ii) First observe that $\mathbb{Q}(n\sqrt{m}) = \mathbb{Q}(\sqrt{m})$, $n \in \mathbb{Z}$.

Let $L = \mathbb{Q}(\sqrt{D})$. Suppose $D = \frac{\gamma}{\delta}$, where γ, δ are integers. Then

$D = \frac{1}{\delta^2} \cdot (\gamma \cdot \delta)$. Therefore, $L = \mathbb{Q}(\sqrt{\gamma \cdot \delta})$, and $\gamma \cdot \delta$ is an integer.

Now write $\gamma \cdot \delta = n^2 \cdot d$, where d is a square-free integer.

Then $L = \mathbb{Q}(\sqrt{d})$.

iii) Note that $\omega = \frac{-1 + i\sqrt{3}}{2}$. Now prove the statement.

E4) A cubic polynomial is reducible over K if and only if it has a linear factor, i.e., if and only if it has a root in K, where $K \subseteq \mathbb{C}$. This answers both (i) and (ii). We have not used any special property of $\mathbb{Q}$ here.

For the second question in (i), a quartic polynomial can be reducible even when it has no root in K. For example, $f(x) = x^4 - 4 = (x^2 - 2)(x^2 + 2)$ over $\mathbb{Q}$, but $f(x)$ has no root in $\mathbb{Q}$.

E5) i) We have, $K \subset K(\alpha) \subset L$. Therefore $[L : K] = [L : K(\alpha)][K(\alpha) : K]$.
Therefore, $[K(\alpha) : K] = 2$ or 4, since $[K(\alpha) : K] \neq 1$.
If $[K(\alpha) : K] = 4$, $K(\alpha) = L$, which is not the case.
Hence $[K(\alpha) : K] = 2$. Hence $[L : K(\alpha)] = 2$.

ii) By E3 (i), $K' = K(\sqrt{d})$ for some $d \in K$, where d is not a square in K. Similarly, there exists $\beta = a + b\sqrt{d} \in K' = K(\sqrt{d})$, which is not a square in K', such that $L = K'(\sqrt{a + b\sqrt{d}}) = K'(\sqrt{\beta})$.

iii) Note that if $\sqrt{\alpha} + \sqrt{\beta}$ is a root of a polynomial over K, then so are $\sqrt{\alpha} - \sqrt{\beta}, -\sqrt{\alpha} + \sqrt{\beta}, -\sqrt{\alpha} - \sqrt{\beta}$. Thus, the minimal polynomial is $f(x) = x^4 - 2(\beta + \alpha)x^2 + (\beta - \alpha)^2 \in K[x]$.

E6) You can do this by direct computation, and by applying De Moivre's theorem as well as the fact that $e^{i\theta} = 1$ if and only if θ is a multiple of 2π.

E7) Note that $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\alpha)$, where ζ and α are primitive nth and $(2n)$th roots of unity. Also, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \phi(2n) = \phi(2)\phi(n)$, since $(2, n) = 1$.
So $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \phi(n) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$.
Hence $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta)$.
Hence $\mathbb{Q}(\alpha) \subseteq K$.

For the second part, consider $n = 2$ for a counterexample. Then $\mathbb{Q}$ is the 2^{nd} cyclotomic field, and $\mathbb{Q} \subseteq \mathbb{Q}$. $\mathbb{Q}(i)$ is the 4^{th} cyclotomic field, and $\mathbb{Q} \not\supseteq \mathbb{Q}(i)$.

E8) You can check that if σ and τ are automorphisms of K, then $\sigma \circ \tau$ is defined and is an automorphism of K.
Next, $\circ$ satisfies associativity.

Further, I is the identity w.r.t. $\circ$, and if $\sigma \in \text{Aut}(K)$, so does σ^{-1}.
Thus, $(\text{Aut}(K), \circ)$ is a group.
Now, $\text{Aut}(K/F) \neq \phi$ since I is in it.
Also, for σ and $\tau \in \text{Aut}(K/F)$, $\sigma\tau$ and σ^{-1} are the identity on F, so that $\sigma\tau$ and σ^{-1} are in $\text{Aut}(K/F)$. Thus, $\text{Aut}(K/F)$ is a subgroup of $\text{Aut}(K)$.

E9) Let $L = K(\sqrt{d})$, $\sqrt{d} \notin K$. Let $\theta : L \to L' \subseteq \mathbb{C}$ be an isomorphism. Since the minimal polynomial of $\sqrt{d}$ is $x^2 - d$, and $\theta(\sqrt{d})$ is also a root of $x^2 - d$, $\theta(\sqrt{d}) = \pm\sqrt{d}$.
So $\theta(L) \subseteq K(\sqrt{d}) = L$.
Thus, $\theta \in \text{Aut}(L)$.

E10) There are three $\mathbb{Q}$-homomorphisms from $K = \mathbb{Q}(\sqrt[3]{2})$ into $\mathbb{C}$. They are given by τ_1, τ_2, τ_3, where
$\tau_1(\sqrt[3]{2}) = \sqrt[3]{2}$, $\tau_2(\sqrt[3]{2}) = \omega(\sqrt[3]{2})$, $\tau_3(\sqrt[3]{2}) = \omega^2(\sqrt[3]{2})$.

E11) Let $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ and $K = \mathbb{Q}(\sqrt[3]{2} + \omega)$. Write down 6 distinct homomorphisms from L to $\mathbb{C}$, and show that the images of $\sqrt[3]{2} + \omega$ are all distinct under these maps. This proves that the number of homomorphisms of K into $\mathbb{C}$ is at least 6. Therefore, $[K : \mathbb{Q}] \geq 6$.
However, $K \subset L$ and $[L : \mathbb{Q}] = 6$. Therefore, $K = L$.

E12) i) This is not normal, since it is not algebraic.

ii) This is the splitting field of $x^2 + 7$ over $\mathbb{Q}$, and hence is normal.

iii) This is the splitting field of $x^2 + 3$ over $\mathbb{Q}(\sqrt{2})$, and hence is normal.

iv) One root of $x^5 - 5 \in \mathbb{Q}(5^{1/5})$ is in $\mathbb{Q}(5^{1/5})$. The other roots are $5^{1/5}\zeta^t$, $t = 1, 2, 3, 4$, which lie in $\mathbb{C} \setminus \mathbb{R}$, and hence not in $\mathbb{Q}(5^{1/5})$. Thus, $\mathbb{Q}(5^{1/5})/\mathbb{Q}$ is not normal.

E13) First, assume L/K is separable.
Consider any $\alpha \in L$. Its minimal polynomial over E divides its minimal polynomial over K. Since L/K is separable, $m_{\alpha,K}(x)$ has no repeated roots. Hence $m_{\alpha,E}(x)$ has no repeated roots. Thus, L/E is separable.
You can easily show that E/K is separable.

E14) Let L/K be separable. Then $L = K(\alpha)$ for some $\alpha \in L$. Let $f(x)$ be the irreducible polynomial of α over K, where $\deg f(x) = n$.
Let N/L be a normal extension. Since $\alpha \in N$, all the roots of $f(x)$ are in N. So, for each root $\alpha_1 (= \alpha), \alpha_2, \ldots, \alpha_n$ of $f(x)$, we can define $\sigma_i : L \to N : \sigma_i(\alpha) = \alpha_i$. Each σ_i defines a distinct K-homomorphism of L into N. Thus, there are $[L : K] = n$ distinct K-homomorphisms from L into N.

Conversely, suppose the condition holds and $\alpha \in L$. Let the irreducible polynomial of α be $f(x)$ over K and its splitting field over L be N. Let $[L:K]=n$ and $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the distinct K-homomorphisms of L into N. Then $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ are roots of $f(x)$. The maximum number of roots can only be $[L:K]$ since $|\mathrm{Aut}(L/K)| \leq [L:K]$. Thus, all the roots of $f(x)$ are distinct, and hence $f(x)$ is separable.

E15) Use E14 to show this.

E16) i) This is false. For example, $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is separable, but not normal.

ii) Since every algebraic extension in characteristic 0 is separable, every such normal extension is separable. Since every extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is separable, any such normal extension will be separable. Hence, the statement is true in all cases.

E17) $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ is a cyclic group of order 2, with a generator being the complex conjugation $z \mapsto \bar{z}$. Hence, $|\mathrm{Aut}(\mathbb{C}/\mathbb{R})| = 2 = [\mathbb{C}:\mathbb{R}]$. Thus, $\mathbb{C}/\mathbb{R}$ is a Galois extension.

E18) i) The Galois group is of order 10 and is isomorphic to $\mathbb{F}_{11}^*$. Since $2^{11} \equiv 1 (\mathrm{mod}\, 11)$ and no smaller power of 2 is congruent to $1 (\mathrm{mod}\, 11)$, $\bar{2}$ is a generator for this group. Therefore, the automorphism τ, defined by $\tau(\zeta) = \zeta^2$, is a generator of the Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$.

ii) Observe that there are $\phi(n)$ generators for a cyclic group of order n. Find this number for the special values given in the problem. Now, you have to find elements of the respective groups whose order is equal to the order of the group.
For example, for $p=7$, the multiplicative group is of order 6. So we expect $\phi(6)=2$ generators for this group.
For $p=11$, verify that the elements $2, 3, 5, 7$ are of order 10, and hence they are generators. It will be good practice for you to find the orders of all the elements of this group. (e.g., I is of order 1, 10 is of order 2.) Find the others.

E19) There are $\phi(p-1)$ generators for a cyclic group of order $p-1$. For example, for $p=5$, $p-1=4$. So there are $\phi(4)=2$ generators. For $p=31$, $p-1=30$. So there are $\phi(30)=\phi(2)\phi(3)\phi(5)=1\times 2\times 4=8$ generators for a cyclic group of order $p-1=30$.

E20) $\mathrm{Aut}(L/\mathbb{Q})$ is trivial, i.e., it consists of the identity only. It is not a Galois extension since $[L:\mathbb{Q}]=3$ and the automorphism group is of order 1.

E21) Let $L=\mathbb{Q}(\sqrt{p}, \sqrt{q})$, where $p \neq q$ are primes. You know that it is a Galois extension. Its Galois group is isomorphic to the Klein four group $C_2 \times C_2$, just like the special case $p=2, q=3$, in Example 9.

E22) Note that $x^8 - 1 = (x^4 - 1)(x^4 + 1)$.

And $x^4 + 1$ is irreducible over $\mathbb{Q}$. If ζ is a complex number such that $\zeta^8 = 1$ and no smaller power of ζ is 1, then $x^4 + 1$ is the minimal polynomial of ζ; for example, you can take $\zeta = e^{2\pi i/8}$. Therefore, $[L : \mathbb{Q}] = 4$. It is a Galois extension, since L is a splitting field over $\mathbb{Q}$.

Let $\tau_1(\zeta) = \zeta^3$, $\tau_2(\zeta) = \zeta^5$, $\tau_3(\zeta) = \zeta^7$.

Then $\tau_1^2(\zeta) = \zeta^9 = \zeta$. Similarly, $\tau_2^2(\zeta) = \zeta^{25} = \zeta$ and $\tau_3^2(\zeta) = \zeta^{49} = \zeta$. This shows that there are three elements of order 2 and the fourth element is the identity element. Hence there is no element of order 4. Therefore, the Galois group is not cyclic. Since a group of order 4 which is not cyclic must be Klein's four group, we get the result.

(**Remark:** The group of invertible elements of $\mathbb{Z}/8\mathbb{Z}$ is $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, which is Klein's four group. The Galois group is isomorphic to this group.)

E23) The extension $L/\mathbb{Q}$ is a Galois extension, since L is a splitting field over $\mathbb{Q}$. Now, prove it step-by-step, as below

i) Let K be a field and d_1, d_2 be non-squares in K, such that $d_1 d_2$ is not a square in K. Let $K' = K(\sqrt{d_1}, \sqrt{d_2})$. Show that $[K' : K] = 4$.

ii) Let $d_1 = 2, d_2 = 3$ and $K = \mathbb{Q}(\sqrt{7})$. Apply (i) to get $[L : \mathbb{Q}] = 8$.

iii) Let $K'' = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Since $[L : \mathbb{Q}] = 8$ and $[K'' : \mathbb{Q}] = 4, 7$ is not a square in K''. Thus, L is a quadratic extension of K''. Write down the isomorphisms (automorphisms) of $K'' = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Extend each of these isomorphisms to $L = K''(\sqrt{7})$. You should be able to work out the details and show that the Galois group is abelian, and except for the identity, all the other elements have order 2.

iv) From Block 1, you know that an abelian group of order 8, in which all the elements other than the identity are of order 2, is isomorphic to $C_2 \times C_2 \times C_2$.