1. There are lots of examples that work. Take $J = \langle x^2 - 3\rangle$, $a(x) = x^3 - 3x$ and $b(x) = x + 1$. Then $(J + a(x))(J + b(x)) = J + a(x)b(x) = J + x^4 + x^3 - 3x^2 - 3x$, but this polynomial is a multiple of $x^2 - 3$ so is already in J. Thus $J + a(x)b(x) = J = J + 0$. Note though that $J + a(x) = J$ already, so this does not prove that $\mathbb{Q}[x]/J$ is not an integral domain. In fact, for this J, $\mathbb{Q}[x]/J$ *is* an integral domain, since $x^2 - 3$ is irreducible. If we picked a non-irreducible polynomial to generate J, then we would be able to find $a(x), b(x) \notin J$ with $(J + a(x))(J + b(x)) = J$, which would make $J + a(x)$ a zero divisor. Remember, zero divisors need to be non-zero elements.

2. (a) No, there is no polynomial that would work here because whenever you multiply polynomials together, the degree increases, so there is no way to get down to the degree 0 polynomail 1.

   (b) Yes. In fact, we know the inverse is $\langle x^4 - 3\rangle + \frac{3}{124}x^2 - \frac{14}{124}x + \frac{24}{124}$.

   (c) Yes. We have $(6 + 3\sqrt[3]{4} + \sqrt[3]{4}^2)^{-1} = \frac{24}{124} - \frac{14}{124}\sqrt[3]{4} + \frac{3}{124}\sqrt[3]{4}^2$.

   (d) We know that $\mathbb{Q}[x]/\langle x^3 - 4\rangle \cong \mathbb{Q}(\sqrt[3]{4})$, where the isomorphism is based on the evaluation homomorphism, evaluating at $\sqrt[3]{4}$. The way we know our answer to part (b) is correct is using the fact about polynomials. Saying that $s(x)a(x) + t(x)b(x) = 1$ (which we can get from the fact by dividing through by 124) is to say that 1 is an element of the coset $\langle b(x)\rangle + s(x)a(x) = (\langle b(x)\rangle + s(x))(\langle b(x)\rangle + a(x))$. This is the same as saying that $\langle b(x)\rangle + s(x)a(x) = \langle b(x)\rangle + 1$, which says that $\langle b(x)\rangle + s(x)$ is the inverse of $\langle b(x)\rangle + a(x)$.

3. (a) Elements of $\mathbb{Q}(\alpha)$ have the form $a + b\alpha$ (we do not every need α^2, as we will see by consider the minimal polynomial for α below). So for example, we have $2 + 4\alpha = 8 + 2\sqrt{5}$ and $-3 + 2\alpha = \sqrt{5}$.

   (b) The minimum polynomial for α is $x^2 - 3x + 1$. We know this is the minimum polynomial because α is irrational (since $\sqrt{5}$ is) so cannot be the root to any degree 1 polynomial. Further, if we consider the homomorphism $\sigma_\alpha : \mathbb{Q}[x] \to \mathbb{Q}(\alpha)$ defined by $\sigma(p(x)) = p(\alpha)$, we see that $K = \langle x^2 - 3x + 1\rangle$ is the kernel (every polynomial which has α as a root is a multiple of α's minimum polynomial). Thus by the Fundamental Homomorphism Theorem, $\mathbb{Q}[x]/\langle x^2 - 3x + 1\rangle \cong \mathbb{Q}(\alpha)$.

   (c) Let $K = \langle x^2 - 3x + 1\rangle$. Then $2 + 4\alpha$ corresponds to $K + (4x + 2)$ and $-3 + 2\alpha$ corresponds to $K + (2x - 3)$.

   (d) $\alpha^4 + 2\alpha^3 + 7$ corresponds to the coset $K + (x^4 + 2x^3 + 7)$. We can "reduce" this coset using the division algorithm. We get $x^4 + 2x^3 + 7 = (x^2 + 5x + 14)(x^2 - 3x + 1) + 37x - 7$. Thus $K + (x^4 + 2x^3 + 7) = K + (37x - 7)$, so $\alpha^4 + 2\alpha^3 + 7 = 37\alpha - 7$

   (e) We must have that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$. We see that $\alpha \in \mathbb{Q}(\sqrt{5})$ so $\mathbb{Q}(\sqrt{5})$ is an extension field of $\mathbb{Q}(\alpha)$. But $\mathbb{Q}(\alpha)$ is already a degree 2 extension of $\mathbb{Q}$, so $\mathbb{Q}(\sqrt{5})$ must be a degree 1 extension of $\mathbb{Q}(\alpha)$, which is to say that $\sqrt{5}$ is already in $\mathbb{Q}(\alpha)$. Indeed, we have $\sqrt{5} = -3 + 2\alpha$.

4. It is easier to work in $\mathbb{Q}[x]/\langle x^3 - 7\rangle$, which is isomorphic to $\mathbb{Q}(\sqrt[3]{7})$, since $x^3 - 7$ is the minimum polynomial for $\sqrt[3]{7}$ over $\mathbb{Q}$. Under that isomorphism, $\sqrt[3]{7} + 4$ corresponds to the coset $\langle x^3 - 7\rangle + x + 4$. We find the inverse coset by using the Euclidean algorithm on $x^3 - 7$ and $x + 4$. We get

$$x^3 - 7 = (x^2 - 4x + 16)(x + 4) - 71$$

   We can rewrite this as $71 = -(x^3 - 7) + (x^2 - 4x + 16)(x + 4)$ or better:

$$1 = \frac{-1}{71}(x^3 - 7) + \frac{1}{71}(x^2 - 4x + 16)(x + 4)$$

   Thinking back to cosets, this means:

$$\langle x^3 - 7\rangle + 1 = (\langle x^3 - 7\rangle + \frac{1}{71}x^2 - \frac{4}{71}x + \frac{16}{71})(\langle x^3 - 7\rangle + x + 4)$$

   This gives us the inverse coset we were looking for. Now going back to $\mathbb{Q}(\sqrt[3]{7})$ we see that the inverse of $\sqrt[3]{7} + 4$ is $\frac{16}{71} - \frac{4}{71}\sqrt[3]{7} + \frac{1}{71}\sqrt[3]{7}^2$.

5. $\mathbb{Q}(\sqrt[7]{2})$ is such an example, because it is isomorphic to $\mathbb{Q}[x]/\langle x^7-2\rangle$. Since x^7-2 is irreducible over $\mathbb{Q}$, by say Eisenstein's criterion, and has $\sqrt[7]{2}$ as a root, x^7-2 is the minimum polynomial for $\sqrt[7]{2}$. It has degree 7, so the field extension has degree 7 as well.

6. It would be tempting to say the degree of $\mathbb{Q}(a)$ over $\mathbb{Q}$ is 6, but x^6+1 is not irreducible over $\mathbb{Q}$, so it cannot be the minimum polynomial for a over $\mathbb{Q}$. The polynomial factors as

$$(x^2+1)(x^4-x^2+1)$$

   We know that a is a root of one of these two factors, both of which are irreducible. Thus $\mathbb{Q}(a)$ either has degree 2 or 4 over $\mathbb{Q}$.

7. (a) Yes. a is a root of the polynomial x^4-6x^2+7.

   (b) Yes, a is a root of the polynomial $x^2-(3+\sqrt{2})\in\mathbb{Q}(\sqrt{2})[x]$

   (c) $[\mathbb{Q}(a):\mathbb{Q}]=4$ and $[\mathbb{Q}(a):\mathbb{Q}(\sqrt{2})]=2$. Note that $\sqrt{2}\in\mathbb{Q}(a)$ so $\mathbb{Q}(a)=\mathbb{Q}(a,\sqrt{2})$. Also $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ since $\sqrt{2}$ has minimum polynomial x^2-2. Also, $x^2-(3+\sqrt{2})$ is irreducible in $\mathbb{Q}(\sqrt{2})$ (If it wasn't there would be a number $a+b\sqrt{2}$ which when squared gave $3+\sqrt{2}$. But $(a+b\sqrt{2})^2=a^2+2b^2+2ab\sqrt{2}$ so this would say that $a^2+2b^2=3$ and $2ab=1$, so $b=1/(2a)$. In other words, $a^2+2(1/(2a))^2=3$ which says $a^2+\frac{2}{4a^2}=3$ or $2a^4-6a^2+1=0$. But there is no rational number which satisfies this equation by the rational roots theorem.) This proves that $[\mathbb{Q}(a):\mathbb{Q}(\sqrt{2})]=2$ and combining this with the fact that $\mathbb{Q}(\sqrt{2})$ is a degree 2 extension over $\mathbb{Q}$, we get $[\mathbb{Q}(a):\mathbb{Q}]=2\cdot 2=4$.

   (d) A basis for $\mathbb{Q}(a)$ over $\mathbb{Q}(\sqrt{2})$ is $\{1,a\}$ (since $\mathbb{Q}(a)=\mathbb{Q}(\sqrt{2},a)$). To get a basis for $\mathbb{Q}(a)$ over $\mathbb{Q}$ we need 4 elements: $\{1,a,\sqrt{2},\sqrt{2}a\}$.

8. We know that $\alpha^3+4\alpha^2+10\alpha+6=0$, which is to say that there is a non-trivial linear combination of the elements in the set that gives 0. This is exactly what it means to say that the set is linearly dependent. However, it is not the case that $\alpha^3\in\mathbb{Q}$, as it is just a linear combination of 1, α, and α^2.

9. Take $p(x)=x^6-10x^4+31x^2-30=(x^2-2)(x^2-3)(x^2-5)$. The splitting field is $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$, which is a degree 8 extension of $\mathbb{Q}$. Elements of the Galois group send $\sqrt{2}$ to itself or to $-\sqrt{2}$, send $\sqrt{3}$ to itself or to $-\sqrt{3}$, and send $\sqrt{5}$ to itself or to $-\sqrt{5}$. These choices can be made independently.

10. Notice that every element of H_1 fixes $\sqrt{2}$. So the fixed field for H_1 is $\mathbb{Q}(\sqrt{2})$. Stated otherwise, $H_1\cong \mathrm{Gal}(E:\mathbb{Q}(\sqrt{2}))$, where E is the splitting field found in the previous problem. This makes sense size wise, since the degree of E over $\mathbb{Q}(\sqrt{2})$ is 4, and there are 4 elements in H_1.

    For H_2, we must be looking for a field of which E is a degree 2 extension. We can take $\mathbb{Q}(\sqrt{3},\sqrt{5})$ as the fixed field.

11. (a) True. We know the field of constructible numbers is an extension of $\mathbb{Q}$ closed under taking square roots. So 7 is constructible, and then $\sqrt{7}$ is as well. Since we are in a field, so is $3+\sqrt{7}$, which means $\sqrt{3+\sqrt{7}}$ is also constructible.

    (b) False. $\sqrt[5]{7}$ is a root of the irreducible polynomial x^5-7. Suppose this was constructible. Then after some finite number of steps, we would have $\sqrt[5]{7}$ constructed, in a finite degree field extension of $\mathbb{Q}$. This field would contain $\mathbb{Q}(\sqrt[5]{7})$, which is a degree 5 extension of $\mathbb{Q}$. But we know that all the constructible numbers belong to field extensions of degree 2^n for some n.

    (c) True, since x^4+3x-6 is irreducible over $\mathbb{Q}$ by Eisenstein's criterion, we see that $\langle x^4+3x-6\rangle$ is a maximal ideal, so the quotient ring is a field.

    (d) False, which we know right away because there is no way for x^4+3x-2 to be irreducible in $\mathbb{R}$ (since it has degree greater than 2). So we have $x^4+3x-6=a(x)b(x)$ for some polynomials $a(x),b(x)\in\mathbb{R}[x]$. Then $\langle x^4+3x-6\rangle+a(x)$ is a zero divisor, so cannot have an inverse.

(e) True. We either have $E = \mathbb{Q}(a, b)$ where a and b are both roots to degree 2 minimum polynomials, in which case $\mathbb{Q}(a)$ is a degree 2 extension between $\mathbb{Q}$ and E, or else $E = \mathbb{Q}(a)$ for a single element number which is the root to some irreducible degree 4 polynomial. In this case, we have a basis for E over $\mathbb{Q}$ as $\{1, a, a^2, a^3\}$. Then consider the extension $\mathbb{Q}(a^2)$ of $\mathbb{Q}$. This has degree 2 over $\mathbb{Q}$ since it has basis $\{1, a^2\}$.