Question 1

Let $f = x^p - x - a \in F[x]$, where F is a field of characteristic p. Show that f is separable over F. Show also that if α is a root of f, then so is $\alpha + i$ for all $0 \leq i \leq p-1$.

Solution: Notice that if α is a root of f, then $\alpha^p - \alpha - a = 0$, this means that

$$(\alpha+1)^p - \alpha - a = \alpha^p + 1^p - \alpha - 1 - a = \alpha^p - \alpha - a = 0$$

So, $\alpha + 1$ is also a root of f.

Then, by induction, assume that $\alpha + n$ is a root of f, then $\alpha + n + 1$ is a root of f, therefore, $\alpha + i$ is a root of f for all $i \in \mathbb{F}_p$.

Now, as $\alpha, \alpha+1, \alpha+2, \cdots, \alpha+p-1$ are p distinct roots of of f, then f must be separable over F.

Question 2

Assume that the polynomial f in problem 1 is irreducible over F. Determine $\mathrm{Gal}(F(\alpha)/F)$, where α is a root of f.

Solution: Let $G = \mathrm{Gal}(F(\alpha)/F)$. Then firstly, $F(\alpha)$ is the splitting field of f because all of the roots of f is contained in $F(\alpha)$. This means that $F(\alpha)/F$ is normal, and separable, thus galois. Moreover, $[F(\alpha) : F] = p$ since the minimal polynomial of α is of degree p. This means that $|G| = p$, therefore, G must be isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Question 3

Let p be a prime and let E/F be a Galois extension such that $\mathrm{Gal}(E/F) \simeq \mathbb{Z}/p^3\mathbb{Z}$. Suppose that there is an intermediate field K such that $[E : K] = p$. Show any intermediate field $M \neq E$ between E and F is contained in K.

Solution: By the Galois correspondence theorem, K corresponds to the subset $H < G = \mathrm{Gal}(E/F)$ of order p. Notice that as G is cyclic, then the cyclic subgroup of order p is unique in G, and H is that subgroup. Now, let M be any intermediate subfield between E and F, with $M \neq E$, then M corresponds to a subgrop $N < G$, where $N = \mathrm{Gal}(E/M)$. Then, as $N < G$, N must either have degree 1, p, p^2, or p^3.

As E/F is Galois, then E/F is normal and separable. Notice that for any subfield K, E/K need to be normal and separable too, by the properties of normal and separable extensions. So, E/K is Galois

- If $|N| = 1$, then $[E : M] = 1$, which is $E = M$, which is not considered.
- If $|N| = p$, then $N = H$ by the uniqueness of cyclic group of order p, thus $M = K$, so K contains M.
- If $|N| = p^2$, then N is a group of order p^2, which must have a subgroup of order p. As $N < G$, it follows that a subgroup of order p of N must be a subgroup of order p of G. Since the subgroup is unique, then $H < N$.
- If $|N| = p^3$, then $[E : M] = p^3$, which is $M = F$, so M is contained in K.

What is left to show is that when $H < N < G$, then K contains M where $H = \mathrm{Gal}(E/K)$ and $N = \mathrm{Gal}(E/M)$. To begin, by the correspondence theorem, $K = E^H$ and $M = E^N$. Now, if every automorphism in N fixes M, then each of the automorphisms in K, is also an element of N, must fix M. This means that the fix point E^H must contains M. Thus, K contains M.

Question 4

Let p be a prime integer and let $\alpha = \eta + \eta^{-1}$, where η is a primitive p-th root of 1. Compute $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Solution: If $p = 2$, then $\eta = -1$ and $\alpha \in \mathbb{Q}$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 1$.

Otherwise, p is an odd prime. Notice that $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subsetneq \mathbb{Q}(\eta)$ because $\mathbb{Q}(\eta)$ contain a complex number while $\alpha = \eta + \eta^{-1} = \cos(\pi/p) + i\sin(\pi/p) + \cos(-\pi/p) + i\sin(-\pi/p) = 2\cos(\pi/p) \in \mathbb{R}$. Notice that $\mathbb{Q}(\eta)/\mathbb{Q}(\alpha)/\mathbb{Q}$ is a field extension, with $\mathbb{Q}(\eta)/\mathbb{Q}$ being a cyclotomic extension, therefore, galois, and $[\mathbb{Q}(\eta) : \mathbb{Q}] = p - 1$. This means that $\mathbb{Q}(\eta)/\mathbb{Q}(\alpha)$ is also galois by the property of normal group.

Considering that $\mathrm{Gal}(\mathbb{Q}(\eta)/\mathbb{Q})$ is the set of $\mathbb{Q}$-automorphism of $\mathbb{Q}(\eta)$, thus, as the extension is cyclotomic, the galois group is the cyclic group permuting the roots of unity, so let $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\eta)/\mathbb{Q})$ such that $\sigma_i : \eta \mapsto \eta^i$ for $1 \leq i < p$.

Now

$$\sigma_i(\alpha) = \sigma_i(\eta + \eta^{-1}) = \eta^i + \eta^{-i}$$

, therefore, only $i = \pm 1$ fixes α.

This means that $\mathrm{Gal}(\mathbb{Q}(\eta)/\mathbb{Q}(\alpha)) = \{\sigma_1, \sigma_{-1}\}$, therefore, $[\mathbb{Q}(\eta) : \mathbb{Q}(\alpha)] = 2$. Lastly, by the tower rule, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{p-1}{2}$

Question 5

Let η be a primitive 5th root of 1. Find an intermediate field K between $\mathbb{Q}(\eta)$ and $\mathbb{Q}$ such that $[K : \mathbb{Q}] = 2$.

Solution: Notice that the minimal polynomial for η is $f(x) = x^4 + x^3 + x^2 + x + 1$, so $[\mathbb{Q}(\eta) : \mathbb{Q}] = 4$. Now, the galois group $\mathrm{Gal}(f) \simeq (\mathbb{Z}/5\mathbb{Z})^\times \simeq C_4$ as $\mathbb{Q}(\eta)$ is a cyclotomic extension. Let $\sigma \in \mathrm{Gal}(f)$ sends η to η^2, then it is of degree 4 as $\sigma^2(\eta) = \sigma(\eta^2) = \eta^4 \neq \eta$. So, σ^2 is an element of degree 2, making a subgroup $\{\sigma^2, id\}$.

Consider a subfield $K = \mathbb{Q}(\eta)^{\{\sigma^2, id\}}$, then, $[\mathbb{Q}(\eta) : K] = 2$ by the galois correspondence theorem, which means that $[K : \mathbb{Q}] = 2$ by the tower rule.

To be more specific, let $\alpha = \eta + \eta^{-1}$. Then, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{5-1}{2} = 2$ by the proof shown in the previous problem.

Question 6

Find the 24th cyclotomic polynomial $\Phi_{24}(x)$ over $\mathbb{Q}$.

Solution: Notice that $\Phi_8(x) = \frac{x^8-1}{\Phi_1(x)\Phi_2(x)\Phi_4(x)} = \frac{x^8-1}{x^4-1} = x^4 + 1$.

Then,

$$\begin{aligned}
\Phi_{24} &= \frac{x^{24} - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_8(x)\Phi_{12}(x)} \\
&= \frac{x^{24} - 1}{\Phi_8(x)(x^{12} - 1)} \\
&= \frac{x^{12} + 1}{\Phi_8(x)} \\
&= \frac{x^{12} + 1}{x^4 + 1} \\
&= x^8 - x^4 + 1
\end{aligned}$$

Therefore, $\Phi_{24}(x) = x^8 - x^4 + 1$.

Question 7

Let p, q, r, s be distinct prime integers and $\alpha = \sqrt[p]{q} + \sqrt[r]{s}$. Calculate $\deg(\alpha)$ over $\mathbb{Q}$.

Solution: Consider that $[\mathbb{Q}(\sqrt[p]{q}) : \mathbb{Q}] = p$ as the minimal polynomial of $\sqrt[p]{q}$ over $\mathbb{Q}$ is $x^p - q$, which is irreducible over $\mathbb{Q}$ by the Eisenstein criterion. Similarly $[\mathbb{Q}(\sqrt[r]{s}) : \mathbb{Q}] = r$ by the same logic.

Then, $[\mathbb{Q}(\sqrt[p]{q}, \sqrt[r]{s}) : \mathbb{Q}] = pr$ since p and r are distinct primes that both divide $[\mathbb{Q}(\sqrt[p]{q}, \sqrt[r]{s}) : \mathbb{Q}]$ by the tower rule.

As $\mathbb{Q}(\sqrt[p]{q}, \sqrt[r]{s}) = \mathbb{Q}(\sqrt[r]{s})(\sqrt[p]{q})$ is a degree p extension over $\mathbb{Q}(\sqrt[r]{s})$, then the set $\{\sqrt[p]{q}, \sqrt[p]{q}^2, \dots, \sqrt[p]{q}^p\}$ is a linearly independent set over $\mathbb{Q}(\sqrt[r]{s})$.

If $\mathbb{Q}(\alpha)$ is a degree p extension over $\mathbb{Q}$, then there exist a minimal polynomial f of degree p as follow:

$$f(\alpha) = f(\sqrt[p]{q} + \sqrt[r]{s}) = f_0 + f_1(\sqrt[p]{q} + \sqrt[r]{s}) + \cdots + f_p(\sqrt[p]{q} + \sqrt[r]{s}) = 0$$

which is that there is a polynomial g of degree p over $\mathbb{Q}(\sqrt[p]{q})$ such that $g(\sqrt[p]{q}) = 0$ by expanding f into a polynomial in $\mathbb{Q}(\sqrt[p]{q})$.

However, as $g(\sqrt[p]{q})$ is a linear combination of $\{\sqrt[p]{q}, \sqrt[p]{q}^2, \cdots, \sqrt[p]{q}^p\}$, which is linearly independent, then $g_i = 0$ for all i. But, by direct expansion of g, the coefficient g_{p-1} is $g_{p-1} = f_p(p)(\sqrt[r]{s}) + f_{p-1}$. This yields a contradiction as

$$0 = g_{p-1} = f_p(p)(\sqrt[r]{s}) + f_{p-1}$$

implies

$$\sqrt[r]{s} = \frac{-f_{p-1}}{pf_p}$$

where p is a prime integer, f_i are rational, but $\sqrt[r]{s}$ is irrational.

This means that $\mathbb{Q}(\alpha)$ is not a degree p extension. Similarly, $\mathbb{Q}(\alpha)$ cannot be a degree r extension over $\mathbb{Q}$.

Next, without loss of generality, $r < p$, otherwise, swap r, p and q, s to get to the same point. Now, assume that α is rational, then $\sqrt[r]{s} = \alpha - \sqrt[p]{q}$, which taking the power of r to both size yields

$$s = \alpha^r - \binom{r}{1}\alpha^{r-1}\sqrt[p]{q} + \cdots - \sqrt[p]{q}^r$$

As $\{\sqrt[p]{q}, \cdots, \sqrt[p]{r}\}$ is linearly independent (as a subset of the basis) and $\alpha \in \mathbb{Q}$, then, $s = \alpha^r$, which is a contraction as

$$\alpha^r > \sqrt[p]{q}^r + \sqrt[r]{s}^r > s$$

Therefore, $\alpha \notin \mathbb{Q}$, which means that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \neq 1$.

Lastly, as $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divides pr, but is not equal to $1, p$, or r, then it must equal to pr. Hence, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = pr$.

Question 8

Determine the Galois group of $x^6 - 3$ over $\mathbb{Q}(\sqrt{-3})$.

Solution: Let E be the splitting field of $x^6 - 3$ over $\mathbb{Q}$. Then, $E = \mathbb{Q}(\eta, \sqrt[6]{3})$ where η is the primitive 6^{th} roof of unity. Then, $(\eta + \eta^2)^2 = \eta^2 + 2\eta^3 + \eta^4 = -2 - 1 = -3$. This is because $\eta^3 = -1$ and $\eta^2 + \eta^4 = \cos(\frac{4}{6}\pi) + i\sin(\frac{4}{6}\pi) + \cos(\frac{8}{6}\pi) - i\sin(\frac{8}{6}\pi) = -1$.

Therefore, $\sqrt{-3}$ is an element of E, which means that $E/\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ is a tower of field extension.

Now, $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[6]{3})][\mathbb{Q}(\sqrt[6]{3}) : \mathbb{Q}]$. Since $x^6 - 3$ is satisfied by $\sqrt[6]{3}$ and the polynomial is irreducible over $\mathbb{Q}$ by the Eisenstein criterion, then $[\mathbb{Q}(\sqrt[6]{3}) : \mathbb{Q}] = 6$. Moreover, as the cyclotomic $\Phi_6(x) = x^2 - x + 1$ is the minimal polynomial of η over $\mathbb{Q}$. Then, $[E : \mathbb{Q}(\sqrt[6]{3})]$ is at most 2. Next, as $\eta \in E$ is a non-real complex number $e^{i\frac{\pi}{3}}$, then it is not in $\mathbb{Q}(\sqrt[6]{3})$, a subfield of real numbers. Therefore, $[E : \mathbb{Q}(\sqrt[6]{3})] = 2$, which means $[E : \mathbb{Q}] = 12$.

Then, $[\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] = 2$, since $x^2 + 3 = 0$ is the minimal polynomial. This implies that $[E : \mathbb{Q}(\sqrt{-3})] = 6$. As $\mathrm{Gal}(x^6 - 3) = \mathrm{Gal}(E/\mathbb{Q}(\sqrt{-3}))$, then it is of order 6.

Consider σ that fixes $\mathbb{Q}$ and $\sigma : \sqrt[6]{3} \mapsto \sqrt[6]{3}\eta$ with $\sigma : \eta \mapsto \eta$. Then, it sends $\sqrt[6]{3}\eta^k$ to $\sqrt[6]{3}\eta^{k+1}$ as it is a field homomorphism. Moreover, σ fixes $\mathbb{Q}(\sqrt{-3})$ as it fixes η and $\sqrt{-3} = \eta + \eta^2$.

As $\sigma^2(\sqrt[6]{3}) = \sigma(\sqrt[6]{3}\eta) = \sqrt[6]{3}\eta^2 \neq \sqrt[6]{3}$ and $\sigma^3(\sqrt[6]{3}) = \sigma(\sqrt[6]{3}\eta^2) = \sqrt[6]{3}\eta^3 \neq \sqrt[6]{3}$, then σ must be of order 6. This means that the galois group of $x^6 - 3$ over must isomorphic to the cyclic group $\mathbb{Z}/6\mathbb{Z}$.

Question 9

Show the only field automorphism of $\mathbb{R}$ is the identity.

Solution: Let ϕ be the field automorphism of $\mathbb{R}$, then must send 1 to 1. This means it must be identity over $\mathbb{Z}$ by the induction using $\phi(a+1) = \phi(a) + \phi(1) = \phi(a) + 1$. Then, it must fix $\mathbb{Q}$ since $\phi(a/b) = \phi(a)/\phi(b) = a/b$ for all integer a and b.

Suppose that f is not an identity automorphism of $\mathbb{R}$, then there is a point x such that $f(x) \neq x$. Then, if $f(x) < x$, then $f(-x) = -f(x) > -x$, so there is a point x such that $f(x) > x$.

Choose $q \in Rat$ such that $f(x) > q > x$, which exists by the denseness of $\mathbb{R}$ so that $y = q - x$ is positive, thus there exists a real number z such that $z^2 = y$. Now,

$$q = f(q) = f(y + x) = f(y) + f(x) > f(y) + q = f(z^2) + q = f(z)^2 + q > q$$

yields a contradictions, thus, f must only be the identity.

Question 10

Let $E = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$. Show that E is algebraically closed.

Solution: Let β be any algebraic element over E, then there is a minimal polynomial over E that is satisfied by β. Let that polynomial be $e_0 + e_1 x + \cdots + e_n x^n$ for $e_i \in E$.

Consider that β is also algebraic over $\mathbb{Q}(e_0, \cdots, e_n)$ as the polynomial is also contained in $\mathbb{Q}(e_0, \cdots, e_n)[x]$. This means that β is also algebraic over $\mathbb{Q}(e_0, \cdots, e_n)$. So, $\mathbb{Q}(e_0, \cdots, e_n, \beta)$ is algebraic, thus finite extension of $\mathbb{Q}$. This means that $\mathbb{Q}(\beta)/\mathbb{Q}$ must also be finite. Hence, β is algebraic over $\mathbb{Q}$. As β is algebraic over E, then $\beta \in \mathbb{C}$ as $\mathbb{C}$ is an algebraically closed field. Lastly, as $\beta \in \mathbb{C}$ and β is algebraic over $\mathbb{Q}$, then $\beta \in E$ by the definition.