Question 1

(a) First we notice that $f(x) = x^5 - 64x + 2 \in \mathbb{Q}[x]$ is irreducible by 2-Eisenstein, and thus it is seperable since $\mathbb{Q}$ is perfect. So, we need to only show that the Galois group of $f(x)$ is S_5, and the insolvability will follow from the insolvability of S_5. For $f(x)$ to have Galois group that is S_5, we need that it has exactly two non-real roots. Notice, $f(-1000) < 0$, $f(-1) > 0$, $f(1) < 0$ and $f(1000) > 0$, so by the intermediate value theorem, we must have atleast 3 real roots. Suppose the roots of $f(x)$ are α_i for $1 \leq i \leq 5$, then we know $\sum_i \alpha_i = 0$ and $\sum_{i<j} \alpha_i \alpha_j = 0$ thus,

$$\left(\sum_i \alpha_i\right)^2 = \sum_i \alpha_i^2 - 2\sum_{i<j} \alpha_i \alpha_j = 0 - 2 \cdot (0) = 0\,.$$

Therefore, we see that not all the roots of $f(x)$ are real, and thus we need atleast two non-real roots, and our lemma applies and $\mathrm{Gal}(f(x)) \cong S_5$ and $f(x)$ is not solvable by radicals over $\mathbb{Q}$.

(b) Since $f(x)$ is irreducible over $\mathbb{Q}$, it is also seperable. Thus, since K is the splitting field of $f(x)$, K is a Galois Extensions. Thus, $|G| = |\mathrm{Gal}(f(x))| = [K : \mathbb{Q}] = p^n$. This is useful, since by Galois' Theorem, it suffices to show that the Galois Extension is solvable. We apply induction on the power of the order of the group. The base case is $|G| = p$, with prime p. This is clearly solvable since it is simple and abelian. Proceeding by induction, suppose the result for $|G| = p^{n-1}$. If we have a group G such that $|G| = p^n$, then since $p \,|\, |G|$, we have a subgroup N with $|N| = p$ that is generated by a single element of G. Moreover, $N \trianglelefteq G$, and N is solvable by the base case. Finally, G/N is solvable since $|G/N| = |G|/|N| = p^{n-1}$, and thus by proposition G must be solvable.

Question 2

First, we check if $f(x)$ is irreducible. Using the Mod-2 irreducibility test we see that

$$\bar{f}(x) = x^3 + x + 1 \implies \bar{f}(0) = 1 \quad \& \quad \bar{f}(1) = 1\,.$$

Clearly we have no roots over $\mathbb{Z}_2$ and thus $f(x)$ is irreducible over $\mathbb{Q}$, and thus seperable. First we show that $f(x)$ is indeed solvable by radicals over $\mathbb{Q}$, which by Galois' Theorem requires us to find $\text{Gal}(f(x))$. Since $f(x)$ is a cubic, already in it's depressed form, we see that

$$\text{disc}(f(x)) = -4(-3)^3 - 27(-1)^2 = 4 \cdot 3^3 - 3^3 = 3 \cdot 3^3 = 3^4 = 9^2$$

which is a perfect square, and hence $\text{Gal}(f(x)) \cong A_3$. But, A_3 is abelian and simple since $|A_3| = 3$, and thus $\text{Gal}(f(x))$ is sovable, and $f(x)$ is solvable by radicals over $\mathbb{Q}$.

Now we need to show that K is not a radical extension of $\mathbb{Q}$. Suppose that K is indeed a radical extension. Notice, we already have found that $\text{Gal}(f(x)) = A_3$, and thus we know that all of the roots of $f(x)$ must be real, from the contrapositive of our two non-real roots lemma. Moreover, since the Galois group of $f(x)$ is simple and abelian, the field structure must be just a single extension, by the Fundemental theorem of Galois Theory, and thus K must be a simple radical extension. However, this is a contradiction, since we can't have real simple radical extensions for irreducible cubics.

Question 3

(a) First, we notice that since $g(x)$ is a minimal polynomial, and it is over the perfect field $\mathbb{R}$, and thus $g(x)$ is also seperable. Since K is the splitting field of a seperable irreducible polynomial, $g(x)$, it is a Finite Galois Extension.

(b) By the Fundemental Theorem, we have

$$[K : E] = |\mathrm{Gal}(K/E)| = |\mathrm{Gal}(K/\mathrm{Fix}(H))| = |H| = 2^j$$

and the Tower Theorem give us

$$2^j m = |\mathrm{Gal}(K/\mathbb{R})| = [K : \mathbb{R}] = [K : E][E : \mathbb{R}] = 2^j[E : \mathbb{R}] \implies [E : \mathbb{R}] = m.$$

(c) Notice that since E is an intermediate field of $K/\mathbb{R}$, we know it is algebraic. By the simple extension lemma, we know that $E = \mathbb{R}(\beta)$ where for some $\beta \in E \setminus \mathbb{R}$. Suppose $f(x) \in \mathbb{R}[x]$ is the minimal polynomial of β over $\mathbb{R}$, but we know that since $[E : \mathbb{R}] = m$ the degree of $f(x)$ is odd, and by the intermediate value theorem, this tells us that $f(x)$ has atleast one real root. But, this implies that $f(x)$ is reducible over $\mathbb{R}$, and so the only way this is true is if the degree of $f(x)$ is $1 \implies [E : \mathbb{R}] = 1$.

(d) From above, we now know that $|G| = |\mathrm{Gal}(K/\mathbb{R})| = [K : \mathbb{R}] = 2^j$, and we know that the tower $K/\mathbb{C}/\mathbb{R}$ is useful here, since $\mathbb{R}(i) = \mathbb{C}$, and thus we can compute that

$$[K : \mathbb{C}] = \frac{[K : \mathbb{R}]}{[\mathbb{C} : \mathbb{R}]} = 2^{j-1}.$$

So, we need to see that there is an intermediate field between $\mathbb{C}$ and K. Notice, $2 \mid \mathrm{Gal}(K/\mathbb{C})$, hence $\exists H \leq \mathrm{Gal}(K/\mathbb{C})$ such that $|H| = 2$, and so by the fundamental theorem, which is inclusion reversing, we have

$$[\mathrm{Fix}(H) : \mathbb{C}] = 2$$

and so our intermediate field is $\mathrm{Fix}(H)$.