1. First note that $[k(x,y):k(x^p,y^p)]=p^2$. It is obvious that $[k(x,y^p):k(x^p,y^p)]=p$, then I claim that $\min(y;k(x,y^p))=f(T):=T^p-y^p$ in $k(x,y^p)[T]$. Proof being, firstly that $f(y)=0$, and appealing to Gauss' lemma, and eisenstein's Criterion (for y^p prime) f is irreducible.

Define $u(n)$ as $y+x^{np+1}$, then the following extensions satisfy the criteria.

$$k(x^p,y^p)\subsetneq k(x^p,y^p,u(n))\subsetneq k(x,y),\quad \forall n\in\mathbb{N}$$

Furthermore, if $n\neq m$, then $k(x^p,y^p,u(n))\neq k(x^p,y^p,u(m))$. The first inequality is obvious, since if $f\in k[x^p,y^p]$, then $p|\deg_y f$. As for the second inequality, $[k(x^p,y^p,u(n)):k(x^p,y^p)]=p$, since $p|[k(x^p,y^p,u(n)):k(x^p,y^p)]$, and $u(n)$ satisfies the polynomial $T^p-y^p-x^{p^{np+1}}$.

Now suppose $n\neq m$, then

$$\begin{aligned}k(x^p,y^p,u(n),u(m))&=k(x^p,y^p,u(n)-u(m),u(n))\\&=k(x^p,y^p,x(x^{np}-x^{mp}),u(n))\\&=k(x,y^p,u(n))=k(x,y)\end{aligned}$$

And hence $k(x^p,y^p,u(n))k(x^p,y^p,u(m))\supsetneq k(x^p,y^p,u(n))$ and $k(x^p,y^p,u(m))$, implying that the extensions are not equal.

2. We first show that $\min(a^{1/p}:\mathbb{Q})=X^p-a$, proof being we can factor $X^p-a=\prod_{k=1}^p(X-a^{1/p}\zeta_p^k)$ in $\mathbb{C}[X]$. If this polynomial were reducible in $\mathbb{Q}$, then if g were a factor, the last coefficient of g must be of the form $\pm a^{k/p}$. This is impossible since $a^{k/p}\in\mathbb{Q},\ k<p$, then by bezouts identity, there exist u,v such that $uk+vp=1$, implying that $a^{1/p}=a^{uk/p}a^{vp/p}\in\mathbb{Q}$.

This gives the desired result for both L and F extensions, since by multiplicativity of degree,

$$p|[F(a^{1/p}):\mathbb{Q}]\text{ and }[F:\mathbb{Q}]\leq p-1$$
$$p|[L(a^{1/p}):\mathbb{Q}]\text{ and }[L:\mathbb{Q}]\leq p-1$$

implying that $p|[F(a^{1/p}):F],[L(a^{1/p}):L]$. Then since $F\supset\cos(2\pi/p),-\sin^2(2\pi/p)$ (proven below), we get that $L=F(\sqrt{-\sin^2(2\pi/p)})$, i.e. $[L:F]=2$, also note that $N=L(a^{1/p})$. So that $[L(a^{1/p}):F]=[L(a^{1/p}):L][L:F]=2p$, implies $\#\mathrm{Gal}(N/F)=2p$. Finally, we have that $\mathrm{Gal}(N/F)\supset\langle\tau,\sigma\rangle\simeq D_p$, where τ is complex conjugation and σ is a generator of the cyclic group $\mathrm{Gal}(\mathbb{Q}(\zeta_p):\mathbb{Q})$. The isomorphism follows from $\sigma\tau=\tau\sigma^{-1},\tau^2=1,\sigma^p=1$, meaning the multiplication rules of D_p are satisfied. Then since $\#\mathrm{Gal}(N/F)=2p=\#\langle\tau,\sigma\rangle$ we have equality.

To show that $F\supset\cos(2\pi/p),\sin^2(2\pi/p)$, we have $\zeta_p,\zeta_p^{-1}\in F$, hence we have $\frac{1}{2}(\zeta_p+\zeta_p^{-1})=\cos(2\pi/p)\in F$. This implies we also have $(\zeta_p-\cos(2\pi/p))^2=-\sin^2(2\pi/p)$.

3.

$$[F:\mathbb{Q}]=2^9$$

First note that $F=\mathbb{Q}(\sqrt{p}|p$ prime and $p\leq 28)$, since the other radicals are simply products of these radicals, furthermore there are 9 primes less than or equal to 28.

First we prove a lemma, namely: if K has characteristic 0, $a,b\in K$ then $[K(\sqrt{a},\sqrt{b}):K]=4$ when $\sqrt{a},\sqrt{b},\sqrt{ab}\notin K$. Proof being: since $\sqrt{a}\notin K$ we have $[K(\sqrt{a}):K]=2$, so we need to show that $\sqrt{b}\notin K(\sqrt{a})$, so that $[K(\sqrt{a},\sqrt{b}):K(\sqrt{a})]=2$, allowing us to conclude by multiplicativity of degree. So suppose for contradiction that $\sqrt{b} = s\sqrt{a} + t$ for $s, t \in K$. This implies that:

$$b = as^2 + 2ts\sqrt{a} + t^2$$

it follows that one of t or s must be zero (if both are zero we get $b = 0$ an immediate contradiction), else this contradicts $\sqrt{a} \notin K$. Suppose first $s = 0$, then $b = t^2 \implies t = \sqrt{b} \in K$ a contradiction. Then it must be the case that $t = 0$, implying that $b = as^2$, so that $\sqrt{ab} = (\sqrt{a})(\sqrt{a}s) = as \in K$ also a contradiction, hence proving the lemma.

Now we finish the proof using the lemma, we have $[\mathbb{Q}(\sqrt{p_1}) : \mathbb{Q}] = 2$ by irrationality. Now assume that $[\mathbb{Q}(P) : \mathbb{Q}] = 2^{\#P}$, for P a collection of at most n square roots of elements of $\mathbb{Q}$, such that none of the 2^n products of elements of the collection lie in $\mathbb{Q}$, define $K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots \sqrt{p_{n-1}})$, then by induction we have

$$[K(\sqrt{p_n}) : K] = [K(\sqrt{p_{n+1}}) : K] = [K(\sqrt{p_n p_{n+1}}) : K] = 2$$

So that none of these elements lie in K. We may apply the lemma that

$$[K(\sqrt{p_n}, \sqrt{p_{n+1}}) : K] = 4 \implies [\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n+1}}) : \mathbb{Q}] = 2^{n+1}$$

The result is proven, given that

$$F = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \sqrt{17}, \sqrt{19}, \sqrt{23})$$

where clearly none of the products of square roots adjoined lie in $\mathbb{Q}$.

4. Suppose that $\#F = p^m = q$, and that $\#K = q^n$, note that $N_{K/F} : K \to F$, as it sends any element to the constant term of its minimum polynomial raised to some exponent. We know that $\mathrm{Gal}(K/F)$ is cyclic, with generator $\Phi : a \mapsto a^q$. Let $a \in K$, then

$$N_{K/F}(a) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(a) = \prod_{k=0}^{n-1} \Phi^k(a) = \prod_{k=0}^{n-1} a^{kq} = a^{\sum_{k=0}^{n-1} kq} = a^{\frac{q^n - 1}{q-1}}$$

It is immediate that $N_{K/F}(0) = 0$, since K is a field, and an element cannot be conjugate to 0 any other element must be sent to F^* having order $q - 1$. Now since K is finite, we have shown K^* is cyclic, hence it has a generator α with order $q^n - 1$, this implies that each of $N(\alpha^i)$ are distinct for $i \in \{1, \dots, q-1\}$ by the formula above and hence $\#\{N_{K/F}(\alpha^i)\}_{i=1}^{q-1} = q - 1 = \#F^*$, so that N maps onto both 0 and F^*.

5. We can define the map $\varphi : \mathbb{Z}/2\mathbb{Z} \xrightarrow{\varphi} (\mathbb{Z}/4\mathbb{Z})$ as $\varphi(1) : x \mapsto -x$, this is a well defined automorphism, since $\varphi(1)^2 = \mathbf{1}_{\mathbb{Z}/4\mathbb{Z}} = \varphi(0) = \varphi(1+1)$. Any element $x \in D_4$ can be written in the form of $\sigma^i \tau^j$ using the relation $\sigma\tau = \tau\sigma^{-1}$. So define the map

$$\psi : D_4 \to \mathbb{Z}/4\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z}$$
$$\sigma^i \tau^j \mapsto (i, j)$$

is an isomorphism. $\mathbf{1} \mapsto (0, 0)$ is immediate. And (here I deal with both possible cases $j = 1, 0$ seperately)

$$\psi(\sigma^i \tau \sigma^k \tau^\ell) = \psi(\sigma^{i-k} \tau^{1+\ell}) = (i - k, 1 + \ell) = (i + \varphi(1)(k), 1 + \ell) = (i, 1)(k, \ell) = \psi(\sigma^i \tau)\psi(\sigma^k \tau^\ell)$$
$$\psi(\sigma^i \tau^0 \sigma^k \tau^\ell) = \psi(\sigma^{i+k} \tau^\ell) = (i + k, \ell) = (i + \varphi(0)(k), 0 + \ell) = (i, 0)(k, \ell) = \psi(\sigma^i \tau^0)\psi(\sigma^k \tau^\ell)$$

This proves that ψ is a homomorphism, and

$$\psi(\sigma^i\tau^j) = (0,0) \iff i \equiv 0 \text{mod} 4 \text{ and } j \equiv 0 \text{mod} 2 \iff \sigma^i\tau^j = \mathbf{1}$$

proving that $\ker\psi = \mathbf{1}$. Then since $\#D_4 = \#\mathbb{Z}/4\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z}$ and the map is injective, it must also be surjective.

6. (a) It is immediate that $\mathbb{Q}$ satisfies the conditions of containing ± 1. The degree being at most 2^r is immediate since K is a tower of r extensions of degree at most 2. An example of when the degree is equal to 2^r is when each of the a_i are primes, as shown in the solution to exercise 3. An example of the degree less than 2^r is when $a_r = a_1 a_2$, since this is contained in the previous extension having degree at most 2^{r-1}. Explicit examples would be $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ having degree 4, and $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$ having degree $4 < 8$. It remains to show that $K/\mathbb{Q}$ is a 2-Kummer extension, the extension is clearly normal and seperable hence Galois, since it is the splitting field of a family of degree 2 polynomials algebraic over a characteristic 0 field. Suppose that $K/\mathbb{Q} = 2^r$, else we can simply remove dependent $\sqrt{a_i}$ until it does. Then each of $\sigma_1, \ldots, \sigma_r$ are in $\text{Gal}(K/\mathbb{Q})$ where $\sigma_i|_{\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}, \sqrt{a_{i+1}} \ldots, \sqrt{a_r})} = 1, \sigma(\sqrt{a_i} = -a_i)$. It follows that each of the 2^r combinations of these permutations are unique, hence $\text{Gal}(K/\mathbb{Q}) = \langle \sigma_1, \ldots, \sigma_r \rangle$. Since the group is generated by order 2 elements, all of its elements have order 2 and groups with exponent 2 are abelian, hence $K/\mathbb{Q}$ is 2-Kummer

Proof That Groups of Exponent 2 Are Abelian: $a, b \in G$, then $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$

(b) It is immediate that both are less than or equal to n.

First suppose that $a^k \in K^{*^n}$, then $a^{k/n} \in K^*$, so that $\min(a^{1/n}; K) | x^k - a^{k/n}$, implying that $[K(\sqrt[n]{a}) : K] \leq k$, so that $[K(\sqrt[n]{a}) : K] \leq o(aK^{*^n})$

Conversely, supppose that $[K(\sqrt[n]{a}) : K] = k$, then $a^{1/n}$ has minimum polynomial g of degree k, furthermore $g | x^n - a = \prod_0^{n-1}(x - a^{1/n}\zeta_n^j)$, so that the constant term of g must be $a^{k/n}\zeta_n^r$ for some r, then since $\zeta_n \in K$, this implies that $a^{k/n} \in K^*$, so that $a^k \in K^{*^n}$ this implies that $[K(\sqrt[n]{a}) : K] \geq o(aK^{*^n})$. Both inequalities taken together implies equality.