Question 1

Give an example of a finite field extension that is not generated by a single element.

Solution: Consider $E = \mathbb{F}_p(X, Y)$ to be a field of rational functions with two variables and $F = \mathbb{F}_p(X^p, Y^p)$ so that E/F. Since $T^p - X^p = 0$, $X \in E$ is a of degree at most p over F and similarly, as $T^p - Y^p = 0$, Y is of degree at most p over F. This means that E/F is finite, therefore F should be a field of rational functions of two variables. Otherwise, if X^p or Y^p is algebraic, then X or Y respectively will be algebraic, contradicting the assumption.

Next, notice that $f(T) = T^p - X^p$ and X^p is irreducible in $\mathbb{F}_p(Y^p)[X^p]$. This means $f(T)$ is irreducible over F by the Eisenstein criterion. Moreover $f(X) = 0$, therefore, the degree of $\mathbb{F}_p(X, Y^p)$ over F is p. Then considering $g(P) = T^p - Y^p$ in $\mathbb{F}_p(X)[Y^p]$ gives that $\mathbb{F}_p(X, Y)$ is a degree p extension over $\mathbb{F}_p(X, Y^p)$ using similar reasoning.

Now, let α be an arbitrary element of E, which is that

$$\alpha = \alpha_{0,0} + \alpha_{1,0}X + \alpha_{0,1}Y + \cdots + \alpha_{n,m}X^nY^m$$

where $\alpha_{i,j} \in \mathbb{F}_p$.

Then,

$$\alpha^p = \alpha_{0,0}^p + \alpha_{1,0}^p X^p + \cdots + \alpha_{n,m}^p (X^p)^n (Y^p)^m$$

is an element in F. Thus, $\alpha^p \in F$, which means that α is the root of some polynomial $T^p - \alpha^p$ over F. Since α can be at most degree p, then $E \neq F(\alpha)$ for any $\alpha \in E$. Thus, E/F is finite generated by a single element.

Question 2

Let $\alpha = 1 + \sqrt[3]{2} + \sqrt[3]{4}$. Determine whether or not $\mathbb{Q}(\alpha)/\mathbb{Q}$ is normal.

Solution: Consider that

$$\alpha^2 = 1 + \sqrt[3]{4} + 2\sqrt[3]{2} + 2\sqrt[3]{4} + 2\sqrt[3]{2} + 4 = 5 + 4\sqrt[3]{2} + 3\sqrt[3]{2}$$

so $\alpha^2 - 3\alpha - 2 = \sqrt[3]{2}$, which means

$$\alpha^3 - 3\alpha^2 - 2\alpha = 2 + \sqrt[3]{2} + \sqrt[3]{4}$$

Then, $\alpha^3 - 3\alpha^2 - 3\alpha - 1 = 0$. Thus, $f(x) = x^3 - 3x^2 - 3x - 1$ has α as a root.

Moreover, consider that $f(x+1) = x^3 - 6x - 6$ where 3 is irreducible in $\mathbb{Z}$ dividing 6 but $3^2 \nmid 6$. Then, the Eisenstein criterion applies. So, $f(x+1)$ and thus $f(x)$ is irreducible.

Now, notice that

$$f(x+\alpha) = x^3 + (3\alpha - 3)x^2 + (3\alpha^2 - 6\alpha - 3)x + f(\alpha) = x^3 + 3(\alpha - 1)x^2 + 3((\alpha - 1)^2 - 2)x$$

Consider the root β of f, for if $\beta \neq \alpha$, then $x \neq 0$ in above equation, which gives

$$\beta^2 + 3(\alpha - 1)\beta + 3((\alpha - 1)^2 - 2) = 0$$

Now, as $\alpha - 1 = \sqrt[3]{2} + \sqrt[3]{4}$ and $(\sqrt[3]{4} + 2\sqrt[3]{2})^2 = 2\sqrt[3]{2} + 4\sqrt[3]{4} + 4 > 7 + (\sqrt[3]{4} + 2\sqrt[3]{2})$ because $\sqrt[3]{x} > 1$ for any $x > 1$.

With the monotonicity of the polynomial function $h(x) = x^2 - x$ for $x > 1$, it follows that $\sqrt[3]{4} + 2\sqrt[3]{2} > 4$

Thus,

$$(\alpha - 1)^2 = \sqrt[3]{4} + 2\sqrt[3]{2} + 4 > 8$$

So, $(3(\alpha - 1))^2 - 4 \cdot 3((\alpha - 1)^2 - 2) = -3(\alpha - 1)^2 + 24 < 0$. This means that β must be a complex number. However, $\mathbb{Q}(\alpha)$ is the smallest field generated by α, a real number. Thus, since $\mathbb{R}$ is a field and $\mathbb{Q}(\alpha) \subset \mathbb{R}$, $\beta \notin \mathbb{Q}(\alpha)$. This means that $\mathbb{Q}(\alpha)$ is not normal since it does not split $f(x)$.

Question 3

Find the Galois group of $\mathbb{Q}(\sqrt{2}, \sqrt{7}, \sqrt{19})/\mathbb{Q}$

Solution: Notice that the degree $[\mathbb{Q}(\sqrt{2}, \sqrt{7}, \sqrt{19}) : \mathbb{Q}]$ is at most $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}][\mathbb{Q}(\sqrt{7}) : \mathbb{Q}][\mathbb{Q}(\sqrt{19}) : \mathbb{Q}] = 8$ So the galois group G of the extension must be at most order 8.

Considering $\mathbb{Q}$-automorphisms, it must send $\sqrt{2} \to \pm\sqrt{2}$, $\sqrt{7} \to \pm\sqrt{7}$ and $\sqrt{19} \to \pm\sqrt{19}$. since it must preserve the root of $f(x) = x^2 - 2$, $g(x) = x^2 - 7$, and $h(x) = x^2 - 19$.

Let

$$\sigma_2 : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{7} \mapsto \sqrt{7}, \text{ and } \sqrt{19} \mapsto \sqrt{19}$$
$$\sigma_7 : \sqrt{2} \mapsto \sqrt{2}, \sqrt{7} \mapsto -\sqrt{7}, \text{ and } \sqrt{19} \mapsto \sqrt{19}$$
$$\sigma_{19} : \sqrt{2} \mapsto \sqrt{2}, \sqrt{7} \mapsto \sqrt{7}, \text{ and } \sqrt{19} \mapsto -\sqrt{19}$$

Then all of them are $\mathbb{Q}$-automorphisms.

Moreover, the compositions of them are also $\mathbb{Q}$-automorphisms, and the composition of them, in this case is commutative. This is because σ_2 permutes only $\sqrt{2}$ and $-\sqrt{2}$, and similarly for σ_7 and σ_{19}. It also means that they are of degree 2.

Thus, there are total of 8 $\mathbb{Q}$-automorphisms, which are $id, \sigma_2, \sigma_7, \sigma_{19}, \sigma_2 \circ \sigma_7, \sigma_2 \circ \sigma_{19}, \sigma_7 \circ \sigma_{19}$, and $\sigma_2 \circ \sigma_7 \circ \sigma_{19}$.

The group is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ by the isomorphism

$$\psi : \sigma_2 \mapsto (1, 0, 0), \sigma_7 \mapsto (0, 1, 0), \text{ and } \sigma_{19} \mapsto (0, 0, 1)$$

Question 4

Let E be a splitting field of $x^4 + 3x^2 + 1$ over $\mathbb{Q}$. Determine $\text{Gal}(E/\mathbb{Q})$

Solution: The galois group $G = \text{Gal}(E/\mathbb{Q})$ should be a subgroup of S_4 as $f(x) = x^4 + 3x^2 + 1$ is of degree 4.

Firstly, $f(x)$ is irreducible over $\mathbb{Q}$, which equivalent to that it is irreducible over $\mathbb{Z}$ as $f(x)$ is monic, thus primitive. Now, if $f(x)$ is reducible to $P(x)Q(x)$ over $\mathbb{Z}$, then one of the divisor of $f(x)$ must be of degree not more than 2 and monic since f(x) is monic.

If $f(x) = P(x)Q(x)$, then $f(x) = P(x)Q(x)$ modulo 2. which means that $f_2(x)$ is reducible over $\mathbb{F}_2$, where $f_2(x) = x^4 + x^2 + 1 \equiv f(x) \pmod 2$. But since $\gcd(x^4 + x^2 + 1, x^{2^2} - x) = \gcd(x^4 + x^2 + 1, x^3 - 1) = \gcd(x^3 + x^2 + 1, x^3 + 1) = \gcd(x^2, x^3 + 1) = 1$, then, $f_2(x)$ is irreducible over $\mathbb{F}_2$, which means that $f(x)$ is irreducible over $\mathbb{Q}$.

Now, notice that when letting $\alpha = \sqrt{\frac{3+\sqrt{5}}{2}}$ and $\bar{\alpha} = \sqrt{\frac{3-\sqrt{5}}{2}}$

$$f(x) = (x^2 + \alpha^2)(x^2 + \bar{\alpha}^2) = (x + i\alpha)(x - i\alpha)(x + i\bar{\alpha})(x - i\bar{\alpha})$$

And $\alpha \cdot \bar{\alpha} = \sqrt{\frac{(3+\sqrt{5})(3-\sqrt{5})}{4}} = \sqrt{\frac{9-5}{4}} = 1$ which means $\bar{\alpha} = 1/\alpha$. So, $E = \mathbb{Q}(i\alpha)$.

Since $f(x)$ is irreducible, then $[\mathbb{Q}(i\alpha) : \mathbb{Q}] = 4$. Thus, the order of the galois group $G = \text{Gal}(E/\mathbb{Q})$ is 4.

Now, let consider two $\mathbb{Q}$-automorphisms $\phi : i\alpha \to -i\alpha$ and $\psi : i\alpha \to i\bar{\alpha}$. Then, $\phi^2(i\alpha) = -\phi(i\alpha) = i\alpha$. Since ϕ^2 fixes the generator of E, it is id. Moreover, $\psi^2(i\alpha) = \psi(i\bar{\alpha}) = -\psi(1/i\alpha) = -1/(i\bar{\alpha}) = i\alpha$. Therefore, $\psi^2 = id$. Since $\psi \neq \phi$ but both are of order 2, then $G \simeq K_4$, as it is the only group with the properties.

Question 5

Let $E = \mathbb{Q}(\sqrt[3]{13}, \eta)/\mathbb{Q}$ where η is a primitive 3rd root of 1. Determine $\text{Gal}(E/\mathbb{Q})$

Solution: Notice that the splitting field of $f(x) = x^3 - 13 = (x - \sqrt[3]{13})(x - \sqrt[3]{13}\eta)(x - \sqrt[3]{13}\eta^2)$ is E. Thus, the galois group $G = \text{Gal}(E/\mathbb{Q})$ is a subgroup of S_3 and is of degree 6.

This is because $E/\mathbb{Q}$ is Galois (as it is a splitting field, thus normal, of a separable field, as $\mathbb{Q}$ is perfect), and the degree $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{13})][\mathbb{Q}(\sqrt[3]{13}) : \mathbb{Q}]$ where the first term is 2 as $\eta^2 + \eta + 1 = 0$ and $\eta \notin \mathbb{Q}(\sqrt[3]{13})$ as $\mathbb{Q}(\sqrt[3]{13}) \subset \mathbb{R}$ but $\eta \notin \mathbb{R}$. And the second term is 3 because the polynomial $f(x) = x^3 - 13$ is irreducible over $\mathbb{Q}$ by the eisenstein criterion with $f(\sqrt[3]{13}) = 0$.

Therefore, $G \simeq S_3$ as $|S_3| = 6$.

Question 6

Let E be a splitting field of $x^4 - 2$ over $\mathbb{Q}$. Compute $\text{Gal}(E/\mathbb{Q})$

Solution: Notice that $f(x) = x^4 - 2$ is irreducible over $\mathbb{Q}$ by the eisenstein criterion.

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

Then, it is evident that $E = \mathbb{Q}(\sqrt[4]{2}, i)$

As $E/\mathbb{Q}$ is a splitting field over $\mathbb{Q}$, which is a perfect field, then it is normal and separable, thus galois.

Now, $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$, where the first term is 2 as the polynomial x^2+1 is satisfied by i, and $i \notin \mathbb{Q}(\sqrt[4]{2})$ and $i \notin \mathbb{R}$ but $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$. The second term is $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ as $f(x)$ is irreducible and $f(\sqrt[4]{2}) = 0$. Therefore, $[E : \mathbb{Q}] = 8 = |G|$.

As $G = \text{Gal}(E/\mathbb{Q})$ is a splitting field of $f(x)$, then $G \subset S_4$

Notice that $|S_4| = 24 = 8 \cdot 3$, so the subgroup of order 8 of S_4 is unique, and since

$$\{ id, (1234), (13)(24), (1432), (13), (24), (14)(23), (12)(34) \}$$

is a subgroup of S_4, and it is isomorphic to D_8 with $(1234) \mapsto r$ and $(13) \mapsto f$.

Thus, the galois group $\text{Gal}(E/\mathbb{Q}) \simeq D_8$

Question 7

Let η be a primitive 3rd root of 1 and $E = \mathbb{Q}(\sqrt{3}, \sqrt{11}, \eta)$. Find $\text{Gal}(E/\mathbb{Q})$

Solution: Firstly, E is normal if and only if it splits the minimal polynomial of $\sqrt{3}$, $\sqrt{11}$, and η, which it does as

- $m_{\sqrt{3}} \mid x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$
- $m_{\sqrt{11}} \mid x^2 - 11 = (x - \sqrt{11})(x + \sqrt{11})$
- $m_\eta \mid x^2 + x + 1 = (x - \eta)(x - \eta^2)$

Since E is normal, and $\mathbb{Q}$ is perfect, then $E/\mathbb{Q}$ is galois.

Now,

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{3}, \sqrt{11})][\mathbb{Q}(\sqrt{3}, \sqrt{11}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$$

Firstly, $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ since $x^2 - 3$ is irreducible over $\mathbb{Q}$ by the Eisenstein criterion.

Next, $[\mathbb{Q}(\sqrt{3}, \sqrt{11}) : \mathbb{Q}] = 2$ since the minimal polynomial of $\sqrt{11}$ over $\mathbb{Q}(\sqrt{3})$ must divide x^2-11, and $\sqrt{11} \notin \mathbb{Q}(\sqrt{3})$. This is because if it is, $\sqrt{11} = a+b\sqrt{3}$ for some $a, b \in \mathbb{Q}$ as $\sqrt{3}^2 = 3 \in \mathbb{Q}$. Now, squaring both sides gives $11 = a^2+3b^2+2ab\sqrt{3}$, so $a = 0$ or $b = 0$. If $a = 0$, then $11 = 3b^2$ is imposible as $3 \nmid 11$, and if $b = 0$, $11 = a^2$ is not possible as $\sqrt{11} \notin \mathbb{Q}$. This is because $x^2 - 11$ is irreducible over $\mathbb{Q}$ by the Eisenstein criterion.

Then, $[E : \mathbb{Q}(\sqrt{3}, \sqrt{11})] = 2$ as $x^2 + x + 1$ is satisfied by η and $\eta \notin \mathbb{R}$ but $\mathbb{Q}(\sqrt{3}, \sqrt{11}) \subset \mathbb{R}$. So, $\eta \notin \mathbb{Q}(\sqrt{3}, \sqrt{11})$.

Therefore, $[E : \mathbb{Q}] = 8 = |\text{Gal}(E/\mathbb{Q})|$.

As the $\mathbb{Q}$-automorphism must fix the root of x^2-3, x^2-11, and x^2+x+1, then it must send $\sqrt{3} \mapsto \pm\sqrt{3}$, $\sqrt{11} \mapsto \pm\sqrt{11}$, and $\eta \mapsto \eta$ or $\eta \mapsto \eta^2$.

Let

$$\sigma_3 : \sqrt{3} \mapsto -\sqrt{3}, \sqrt{11} \mapsto \sqrt{11}, \text{ and } \eta \mapsto \eta$$
$$\sigma_{11} : \sqrt{3} \mapsto \sqrt{3}, \sqrt{11} \mapsto -\sqrt{11}, \text{ and } \eta \mapsto \eta$$
$$\sigma_\eta : \sqrt{3} \mapsto \sqrt{3}, \sqrt{11} \mapsto \sqrt{11}, \text{ and } \eta \mapsto \eta^2$$

Then, each of σ_3, σ_{11}, and σ_η is of order 2, and the composition are always commutative. Notice that the set $\{ id, \sigma_3, \sigma_{11}, \sigma_\eta, \sigma_3 \circ \sigma_{11}, \sigma_3 \circ \sigma_\eta, \sigma_{11} \circ \sigma_\eta, \sigma_3 \circ \sigma_{11} \circ \sigma_\eta \}$ is a group of order 8 containing $\mathbb{Q}$-automorphisms of E, thus $G = \text{Gal}(E/\mathbb{Q})$ must be that group.

Moreover, as every elements in the group is of order 2, then $G \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$

Question 8

Let α be a root of $x^6 + 3$ and let $E = \mathbb{Q}(\alpha)$. Show that $E/\mathbb{Q}$ is Galois and determine $\text{Gal}(E/\mathbb{Q})$.

Solution: Firstly, notice that $f(x) = x^6 + 3$ is irreducible over $\mathbb{Q}$ by the Eisenstein criterion. Then, if α is a root of $f(x)$, it must follows, that $\alpha, \alpha\eta$, $\alpha\eta^2$, $-\alpha$, $-\alpha\eta$, $-\alpha\eta^2$ are all of the roots of f. This is because f is of degree 6, and $1, \eta, \eta^2, -1, -\eta, -\eta^2$ are pairwise distinct with $\eta^6 = (-1)^6 = 1$, which is because $\eta = e^{i\frac{\pi}{3}}$.

Now, as $\alpha^6 + 3 = 0$, so let $x^2 + x + 1 = 0 = \alpha^6 + 3$. Solving for x gives

$$\begin{aligned} x^2 + x - (\alpha^6 - 2) = 0 \\ x &= \frac{-1 \pm \sqrt{1 + 4\alpha^6 + 8}}{2} \\ &= \frac{-1 \pm \sqrt{9 + 3\alpha^6}}{2} \\ &= \frac{-1 \pm \alpha^3}{2} \end{aligned}$$

Disregarding one of the solutions, it is possible to assigh $\bar{\eta} = \frac{\alpha^3 - 1}{2}$ so that

$$\bar{\eta}^2 + \bar{\eta} + 1 = \frac{\alpha^6 - 2\alpha^3 + 1}{4} + \frac{\alpha^3 - 1}{2} + 1 = \frac{1}{4}(\alpha^6 - 2\alpha^3 + 1 + 2\alpha^3 - 2 + 4) = 0$$

Morover, $\bar{\eta} \neq 1$ as otherwise the minimal polynomial of α must be of degree 3 contradicting the irreducibility of f.

Thus, $\bar{\eta}$ is a primitive third root, which means that

$$\left\{ \alpha, \alpha\eta, \alpha\eta^2, -\alpha, -\alpha\eta, -\alpha\eta^2 \right\} = \left\{ \alpha, \alpha\bar{\eta}, \alpha\bar{\eta}^2, -\alpha, -\alpha\bar{\eta}, -\alpha\bar{\eta}^2 \right\}$$

Now, as $\bar{\eta} \in \mathbb{Q}(\alpha)$, it follows that $\mathbb{Q}(\alpha)$ contains all the roots of f, so it is the splitting field of f. So, $[E : \mathbb{Q}] = \deg(f) = 6$.

Then, let $G = \mathrm{Gal}(E/\mathbb{Q})$ is of order 6. Consider two $\mathbb{Q}$-automorphisms of E which are ϕ and ψ such that $\phi(\alpha) = -\alpha$ and $\psi(\alpha) = \alpha\bar{\eta}$. Then,

$$\begin{aligned} \phi \circ \psi(\alpha) &= \phi(\alpha\bar{\eta}) \\ &= -\alpha \cdot \phi\left(\frac{\alpha^3 - 1}{2}\right) \\ &= -\alpha\left(\frac{-\alpha^3 - 1}{2}\right) \\ &= \alpha\left(\frac{\alpha^3 - 1}{2} + 1\right) \\ &= \alpha(\bar{\eta} + 1) \end{aligned}$$

and

$$\begin{aligned} \psi \circ \phi(\alpha) &= \psi(-\alpha) \\ &= -\psi(\alpha) \\ &= -\alpha\bar{\eta} \end{aligned}$$

Now, as $\alpha(\bar{\eta} + 1) - -\alpha\bar{\eta} = \alpha\bar{\eta}^2 + \alpha\bar{\eta} = \alpha\bar{\eta}(\bar{\eta}^2) = \alpha \neq 0$, then $\phi \circ \psi \neq \psi \circ \phi$.

Thus G is not abelian. Therefore $G \simeq D_6$, as it is the unique non-abeian group of order 6.

Question 9

Let E be a splitting field of $x^4 + 1$ over $\mathbb{Q}$. Find $\mathrm{Gal}(E/\mathbb{Q})$.

Solution: Notice that $f(x) = x^4 + 1$ is irreducible because if it is not, then $x^4 + 1$ should be reducible over $\mathbb{F}_2$. This is because if $f(x) = P(x)Q(x)$ over $\mathbb{Q}$, then $\bar{f}(x) = \bar{P}(x)\bar{Q}(x)$, where $f = \bar{f}, P = \bar{P}, Q = \bar{Q} \pmod 2$. As f is monic, this also means that one of the irreducible divisors of $\bar{f}$ is a monic.

However, $\gcd(x^4 + 1, x^{2^2} - x) = \gcd(x + 1, x^3 - 1) = \gcd(x + 1, x - 1) = 1$, which contradicts the existence of such divisors, so $f(x)$ must be irreducible.

Since

$$f(x) = x^4 + 1 = (x^2 - i)(x^2 + i) = (x - \sqrt{i})(x + \sqrt{i})(x - i\sqrt{i})(x + i\sqrt{i})$$

Notice that $-\sqrt{i} = \sqrt{i}^5$, $i\sqrt{i} = \sqrt{i}^3$, and $-i\sqrt{i} = \sqrt{i}^7$. Then, clearly, $E = \mathbb{Q}(\sqrt{i})$. Therefore, $[E : \mathbb{Q}] = 4$.

This means that $G = \mathrm{Gal}(E/\mathbb{Q})$ is a subgroup of order 4.

Let ϕ be a $\mathbb{Q}$-automorphism of E that sends $\sqrt{i}$ to $i\sqrt{i}$. Then,

$$\phi^2(\sqrt{i}^k) = \phi((i\sqrt{i})^k) = \phi(\sqrt{i}^{3k}) = (i\sqrt{i})^{3k} = \sqrt{i}^{9k} = \sqrt{i}^k$$

As ϕ^2 fixes $\mathbb{Q}$ and all the roots of $f(x)$, it fixes E. So, $\phi^2 = id$.

Now, let ψ be another $\mathbb{Q}$-automorphism of E that sends $\sqrt{i}$ to $-\sqrt{i}$. Then,

$$\psi^2(\sqrt{i}^k) = \psi((-1)^k\sqrt{i}^k) = (-1)^k\psi(\sqrt{i}) = (-1)^{2k}\sqrt{i}^k = \sqrt{i}^k$$

Again, ψ^2 fixes $\mathbb{Q}$ and all roots of E, so it is the identity.

As $\phi \neq \psi$ because $\phi(\sqrt{i}) \neq \psi(\sqrt{i})$, there are at least two elements of G of order 2. However, there is only one group with these properties, which is K_4, so $G \simeq K_4 \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. This is because there are two groups of order 4, which are C_4 and K_4, but C_4 contains only one element with order 2.

Question 10

Let E/F be a Galois extension such that $[E : F]$ is even. Prove that there exists a subfield K of E containing F such that $[E : K] = 2$

Solution: Let $G = \mathrm{Gal}(E/F)$ so that $|G| = 2n$ for some n. By the Sylow's theorems, there is a subgroup of order of order 2, let $H < G$ with $|H| = 2$.

Then, consider the fixed point of H, which is

$$K = \{\, a \in E \mid \sigma(a) = a \forall \sigma \in H \,\}$$

Notice that $H < G = \mathrm{Gal}(E/F)$, thus all elements of H fixes F. Hence, $F \subset K$. Also, K is a field because $\sigma \in H$ is an automorphism. If σ fixes $k, linK$, then it must also fix $k^{-1}, kl, k - l$, as $\sigma(1) = \sigma(k)\sigma(k^{-1})$ and the rest due to the properties of homomorphism.

By the Galois correspondence theorem, $\mathrm{Gal}(E/K) = H$, therefore, $[E : K] = |H| = 2$.