properties in $\mathbb{Q}(\sqrt{d})$ also. The additive and multiplicative identities in $\mathbb{R}$ are 0 and 1, which lie in $\mathbb{Q}(\sqrt{d})$.

The additive inverse of $(a+b\sqrt{d})$ is $[(-a)+(-b)\sqrt{d}]\in\mathbb{Q}(\sqrt{d})$.

The multiplicative inverse of $(a+b\sqrt{d})$ is

$(a^2-b^2d)^{-1}(a-b\sqrt{d})\in\mathbb{Q}(\sqrt{d})$ since $a^2-b^2d\neq 0, d$ being square-free.

Since $\cdot$ distributes over + in $\mathbb{R}$, it does so in $\mathbb{Q}(\sqrt{d})$ also.

Hence $\mathbb{Q}(\sqrt{d})$ is a field.

E2) Let $h\in G$ s.t. $o(h)=m$. Suppose $\exists\, x\in G$ s.t. $o(x)\nmid m$. Let p be a prime such that $p\,|\,o(x)$ and $p^{\alpha}\,|\,m$, $p^{\alpha+1}\nmid m$, where $\alpha\geq 0$. Let $o(x)=p^t r$, $(p,r)=1$, $t\geq 1$, and $y=x^r$. Then $o(y)=p^t$ and $yh\in G$ s.t. $o(yh)=o(y)o(h)>m$, which is a contradiction. Hence $o(g)\,|\,m\ \forall\ g\in G$.

E3) I is maximal in R iff R/I has no proper non-trivial ideals, iff R/I is a field.

E4) Ker ϕ is an ideal of F, a field. Hence, Ker $\phi=\{0\}$ or Ker $\phi=F$.
Accordingly, ϕ is 1-1 or $\phi\equiv\mathbf{0}$.

E5) i) $(a,b)\sim(a,b)\ \forall\,(a,b)\in R$, since R is commutative. Thus, $\sim$ is reflexive.

ii) Let $(a,b),(c,d)\in R$ such that $(a,b)\sim(c,d)$. Then $ad=bc$, i.e., $cb=da$. Therefore, $(c,d)\sim(a,b)$. Thus, $\sim$ is symmetric.

iii) Finally, let $(a,b),(c,d),(u,v)\in R$ such that $(a,b)\sim(c,d)$ and $(c,d)\sim(u,v)$. Then $ad=bc$ and $cv=du$.
Therefore, $(ad)v=(bc)v=bdu$, i.e., $avd=bud$. Thus, $av=bu$, since $d\neq 0$.
$\therefore (a,b)\sim(u,v)$. Thus, $\sim$ is transitive.

Hence, $\sim$ is an equivalence relation.

E6) For $[a,b],[c,d],[u,v]\in F$,

$([a,b]+[c,d])+[u,v]=[ad+bc,bd]+[u,v]$

$=[(ad+bc)v+bdu,bdv]=[adv+b(cv+du),bdv]$

$=[ab]+[cv+du,dv]=[a,b]+([c,d]+[u,v])$.

Hence + is associative.

You can similarly show that $\cdot$ is associative, and + and $\cdot$ are commutative, as well as $\cdot$ distributes over +.

Finally, $[1,1]\cdot[a,b]=[a,b]$ and $[a,b][b,a]=[ab,ab]=[1,1]$, since $(\alpha,\alpha)\sim(1,1)\ \forall\,\alpha\in R$.

E7) Since F is the smallest field containing itself, it is its own quotient field.

E8) Since $\mathbb{Z}[\sqrt{2}]\subsetneq\mathbb{Q}(\sqrt{2})\subsetneq\mathbb{R}$, $\mathbb{R}$ is **not** the smallest field containing $\mathbb{Z}[\sqrt{2}]$, and hence not its quotient field.

E9) Since $\langle x^2+1\rangle$ is irreducible over $\mathbb{R}$, $\mathbb{R}[x]/\langle x^2+1\rangle$ is a field, and hence is its own quotient field.

E10) Since $\mathbb{Z}$ is a subring of $\mathbb{Q}$, and $\mathbb{Z}$ is not a field, we have a counterexample to the given statement. Hence, the statement is false.

E11) i) By definition, K is the prime subfield of F.

ii) Here $K = \left\{ n\cdot 1/m\cdot 1 \,\middle|\, n, m\in\mathbb{Z}, m\cdot 1\neq 0\right\}$, and hence is the smallest field contained in F. Hence it is the prime subfield.

iii) This means that K is the least subfield of F, and hence is its prime subfield.

E12) Let $\{F_\lambda \,|\, \lambda\in I\}$ be a family of subfields of F, indexed by the set I. Let $\alpha,\beta\in\bigcap_{\lambda\in I}F_\lambda$. Then $\alpha,\beta\in F_\lambda$ for every $\lambda\in I$. Now, for each $\lambda\in I$, F_λ is a field. Hence, $\alpha\pm\beta$, $\alpha\beta$, $\alpha/\beta(\beta\neq 0)\in F_\lambda\ \forall\ \lambda\in I$, and hence belong to $\bigcap_{\lambda\in I}F_\lambda$. Thus, $\bigcap_{\lambda\in I}F_\lambda$ is a subfield of F.

E13) No. For instance, consider $\mathbb{Q}(\sqrt{2})\cup\mathbb{Q}(\sqrt{3}) = L$, say. So $\sqrt{2}\in L$, $\sqrt{3}\in L$, but $\sqrt{2}+\sqrt{3}\notin L$ since any element of L is of the form $a+b\sqrt{2}$ or $a+b\sqrt{3}$, for $a, b\in\mathbb{Q}$.

E14) Since $\mathbb{Z}_p$ is a field, it is its own prime subfield. It is also the prime subfield of any field containing $\mathbb{Z}_p$. Hence, it is the prime subfield of $\mathbb{Z}_p(x)$.

E15) The prime subfield of $\mathbb{R}$ is $\mathbb{Q}$, which doesn't contain $\sqrt{2}$. So, the required field is $\mathbb{Q}(\sqrt{2})$.
Since this contains $\mathbb{Q}$, its characteristic is zero.

E16) Since k is a subfield, it will contain the least subfield of F, and hence will have the same prime subfield as that of F. Thus, both F and k will have the same characteristic.

E17) The prime subfield of k is
$P = \{(m\cdot 1)/(n\cdot 1) \,|\, m, n\in\mathbb{Z},\ n\cdot 1\neq 0\}$.
For any $\alpha\in P$, $\alpha = (m\cdot 1)/(n\cdot 1)$.

$$\text{Now, } \sigma\left(\frac{m\cdot 1}{n\cdot 1}\right) = \frac{\sigma(m\cdot 1)}{\sigma(n\cdot 1)}$$

$$= \frac{m\cdot\sigma(1)}{n\cdot\sigma(1)}, \text{ and } \sigma(1) = 1.$$

$$\therefore \sigma\left(\frac{m\cdot 1}{n\cdot 1}\right) = \frac{m\cdot 1}{n\cdot 1}.$$

E18) Since a field homomorphism is injective (see E4), $k \simeq \sigma(k)$ and $F \simeq \sigma(F)$. Let $\mathcal{B}$ be any k-basis of F and $\mathcal{B}' = \sigma(\mathcal{B})$ its image in $\sigma(F)$. We claim that $\mathcal{B}'$ is a $\sigma(k)$-basis of $\sigma(F)$.

Linearly Independent: Let $\{\alpha_1', \alpha_2', \ldots, \alpha_n'\}$ be any finite subset of $\mathcal{B}'$ such that

$a_1'\alpha_1' + a_2'\alpha_2' + \cdots + a_n'\alpha_n' = 0$, for some $a_1', a_2', \ldots, a_n' \in \sigma(k)$. …(4)

Then there exist unique $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathcal{B}$ and $a_1, a_2, \ldots, a_n \in k$ such that $\sigma(\alpha_i) = \alpha_i'$ and $\sigma(a_i) = a_i'$ for $1 \le i \le n$. Then (4) becomes

$\sigma(a_1)\sigma(\alpha_1) + \sigma(a_2)\sigma(\alpha_2) + \cdots + \sigma(a_n)\sigma(\alpha_n) = 0$

$\Rightarrow \sigma(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n) = \sigma(0)$,

$\Rightarrow a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n = 0$.

Since $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathcal{B}$ are linearly independent over k, $a_1 = a_2 = \cdots = a_n = 0$, which implies that $a_i' = \sigma(a_i) = 0 \ \forall\ i \in \{1,2,\ldots,n\}$, i.e., $\alpha_1', \alpha_2', \ldots, \alpha_n'$ are linearly independent over $\sigma(k)$.

Spanning: For an arbitrary element $\alpha' \in \sigma(F)$ there exists $\alpha \in F$ such that $\alpha' = \sigma(\alpha)$. Since $\mathcal{B}$ forms a k-basis of F, there exist unique elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathcal{B}$ and $a_1, a_2, \ldots, a_n \in k$ such that

$\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$.

$\Rightarrow \sigma(\alpha) = \sigma(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n)$

$\Rightarrow \alpha' = \sigma(a_1)\sigma(\alpha_1) + \sigma(a_2)\sigma(\alpha_2) + \cdots + \sigma(a_n)\sigma(\alpha_n)$,

i.e., $\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n) \in \mathcal{B}'$ spans α' over $\sigma(k)$.

E19) Let F/k be a finite extension and σ be a k-endomorphism of F. Since every field homomorphism is injective, it only remains to show that σ is surjective. Now, by the Fundamental Theorem of Homomorphism, $F \simeq \sigma(F)$. Also σ is identity on k. Thus, by E18, $[F:k] = [\sigma(F):\sigma(k)] = [\sigma(F):k]$, i.e., both F and $\sigma(F)$ are finite-dimensional vector spaces over k having the same dimension. Also, $\sigma(F)$ is a subfield, and hence a subspace, of the k-vector space F, having the same dimension as that of F. Hence, $\sigma(F) = F$, and σ is an automorphism of F.

For the second part, note that $\mathbb{Q}(\pi)/\mathbb{Q}$ is not finite. Consider $\sigma : \mathbb{Q}(\pi) \to \mathbb{Q}(\pi)$ given by $\sigma(\pi) = \pi^2$. You can verify that σ is a $\mathbb{Q}$-endomorphism of $\mathbb{Q}(\pi)$. We will now show that σ is not surjective. Suppose, to the contrary, that σ is surjective. Then π must have a pre-image, i.e., there exist $p(\pi), q(\pi)(\neq 0) \in \mathbb{Q}[\pi]$ such that

$\sigma(p(\pi)/q(\pi)) = \pi \Rightarrow p(\pi^2) - \pi q(\pi^2) = 0$

$\Rightarrow \pi$ is a root of $f(x) = p(x^2) - xq(x^2)$ over $\mathbb{Q}$,

contradicting the fact that π is transcendental over $\mathbb{Q}$.

Hence, σ is not an automorphism of $\mathbb{Q}(\pi)$.

E20) Note that $F(x) \supseteq F[x]$, and $F[x]$ has $\{1, x, x^2, \ldots\}$ as an F-basis. Hence $F(x)$ is an infinite extension of F.

E21) Since $k(\alpha,\beta)$ is the smallest field containing k, α and β, $k(\alpha,\beta) \subseteq k(\alpha)(\beta)$. Further, since $k(\alpha)(\beta)$ is the smallest field containing $k(\alpha)$ and β, $k(\alpha)(\beta) \subseteq k(\alpha,\beta)$.
Hence $k(\alpha,\beta) = k(\alpha)(\beta)$. Similarly, $k(\alpha,\beta) = k(\beta)(\alpha)$.

E22) i) Since α is a root of $x^3 - 3x + 4$, $\alpha^3 = 3\alpha - 4$. …(5)
Therefore, $\alpha^4 = 3\alpha^2 - 4\alpha$ …(6)
Now, for $a, b, c \in \mathbb{Q}$, $(\alpha^2 + \alpha + 1)(c\alpha^2 + b\alpha + a) = 1$
$\Rightarrow \alpha^2(a + b + 4c) + \alpha(a + 4b - c) + (a - 4b - 4c - 1) = 0$, using (5) and (6).
Since α cannot satisfy an equation over $\mathbb{Q}$ of degree less than 3,
$a + b + 4c = 0, a + 4b - c = 0, a - 4b - 4c - 1 = 0$.
Solving these equations for a, b, c we obtain the inverse as
$\frac{1}{49}(17 - 5\alpha - 3\alpha^2)$.

ii) Since α is a root of $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, and $f(x)$ is irreducible, $a_0 \neq 0$. So,
$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$.
$\Rightarrow \alpha(-a_0^{-1}\alpha^{n-1} - a_0^{-1}a_{n-1}\alpha^{n-1} - \cdots - a_0^{-1}a_1) = 1$
$\Rightarrow \alpha^{-1} = -a_0^{-1}\alpha^{n-1} - a_0^{-1}a_{n-1}\alpha^{n-2} - \cdots - a_0^{-1}a_1$.

E23) Since $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$, $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$.
Hence $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$. …(7)
So $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}]$ divides $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$.
Now, $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\sqrt{2})(\sqrt{3})$ (since $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$), so that
$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4$ …(8)
So $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 1, 2$ or 4.
Since $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$, $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] \neq 1$.
Also $(\sqrt{2} + \sqrt{3})$ satisfies the irreducible polynomial
$(x - \sqrt{2})^2 - 3 \in \mathbb{Q}(\sqrt{2})$. Thus, $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$.
Hence $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$.
Thus, $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. …(9)
Hence, (7), (8), (9) tell us that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$.

E24) i) By the 'Tower theorem', $[E : k] = [E : F][F : k]$. Hence the result.

ii) If $[E : k] = p$, then $[E : F] = 1$ or $[E : F] = p$ in (i) above. Thus, $F = E$ or $F = k$.

E25) True. For instance, $x^n - 2$ is irreducible over $\mathbb{Q}$ $\forall$ $n \in \mathbb{N}$, using Eisenstein's criterion. Hence $\mathbb{Q}[x] \Big/ \langle x^n - 2 \rangle$ is a finite extension of degree n of $\mathbb{Q}$.

E26) Let $[F:k]=p$ and $\alpha \in F \setminus k$. Then $k \subsetneq k(\alpha) \subseteq F$.
By E24 (ii), $k(\alpha)=F$, i.e., F is simple.

E27) $\forall\ \alpha \in k$, $x-\alpha \in k[x]$ is satisfied by α. Hence k/k is algebraic.

E28) Since α is algebraic over k, $\exists\ f(x) \in k[x]$ s.t. $f(\alpha)=0$. Since $k \subseteq E$, $f(x) \in E[x]$ also. Hence, α is also algebraic over E.

E29) i) Since $\omega \notin \mathbb{Q}$ and $1+\omega+\omega^2=0$,
$m_{\omega,\mathbb{Q}}(x)=x^2+x+1$.
Similarly, $m_{\omega,\mathbb{R}}(x)=x^2+x+1$.
Since $\omega \in \mathbb{C}$, $m_{\omega,\mathbb{C}}(x)=x-\omega$.
As $(x-\omega) \mid (x^2+x+1)$ in $\mathbb{C}[x]$, the rest follows.

ii) Let $p(x)=m_{\alpha,k}(x)$. Since $p(\alpha)=0$ in $E[x]$, $m_{\alpha,E}(x) \mid p(x)$. Hence the result.

E30) Suppose first that $k[\alpha]$ is a field. Then every non-zero element of $k[\alpha]$ is invertible. In particular, α is invertible. So $\exists\ \beta \in k[\alpha]$ such that $\alpha\beta=1$. Now, $\beta=a_0+a_1\alpha+\cdots+a_n\alpha^n$, where $a_i \in k$ for $0 \le i \le n$ and n is a non-negative integer.
So, $\alpha\beta=1 \Rightarrow -1+a_0\alpha+a_1\alpha^2+\cdots+a_n\alpha^{n+1}=0$, i.e., α is a root of a polynomial over k, and hence, α is algebraic over k.
Conversely, assume that α is algebraic over k. Then, by Theorem 7, $k[\alpha]$ is a field.

E31) $\mathbb{R}/\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Q}$ are the required extensions. There can be several other examples.

E32) Suppose, if possible, that $k(\alpha^2) \subsetneq F=k(\alpha)$, then $\alpha \notin k(\alpha^2)$. As $\alpha^2 \in k(\alpha^2)$, α satisfies the polynomial $f(x)=x^2-\alpha^2$ over $k(\alpha^2)$.
Since $\alpha \notin k(\alpha^2)$, it follows that $f(x)$ is irreducible over $k(\alpha^2)$, and hence $[k(\alpha):k(\alpha^2)]=[k(\alpha^2)(\alpha):k(\alpha^2)]=\deg f(x)=2$.
In view of the Tower Theorem, this implies that 2 divides the degree of $k(\alpha)/k$, contradicting the fact that $k(\alpha)/k$ is an odd degree extension.
Hence, $k(\alpha)=k(\alpha^2)$.
For the second part, consider $\sqrt{2} \in \mathbb{Q}$. Its degree is even. Also $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{2^2})=\mathbb{Q}$. Hence, it need not be true if $\deg \alpha$ is even.

E33) The converse is: If $k \subseteq F \subseteq E$ are fields such that E/k is algebraic, then E/F and F/k are algebraic. You have already proved that E/F is algebraic.
Now, consider $\alpha \in F$. Then $\alpha \in E$, and hence, is algebraic over k. Thus, F/k is algebraic also.

E34) First, let us prove that $\sqrt{p_1} \notin \mathbb{Q}(\sqrt{p_2})$ by contradiction. So, suppose $\sqrt{p_1} \in \mathbb{Q}(\sqrt{p_2})$.

Then $\sqrt{p_1} = \alpha + \beta\sqrt{p_2}$, $\alpha, \beta \in \mathbb{Q}^*$. So $p_1 = \alpha^2 + \beta^2 p_2 + 2\alpha\beta\sqrt{2}$, and hence $\sqrt{p_2} \in \mathbb{Q}$, a contradiction.

Hence $\sqrt{p_1} \notin \mathbb{Q}(\sqrt{p_2})$.

Similarly, $\sqrt{p_2} \notin \mathbb{Q}(\sqrt{p_1})$.

Now, we have a tower $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{p_1}) \subsetneq \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$. So

$[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}) : \mathbb{Q}(\sqrt{p_2})][\mathbb{Q}(\sqrt{p_2}) : \mathbb{Q}] = 2 \times 2 = 4$

(since $\sqrt{p_2}$ has the minimal polynomial $x^2 - p_2 \in \mathbb{Q}[x]$ and $\sqrt{p_1}$ has the minimal polynomial $x^2 - p_1 \in \mathbb{Q}(\sqrt{p_2})[x]$).

Further, since $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})/\mathbb{Q}$ is finite, it is algebraic.

E35) As $F = k(\alpha)$, it is finitely generated. Suppose, if possible, that F/k is a finite extension. Then it must be algebraic, which implies that every element of F is algebraic over k. As $\alpha \in F, \alpha$ must also be algebraic over k, which contradicts the hypothesis that α is transcendental. Thus, F/k is not finite.