1. Let $f(X) = X^3 - 3X + 4$. The polynomial $f(X)$ has a unique root $X = 4$ in $\mathbb{F}_7$. The only primes dividing $\operatorname{disc} f$ are 2 and 3. Therefore Hensel's lemma says that $f(X)$ also has a unique root in $\mathbb{Z}_7$.

   The polynomial $f(X)$ has no roots in $\mathbb{F}_5$, hence no roots in $\mathbb{Z}_5$. It has a unique root 2 mod 3 in $\mathbb{F}_3$, but as 3 divides the discriminant this does not immediately imply the existence of a root in $\mathbb{Z}_3$. We check that $f(X)$ has no roots in $\mathbb{Z}/9\mathbb{Z}$ (we only need to check $X = 2, 5, 8 \bmod 9$), so in fact that are no roots in $\mathbb{Z}_3$.

   Finally we consider roots in $\mathbb{Z}_2$. There is a unique root $X = 0$ in $\mathbb{F}_2$, and $f'(0) = -3$ is odd, so the simple version of Hensel's lemma shows that $f(X)$ has a unique root in $\mathbb{Z}_2$.

2. Let $x \in 1 + p\mathbb{Z}_p$, and let $f(X) = X^n - x$. Then $f'(X) = nX^{n-1}$, so $f'(1) = n$ is prime to p, while $f(1) \equiv 1 - 1 = 0 \bmod (p)$. The simple version of Hensel's lemma shows that there is a unique $y \in \mathbb{Z}_p$ such that $y \equiv 1 \bmod (p)$ and $y^n = x$.

3. Clearly the given condition is necessary. We show that it is sufficient. Let $\alpha \in \mathbb{Z}_p^\times$, and suppose that $\alpha \bmod (p^2) \in ((\mathbb{Z}/p^2\mathbb{Z})^\times)^p$. Since every element of $\mathbb{F}_p^\times$ is a p^{th} power, we can multiply α to assume that $\alpha \equiv 1 \bmod p$, in which case $\alpha \equiv 1 \bmod (p^2)$ and we can write $\alpha = 1 + p^2\beta$ for some $\beta \in \mathbb{Z}_p$.

   If $\gamma \in \mathbb{Z}_p$ then $(1 + p\gamma)^p = 1 + p^2\gamma + \binom{p}{2}p^2\gamma^2 + \cdots \equiv 1 + p^2\gamma + \binom{p}{2}p^2\gamma^2 \bmod (p^3)$. Assuming further that p is odd, this is congruent to $1 + p^2\gamma \bmod (p^3)$, and so choosing $\gamma = \beta$ gives an approximate root of $f(X) = X^p - \alpha$ to which we can apply the strong version of Hensel's lemma (note that $f'(1 + p\gamma)$ has p-adic valuation 1).

   Now suppose that $p = 2$. In this case 5 is a square modulo 4 but not modulo 8, so it is not sufficient to be a p^{th} power modulo p^2 in this case. We claim however that it is sufficient to be a p^{th} power modulo p^3. To see this, consider the polynomial $f(X) = X^2 - \alpha$. Then $f'(X) = 2X$, so we must show that given $\alpha = 1 + 8\beta$, we can find γ such that $(1 + 2\gamma)^2 = 1 + 4\gamma + 4\gamma^2 \equiv 1 + 8\beta \bmod (16)$, or equivalently $\gamma(1 + \gamma) \equiv 2\beta \bmod (4)$. If $\beta \equiv 0 \bmod (2)$, we take $\gamma \equiv 0 \bmod (4)$. If $\beta \equiv 1 \bmod (2)$, we take $\gamma \equiv 1 \bmod (2)$. In either case we see that Hensel's lemma provides a root of $f(X)$ in $\mathbb{Z}_2$.

4. (a) Let $G = \operatorname{Gal}(E/K)$. In general, if $E/L/K$ is an intermediate field, $H = \operatorname{Gal}(E/L)$, and $\mathfrak{q}_L = \mathfrak{q} \cap \mathcal{O}_L$, then $D_{\mathfrak{q}/\mathfrak{q}_L} = D_{\mathfrak{q}/\mathfrak{p}} \cap H$ and $I_{\mathfrak{q}/\mathfrak{q}_L} = I_{\mathfrak{q}/\mathfrak{p}} \cap H$, as follows immediately from the definitions. In

the present case we have $I_{\mathfrak{q}/\mathfrak{q}^I} = I_{\mathfrak{q}/\mathfrak{p}} = \mathrm{Gal}(E/E^I)$, hence $\mathfrak{q}/\mathfrak{q}^I$ is totally ramified. We also have $D_{\mathfrak{q}/\mathfrak{q}^D} = D_{\mathfrak{q}/\mathfrak{p}} = \mathrm{Gal}(E/E^D)$, hence $\mathfrak{q}$ is the unique prime of E above $\mathfrak{q}^D$ (as $\mathrm{Gal}(E/E^D)$ acts transitively on the set of such primes, but fixes $\mathfrak{q}$). Finally, we also have $I_{\mathfrak{q}/\mathfrak{q}^D} = I_{\mathfrak{q}/\mathfrak{p}}$, showing that $e_{\mathfrak{q}/\mathfrak{q}^D} = e_{\mathfrak{q}/\mathfrak{q}^I}$. Since e and f are multiplicative in towers, we conclude that $e_{\mathfrak{q}^I/\mathfrak{q}^D} = 1$ and hence $\mathfrak{q}^D$ is totally inert in E^I/E^D.

(b) Let $H = \mathrm{Gal}(E/L)$. We have $D_{\mathfrak{q}/\mathfrak{q}_L} = D_{\mathfrak{q}/\mathfrak{p}} \cap H$. If $e_{\mathfrak{q}_L/\mathfrak{p}} = f_{\mathfrak{q}_L/\mathfrak{p}} = 1$ then $e_{\mathfrak{q}/\mathfrak{q}_L} = e_{\mathfrak{q}/\mathfrak{p}}$ and $f_{\mathfrak{q}/\mathfrak{q}_L} = f_{\mathfrak{q}/\mathfrak{p}}$, hence $D_{\mathfrak{q}/\mathfrak{q}_L} = D_{\mathfrak{q}/\mathfrak{p}}$ and $D_{\mathfrak{q}/\mathfrak{p}} \subset H$, hence $L \subset E^D$, by Galois theory. If $e_{\mathfrak{q}_L/\mathfrak{p}} = 1$ then the same argument with D replaced by I shows that $L \subset E^I$. Finally, if $\mathfrak{q}$ is the only prime of $\mathcal{O}_E$ above $\mathfrak{q}_L$, then $D_{\mathfrak{q}/\mathfrak{q}_L} = H \cap D_{\mathfrak{q}/\mathfrak{p}} = H$, hence $H \subset D_{\mathfrak{q}/\mathfrak{p}}$, hence $E^D \subset L$, by Galois theory.

5. We can assume without loss of generality that E/K is Galois. Let $\mathfrak{q}$ be a prime of $\mathcal{O}_E$ above $\mathfrak{p}$. We will show that $L_1 \cdot L_2/K$ is unramified at the unique prime below $\mathfrak{q}$; since every prime of $L_1 \cdot L_2$ arises in this way, this will show the result. Let $I = I_{\mathfrak{q}/\mathfrak{p}}$. By the previous exercise, the fact that the extensions L_1/K and L_2/K are unramified shows that $L_1 \subset E^I$ and $L_2 \subset E^I$, hence $L_1 \cdot L_2 \subset E^I$. But $e_{\mathfrak{q}/\mathfrak{q}^I} = e_{\mathfrak{q}/\mathfrak{p}}$, so by multiplicativity in towers we conclude that $e_{\mathfrak{q}^I/\mathfrak{p}} = 1$, hence $e_{\mathfrak{q}_{L_1 \cdot L_2}/\mathfrak{p}} = 1$, as desired.

   The argument is similar in the case that $\mathfrak{p}$ splits completely in L_1 and in L_2, using the fact that $\mathfrak{p}$ splits completely in an extension L/K if and only if for each prime ideal $\mathfrak{r}$ of $\mathcal{O}_L$ lying above $\mathfrak{p}$, we have $e_{\mathfrak{r}/\mathfrak{p}} = f_{\mathfrak{r}/\mathfrak{p}} = 1$.

6. We take the biquadratic extension $E = \mathbb{Q}(i, \sqrt{17})$. We observe that if a prime p is unramified in E, then the decomposition group $D_{\mathfrak{q}/(p)} \subset \mathrm{Gal}(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ is cyclic (it is generated by the Frobenius element), hence its index is divisible by 2. This index equals the number of prime ideals of $\mathcal{O}_E$ above 2, which is therefore even.

   By the previous exercise, a prime p is ramified in E only if it is ramified in either $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{17})$; so the only ramified primes are 2 and 17. The prime 2 splits into two factors in $\mathbb{Q}(\sqrt{17})$ (since $17 \equiv 1 \bmod 8$). The prime 17 splits into an even number of factors in $\mathbb{Q}(i)$ (since $17 \equiv 1 \bmod 4$, so -1 is a square mod 17). So we're done.

7. (a) The uniqueness is clear. If $\alpha \in \overline{\mathbb{Q}}_p$, then we define $v(\alpha) = e^{-1}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p} v_{\mathbb{Q}_p(\alpha)}(\alpha)$. If $K/\mathbb{Q}_p$ is a finite extension inside $\overline{\mathbb{Q}}_p$, then the formulae $e_{K/\mathbb{Q}_p} = e_{K/\mathbb{Q}_p(\alpha)} e_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}$ and $v_K|_{\mathbb{Q}_p(\alpha)} = e_{K/\mathbb{Q}_p(\alpha)} v_{\mathbb{Q}_p(\alpha)}$ show that $v|_K = e^{-1}_{K/\mathbb{Q}_p} v_K$.

(b) If $x, y \in \overline{\mathbb{Q}}_p$ then the formulae for $v(xy)$ and $v(x+y)$ follow from the corresponding formulae for $v|_K$, where $K = \mathbb{Q}_p(x, y)$. If α is a root of $X^b - p^a$ with $a, b \in \mathbb{Z}_{\geq 1}$, then $bv(\alpha) = av(p) = a$ and hence $v(\alpha) = a/b$. This shows that v is surjective.

(c) $\overline{\mathbb{Q}}_p$ is not complete. Here is (one of many) ways to show this. Suppose for contradiction that $\overline{\mathbb{Q}}_p$ is complete. If $k \geq 1$, define $x_k = \sum_{i=k}^{\infty} p^{i+1/i}$, where $p^{1/i}$ is a solution of $X^i = p$. The partial sums are Cauchy, so if $\overline{\mathbb{Q}}_p$ is complete then this sum really exists in $\overline{\mathbb{Q}}_p$. Note that $x_1 = x_k + p^2 + p^{2+1/2} + \cdots + p^{k-1+1/(k-1)}$. We have $v(x_k) = k + 1/k$.

If $x_1 \in \overline{\mathbb{Q}}_p$, then $K = \mathbb{Q}_p(x_1)$ is a finite extension of $\mathbb{Q}_p$, say of degree N. We have $v(K^\times) \subset \frac{1}{N}\mathbb{Z}$. For any $r \geq 1$, let $K_r = K(p^{1/2}, p^{1/3}, \ldots, p^{1/r})$. Then $v(K_r^\times) \subset \frac{1}{Nr!}\mathbb{Z}$, and $x_{r+1} \in K_r$, hence $1/(r+1) \in \frac{1}{Nr!}\mathbb{Z}$. Choosing r so that $r+1$ is a prime not dividing N yields a contradiction.

8. Since v_E is Galois invariant, if $\sigma \in \mathrm{Gal}(E/K(x))$ then $v_E(x - \sigma(y)) = v_E(x-y)$. The assumption $v_E(x-y_i) < v_E(x-y)$ if $i \geq 2$ shows that we must have $\sigma(y) = y$ for all $\sigma \in \mathrm{Gal}(E/K(x))$, hence $\mathrm{Gal}(E/K(x)) \subset \mathrm{Gal}(E/K(y))$, hence $K(y) \subset K(x)$.

9. (a) Let $\pi \in A_K$ be a uniformizer. We consider polynomials of the form $g(X) = f(X) + \pi^N h(X)$, for some integer $N \geq 1$, where $h(X) \in A_K[X]$ has degree at most $n-1$. If $\alpha \in A_E$ is a root of $f(X)$ with $k = v_E(f'(\alpha))$, and $N > k$, then we get $v_E(g(\alpha)) \geq N$ and $v_E(g'(\alpha)) = k$. Therefore if $N \geq 2k+1$ then Hensel's lemma shows that there is a unique $\beta \in A_E$ such that $g(\beta) = 0$ and $v_E(\alpha - \beta) > k$; the uniqueness shows (using Krasner's lemma) that $K(\beta) \subset K(\alpha)$.

We also get $v_E(f'(\beta)) = k$ and $v_E(f(\beta)) \geq N \geq 2k+1$, so Hensel's lemma shows that α is the unique root of $f(X)$ such that $v_E(\beta - \alpha) > k$; applying Krasner's lemma again shows that $K(\alpha) \subset K(\beta)$. We deduce that $K(\alpha) = K(\beta)$ and that $g(X)$ is irreducible.

(b) Every extension $K/\mathbb{Q}_p$ can be written $K/K_0/\mathbb{Q}_p$, where K_0 is the unique unramified extension of $\mathbb{Q}_p$ of degree $f_{K/\mathbb{Q}_p}$. It therefore suffices to show that for each $n \geq 1$, there exist only finitely many isomorphism classes of extension K/K_0 which are totally ramified of degree n. Each such extension is cut out by an Eisenstein polynomial of degree n; the space of Eisenstein polynomials degree n is homeomorphic to $pA_{K_0}^{n-1} \times pA_{K_0}^\times$, a compact topological space.

The previous part of the exercise gives an open ball around each Eisenstein polynomial in which the isomorphism class of the corresponding extension does not change. We can refine this to a finite cover, giving the finitely many isomorphism classes.

10. We just record the slopes. The 2-adic polygon has slopes $0, 3/4$. The 3-adic polygon has slopes $0, 1/3$. The 5-adic polygon has slope $1/5$.

The polynomial $f(X)$ is Eisenstein at 5, so is irreducible. To calculate the Galois group, we use the following observation: if K is a finite extension of $\mathbb{Q}_p$, $g(X) \in A_K[X]$ is monic with non-zero constant term, and a/b is a slope of $N_K(g)$ with a, b coprime integers, then b divides $e_{L/K}$ where L/K is the splitting field of $g(X)$. Indeed, $N_L(g) = e_{L/K} N_K(g)$ has integer slopes.

If E denotes the splitting field of $f(X)$, and $\mathfrak{q}$ is a prime of $\mathcal{O}_E$ above the prime p, then $E_\mathfrak{q}$ is the splitting field of $f(X)$ over $\mathbb{Q}_p$. More precisely, $E_\mathfrak{q}$ is generated over $\mathbb{Q}_p$ by the roots of $f(X)$ in $E_\mathfrak{q}$. In particular, if a/b is a slope of $N_{\mathbb{Q}_p}(f)$, a, b coprime integers, then b divides $e_{E_\mathfrak{q}/\mathbb{Q}_p}$, hence $[E : \mathbb{Q}]$.

We conclude that $[E : \mathbb{Q}]$ is divisible by $4 \times 3 \times 5 = 60$. So the Galois group is A_5 or S_5. To finish the proof we calculate the discriminant. If it is a non-square in $\mathbb{Q}^\times$, then the Galois group will be S_5. But we have $f(X) = X^5 + f'(X)$; if $\alpha \in E$ is a root of $f(X)$, and $K = \mathbb{Q}(\alpha)$, then we have

$$\operatorname{disc} f = \pm \mathbb{N}_{K/\mathbb{Q}} f'(\alpha) = \pm \mathbb{N}_{K/\mathbb{Q}} \alpha^5 = \pm (5!)^5.$$

Since the 5-adic valuation of $(5!)^5$ is odd, the discriminant can not be a square.