1

a

Since $K \subseteq \mathbb{Q}(\zeta_n)$, then the characteristic of K is 0, so K must contain $\mathbb{Q}$, i.e., $K/\mathbb{Q}$ is a subextension of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, so

$$\operatorname{Gal}(\mathbb{Q}(\zeta_n)/K) \leq \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

Since $(\mathbb{Z}/n\mathbb{Z})^\times$ is abelian, every subgroup is normal, so $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/K)$ is a normal subgroup. Hence $K/\mathbb{Q}$ is Galois by the fundamental theorem.

b

Moreover, the fundamental theorem gives us

$$\operatorname{Gal}(K/\mathbb{Q}) \cong \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})/\operatorname{Gal}(\mathbb{Q}(\zeta_n)/K)$$

and the quotient of an abelian group is, again, abelian.

2

a

The polynomial $x^4 - 2x^2 + 20 \in \mathbb{Q}[x]$ has α as a root, so has the minimal polynomial of α over $\mathbb{Q}$ as a factor. In particular, $\deg m_{\alpha,\mathbb{Q}}(x) \leq 4$.

Since $\alpha^2 - 5 = \sqrt{5}$, then we know $\sqrt{5} \in \mathbb{Q}(\alpha)$. Then $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\alpha)$, so

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{5})] \cdot 2.$$

So $2 \mid [\mathbb{Q}(\alpha) : \mathbb{Q}]$, and we already have $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 4$. So the degree is either 2 or 4. We claim that $\alpha \notin \mathbb{Q}(\sqrt{5})$, which will imply $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{5})] > 1$, from which it then follows that $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 4$. If this is the case, then $m_{\alpha,\mathbb{Q}}(x) = x^4 - 2x^2 + 20$.

Suppose to the contrary that $\alpha \in \mathbb{Q}(\sqrt{5})$ so $\alpha = a + b\sqrt{5}$ for some $a, b \in \mathbb{Q}$.

b

3

a

As the splitting field of $x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$, a separable polynomial in $\mathbb{Q}[x]$, we have that $K/\mathbb{Q}$ is Galois

b

The roots of the above polynomial are $\pm\sqrt{2}, \pm\sqrt{3}$, so in particular we know $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Since $\sqrt{2}, \sqrt{3}, \sqrt{6}$ are all not squares in $\mathbb{Q}$, then K is a biquadratic extension, so its Galois group is isomorphic to the Klein 4-group.

c

The Klein 4-group has the subgroups 0×0, $\mathbb{Z}/2\mathbb{Z} \times 0$, $0 \times \mathbb{Z}/2\mathbb{Z}$, and itself. By the fundamental theorem on $\mathrm{Gal}(K/\mathbb{Q})$, these correspond to the fixed subfields K, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}$, respectively.

4

a

Let $S \subseteq \overline{\mathbb{Q}}$ be the set of roots in $\overline{\mathbb{Q}}$ of the polynomial $f(x)$, then as the splitting field of $f(x)$, we know $K = \mathbb{Q}(S)$. In particular, for any $\alpha \in S$, the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a subextension of $K/\mathbb{Q}$, and is the fixed field of some subgroup of $\mathrm{Gal}(K/\mathbb{Q})$, by the fundamental theorem.

Since $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, then every subgroup is a normal subgroup, which implies that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension. In particular, it is a normal extension, so $m_{\alpha,\mathbb{Q}}(x)$ splits completely in $(\mathbb{Q}(\alpha))[x]$. Since α is a root of the irreducible polynomial $f(x)$, then we must have $m_{\alpha,\mathbb{Q}}(x) = af(x)$ for some $a \in \mathbb{Q}^{\times}$. Therefore, $f(x) = a^{-1}m_{\alpha,\mathbb{Q}}(x)$ also splits over $\mathbb{Q}(\alpha)$, so $\mathbb{Q}(\alpha)$ must contain its splitting field K. This implies

$$[K : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg m_{\alpha,\mathbb{Q}}(x) = \deg f(x) = n.$$

Since $\alpha \in K$, then $\mathbb{Q}(\alpha) \subseteq K$, so $n = [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [K : \mathbb{Q}]$, hence $[K : \mathbb{Q}] = n$.

b

If $f(x)$ is not irreducible, then we cannot necessarily deduce that it splits over any given $\mathbb{Q}(\alpha)$, as the minimal polynomial of α will simply divide, but may not equal, $f(x)$.

5

We know that $K/\mathbb{F}_7$ is a finite extension, so we must have $K = \mathbb{F}_{7^d}$ for some $d \in \mathbb{Z}_{>0}$. Then

$$\mathrm{Gal}(K/\mathbb{F}_7) = \mathrm{Gal}(\mathbb{F}_{7^d}/\mathbb{F}_7) \cong \mathbb{Z}/d\mathbb{Z}.$$

Since $\mathbb{F}_{7^2} = \mathbb{F}_{49} \subseteq K = \mathbb{F}_{7^d}$, then we know $2 \mid d$.

One can check that $x^3 - \overline{2}$ has no roots in $\mathbb{F}_7$, so it is irreducible in $\mathbb{F}_y[x]$. So if $\alpha \in \overline{\mathbb{F}_7}$ is a root of $x^3 - \overline{2}$, then $m_{\alpha,\mathbb{F}_7}(x) = x^3 - \overline{2}$, so

$$[\mathbb{F}_7(\alpha) : \mathbb{F}_7] = \deg m_{\alpha,\mathbb{F}_7}(x) = \deg(x^3 - \overline{2}) = 3.$$

Moreover, $\mathbb{F}_7(\alpha)$ must be contained in the splitting field of $x^3 - \overline{2}$, which is K, so

$$d = [K : \mathbb{F}_7] = [K : \mathbb{F}_7(\alpha)][\mathbb{F}_7(\alpha) : \mathbb{F}_7] = [K : \mathbb{F}_7(\alpha)] \cdot 3,$$

implying $3 \mid d$.

As the splitting field of a degree 3 polynomial over $\mathbb{F}_{7^2}$, the degree of K over $\mathbb{F}_{7^2}$ is at most $3! = 6$, and

$$[K : \mathbb{F}_7] = [K : \mathbb{F}_{7^2}][\mathbb{F}_{7^2} : \mathbb{F}] = [K : \mathbb{F}_{7^2}] \cdot 2.$$

And we know that $3 \mid [K : \mathbb{F}_7]$, so $[K : \mathbb{F}_{7^2}]$ is either 6 or 12.

Since both 2 and 3 divide $d = [K : \mathbb{F}_7] \leq 6$, then it must be exactly 6. Hence,

$$\mathrm{Gal}(K/\mathbb{F}_7) = \mathrm{Gal}(\mathbb{F}_{7^6}/\mathbb{F}_7) \cong \mathbb{Z}/6\mathbb{Z}.$$

6

Each $\mathbb{Q}$-embedding $\sigma : K \hookrightarrow \overline{\mathbb{Q}}$ can be extended (not necessarily uniquely) to a $\mathbb{Q}$-embedding $\tilde{\sigma} : L \hookrightarrow \overline{\mathbb{Q}}$ such that $\tilde{\sigma}|_K - \sigma$. As $L/\mathbb{Q}$ is Galois, therefore normal, $\tilde{\sigma}(L) = L$, and since $\tilde{\sigma}|_{\mathbb{Q}} = \sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$, then we have $\tilde{\sigma} \in \mathrm{Gal}(L/\mathbb{Q})$.

Since $K/\mathbb{Q}$ is finite, it is separable, so $[K : \mathbb{Q}] = n$ is the number of $\mathbb{Q}$-embeddings from $K \to \overline{\mathbb{Q}}$.