a root of $x^4 - 4x^2 + 2$, which can be observed from the following,

$$x^4 - 4x^2 + 2 = \left(x^2 - 2\right)^2 - 2,$$

From this expression, it becomes evident that $\sqrt{2+\sqrt{2}}$ is indeed a root of x^4-4x^2+2. Hence, it suffices to establish the irreducibility of x^4-4x^2+2 over $\mathbb{Q}$. Employing Eisenstein's criterion with $p=2$, we conclude that x^4-4x^2+2 is irreducible over $\mathbb{Z}$. Consequently, by Gauss' Lemma, it is also irreducible over $\mathbb{Q}$. Thus, x^4-4x^2+2 indeed represents the minimal polynomial of $\sqrt{2+\sqrt{2}}$ over $\mathbb{Q}$.

Subsequently, we ascertain $[\mathbb{Q}(\sqrt{2+\sqrt{2}}):\mathbb{Q}]=4$. To complete the proof, it remains to demonstrate the existence of an element of order 4 within $\mathrm{Aut}(\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q})$. We establish that $\sqrt{2}\in\mathbb{Q}(\sqrt{2+\sqrt{2}})$, as it follows from $\sqrt{2}=(\sqrt{2+\sqrt{2}})^2-2\in\mathbb{Q}(\sqrt{2+\sqrt{2}})$. Consequently, we also deduce that

$$\sqrt{2-\sqrt{2}}=\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}\in\mathbb{Q}(\sqrt{2+\sqrt{2}}).$$

As a result,

$$x^4-4x^2+2=(x+\sqrt{2+\sqrt{2}})(x-\sqrt{2+\sqrt{2}})(x+\sqrt{2-\sqrt{2}})(x-\sqrt{2-\sqrt{2}}),$$

splits over $\mathbb{Q}(\sqrt{2+\sqrt{2}})$. Thus, $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ functions as the splitting field of x^4-4x^2+2. Since x^4-4x^2+2 possesses all distinct roots within its splitting field, we deduce that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a Galois extension over $\mathbb{Q}$. Applying the Isomorphism Extension Theorem, we conclude the existence of a $\sigma\in\mathrm{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{2}})\mid\mathbb{Q})$ such that $\sigma(\sqrt{2+\sqrt{2}})=\sqrt{2-\sqrt{2}}$. We assert that the order of σ is 4. Observe that

$$\sigma(\sqrt{2})=\sigma\left((\sqrt{2+\sqrt{2}})^2-2\right)=\sigma(\sqrt{2+\sqrt{2}})^2-2=(\sqrt{2-\sqrt{2}})^2-2=-\sqrt{2}.$$

Hence, we deduce

$$\sigma^2(\sqrt{2+\sqrt{2}})=\sigma\left(\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}\right)=\frac{\sigma(\sqrt{2})}{\sigma(\sqrt{2+\sqrt{2}})}=-\frac{\sqrt{2}}{\sqrt{2-\sqrt{2}}}=-\sqrt{2+\sqrt{2}}.$$

Thus, $o(\sigma)>2$, and $o(\sigma)\mid\left|\mathrm{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q})\right|=4$. Consequently, $o(\sigma)=4$. As a result, we have demonstrated that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{2}})\mid\mathbb{Q})\cong\mathbb{Z}/4\mathbb{Z}$, establishing that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ represents a cyclic extension over $\mathbb{Q}$. ■

§ Problem 7

Problem. Let K be a Galois extension of a field F such that $\mathrm{Gal}(K\mid F)\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$. How many intermediate fields L are there such that
(a) $[L:F]=4$,
(b) $[L:F]=9$,
(c) $\mathrm{Gal}(K\mid L)\cong\mathbb{Z}/4\mathbb{Z}$.

Proof. Given that K is a Galois extension over F with $\mathrm{Gal}(K\mid F)\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$, implying $[K:F]=|\mathrm{Gal}(K\mid F)|=24$, we proceed to analyze the intermediate fields:

(a) When $[L:F]=4$, we find that $[K:L]=[K:F]/[L:F]=6$. By the Galois Correspondence Theorem, the number of such intermediate fields L corresponds to the number of order 6 subgroups of $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$. To count these, we note that any subgroup of $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ is abelian, and the only abelian group of order 6 is isomorphic to $\mathbb{Z}/6\mathbb{Z}$. The elements of order 6 in $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ are:

$$\{(0,2),(0,10),(1,2),(1,10),(1,4),(1,8)\}.$$

Since $(0,10) \in \langle(0,2)\rangle$ and $(1,10) \in \langle(1,2)\rangle$, there are 4 distinct subgroups of order 6 in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, namely, $\langle(0,2)\rangle$, $\langle(1,2)\rangle$, $\langle(1,4)\rangle$, and $\langle(1,8)\rangle$. Therefore, there are 4 distinct intermediate fields $F \subseteq L \subseteq K$ such that $[L:F] = 4$.

(b) Since 9 does not divide 24, it follows that $[L:F] \nmid [K:F]$. Consequently, there are no intermediate fields $F \subseteq L \subseteq K$ with $[L:F] = 9$.

(c) To determine the number of intermediate fields $F \subseteq L \subseteq K$ such that $\mathrm{Gal}(K \mid L) \cong \mathbb{Z}/4\mathbb{Z}$, we employ the Galois Correspondence Theorem once more. The count is equivalent to the number of cyclic subgroups of order 4 in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. Elements of order 4 in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ are:

$$\{(0,3),(0,9),(1,3),(1,9)\}.$$

Since $(0,9) \in \langle(0,3)\rangle$ and $(1,9) \in \langle(1,3)\rangle$, there are 2 distinct cyclic subgroups of order 4 in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, which are $\langle(0,3)\rangle$ and $\langle(1,3)\rangle$. Hence, there exist 2 distinct intermediate fields $F \subseteq L \subseteq K$ such that $\mathrm{Gal}(K \mid L) \cong \mathbb{Z}/4\mathbb{Z}$. ■

§ Problem 8

Problem. Let $f(x) = x^4 + bx^2 + c$ be over F and let K be the splitting field of f. Prove that $\mathrm{Gal}(K \mid F)$ is contained in D_8 (the dihedral group with 8 elements).

Proof. We will deal with two separate cases. First when c is 0. Then the splitting filed of $f(x) = x^4 + bx^2$ will depend on the roots of $x^2 + b$. Splitting field K of it has degree 2 then the automorphism group $\mathrm{Aut}(K/F)$ will have order at-most 2 hence it is subgroup of $\mathbb{Z}/2\mathbb{Z}$. Since there is a copy of $\mathbb{Z}/2\mathbb{Z}$ in D_8, $\mathrm{Aut}(K/F)$ is subgroup of D_8.

If $c \neq 0$ we shall show that the automorphism group, $\mathrm{Aut}(K/F)$ cannot contain an element of order 3. In this case none of the roots are zero. Let, $\alpha, \beta, -\alpha, -\beta$ are the roots of $f(x)$. Any order 3 element of $\mathrm{Aut}(K/F)$ can be treated as a 3-cycle $(a,b,c)(d)$ so σ can fix exactly one root of $f(x)$. But this is not possible as if the element fixes α it must fix $-\alpha$. We know $\mathrm{Aut}(K/F) \leq S_4$. Now $|S_4| = 24 = 3 \times 2^3$, elements of automorphism group must lie in the 2-sylow subgroups of S_4. We know S_4 has three 2-sylow subgroup which are isomorphic to D_8. Thus $\mathrm{Aut}(K/F) \leq D_8$. ■

§ Problem 9

Problem. Let $K \mid_F$ be a field extension of characteristic $p \neq 0$, and let α be a root in K of an irreducible polynomial $f(x) = x^p - x - a$ over F.
(a) Prove that $\alpha + 1$ is also a root of $f(x)$.
(b) Prove that the Galois group of f over F is cyclic of order p.

Solution. (a) Consider α as a root of f, which implies $f(\alpha) = \alpha^p - \alpha - a = 0$. Now, take a closer look:

$$\begin{aligned} f(\alpha+1) &= (\alpha+1)^p - (\alpha+1) - a \\ &= \alpha^p + 1 - (\alpha+1) - a(\text{ as it a characteristic p field}) \\ &= \alpha^p - \alpha - a \\ &= 0. \end{aligned}$$

As a result, if α serves as a root of f, it follows that $\alpha + 1$ is also a root of f.

(b) Let's consider K as the splitting field of f over F. It's worth noting that f is separable since it's irreducible, and $f(x) \notin F[x^p]$. Now, as demonstrated in part (a), if α is a root of f, then so is $\alpha + 1$. Assume $\alpha \in K$ is a root of f. This implies that $\{\alpha, \alpha+1, \ldots, \alpha+(p-1)\}$ are all within K and are distinct roots of f. Consequently, $K = F(\alpha)$. To complete the proof, we need to show that $f(x)$ is the minimal polynomial

of α over F, this is true as $f(x)$ is irreducible in F. Using the Extension Isomorphism Theorem, we conclude that there exists a $\sigma \in \mathrm{Gal}(K/F)$ such that $\sigma(\alpha) = \alpha + 1$. Consequently, we have $o(\sigma) = p$. However, $|\mathrm{Gal}(K/F)| = [F(\alpha) : F] = \deg(f) = p$. Therefore, $\mathrm{Gal}(K/F)$ is a cyclic group of order p. ■

§ Problem 10

Problem. Prove or disprove: Normal extensions of normal extensions is normal.

Solution. We present a counterexample to illustrate that a normal extension of a normal extension may not necessarily be normal. Consider the following extension sequence: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. Firstly, $\mathbb{Q}(\sqrt{2})$ is the splitting field of the separable and irreducible polynomial $x^2 - 2$ over $\mathbb{Q}$, and consequently, it qualifies as a normal extension.

Similarly, we have previously established that $\mathbb{Q}(\sqrt[4]{2})$ is also a normal extension of $\mathbb{Q}(\sqrt{2})$. However, it's important to note that $\mathbb{Q}(\sqrt[4]{2})$ is not normal over $\mathbb{Q}$. This can be discerned from the fact that the splitting field of the minimal polynomial $x^4 - 2$ is $\mathbb{Q}(\sqrt[4]{2}, i)$, which extends beyond $\mathbb{Q}(\sqrt[4]{2})$. Therefore, we have a case where a normal extension $\mathbb{Q}(\sqrt[4]{2})|_{\mathbb{Q}(\sqrt{2})}$ of a normal extension $\mathbb{Q}(\sqrt{2})|_{\mathbb{Q}}$ does not maintain its normality when considered over the original field $\mathbb{Q}$. ■

Acknowledgement

While solving Assignment-1A and Assignment-1B, I have discussed some problems with my fiends, Soumya Dasgupta, Aaratick Basu and Proggadipto Majumdar. I have mentioned references (Books) wherever I have used some theorem or results from that book. I have also used some group theoretic fact which are mostly from 'Artin' otherwise the corresponding references are mentioned.