15.8.1 Since we're doing this proof by induction, we only need to find that for a given finite field F, that for $K = F(\alpha, \beta)$, there exists $\gamma \in K$ such that $K = F(\gamma)$. Note that since $[K : F]$ is finite implies that K is a finite field as well. We know that $K^\times$ is a cyclic group from chapter 15.7. Furthermore we know that cyclic groups have a single generator. Let γ be the generator of $K^\times$. Since K will contain all of the powers of γ, and there exists $m, n \in \mathbb{N}$ such that $\gamma^m = \alpha, \gamma^n = \beta$, therefore $F(\gamma) = K$.

16.3.1 Suppose f is degree n with coefficents in the field F, and let L be the spliting field. We want to show that $[K : F] \mid n!$. Note that since K is a splitting field then $[K : F]$ is the cardinality of the galois group $G(K/F)$. Since $G(K/F)$ is a group operating on n elements, then we know by Cayley's theorem that $G(K/F) < S_n$. Therefore by Lagranges theorem $|G(K/F)| \mid n! = [K : F] \mid n!$.

16.3.2 b Note that $x^4 - 1 = (x^2 + 1)(x - 1)(x + 1)$ over $\mathbb{Q}$. Since we only need the splitting field of $x^2 + 1$ then we only need to adjoin i, making the extension degree 2.

c For $x^4 + 1$, we can see that $\sqrt{i}$ satisfies this equation. Since $\sqrt{i}$ is not in the extension $\mathbb{Q}(i)$ then we have the further degree two extension of $\mathbb{Q}(\sqrt{i})$. Since we have two degree 2 extensions, then the total extension is of degree 4.

16.3.3 Let $F = \mathbb{F}_2(u)$, where F is the field of rational functions. We want to show that $x^2 - u$ is irreducible. Note that if $x^2 - u$ is reducible then there exists $f, g \in F$ such that $(x - f)(x - g) = x^2 - u$, with $fg = -u, f + g = 0$. Therefore $g = \frac{-u}{f}, f^2 = u$. This implies that $f = \sqrt{u}$, however this is a contradiction as u is a transcendental element, and $\sqrt{u}$ is not defined in F. If we however consider the field extension $F(i\sqrt{u})$ then $(x + i\sqrt{u})^2 = x^2 + 2i\sqrt{u}x - u = x^2 - u$, demonstrating a double root.

16.4.1 (a) For $\mathbb{Q}(\sqrt[3]{2})$, there is either 1 or 3 automorphisms, and since $x^3 - 2$ is the irreducible polynomial of $\sqrt[3]{2}$ then an automorphism must map to another root. Since the other roots of $x^3 - 2$ are complex, and $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ then the only automorphism is the identity, and there is exactly 1. For $\mathbb{Q}(\sqrt[3]{2}, \omega)$, since this is the splitting field for $x^3 - 2$ implies that there must be 6 automorphisms. Futhermore $\mathbb{Q}(\sqrt[3]{2}, \omega)$ must contain all of the automorphisms of $\mathbb{Q}(\omega)$, in which there are 2, $\{id, \omega \mapsto \omega^2\}$. Thus to exhaustively find the galois group $G(\mathbb{Q}(\sqrt[3]{2}, \omega), \mathbb{Q})$, we need to find the 3 automorphisms within $G(\mathbb{Q}(\sqrt[3]{2}, \omega), \mathbb{Q}(\omega)$. Note that the only automorphism which leaves $\{1, \omega, \omega^2\}$ untouched is $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$ and composing it once more, $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2$. Note that if we take first $\omega \mapsto \omega^2$ and then $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$ we get that $\sqrt[3]{2}\omega^2 \mapsto \sqrt[3]{2}\omega^2$, however if done in the opposite order we get that $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2$. Thus our group of automorphisms is isomorphic to the non-abelian group of order 6, which would be S_3. This means that all of the automorphisms simply permute the three roots.