Question 1

(a) We know that $K/E/F$ is a tower of fields, and since K/F is algebraic, we better have that E/F and K/E are algebraic. Suppose $\alpha \in K$, since K/F is seperable, then $\exists\, p(x) \in F[x]$ minimal polynomial of α, which is seperable over its splitting field. Then, we know that α has a minimal polynomial, say $g(x) \in E[x]$, and know that $g(x)\,|\,p(x)$ over E by the fact that $g(x)$ is the minimal polynomial of α in this field. Then, since $p(x)$ is seperable, $g(x)$ is seperable, and thus K/E is seperable.

(b) First, we know that E/F is algebraic, since $E \subset K$, and K/F is algebraic, hence any element of E is also in K, and hence will have a minimal polynomial over F. Seperability follows in exactly the same way, since we can again say that every element of K is seperable, and since $E \subset K$, therefore E/F is seperable.

(c) Suppose K/F is an algebraic extension and F is perfect. Since F is perfect, K is seperable. Moreonver, suppose H/K is an algebraic extension of $K \implies H/K/F \implies H/F$ is algebraic. F is perfect $\implies H$ is seperable, but since $F \subseteq K$, H is seperable over K, and so K is perfect.

Question 2

(a) This is not true. Consider the Tower fields $\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}(\sqrt{3})/\mathbb{Q}$, where we see that $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ is normal since $x^2 - 3$ $in\mathbb{Q}[x]$ splits over the extension and $\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}(\sqrt{3})$ is normal since $x^2 - \sqrt{3}$ splits over the extension. However, notice that $\sqrt[4]{3} \in \mathbb{Q}(\sqrt[4]{3})$ has minimal polynomial $x^4 - 3$ but it does not split over the extension, so it is not normal.

(b) Since $[K : F] < \infty$, we know K/F is algebraic, and moreover, by the normality theorem if $\alpha \in K$, its minimal polynomial in $F[x]$ splits over K. We know that since K/F is algebraic, so is K/E, and so $\alpha \in K$ has a minimal polynomial $g(x) \in E[x]$, and minimal polynomial $f(x) \in F[x]$ and we must have that $g(x) \mid f(x)$. However, $f(x)$ splits over K, and so then so does $g(x)$, and hence K/E is normal.

(c) This is false. To see this, consider the tower of fields $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[4]{3}, \xi_3)$. We notice that first $[\mathbb{Q}(\sqrt[4]{3}, \xi_3) : \mathbb{Q}] < \infty$ and it is normal since it splits $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. However, notice that the extension $\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}$ has the element $\sqrt[4]{3}$ which has minimal polynomial $f(x)$, which clearly does not split over this extension, and hence it is not normal.

(d) Since $[K : F] = 2$, we know that $\exists \alpha$ such that $K = \text{span}_F\{1, \alpha\}$, but this tells us that $K = F(\alpha)$ since $\{1, \alpha, \alpha^2\}$ is linearly dependent and thus K is an extension for some degree two polynomial, say $f(x) \in F[x]$. Now, for K to be normal, we just need that the other root of $f(x)$ also is in K. Suppose it was not, but then since $\alpha \in K$, we can factor $f(x)$ over $K[x]$, and by the division algorithm our remaining coeffecient will be the root, and in K. So, we must have both roots in K, and so K is normal.

Question 3

(a) We know that $f(x) = x^p - x - a$ is irreducible iff $g(x) = f(x - a) = (x - a)^p - (x - a) - a$ is irreducible, but notice by freshmen's dream

$$g(x) = (x - a)^p - (x - a) - a = x^p - a^p - x + a - a = x^p - x - a^p = x^p - x - 1\,.$$

So, we need only show that $g(x) = x^p - x - 1 \in \mathbb{Z}_p[x]$ is irreducible. Next, notice that if α is a root of $g(x)$, then we see that since $g(x - 1) = (x - 1)^p - (x - 1) - 1 = x^p - 1 - x = x^p - x - 1 = g(x)$, then $\alpha - 1$ is also a root of $g(x)$, and moreover, so are $\alpha - 2, \alpha - 3, \ldots, \alpha - p + 1$. Now, suppose $\alpha \in \mathbb{Z}_p$, then $g(\alpha) = \alpha^p - \alpha - 1 = 0 \implies (1) - \alpha - 1 = 0 \implies \alpha = 0$, but this is a contradiction since clearly 0 is not a root of $g(x)$. So, $\alpha \notin \mathbb{Z}_p$. Next, we see that $g(x)$ is irreducible iff it's galois group is transitive (which we proved in the previous assignment). Suppose $\mathrm{Gal}(g(x))$ was not transitive, then we can't send α to $\alpha - c$, $c \in \mathbb{Z}_p^\times$, but since we have p different roots, this implies that we can only fix every root, since compositions would generate the entire set of roots. However, if every root is fixed in the Galois group, then $g(x)$ is actually the product of p degree 1 polynomials, which is a contradiction, since $\alpha \notin \mathbb{Z}_p$. Therefore, $g(x)$ is irreducible, and thus $f(x)$ is irreducible over $\mathbb{Z}_p$.

(b) To see that $\mathbb{Z}_p(\alpha)/\mathbb{Z}_p$ is Galois, we know that $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = p$, and we notice it is the splitting field of the minimal polynomial $f(x) = x^p - x - a \in \mathbb{Z}_p[x]$ where $a \in \mathbb{Z}_p^\times$ since $\alpha \in \mathbb{Z}_p(\alpha) \implies \alpha - a \in \mathbb{Z}_p(\alpha)$. Which is a seperable polynomial, and so we have Galois by the chracteristic theorem.

(c) We know that $|\mathrm{Gal}(\mathbb{Z}_p(\alpha)/\mathbb{Z}_p)| = [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = p$, and all prime groups are known up to isomorphism, so $\mathrm{Gal}(\mathbb{Z}_p(\alpha)/\mathbb{Z}_p) \cong \mathbb{Z}_p$.

Question 4

(a) We find the minimal polynomial,

$$c^2 = 2 + \sqrt{2} \implies (c^2 - 2)^2 = 2 \implies c^4 - 4c^2 + 2 = 0.$$

So we get $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$ to be the minimal polynomial, which is irreducible by 2-Eisenstien. So, we have that $[\mathbb{Q}(c) : \mathbb{Q}] = 4$.

(b) $\mathbb{Q}$ is perfect, so we only need to check normality. Notice if we let $y = x^2$, then $x^4 - 4x^2 + 2 = y^2 - 4y^2 + 2 \implies y = 2 \pm \sqrt{2}$ and $x = \pm\sqrt{2 \pm \sqrt{2}}$, so we let $d = \sqrt{2 - \sqrt{2}}$. Therefore the $\mathbb{Q}$-conjugates of c are $\pm c$ and $\pm d$. Further, notice that $(\sqrt{2 + \sqrt{2}})^2 \in \mathbb{Q}(c) \implies 2 + \sqrt{2} \in \mathbb{Q}(c) \implies \sqrt{2} \in \mathbb{Q}(c)$, so, since $c\frac{d}{\sqrt{2}} = \frac{(\sqrt{2+\sqrt{2}})(\sqrt{2-\sqrt{2}})}{\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2}} = 1$, we know $\pm c, \pm d \in \mathbb{Q}(c) \implies \mathbb{Q}(c)/\mathbb{Q}$ is normal $\implies \mathbb{Q}(c)/\mathbb{Q}$ is Galois.

(c) We build a table

	c	$-c$	d	$-d$	S_4
φ_1	c	$-c$	d	$-d$	ε
φ_2	$-c$	c	$-d$	d	$(12)(23)$
φ_3	d	$-d$	$-c$	c	(1324)
φ_4	$-d$	d	c	$-c$	(1423)

The first two rows are quite simple, since we need to have the identity, and we would definitely also require the swapping of negatives to still be in our Galois group. From transitivity, we know that c needs to be sent to every element atleast once, so the first two entries of the last two rows come from that, and the fact that $-c$ is fixed by the choice of c. The last bottom-right block is tougher. Notice, since $\varphi_3(c) = d$, we have

$$d^2 = \varphi_3(c)^2 = \varphi_3(c^2) = \varphi_3(2 + \sqrt{2}) = 2 + \varphi_3(\sqrt{2})$$

$$\implies \varphi_3(\sqrt{2}) = d^2 - 2 = -\sqrt{2}.$$

Thus, we see

$$cd = \sqrt{2} \implies \varphi_3(cd) = \varphi_3(\sqrt{2}) \implies \varphi_3(c)\varphi_3(d) = -\sqrt{2}$$

$$\varphi_3(d) = -\frac{\sqrt{2}}{\varphi_3(c)} = -\frac{\sqrt{2}}{d} = -c$$

which then fixes the rest of the chart from transitivity.

(d) This clearly isn't $\mathbb{Z}_2 \times \mathbb{Z}_2$, so we can conclude $G \cong \mathbb{Z}_4$.