Question 1

Let $F = \mathbb{Q}(\eta)$, where $\eta = \cos(2\pi/7) + i\sin(2\pi/7) \in \mathbb{C}$. Assume that E/F is a Galois extension of degree 7. Show that there exists $\alpha \in E$ such that $\alpha^7 \in F$ and $E = F(\alpha)$.

Solution: As $\eta = e^{i2\pi/7}$, then let $\mu = \left\{ \eta, \eta^2, \cdots, \eta^6, 1 \right\}$. It is easy to check that μ is a set of solutions of $x^7 - 1$. As $F = \mathbb{Q}(\eta)$, then $\mu \subset F$.

Now, assuming that E/F is galois of degree 7, then $\mathrm{Gal}(E/F) \simeq \mathbb{Z}/7\mathbb{Z}$ as it is the only group with order 7. As a kummer extension, E/F is cyclic of order 7 if and only it is a splitting field of $x^7 - a$ for some $a \in F$. Therefore, there exists a root of $x^7 - a$, say α in the field E such that $\alpha^7 = a \in F$.

Then, consider that the set of all roots of $x^7 - a$ is $\left\{ \alpha, \alpha\eta, \cdots, \alpha\eta^6 \right\}$. Thus, $E = F(\alpha)$ as $\eta \in F$.

Question 2

Let G be a finite group. Prove that there exists a polynomial f over a field F such that $\mathrm{Gal}(f) \simeq G$.

Solution: Let G be a finite group of order n, then there is an embedding of G to S_n, ie. G is isomorphic to a subgroup of S_n. If there is a galois field extension E/F such that $\mathrm{Gal}(E/F) \simeq S_n$, then by the galois correspondence, there must be a field extension $E/K/F$ such that $\mathrm{Gal}(E/K) \simeq G$. Since E/K is normal, then E must be a splitting field of some f over field K. Hence, it is left to find a galois field extension E/F such that $\mathrm{Gal}(E/F) \simeq S_n$.

Let $x_1, x_2, \ldots, x_n$ be n variables and let

$$s_1 = x_1 + x_2 + \cdots + x_n$$

$$s_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n$$

$$\cdots$$

$$s_n = x_1 \cdot x_2 \cdots x_n$$

Then, notice that

$$(x - x_1)(x - x_2)\cdots(x - x_n) = x^n - s_1x^{n-1} + \cdots \pm s_n$$

is a polynomial in $\mathbb{Q}(s_1, s_2, \ldots, s_n)[x]$ So, $\mathbb{Q}(x_1, x_2, \ldots, x_n)$ is the splitting field of f over $\mathbb{Q}(s_1, s_2, \ldots, s_n)$, and as x_i are distinct, $E = \mathbb{Q}(x_1, x_2, \ldots, x_n)$ is galois over $F = \mathbb{Q}(s_1, s_2, \ldots, s_n)$.

Let $\sigma \in S_n$ be any permutation on the set of roots, then σ is an automorphism of E that fixes F as every s_i is fixed by a permutation of roots. Moreover, $\mathrm{Gal}(E/F) < S_n$ since the degree of f is n. Thus, it must be the case that $\mathrm{Gal}(E/F) \simeq S_n$, which finishes the proof.

Question 3

Let p be a prime integer and let H be a subgroup of S_p containing a p-cycle and a transposition. Prove that $H = S_p$.

Solution: To avoid using confusing notation, the cycle notation which was normall $(1, 2, \ldots, n)$ be be written as $[1\ 2\ \cdots\ n]$ instead.

Without loss of generality, let the given transposition shuffles 1 and 2 and let $\bar{\sigma}$ be the p cycle. Then, there is some $q < p$ such that $\bar{\sigma}^q(1) = 2$. Then, let $\sigma = \bar{\sigma}^q$

Now, as p is a prime, $\gcd(q, p) = 1$, therefore, σ is of order p, which means that σ is also a p-cycle.

Then, $\sigma[1\ 2]\sigma^{-1}$ is a transposition that shuffles $\sigma(1)$ and $\sigma(2)$. Now, as $\sigma(1) = 2$, then it maps 2 to $\sigma(2)$. By this construction, it is possible to create n transpositions, which are

$$[\sigma^{p-1}(2)\ 2], [2\ \sigma(2)], \ldots, [\sigma^{p-2}(2)\ \sigma^{p-1}(2)]$$

Since σ is cyclic, then it is of degree $p - 1$, thus listed transpositions are pairwise distinct.

Write $(n)^\sigma$ instead $\sigma^n(2)$ for $0 \leq n < m < p$ for brevity, so that the constructed transposition are

$$[(0)^\sigma\ (1)^\sigma], [(1)^\sigma\ (2)^\sigma], \ldots, [(p-2)^\sigma\ (p-1)^\sigma], [(p-1)^\sigma\ (0)^\sigma]$$

Then, let $[a, b]$ be an arbitrary transposition in S_p, then $a = \sigma^n(2)$ and $b = \sigma^m(2)$. for some n and m. Assume without loss of generality that $0 \leq n < m < p$. Thus, $a = (n)^\sigma$ and $b = (m)^\sigma$.

Then,

$$[(n)^\sigma \ \cdots \ (m)^\sigma] = [(n)^\sigma \ (n+1)^\sigma][(n+1)^\sigma \ (n+2)^\sigma] \cdots [(m-1)^\sigma \ (m)^\sigma]$$

And

$$[(n)^\sigma \ (m)^\sigma] = [(n)^\sigma \ \cdots \ (m)^\sigma][(m-1)^\sigma \ (m)^\sigma][(n)^\sigma \ \cdots \ (m)^\sigma]^{-1}$$

Thus, all transpositions are generated by a transposition and a p-cycle. Now, as all transpositions are the generator of symmetric group as a cycle

$$[a_1 \ a_2 \ \cdots \ a_k] = [a_1 \ a_2][a_2 \ a_3] \cdots [a_{k-1} \ a_k]$$

then, a transposition and a p-cycle generate S_p.

Question 4

Let f be a polynomial of degree 3 over $\mathbb{Q}$. Prove that if $\mathrm{Gal}(f) = \mathbb{Z}/3\mathbb{Z}$, then f has exactly three real roots.

Solution: Notice that f can have a maximum of 3 roots. As when x approaches ∞, $f(x)$ approaches ∞ and as x approaches $-\infty$, then $f(x)$ approaches ∞, then $f(x)$ must cross the x-axis at least once. This means that x has at least one real root.

Assuming for contradiction that f has a non-real complex root. Then, there must be at least 2 non-real complex roots, otherwise, the product of all roots, which is the constant term in the minimal polynomial will be non-real, thus non-rational.

First, assuming that f is irreducible, then f contain exactly 2 non-real complex roots, which must be x and $\bar{x}$, a complex and its complex conjugation. As f is irreducible, then $\mathrm{Gal}(f)$ acts on the roots transitively, therefore, $\mathrm{Gal}(f) \simeq S_3$ since a transposition and a cycle generate the symmetric group.

Then, if f is reducible, then $f(x) = m(x-a)(x^2 - bx - c)$ such that $x^2 - bx - c$ has no real roots Therefore $\mathrm{Gal}(f) = \mathrm{Gal}(x^2 - bx - c)$ is of degree 2.

So, the same conclusion that $\mathrm{Gal}(f) \neq \mathbb{Z}/3\mathbb{Z}$ is reached, thus the statement holds by contraposition.

Question 5

Determine $\mathrm{Gal}(f)$ of $f(x) = x^3 + 4x + 2$ over $\mathbb{Q}$

Solution: Firstly, the polynomial $f(x)$ is irreducible by the eisenstein criterion with $p = 2$. Therefore, the group $G = \mathrm{Gal}(f)$ must acts transitively on the set of 3 roots. Thus $G \simeq A_3$ or $G \simeq S_3$.

Consider that the discriminant of the polynomial is $-4(4^3) - 27(2^2) = -364$ is not a square, then G is not a subgroup of A_3. Thus, $G \simeq S_3$.

Question 6

Let f be a polynomial of degree 3 over $\mathbb{Q}$. Find all possible $\mathrm{Gal}(f)$.

Solution: If f is irreducible, then $G = \mathrm{Gal}(f)$ acts transitively. Thus G is a transitive subgroup of S_3. In this case, either $G \simeq S_3$ or $G \simeq A_3$. It can also be shown that $G \simeq A_3$ if and only if the discriminant, $D(f)$, is a square.

Otherwise, f is reducible. If f is a product of one linear and one irreducible quadratic, then the galois group G must isomorphic to S_2, as it is the product of the group of the linear polynomial, which is $\{ e \}$, and the group of the quadratic part, which is S_2, as it is the only transitive subgroup of S_2.

Lastly, if f is a product of three linear polynomials, then all roots are a member of F, which is that $G \simeq \{ e \}$.

To show that all of the cases are possible, consider

$$\mathrm{Gal}(x^3 - 2) \simeq S_3$$

as it is irreducible by eisenstein and have non-squared discriminant.

$$\mathrm{Gal}(x^3 - 3x + 1) \simeq A_3$$

as x^3-x+1 is irreducible over $\mathbb{F}_2$, so it x^3-3x+1 is irreducible over $\mathbb{Q}$. Moreover, the discriminant is $D(x^3-3x+1) = -4\cdot(-3)^3 - 27\cdot 1^2 = 81 = 9^2$ is a square.

$$\mathrm{Gal}(x^3-1) \simeq \mathbb{Z}/2\mathbb{Z}$$

as the splitting field of x^3-1 is of degree $\phi(3)=2$ over $\mathbb{Q}$.

$$\mathrm{Gal}(x^3-x) \simeq \{\, e \,\}$$

as $x^3-x = x(x-1)(x+1)$.

Question 7

Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 4 with $\mathrm{Gal}(f) = S_4$. Show that there is no nontrivial intermediate field between $\mathbb{Q}(\alpha)$ and $\mathbb{Q}$ where α is a root of f.

Solution: Let E be the splitting field of f over $\mathbb{Q}$. Let $\alpha_1,\dots,\alpha_4$ be roots of f such that $\alpha=\alpha_1$ then $G = \mathrm{Gal}(E/\mathbb{Q}(\alpha))$ is a subgroup of S_4 that fixes α_1 and only α_1. This implies that G must be a transitive subgroup of S_4, which is either S_3 or A_3.

If $G \simeq S_3$, then there is no other proper subgroup of S_4 that contains S_3, thus, there is no nontrivial intermediate subfield by the galois correspondence theorem. This is true because if there is proper subgroup of S_4 containing S_3, then it must have order 12 as $6 \mid 12$ and $12 \mid 24$ is the only number satisfying this properties. However, the only group of order 12 in S_4 is A_4, and S_3 is not contained by A_4.

If $G \simeq A_3$, then G is cyclic, thus $\mathbb{Q}(\alpha)$ must be a splitting field of x^3-a for some $a \in \mathbb{Q}$. So, $\mathbb{Q}(\alpha)$ must be galois over $\mathbb{Q}$. However, as A_3 is not a normal subgroup of S_4, $\mathbb{Q}(\alpha)/\mathbb{Q}$ cannot be normal. This yield a contradiction.

Question 8

Prove the following statements.
a. If L/F is a radical extension and $\sigma : L \to K$ is a field homomorphism, then $\sigma(L)/\sigma(F)$ is a radical extension
b. Let $K/L_i/F$ be fields with $1 \le i \le m$. If each L_i/F is a radical extension, then $L_1\cdots L_m/F$ is a radical extension

Solution:

a. If L/F is a radical extension, then assume WLOG that it is an n-radical for some n. Then,

$$F \subset F(\alpha_1) \subset \cdots \subset F(\alpha_1,\dots,\alpha_m) = L$$

where $\alpha_i^n \in F(\alpha_1,\cdots,\alpha_{i-1})$ and for $i>1$ and $\alpha_1^n \in F$. As σ is a field homomorphism, then for any field E and β

$$\sigma(E(\beta)) = \sigma(E)(\sigma(\beta))$$

which means

$$\sigma(F) \subset \sigma(F)(\sigma(\alpha_1)) \subset \cdots \subset \sigma(F)(\sigma(\alpha_1),\dots,\sigma(\alpha_m)) = \sigma(L)$$

From here, $\sigma(\alpha_1)^n = \sigma(\alpha_1^n) \in \sigma(F)$ since $\alpha_1 \in F$. Moreover, for all $i>1$, $\sigma(\alpha_i)^n = \sigma(\alpha_i^n) \in \sigma(F(\alpha_1,\dots,\alpha_{i-1}))$ by similar logic.

Thus, $\sigma(L)/\sigma(F)$ is a radical extension.

b. Firstly, consider when $m=2$. Since L_2 is radical, then let L_2 be k radical, without loss of generality. So, $L_2 = F(\alpha_1,\dots,\alpha_m)$ for $\alpha_i \in L_2$, such that there are chains

$$F \subset F(\alpha_1) \subset \cdots \subset F(\alpha_1,\dots,\alpha_n) = L_2$$

with $\alpha_1^k \in F$ and for$i>1$, $\alpha_i^k \in F(\alpha_1,\dots,\alpha_{i-1})$.

As

$$L_1L_2 = L_1(\beta_1,\dots,\beta_m)$$

by definition. Then, consider a chain

$$L_1 \subset L_1(\alpha_1) \subset \cdots \subset L_1(\alpha_1,\dots,\alpha_n) = L_1L_2$$

then, $\alpha_1^k \in F \subset L_1$ and for $i>1$, $\alpha_i^k \in F(\alpha_1,\dots,\alpha_{i-1}) \subset L_1(\alpha_1,\dots,\alpha_{i-1})$. Thus, L_1L_2 is k-radical over L_1.

As L_1L_2/L_1 and L_1/F are both radical, then by the transitivity, L_1L_2/F is also radical. Hence, the statement is proved for $m = 2$.

Now, for $m > 2$, assume for induction that $L_1L_2\cdots L_{m-1}$ is radical over F under the given condition. Then, let $K_1 = L_1L_2\cdots L_{m-1}$ and $K_2 = L_m$ so that the conditions for the case $m = 2$ are satisfied. By the proof, K_1K_2 is radical. However, as $K_1K_2 = L_1\cdots L_m$, then $L_1\cdots L_m$ is radical over F. Hence, the statement was proven by induction.

Question 9

Show that the polynomial $f(x) = 2x^5 - 5x^4 + 5$ over $\mathbb{Q}$ is not solvable by radicals.

Solution: Notice that $f'(x) = 10x^4 - 20x^3$ has just two solutions, which are $x = 0$ and $x = 2$. It can be checked that $f(0) = 5 > 0$ and $f(2) = -11 < 0$. With $f(x)$ being a degree 5 polynomial, as $x \to \infty$, $f(x)$ approaches ∞ and as $x \to -\infty$, $f(x)$ approaches $-\infty$. This means that the graph of $f(x)$ must intercept the x-axis exactly 3 times by the intermediate value theorem.

Since $f(x)$ has 5 roots and exactly 3 are real roots, then $f(x)$ has exactly 2 non-real complex roots. Moreover, $f(x)$ is irreducible by the eisenstein criterion at $p = 5$. Thus $G = \mathrm{Gal}(f)$ is a transitive subgroup of S_5. With the presence of tranposition automorphism that map the complex root to its conjugate, and the fact that G is a transitive subgroup thus contain a 5-cycle, the only possibility is that $G \simeq S_5$ as a tranposition and 5-cycle generates S_5.

As S_5 is not solvable, f is not solvable by radicals according to the galois theorem.

Question 10

Determine $\mathrm{Gal}(f)$ of $f(x) = x^4 + 4x^2 + 2$ over $\mathbb{Q}$.

Solution: Let E be a splitting field of f over $\mathbb{Q}$ and consider that

$$\begin{aligned} f(x) = x^4 + 4x^2 + 2 &= \left(x^2 + 2 - \sqrt{2} \right) \left(x^2 + 2 + \sqrt{2} \right) \\ &= \left(x - \sqrt{2 - \sqrt{2}} \right) \left(x + \sqrt{2 - \sqrt{2}} \right) \left(x - \sqrt{2 + \sqrt{2}} \right) \left(x + \sqrt{2 + \sqrt{2}} \right) \end{aligned}$$

Let $\alpha_1 = \sqrt{2 - \sqrt{2}}$, $\alpha_2 = -\sqrt{2 - \sqrt{2}}$, $\alpha_3 = \sqrt{2 + \sqrt{2}}$, $\alpha_4 = -\sqrt{2 + \sqrt{2}}$ be the four roots of f.

And let

$$\begin{aligned} \beta_1 &= \alpha_1\alpha_2 + \alpha_3\alpha_4 = (-(2 - \sqrt{2})) + (-(2 + \sqrt{2})) = -4 \\ \beta_2 &= \alpha_1\alpha_3 + \alpha_2\alpha_4 = (\sqrt{2}) + (\sqrt{2}) = 2\sqrt{2} \\ \beta_3 &= \alpha_1\alpha_4 + \alpha_2\alpha_3 = (-\sqrt{2}) + (-\sqrt{2}) = -2\sqrt{2} \end{aligned}$$

Thus, $K = F(\beta_1, \beta_2, \beta_3)$ is galois over $\mathbb{Q}$ and let $G = \mathrm{Gal}(f)$ so that $K = E^{G\cap V}$. As $K/\mathbb{Q}$ and $E/\mathbb{Q}$ are galois, then

$$m = \frac{|G|}{|G \cap V|} = [K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$$

Then, notice that f is reducible over K as shown above, therefore, $G \simeq \mathbb{Z}/4\mathbb{Z}$.