Problem 4

Let ρ be a primitive cube root of 1.

(a) We wish to write $\frac{1}{\rho^2+1}$ as a polynomial in ρ.

$$\frac{1}{\rho^2+1} = \frac{1}{\rho^2+1} \cdot \frac{\rho^2-1}{\rho^2-1} = \frac{\rho^2-1}{\rho^4-1} = \frac{\rho^2-1}{\rho-1} = \frac{(\rho+1)(\rho-1)}{\rho-1} = \rho+1$$

(b) We will build the minimal polynomial in reverse by assuming that we have a solution to a polynomial $X = \sqrt[3]{4} + \sqrt[3]{2}$. We will then mess around with this equation until we get a polynomial in $\mathbb{Q}[X]$. Cubing both sides we get

$$\begin{aligned} X^3 &= 4 + 3\big(\sqrt[3]{4}\big)^2\sqrt[3]{2} + 3\sqrt[3]{4}\big(\sqrt[3]{2}\big)^2 + 2 \\ &= 6 + 3\sqrt[3]{4}\sqrt[3]{2}\big(\sqrt[3]{4} + \sqrt[3]{2}\big) \\ &= 6 + 3\sqrt[3]{8}X \\ &= 6 + 6X \end{aligned}$$

Thus $\sqrt[3]{4} + \sqrt[3]{2}$ is a root of the polynomial $X^3 - 6X - 6$. Also, by Eisenstein's criteria (with p=2 or 3) we see that this is an irreducible polynomial. Since it is a monic irreducible polynomial, it must be the minimal polynomial of $\sqrt[3]{4} + \sqrt[3]{2}$.

(c) I claim that $\mathbb{F} = \mathbb{Q}(\rho, \sqrt[3]{2})$ is the splitting field of $X^3 - 2$ (and thus a normal extension of $\mathbb{Q}$). The three roots of $X^3 - 2$ are $\sqrt[3]{2}, \rho\sqrt[3]{2}$, and $\rho^2\sqrt[3]{2}$. Thus, $\mathbb{Q}(\sqrt[3]{2})$ is a subfield of the splitting field. However, it cannot be the splitting field itself since it is an entirely real extension, while the other two roots are complex. Thus the splitting field has degree at least 6. However, $\mathbb{F}$ has degree 6 and contains all three roots of $X^3 - 2$ so it must be the splitting field. Since the degree of $X^3 - 2$ is 3, the Galois group $Gal(\mathbb{F}/\mathbb{Q})$ is a subgroup of S_3, the symmetric group on 3 elements. However, since the degree of the extension $\mathbb{F}$ is 6, $Gal(\mathbb{F}/\mathbb{Q}$ must have order 6. Thus the Galois group must be S_3.

(d) We could look at the generators of the Galois group and look at their fixed elements to find the intermediate fields between $\mathbb{Q}$ and $\mathbb{F}$, but there is an easier way. Since S_3 has one subgroup of order 3 (A_3) and 3 subgroups of order 2 (generated by the three transpositions), we know by the fundamental theorem of Galois theory that there is one subfield of $\mathbb{F}$ of degree 2 over $\mathbb{Q}$ and 3 subfields of $\mathbb{F}$ of degree 3 over $\mathbb{Q}$. It is clear that $\mathbb{Q}(\rho)$ is a subfield of $\mathbb{F}$ and that it has degree $\phi(3) = 2$. Also, the fields $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\rho\sqrt[3]{2})$, and $\mathbb{Q}(\rho^2\sqrt[3]{2})$ are all distinct intermediate fields between $\mathbb{Q}$ and $\mathbb{F}$ of degree 3. Thus, we have found all intermediate fields.

(e) For this part it actually helps to know the generators of the Galois group. It is easy to see that $Gal(\mathbb{F}/\mathbb{Q})$ is generated by:

$$\begin{aligned} \sigma : \rho &\mapsto \rho \\ \sqrt[3]{2} &\mapsto \rho\sqrt[3]{2} \\ \text{and } \tau : \rho &\mapsto \rho^2 \\ \sqrt[3]{2} &\mapsto \sqrt[3]{2} \end{aligned}$$

For σ has order 3 and τ has order 2 and $\sigma\tau = \tau\sigma^2$ so they generate an non-abelian group of order 6 (it must be S_3). Now, looking at the proof of the primitive element theorem, the primitive element constructed is of the form $\rho + c\sqrt[3]{2}$ where $c \in \mathbb{Q}$. We start by guessing that $x = \rho + \sqrt[3]{2}$ is the primitive element. The easiest way to do this is to show that it is not fixed by any of the elements of the Galois group. Actually, we need only to check that it is not fixed by any of the generators of the subgroups: $\sigma, \tau, \sigma\tau, \sigma^2\tau$. It is not fixed by any of these, and so $\mathbb{F} = \mathbb{Q}(\rho + \sqrt[3]{2})$.