Question 1

(a) First, we need to check that the polynomial is irreducible. Using Mod-2 irreducibility we see

$$\bar{f}(x) = x^3 + x^2 + 1 \implies \bar{f}(0) = 1 \quad \& \quad \bar{f}(1) = 1$$

so $f(x)$ is irreducible, and since $\mathbb{Q}$ is perfect, we know $f(x)$ is also seperable. Thus, we first need to find the depressed cubic $f(x)$ corresponds with. Notice, if we let $g(x) = f(x-1)$, we get

$$g(x) = (x-1)^3 + 3(x-1)^2 - 2(x-1) + 1 = (x^2 - 2x + 1)(x+2) - 2x + 3 = x^3 + 2x^2 - 2x^2 - 4x + x + 2 - 2x + 3$$

$$g(x) = x^3 - 5x + 1$$

and we see that the discriminant is

$$\operatorname{disc}(g(x)) = -4(-5)^3 - 27(5)^2 < 0$$

which is not a perfect square, and so we can conclude that $\operatorname{Gal}(f(x)) \cong S_3$.

(b) We know $f(x) = x^4 + 3x + 3$ is irreducible by 3-Eisenstien, and thus also seperable. We have

$$\operatorname{Res}(f(x)) = x^3 - 12x - 9\,.$$

This is not irreducible, and we know that -3 is a root of this polynomial. So, we can see that

$$\operatorname{Res}(f(x)) = (x+3)(x^2 - 3x - 3)$$

where the quadratic is irreducible by 3-Eisenstien. So, we need to find the size of the Galois group of $\operatorname{Res}(f(x))$, but we see that $\operatorname{Gal}(f(x)) \cong \mathbb{Z}_2$, and so $m = 2$. Thus, we need to check if the Galois group of $f(x)$ is isomorphic to $\mathbb{Z}_4$ or D_4. Let $u = -3$, and L the splitting field of $\operatorname{Res}(f(x))$, then consider

$$x^2 + 3x + 3 \qquad\qquad \& \qquad\qquad x^2 + 3\,.$$

Notice that the roots of $x^2 - 3x - 3$ are

$$\frac{3 \pm \sqrt{9+12}}{2} = \frac{3 \pm \sqrt{21}}{2} = \frac{3 \pm \sqrt{3 \cdot 7}2}{}.$$

Notice that the second polynomial has roots $\pm i\sqrt{3}$ and this clearly does not split over L. So, we see that

$$\operatorname{Gal}(f(x)) = D_4\,.$$

(c) If $f(x) = x^4 + 4x^2 + 1$, then we first check if $f(x)$ is irreducible. We try the Mod-3 irreducibility,

$$\operatorname{Res}(f(x)) = x^3 - 4x^2 - 4x + 16 = (x-2)(x^2 - 2x - 8) = (x-2)(x-4)(x+2)\,.$$

So, we have that the resolvant splits over $\mathbb{Q}$, and so $|\operatorname{Gal}(\operatorname{Res}(f(x)))| = 1$, and thus

$$\operatorname{Gal}(f(x)) \cong \mathbb{Z}_2 \times \mathbb{Z}_2\,.$$

Question 2

It suffices to show that the two groups have different sizes. To see this, we first find the roots of $p(x)$ and $q(x)$. Notice that they are $\frac{-1\pm i\sqrt{3}}{2}$ and $\pm i\sqrt{3}$ respectively. But, this just means that both polynomials have the same splitting field, $\mathbb{Q}(i\sqrt{3})$, which is Galois by construction. Thus, both polynomials have the same Galois group, $\mathrm{Gal}(p(x)) = \mathrm{Gal}(q(x))$. Then, we see that $p(x)q(x)$ will still split over $\mathbb{Q}(i\sqrt{3})$, and since it is galois, $|\mathrm{Gal}(p(x)q(x))| = |\mathbb{Q}(i\sqrt{3})|$ but $|\mathrm{Gal}(p(x)) \times \mathrm{Gal}(q(x))| = |\mathrm{Gal}(p(x))| \times |\mathrm{Gal}(q(x))| = |\mathbb{Q}(i\sqrt{3})| \cdot |\mathbb{Q}(i\sqrt{3})|$, as required.

Question 3

First, we see that since $f(x)$ is irreducible, we know that G is transitive. However, since G is galois, we know hat $|G| = [K : F]$, and if the degree of $\deg(f(x)) = n$ we get that $G \leq S_n$. So, we need a transitive and abelian subgroup of S_n, but from group theory we recall this is a group of order n, and thus

$$|G| = [K : F] = n = \deg(f(x))$$

as required.

Question 4

We wish to find a polynomial of degree 3 that splits over K. To see this, we know by the Fundemental Theorem of Galois Theory that $\exists\, E \in \mathcal{E}$ such that $[E : F] = 3$. Moreover, by the primitive element theorem, we can gurentee that $\exists\, \alpha \in K$ such that $E = F(\alpha)$. Since K is Galois, it is Normal, and thus the minimal polynomial of α over F splits in K, and moreover, if $p(x) \in F[x]$ is the minimal polynomial, then $\deg(p(x)) = 3$ by construction. Suppose $\beta \in K$ is another root of $p(x)$. However, we notice that the only non-trivial normal subgroup of S_3 is A_3, but by the fundemental theorem this corresponds with a Field $L \in \mathcal{E}$ such that $[L : F] = 2$, and so $\beta \notin E$, and hence can only be in K, and thus the splitting field of $p(x)$ is K.

Question 5

It suffices to show that the Galois Group of $f(x)$ is isomorphic to A_3 from our theory. First, we know $f(x)$ is irreducible over F, so we know that $\mathrm{Gal}(f(x))$ is transitive, which forces $\mathrm{Gal}(f(x)) \cong S_3$ or A_3. Next, we know that F is finite, so suppose $\mathrm{Char}(F) = p > 3$, with p prime, and let K be the splitting field of $f(x)$. Notice, since $f(x)$ is cubic and irreducible, then none of the roots of $f(x)$ are in F. In particular, suppose $\alpha \in K$ is such a root. We know that finite extensions of finite fields are finite fields, and so $F(\alpha)$ is a finite field. Moreover, $F(\alpha)/\mathbb{Z}_p$ is Galois, since it is the splitting field of $x^{p^m} - x$ over $\mathbb{Z}_p$. But, since this is Galois, then $F(\alpha)/F$ is Galois and so $F(\alpha) = K$. However, since the minimal polynmial of α is $f(x)$, then

$$|G| = [K : F] = [F(\alpha) : F] = 3 \implies G \cong A_3$$

and the result follows.