1. We have that $\mathbf{Q}(\zeta_7)/\mathbf{Q} \simeq (\mathbf{Z}/n\mathbf{Z})^\times \simeq \mathbf{Z}/(2) \oplus \mathbf{Z}/(3)$. Since this is an abelian group, all of its subgroups are normal. So that $\varphi : \sigma \mapsto \sigma|_{\mathbf{Q}(a)}$ maps surjectively onto $\mathrm{Gal}(\mathbf{Q}(a)/\mathbf{Q})$ by the galois correspondence. It is immediate that $\mathrm{Gal}(\mathbf{Q}(\zeta_7)/\mathbf{Q}) = \langle\tau\rangle \oplus \langle\sigma\rangle$, where τ represents complex conjugation and $\sigma : \zeta_7 \mapsto \zeta_7^2$. $\sigma(a) \neq a$ and $\tau(a) = a$ verifies that $\ker\varphi = \tau$, i.e.

$$\mathrm{Gal}(\min(a;\mathbf{Q})) = \mathrm{Gal}(\mathbf{Q}(a)/\mathbf{Q}) \simeq \mathrm{Gal}(\mathbf{Q}(\zeta_7)/\mathbf{Q})/\langle\tau\rangle \simeq \langle\sigma\rangle \simeq \mathbf{Z}/(3)$$

This also implies that

$$\min(a;\mathbf{Q}) = (x-a)(x-\sigma(a))(x-\sigma^2(a)) = (x-(\zeta_7^3+\zeta_7^4))(x-(\zeta_7^6+\zeta_7))(x-(\zeta_7^5+\zeta_7^2))$$

2. Denote $K := \mathbf{Q}(\sqrt[3]{2}, \zeta_3, \sqrt{3})$. Then K is the splitting field of polynomials x^3-2, and x^2-3 over $\mathbf{Q}$, hence is galois. To see that $[K:\mathbf{Q}] = 12$, denote $F = \mathbf{Q}(2^{1/3}, \sqrt{3})$. Then

$$3 = [\mathbf{Q}(2^{1/3}) : \mathbf{Q}]|[F:\mathbf{Q}] \text{ and } 2 = [\mathbf{Q}(\sqrt{3}) : \mathbf{Q}]|[F:\mathbf{Q}]$$

Similarly it is immediate that $[F:\mathbf{Q}] \leq 6$, so that it is in fact equal to 6. Now since $F \subset \mathbf{R}$, we have $[F(i):F] = 2$, but note that by the expanded form for ζ_3 we have $K = F(i)$, so that by multiplicativity of degree $[K:\mathbf{Q}] = 12$. We can equivelantly write $K = \mathbf{Q}(\sqrt[6]{108}, i)$ then we have

$$\mathrm{Gal}(K/\mathbf{Q}) = \langle\sigma,\tau\rangle$$

where $\sigma : \sqrt[6]{108} \mapsto \sqrt[6]{108}\zeta_6$, and τ represents complex conjugation. Furthermore we have $\sigma\tau \neq \tau\sigma$, as they do not agree on $\sqrt[6]{108}$. But since $[G : \langle\sigma\rangle] = 2$, $\langle\sigma\rangle$ must be normal and hence $\tau\langle\sigma\rangle\tau = \langle\sigma\rangle$, these two conditions together imply that $\tau\sigma\tau$ is a generator of $\langle\sigma\rangle$ not equal to σ, hence we must have $\tau\sigma\tau = \sigma^{-1}$ implying that $\tau\sigma = \sigma^{-1}\tau$, i.e. that $\mathrm{Gal}(K/\mathbf{Q})$ satisfies the relations of the dihedral group;

$$\mathrm{Gal}(K/\mathbf{Q}) \simeq D_{12}$$

3. Let f be a monic polynomial, such that

$$f|\Phi_n(x) \text{ and } f|\Phi_m(x)$$

in $\mathbf{F_p}(x)$. It follows that $f^2|\Phi_n(x)\Phi_m(x)|x^{nm}-1$, but the derivative of $x^{nm}-1$ is $nmx^{nm-1} \neq 0$ implies that $x^{nm}-1$ is seperable, so that f must have degree 0 (any root of f is a multiple root of $x^{nm}-1$).

4. We use the recursion formula, $\Phi_8(x)\Phi_4(x)\Phi_2(x)\Phi_1(x) = x^8-1$, then $\Phi_2(x) = x+1$, applying the recursion formula to $\Phi_4(x)$, we find that

$$\Phi_4(x) = \frac{x^4-1}{\Phi_2(x)\Phi_1(x)} = \frac{x^4-1}{x^2-1} = x^2+1$$

Now finally applying it to Φ_8, we find

$$\Phi_8(x) = \frac{x^8-1}{\Phi_4(x)\Phi_2(x)\Phi_1(x)} = \frac{x^8-1}{x^4-1} = x^4+1$$

If $p = 2$, then $x^4+1 = (x+1)^4$ so the result is trivial. So assume $p \neq 2$

First if there exists $a \in \mathbf{F_p}$, such that $a^2 = -1$, then $[\mathbf{F_p}(\sqrt{a}) : \mathbf{F_p}] \leq 2$, and $\sqrt{a}^4+1 = 0$, so that x^4+1 is not irreducible. Assume that $-1 \notin \mathbf{F_p}^2$, then for any $\alpha \in \mathbf{F_p}^2$ we have

$-\alpha \notin \mathbf{F_p}^2$ (otherwise we have $-\alpha/\alpha = -1 \in \mathbf{F_p}^2$), from the previous homework we showed that $\#\mathbf{F_p} = \frac{p+1}{2}$, we may write $\mathbf{F_p} = \{0, 1, \dots, \frac{p-1}{2}, -\frac{p-1}{2}, \dots, -1\}$ so that by counting, $\mathbf{F_p}$ has exactly one of $k, -k$ for each $0 \leq k \leq \frac{p-1}{2}$. This implies that one of $2, -2 \in \mathbf{F_p}^2$. Let α be in $\mathbf{F_p}$, such that $\alpha^2 = \pm 2$. Then we have

$$\Phi_8(x) = x^4 + 1 = (x^2 + \alpha x \pm 1)(x^2 - \alpha x \pm 1)$$

5. We first show that $\phi(p^r) = p^{r-1}(p-1)$, we can show this by showing $\Phi_{p^r}(x) = \Phi_p(x^{r-1})$ this is true for $r = 1$, now assume it for $k < r$, we have that

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{\prod_{0 \leq k < r} \Phi_{p^k}(x)} = \frac{x^{p^r} - 1}{(x-1)\prod_{1 \leq k < r} \Phi_p(x^{p^{k-1}})} = \frac{x^{p^r} - 1}{(x^p - 1)\prod_{2 \leq k < r} \Phi_p(x^{p^{k-1}})}$$

Continuing this process recursively we get

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{(x^{p^{r-1}} - 1)}$$

Substituting u in as $x^{p^{r-1}}$ on the right hand side yields the familiar formula $\frac{u^p - 1}{u - 1} = \Phi_p(u)$, which proves the lemma by substituting back $u \mapsto x^{p^{r-1}}$.

Suppose that ζ is an nk-th root of unity, then ζ satisfies the polynomial $x^{nk} - 1 = 0$, this of course implies that ζ^k satisfies a polynomial of degree n, namely $x^n - 1$. Since Φ_{nk} is the minimal polynomial of ζ, it will suffice to show that $\phi(nk) = \deg \Phi_{nk} = \deg \Phi_n(x^k) = k \deg \Phi_n$. Suppose that $\prod_i p_i^{e_i}$ is the prime factorization of nk, we may write $n = kr$ so that $nk = k^2 r$, then the prime factorizations of k and r may be written as

$$k = \prod p_i^{k_i} \quad \text{and} \quad r = \prod p_i^{r_i} \quad \text{Such that} \quad 2k_i + r_i = e_i$$

It follows from this factorization and the above lemma that

$$\phi(nk) = \prod_i \phi(p_i^{e_i}) = \prod p_i^{e_i - 1}(p_i - 1) = \prod_i p_i^{2k_i + r_i - 1}(p_i - 1)$$

$$k\phi(n) = \left(\prod_i p_i^{k_i}\right)\left(\prod_i \phi(p_i^{k_i + r_i})\right) = \left(\prod_i p_i^{k_i}\right)\left(\prod_i p_i^{k_i + r_i - 1}(p_i - 1)\right) = \prod_i p_i^{2k_i + r_i - 1}(p_i - 1)$$

As desired.

6. Let k denote the order of a in the multiplicative group of $\mathbf{F}$. First assume that $k|n$, then $n = k\ell$ for some ℓ, so that $a^n = a^{k\ell} = 1^\ell = 1$. Conversely, suppose for contradiction that $a^n = 1$ and $k \nmid n$. Then by long division we may write $n = mk + r$ for some $0 < r < k$. It follows that

$$1 = 1^{-m} = a^{-km} = a^{-km}1 = a^{-km}a^n = a^r$$

But $0 < r < k$ contradicts $k = o_{\mathbf{F}}(a)$.