Question 1

(a) Since $f(x)$ is non-constant (since it is irreducible), seperable and of degree n, if we let K be the splitting field of $f(x)$, then by theorem we have that $|\text{Gal}(K/F)| = |\text{Gal}(f(x))| = [K : F]$. However, $f(x)$ is irreducible, so we can consider the field extension $E = F(\alpha)$, where $\alpha \in K$ is a root of $f(x)$. Applying the Tower Theorem,

$$[K : F] = [K : F(\alpha)][F(\alpha) : F] = [K : F(\alpha)]n \implies n \,|\, [K : F] = |G|\,.$$

Moreover, since $f(x)$ is seperable and irreducible, we have that $G \cong H \leq S_n$, and by Lagrange, $|G| \,|\, |S_n| = n!$, as required.

(b) By the previous lemma, $2 \,|\, |G| = |\text{Gal}(f(x))|$ and $|G| \,|\, 2! = 2$, so $|G| = 2$, and all groups of order 2 are known up to isomorphism to be $\mathbb{Z}_2$, so $G \cong Z_2$.

(c) By our previous lemma, we better have that $4 \,|\, |G|$, and $|G| \,|\, 4! = 24$, so $|G| \in \{4, 12\}$, and since $|S_3| = 6$, we clearly can't have an isomorphism, and further there is no quartic that would give such an isomorphism.

(d) We can use the polynomial $f(x) = (x+1)(x^3 - 2) \in \mathbb{Q}[x]$. Notice that it is already separated into it's two irreducible factors just to make it clear that the product is not irreducible. Further, this is seperable, as the four roots are $\{-1, \sqrt[3]{2}, \xi_3 \sqrt[3]{2}, \xi_3^2 \sqrt[3]{2}\}$, which are all distinct. Since we have four distinct roots, in our splitting field, we will have $3 \cdot 2 \cdot 1 = 4!$ choices for $\varphi \in G = \text{Gal}(f(x))$ to send our roots, since the first root already is in $\mathbb{Q}$, and hence is fixed by all φ. Thus, we can form the isomorphism with the indices; label the roots as $\alpha_1, \alpha_2, \alpha_3$, where we ignore the first root (since it is fixed), and we see that $\varphi(\alpha_i) = \alpha_j$, $i, j \in \{1, 2, 3\}$, and this is exactly the S_3 group on the indices. So, $G \cong S_3$.

Question 2

(a) We prove by contrapositive. Suppose $f(x)$ is reducible and seperable with splitting field K, and $f(x) \in F[x]$. Since $f(x)$ is reducible, suppose $p(x), q(x) \in F[x]$ such that $p(x)q(x) = f(x)$ where $p(x)$ and $q(x)$ are irreducible. Since $f(x)$ is seperable, $q(x)$ and $p(x)$ are also seperable. Consider $\phi \in \text{Gal}(f(x))$, then if α is a root of $p(x)$, we know that $\phi(\alpha)$ better also be a root of $p(x)$, since that is the minimal polynomial (up to unit multiple). Thus, there is no way to get from a root of $p(x)$ to a root of $q(x)$ with the galois group, hence $\text{Gal}(f(x))$ is not transitive.

(b) It suffices to show that the two polynomials have the same Galois groups, since **(a)** gave us the converse to a corollary we already know, and thus we have that a polynomial is irreducible iff it's Galois group is transitive. Hence, if $f(x)$ and $g(x)$ have the same Galois group (possibly up to isomorphism), then $f(x)$ is irreducible $\iff$ $\text{Gal}(f(x))$ is transitive $\iff$ $\text{Gal}(g(x))$ is transitive $\iff$ $g(x)$ is irreducible.

To see that the two share a Galois group, we first notice that if $f(\alpha) = 0$, then $g(1/\alpha) = (1/\alpha)^n f(\alpha) = 0$, and we have a motivation for a map between the roots of $f(x)$ and $g(x)$. Let $F = \text{Gal}(f(x))$ and $G = \text{Gal}(g(x))$, and notice we can define a map between the two groups by sending the automorphisms based on where they send roots. That is, consider $\phi \in F$ and let $\alpha \in K$ be a root of $f(x)$, then notice that since ϕ is an automorphism, it is a homomorphism with a trivial kernel, thus

$$1 = \phi(1) = \phi(\alpha\alpha^{-1}) = \phi(\alpha)\phi(1/\alpha) \implies (\phi(\alpha))^{-1} = \phi(1/\alpha)$$

and since ϕ is defined by how it sends its roots to other roots, this just showed us that it better send the inverse of its roots to the appropriate inverse. Then, $\phi \in G$, and similarly, if $\psi \in G$, we can make the same argument as above and get that $\psi \in F$, hence $G \subseteq F$ and $F \subseteq G$ and thus $F = G$.

(c) By definition,

$$g(x) = x^4\left(3\frac{1}{x^4} + 9\frac{1}{x^3} - 21\frac{1}{x^2} + 81\frac{1}{x} + 1\right) = x^4 + 81x^3 - 21x^2 + 9x + 3\,.$$

Notice that $g(x)$ just flips the coeffecient order! From this, we immediatly see that $g(x)$ is irreducible over $\mathbb{Q}$ by 3-Eisenstien, and thus by **(b)** $f(x)$ is irreducible over $\mathbb{Q}$.

Question 3

(a) Suppose $f(x)$ and $g(x)$ share a root in K, call it α, which is not repeated. Since K is a splitting field of $f(x)g(x)$, it is an algebraic extension, and thus $\exists\, p(x) \in F[x]$ minimal polynomial with α as a root. But, both $f(x)$ and $g(x)$ have this root, so we must have that $p(x) \mid f(x)$ and $p(x) \mid g(x)$, but both $f(x)$ and $g(x)$ are irreducibile, so either $p(x) = f(x)$ or $p(x) = g(x)$, but then either way we again have one polynomial dividing the other. This is a contradiction, so we $f(x)$ and $g(x)$ do not share a common root in K.

(b) We prove this by induction on the number of minimal polynomials, n. The base case was done in **(a)**, since we can replace $f(x)$ and $g(x)$ with $p_1(x)$ and $p_2(x)$. Proceeding by induction, suppose the result for the nth case. Consider the following product,

$$f(x) = p_1(x)p_2(x)\dots p_n(x) \cdot p_{n+1}(x)$$

where we know $g(x) = \prod_{k=1}^{n} p_k(x)$ is seperable. Suppose $f(x)$ was not seperable, then we would have a multiple root in the splitting field. By the inductive hypothesis, we already have that $g(x)$ is seperable, so this would imply that $p_{n+1}(x)$ is not seperable, but this is a contradiction. Therefore, $f(x)$ is seperable.

Question 4

(a) for (1324), notice that

$$\alpha_1 = \sqrt[4]{2} \to \alpha_3 = i\sqrt[4]{2} \quad \alpha_3 = i\sqrt[4]{2} \to \alpha_2 = -\sqrt[4]{2}$$

which actually immediately defines the rest of our group, since we now need to send α_2 to α_4 and we need to send α_4 to α_1, in order for the root relationships to be preserved. This permutation group element preserves this, hence (1324)$\in G$.

We note that first (14) gives $\alpha_1 \to \alpha_4$ which forces $\alpha_2 \to \alpha_3$, and if $\alpha_4 \to \alpha_1$, then $\alpha_3 \to \alpha_2$, which agree with the transpositions, and hence $(14)(23) \in G$.

(b) Looking at the plot, and the fact that our two elements of the Galois group above are just a rotation and reflection respectively, we can conclude that the group will be isomorphic to D_8, the dihedral group of a square.