Question 1

Explain why a field homomorphism is either injective or trivial

Solution: Let $\phi : F \to E$ be a homomorphism, then $\ker\phi$ is an ideal of F. But an ideal of F is either $\{ 0 \}$ or F as F is a field. If $\ker\phi = \{ 0 \}$, then ϕ is injective. Otherwise, $\ker\phi = F$ means $\phi : f \mapsto 0$, which is that ϕ is trivial.

Question 2

Let m and k be relatively prime positive integers and let $a \in F$, where F is a field. Show that both polynomials $x^m - a$ and $x^k - a$ are irreducible over F if and only if $x^{mk} - a$ is irreducible over F.

Solution:
$(\Longrightarrow)$:

Let $x^m - a$ and $x^k - a$ be irreducible and α be a root of $x^{mk} - a$. Therefore, $\alpha^{mk} = a$, which means that α^m is a root of $x^k - a$. Now, $\alpha^m \notin F$ therefore $F(\alpha^m)/F$ is an extension with $[F(\alpha^m) : F] = k$. This is because the minimal polynomial of α^m is $x^k - a$ which is a degree k polynomial. Similarly, the field extension $F(\alpha^k)/F$ is an extension with $[F(\alpha^k) : F] = m$.

Now, $[F(\alpha^m, \alpha^k) : F(\alpha^m)] \leq m$ and $[F(\alpha^m, \alpha^k) : F(\alpha^k)] \leq n$, therefore,

$$[F(\alpha^m, \alpha^k) : F] = [F(\alpha^m, \alpha^k) : F(\alpha^m)][F(\alpha^m) : F] = [F(\alpha^m, \alpha^k) : F(\alpha^k)][F(\alpha^k) : F]$$

But since m and k is coprime, then $[F(\alpha^m, \alpha^k) : F] = mk$ since it must be divisible by both m and k.

However, consider that $F(\alpha^m, \alpha^k) = F(\alpha)$ as there exist a, b making $am + bk = 1$ as they are coprime which makes $\alpha^{am}\alpha^{bk} = \alpha \in F(\alpha^m, \alpha^k)$.

Therefore, $[F(\alpha) : F] = mk$ which means that the minimal polynomial of α should be of degree mk. Therefore, as the minimal polynomial of α must divide $x^{mk} - a$, then it is $x^{mk} - a$. This means that $x^{mk} - a$ is irreducible.

$(\Longleftarrow)$:

Assume that $x^m - a$ is reducible. Then, $x^m - a = f(x)g(x)$ where both f, g are not unit. Then, consider $x^{mk} - a = \left(x^k\right)^m - a = f(x^k)g(x^k)$. Notice that $f(x^k)$ cannot be a unit since $f(x^k)$ is not a constant in F because $f(x)$ is at least degree 1, and so is g. Therefore, $x^{mk} - a$ is reducible.

Question 3

Let $a, b \in E/F$ be nonzero elements. Show that $F(a, b)/F(a^{-1}b^{-1}, a + b)$ is an algebraic extension.

Solution: Consider that $(a^{-1}b^{-1})(a + b) = (a^{-1} + b^{-1})$, so $a^{-1} + b^{-1} \in F(a^{-1}b^{-1}, a + b)$. Also, $1 \in F(a^{-1}b^{-1}, a + b)$.

Consider a polynomial $p(x) = (a^{-1}b^{-1})x^2 - (a^{-1} + b^{-1})x + 1$. It is easy to see that $p(x) \in F(a^{-1}b^{-1}, a + b)[x]$.

Notice that $(a^{-1}b^{-1})a^2 - (a^{-1} + b^{-1})a + 1 = ab^{-1} - (1 + ab^{-1}) + 1 = 0$, and similarly, $(a^{-1}b^{-1})b^2 - (a^{-1} + b^{-1})b + 1 = 0$. So, a and b are the root of polynomial p.

Since a and b is algebraic over $F(a^{-1}b^{-1}, a + b)$, then $F(a^{-1}b^{-1}, a + b)(a, b)$ is an algebraic extension of $F(a^{-1}b^{-1}, a + b)$. Lastly, it can be shown that $F(a, b) = F(a^{-1}b^{-1}, a+b, a, b)$ as $F(a, b) \subset F(a^{-1}b^{-1}, a+b, a, b)$ trivially and $a^{-1}b^{-1} \in F(a, b)$ and $a + b \in F(a, b)$.

Therefore, $F(a, b)$ is an algebraic extension of $F(a^{-1}b^{-1}, a + b)$.

Question 4

Find the degree of a splitting field of $x^3 - 17$ over $\mathbb{Q}$.

Solution: Consider that $x^3 - 17 = \left(x - \sqrt[3]{17} \right) \left(x - \eta\sqrt[3]{17} \right) \left(x - \eta^2\sqrt[3]{17} \right)$ where η is the primitive third root of 1. Let E be a splitting field over $\mathbb{Q}$. Then E must contain $\sqrt[3]{17}$ and $\eta\sqrt[3]{17}$. Therefore, E must contain η. However, if E contains $\sqrt[3]{17}$ and η, then E contain $\eta\sqrt[3]{17}$ and $\eta^2\sqrt[3]{17}$, which means that $x^3 - 17$ splits in E, thus $E = \mathbb{Q}(\sqrt[3]{17}, \eta)$ is the splitting field of $x^3 - 17$ over $\mathbb{Q}$.

Now, the set $\left\{ 1, \sqrt[3]{17}, \sqrt[3]{17}^2 \right\}$ is a basis of $\mathbb{Q}(\sqrt[3]{17})/\mathbb{Q}$. This is because $\mathbb{Q}(\sqrt[3]{17}) = \left\{ a + b\sqrt[3]{17} + c\sqrt[3]{17}^2 \mid a, b, c \in \mathbb{Q} \right\}$ as $\sqrt[3]{17}^3 = 17 \in \mathbb{Q}$ and $\sqrt[3]{17}^{-1} = \frac{\sqrt[3]{17}^2}{17}$. So, the set spans $\mathbb{Q}(\sqrt[3]{17})$.

Moreover, the set is a linearly independent set. The reason being that $\left\{ 1, \sqrt[3]{17} \right\}$ is linearly independent over $\mathbb{Q}$ since $\sqrt[3]{17} \notin \mathbb{Q}$. Then, if $\sqrt[3]{17}^2 = a + b\sqrt[3]{17}$ for some $a, b \in \mathbb{Q}$,

$$\begin{aligned} 17 = \sqrt[3]{17}^3 &= (\sqrt[3]{17})(a + b\sqrt[3]{17}) \\ &= b\sqrt[3]{17}^2 + a\sqrt[3]{17} \\ &= b(a + b\sqrt[3]{17}) + a\sqrt[3]{17} \\ &= (a + b^2)\sqrt[3]{17} + ba \end{aligned}$$

which means that $\sqrt[3]{17} \in \mathbb{Q}$. This implication creates contradiction, so the set must be linearly independent.

Next, since $\eta = e^{\frac{2i\pi}{3}}$ is the primitive third root, the set $\{1, \eta\}$ is a basis of $\mathbb{Q}(\sqrt[3]{17}, \eta)/\mathbb{Q}(\sqrt[3]{17})$. This is because is field is spans by $\left\{ 1, \eta, \eta^2 \right\}$ as $\eta^3 = 1$ and $\eta^{-1} = \eta^2$. However, $\eta^2 = -\eta - 1$. Moreover, $\eta \in \mathbb{C} - \mathbb{R}$, so $\{1, \eta\}$ is linearly independent, thus, the set is a basis for the field.

Since $[\mathbb{Q}(\sqrt[3]{17}, \eta) : \mathbb{Q}(\sqrt[3]{17})] = 2$ and $[\mathbb{Q}(\sqrt[3]{17}) : \mathbb{Q}] = 3$, then $[E : \mathbb{Q}] = 6$. So, the degree of a splitting field of $x^3 - 17$ over $\mathbb{Q}$ is 6.

Question 5

Let $\xi \in \mathbb{C}$ be a primitive nth root of unity. Prove that $\mathbb{Q}(\xi)$ is a splitting field of $x^n - 1$ over $\mathbb{Q}$.

Solution: Notice that $\xi = e^{\frac{2i\pi}{n}}$ is a primitive nth root of unity because $\xi^n = 1$ and $\xi^i \neq \xi^j$ for $i, j \in \{0, \cdots, n-1\}$ such that $i \neq j$.

Next, since $(\xi^i)^n - 1 = (\xi^n)^i - 1 = 1 - 1 = 0$, then $(x - \xi^i)$ divides $(x^n - 1)$. Moreover, since $\xi^i \neq \xi^j$, then $(x - \xi^0)(x - \xi^1)\cdots(x - \xi^{n-1})$ divides $(x^n - 1)$. But both polynomial have the same degree, so it leads to concluding that

$$(x^n - 1) = (x - \xi^0)(x - \xi^1)\cdots(x - \xi^{n-1})$$

Now, as $\left\{ \xi^0, \cdots, \xi^{n-1} \right\}$ is the set of all root of $x^n - 1$, it follows that $\mathbb{Q}(\xi^0, \cdots, \xi^{n-1})$ is the smallest field containing all root of $x^n - 1$. Therefore, it is the splitting field of $x^n - 1$.

Lastly, since $\xi^i \in \mathbb{Q}(\xi)$ for all $i \in \{0, \cdots, n-1\}$, $\mathbb{Q}(\xi^0, \cdots, \xi_{n-1}) = \mathbb{Q}(\xi)$

Question 6

Let $f(x) = x^6 - 5x^3 - 2$ be a polynomial in $\mathbb{Q}[x]$. Find the splitting field E of $f(x)$ over $\mathbb{Q}$. Compute $[E : \mathbb{Q}]$.

Solution: Notice that

$$x^6 - 5x^3 - 2 = \left(x^3 + \frac{5 + \sqrt{33}}{2} \right) \left(x^3 + \frac{5 - \sqrt{33}}{2} \right)$$

And $x^3 + \alpha = (x + \eta\sqrt[3]{\alpha})(x + \eta^2\sqrt[3]{\alpha})(x + \eta^3\sqrt[3]{\alpha})$ where η is a primitive third root.

For simplicity, let denote $\alpha = \sqrt[3]{\frac{5+\sqrt{33}}{2}}$ and $\alpha' = \sqrt[3]{\frac{5-\sqrt{33}}{2}}$. Then, the roots of polynomials are $\alpha, \alpha\eta, \alpha\eta^2, \alpha', \alpha'\eta, \alpha'\eta^2$.

If a field contains all roots, then it must contains α and $\alpha\eta$, thus it must contains η. Consider the field $E = \mathbb{Q}(\alpha, \alpha', \eta)$. Then, E contains $\alpha, \alpha\eta, \alpha\eta^2, \alpha', \alpha'\eta, \alpha'\eta^2$. Therefore, it is the smallest field containing all roots of the polynomial. Thus, it is the splitting field.

The splitting field is $\mathbb{Q}\left(\sqrt[3]{\frac{5+\sqrt{33}}{2}}, \sqrt[3]{\frac{5-\sqrt{33}}{2}}, \eta \right)$

To compute the degree, first consider $[\mathbb{Q}(\sqrt{33}) : \mathbb{Q}]$. The degree of that extension is 2 since the basis of the vector space is $\left\{ 1, \sqrt{33} \right\}$ since it spans the space by definition, (as $\sqrt{33}^2 \in \mathbb{Q}$, $\sqrt{33}^{-1} = \sqrt{33}/33$).

Next, consider $\left[\mathbb{Q}\left(\sqrt[3]{\frac{5+\sqrt{33}}{2}} \right) : \mathbb{Q}(\sqrt{33}) \right]$. Notice that $\{1, \alpha\}$ is linearly independent as $(a + b\sqrt{33}) \neq \alpha$ for any $a, b \in \mathbb{Q}$. Since $\{1, \alpha\}$ is linearly independent, it can be shown that $\left\{ 1, \alpha, \alpha^2 \right\}$ is also linearly independent, because otherwise, if

$\alpha^2 = a\alpha + b$ for some $a, b \in \mathbb{Q}(\sqrt{33})$, then

$$\begin{aligned}\alpha^3 &= a\alpha^2 + b\alpha \\ &= a(a\alpha + b) + b\alpha \\ &= (a^2 + b)\alpha + ab\end{aligned}$$

which contradicts that $1, \alpha$ is linearly independent. Moreover, thes set $\{1, \alpha, \alpha^2\}$ spans the space since $\alpha^{-1} = \alpha^2/\alpha^3$ and $\alpha^3 \in \mathbb{Q}(\sqrt{33})$. Therefore, the degree of the extension is 3.

Next, consider the extension $[\mathbb{Q}(\alpha, \alpha') : \mathbb{Q}(\alpha)]$. Notice that the set $\{1, \alpha'\}$ is linearly independent, and similarly to the above proof, $\{1, \alpha', \alpha'^2\}$ is a linearly independent set. Moreover, it spans the space since $\alpha'^{-1} = \alpha'^2/\alpha'^3$ and $\alpha'^3 \in \mathbb{Q}(\alpha)$. Therefore, the degree of the extension is 3.

Lastly, the extension $[\mathbb{Q}(\alpha, \alpha', \eta) : \mathbb{Q}(\alpha, \alpha')]$ is 2 since $\{1, \eta\}$ is clearly independent because $\eta \in \mathbb{C} - \mathbb{R}$ and $\mathbb{Q}(\alpha, \alpha') \subset \mathbb{R}$. Moreover, the set spans the space because $\eta^{-1} = \eta^2 = -\eta - 1$ since it is the primitive third root.

Therefore, the degree of

$$[E : \mathbb{Q}] = [\mathbb{Q}(\alpha, \alpha', \eta) : \mathbb{Q}(\alpha, \alpha')][\mathbb{Q}(\alpha, \alpha') : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{33})][\mathbb{Q}(\sqrt{33}) : \mathbb{Q}]$$

which equates to $2 \cdot 3 \cdot 3 \cdot 2$, which is 36.

Question 7

Show that the field extension $\mathbb{Q}(\sqrt{3} + \sqrt{7})$ over $\mathbb{Q}$ is normal.

Solution: Since 3 and 7 are prime, $\mathbb{Q}(\sqrt{3} + \sqrt{7}) = \mathbb{Q}(\sqrt{3}, \sqrt{7})$. Consider the minimal polynomial, $m_{\sqrt{3}}(x) = x^2 - 3$ and $m_{\sqrt{7}}(x) = x^2 - 7$. The polynomials are minimal since $\sqrt{3}$ and $\sqrt{7}$ is not rational, thus the minimal polynomial cannot be linear.

Now, a field extension is normal if and only if it splits the product of all minimal polynomials, thus, $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ is normal if and only if $(x^2 - 3)(x^2 - 7)$ splits. Which they split since

$$(x^2 - 3)(x^2 - 7) = (x - \sqrt{3})(x + \sqrt{3})(x - \sqrt{7})(x + \sqrt{7})$$

Since $\pm\sqrt{3}, \pm\sqrt{7} \in \mathbb{Q}(\sqrt{3}, \sqrt{7})$, then the field is normal over $\mathbb{Q}$.

As $\mathbb{Q}(\sqrt{3} + \sqrt{7}) = \mathbb{Q}(\sqrt{3}, \sqrt{7})$, the field $\mathbb{Q}(\sqrt{3} + \sqrt{7})$ is normal over $\mathbb{Q}$.

Question 8

Let f be an irreducible polynomial over a field F. Prove that if E/F is normal, then f factors into a product of irreducible polynomials of the same degree over E.

Solution: Let E/F be normal so that for any extension L/E and morphism $\phi : E \to L$ with $\phi\mid_F = id_F$, $\phi(E) = E$. Let f be an irreducible in F such that it is $f = g_1 \cdots g_k$ over E. Then, denote α_i as a root of g_i.

Consider an extension $\phi : E \to L$ of id_F such that $\phi(\alpha_1) = \alpha_i$. Note that the extension is a well-defined homomorphism since $\alpha_i \notin F$ and is the only point not in F that the image is specified. Since the field E is normal, $\phi(E) = E$, therefore

$$g_1(\alpha_1) = 0 = \phi(g_1)(\phi(\alpha_1)) = \phi(g_1)(\alpha_i)$$

So, $g_i \mid \phi(g_1)$. But $\phi(g_1)$ is irreducible, so $g_i \sim \phi(g_1)$, which is that $\deg(g_1) = \deg(g_i)$

Question 9

Let $\alpha = \sqrt{3 + \sqrt{3}}$. Find the normal closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$.

Solution: Consider

$$f(x) = x^4 - 6x^2 + 6 = \left(x - \sqrt{3 - \sqrt{3}}\right)\left(x - \sqrt{3 + \sqrt{3}}\right)\left(x + \sqrt{3 - \sqrt{3}}\right)\left(x + \sqrt{3 + \sqrt{3}}\right)$$

Then, any product of 1 linear factor is not in $\mathbb{Q}[x]$. Any product of 2 linear factors results the constant term being either $\pm 3 \pm \sqrt{3}$ or $\pm\sqrt{3+\sqrt{3}}\sqrt{3-\sqrt{3}} = \pm\sqrt{6}$ which is not in $\mathbb{Q}$. The product of 3 linear factors contain the constant term of $\pm\sqrt{3 \pm \sqrt{3}}\sqrt{6} = \pm 3\sqrt{2 \pm 6\sqrt{3}}$ which is not in $\mathbb{Q}$. So, $f(x)$ is the minimal polynomial of α.

Let $\bar{\alpha} = \sqrt{3-\sqrt{3}}$. As $\mathbb{Q}(\alpha, \bar{\alpha})$ is a splitting field of of m_α, then $\mathbb{Q}(\alpha, \bar{\alpha})/\mathbb{Q}(\alpha)$ is the normal closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$.

Question 10

Find a normal closure of $\mathbb{Q}(\sqrt[4]{11})/\mathbb{Q}$

Solution: Consider that $m_{\sqrt[4]{11}}$ must divide $f(x) = x^4 - 11$ since $f(\sqrt[4]{11}) = 0$. Now,

$$x^4 - 11 = (x^2 - \sqrt{11})(x^2 + \sqrt{11}) = (x - \sqrt[4]{11})(x + \sqrt[4]{11})(x - i\sqrt[4]{11})(x + i\sqrt[4]{11})$$

It can be seen that $m_{\sqrt[4]{11}} = f$ since any combinations of 3 or less factors of the splits will result in the constant term being $\pm\sqrt[4]{11}^3$ or $\pm i\sqrt[4]{11}^3$ which is not an element of $\mathbb{Q}$.

Since $\pm i\sqrt[4]{11} \notin \mathbb{Q}$, then it is clear that $\mathbb{Q}(\sqrt[4]{11})$ is not normal. Moreover, the normal closure should split $m_{\sqrt[4]{11}}$, so the normal closure must contain $i\sqrt[4]{11}$.

Now, if $N/\mathbb{Q}(\sqrt[4]{11})/\mathbb{Q}$ contains $i\sqrt[4]{11}$, then it contains $-i\sqrt[4]{11}$ and $-\sqrt[4]{11}$ by the property of field. Thus, $N = \mathbb{Q}(\sqrt[4]{11}, i\sqrt[4]{11})$ splits $m_{\sqrt[4]{11}}$.

Therefore, $\mathbb{Q}(\sqrt[4]{11}, i\sqrt[4]{11})/\mathbb{Q}(\sqrt[4]{11})$ is a normal closure of $\mathbb{Q}(\sqrt[4]{11})/\mathbb{Q}$