Math 123 Problem Set 1 Solutions.

3. Use the Eisenstein criterion with respect to p.

4a,b. By #3, this polynomial is irreducible, so the extension is of degree 3.
4c. The polynomial has no roots in $\mathbb{Q}$ (by the rational roots theorem, we need only to check that 1 and -1 do not work), and hence is irreducible (since it is of degree 3). Hence the extension is also of degree 3.
4d. We know that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, and that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \leq 2$, since β satisfies a polynomial of degree 2 with coefficients in $\mathbb{Q}(\alpha)$ (namely, $X^2 - 3$). However, $\beta \notin \mathbb{Q}(\alpha)$, else there is some element $a + b\alpha \in \mathbb{Q}(\alpha)$ such that $3 = (a + b\alpha)^2 = a^2 + 2b^2 + 2ab\alpha$; $2ab = 0 \Rightarrow a = 0$ or $b = 0$, in which case either $a^2 = 3$ or $2b^2 = 3$, which doesn't work. Hence $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \neq 1$, so $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2$, and $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2 \cdot 2 = 4$.
4e. We do this the same way as d. $[\mathbb{Q}(i) : Q] = 2$ and $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(i)] \leq 2$, but cannot be 1 since there is no element of $\mathbb{Q}(i)$ whose square is 3: $3 = (a + bi)^2 = a^2 - b^2 + 2abi \Rightarrow a = 0$ or $b = 0$, in which case either $a^2 = 3$ or $b^2 = -3$. Neither is possible, so $[\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}(i)] = 2$, and $[\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

5. We note that $0 = \zeta^3 - 1 = (\zeta - 1)(\zeta^2 + \zeta + 1)$, and since $\zeta \neq 1$, $\zeta^2 + \zeta + 1 = 0$. We also note that $\zeta = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$, and so $2\zeta + 1 = \sqrt{-3}$, so $\sqrt{-3} \in \mathbb{Q}(\zeta)$ and $\mathbb{Q}(\sqrt{-3}) \subset \mathbb{Q}(\zeta)$. However, since $\zeta = \frac{-1}{2} + \frac{1}{2}\sqrt{-3} \in \mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\zeta) \subset \mathbb{Q}(\sqrt{-3})$. Hence the two are equal.

10. Let $I = E_1 \cap E_2$. Say $I \neq F$. Then since I is a field, $[E_1 : I][I : F] = p$, so since $[I : F] \neq 1$, $[E_1 : I] = 1$ so $E_1 = I$. Similarly, $E_2 = I$, so $E_1 = E_2$.

16. We know that if a, b are algebraic, then $\mathbb{Q}(a)$ and $\mathbb{Q}(b)$ are of finite degree over $\mathbb{Q}$; hence $\mathbb{Q}(a, b)$ is as well. Since extensions of finite degree are algebraic, all elements of $\mathbb{Q}(a, b)$, in particular $a^{-1}, -a, a + b, a \cdot b$, are algebraic. Hence A is closed under the operations, and contains 0,1, and all inverses, and hence is a field.

17. Since $\alpha^2 \in F(\alpha)$, $F(\alpha^2) \subset F(\alpha)$. Since α satisfies the polynomial $X^2 - \alpha^2 \in F(\alpha^2)[X]$, the degree $[F(\alpha) : F(\alpha^2)]$ is at most 2. However, we note that $[F(\alpha) : F(\alpha^2)]$ divides $[F(\alpha) : F]$, which is odd, so $[F(\alpha) : F(\alpha^2)]$ cannot be 2, and must then be 1, so $F(\alpha) = F(\alpha^2)$.