1. (a) We note that F is a field because $f(x)$ is an irreducible polynomial in $\mathbb{F}_p$. Due to the inclusion of contants in $\mathbb{F}_p[x]$ and that $\deg f \geq 1$, we get that $\mathbb{F}_p \subset F$. Hence, $f(x) = a_0 + a_1 x + \cdots + a_d x^d$ with $a_i \in \mathbb{F}_p$. We note that:

$$f(\beta)^p = (a_0 + a_1\beta + \cdots + a_d\beta^d)^p = a_0^p + a_1^p\beta^p + \cdots + a_d^p\beta^{dp}$$

Because of $1 \in \mathbb{F}_p \subset F$, $char(\mathbb{F}_p) = p = char(F)$, and that F is a field, the result follows from Frobenius Map of $(a+b)^p \mapsto a^p + b^p$. Hence, we note that $f(\beta)^p = f(\beta^p) = 0^p = 0$. This concludes that β^p is a root of $f(x)$ in F. $\square$

(b) We note that since $\alpha = [x]$, we get that $f(\alpha) = [f(x)] = 0$. Hence α is a root of $f(x)$ in F. From (a), it follows that $\{\alpha, \alpha^p, \cdots, \alpha^{p^{d-1}}\}$ are all roots of $f(x)$.

Claim: $\{\alpha, \alpha^p, \cdots, \alpha^{p^{d-1}}\}$ are distinct

By contradiction, there exist a $0 \leq i < j \leq d-1$ where $\alpha^{p^i} = \alpha^{p^j}$. Hence, $\alpha^{p^j} - \alpha^{p^i} = (\alpha^{p^{j-i}} - \alpha)^{p^i} = 0$ by applying the Frobenius Map $a^{p^i} + b^{p^i} \mapsto (a+b)^{p^i}$. Thus, we get that $[x^{p^{j-i}} - x] = 0$ as we recall that $\alpha = [x]$. This implies that $f(x) \mid x^{p^{j-i}} - x$. By Theorem 9.23, $x^{p^{j-i}} - x$ is the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree dividing $j-i$. However, $j - i < d$, so $d \nmid j - i$, so $f(x)$ is not a monic irreducible factor of $x^{p^{j-i}} - x$, which gives us a contradiction. Hence, they must be distinct. $\square$

Since we have found d distinct roots for a monic polynomial $f(x)$, by Corollary 9.7, it follows that $\prod_{i=0}^{d-1}(x - \alpha^{p^i}) \mid f(x)$. Since $f(x)$ is monic and the product has degree d, we get that $\prod_{i=0}^{d-1}(x - \alpha^{p^i}) = f(x)$ as desired. $\square$

(c) By Proposition 9.21, defining a homomorphism of $\varphi : F \to E$ is the same as giving a root β of $f(x)$ in E, which exists as defined. By the First Isomorphism Theorem, the natural map of $\phi : F/ker(\varphi) \to im(\varphi)$ is an isomorphism. Note that F is a field, so any homomorphism is injective, which implies that only $\varphi(0) = 0$. Thus, the $ker(\varphi) = \{0\}$, which further implies that $F/ker(\varphi) = F$. Since $im(\varphi)$ is a subring of a field E, it is also a subfield of E. Since ϕ is an isomorphism, note that $\{\phi(\alpha), \phi(\alpha^p), \cdots, \phi(\alpha^{p^{d-1}})\} \subset E$ must also be all distinct.

We then note that since $char(E) = p$, $\mathbb{F}_p$ is a subring of E. Since all of $f(x)$'s coefficients lie in $\mathbb{F}_p$ and that $\phi(1) = 1$, for any $a \in \mathbb{F}_p$, $\phi(a) = a$. Hence, $\phi(f(x)) = \phi(a_0 + a_1 x + \cdots + a_d x^d) = a_0 + a_1\phi(x) + \cdots + a_d\phi(x)^d = f(\phi(x))$. For any root $\alpha^{p^i} \in F$, we note that $\phi(f(\alpha^{p^i})) = \phi(0) = 0 = f(\phi(\alpha^{p^i}))$. Hence, $\{\phi(\alpha), \phi(\alpha^p), \cdots, \phi(\alpha^{p^{d-1}})\}$ are all roots of $f(x) \in E$. Since $f(x)$ has d distinct roots, by Corollary 9.7, it must be in the form $c(x - \phi(\alpha)) \cdots (x - \phi(\alpha^{p^{d-1}}))$, so it splits completely. $\square$

2. (a) We assume $o(\alpha) = m$. Since $|\mathbb{F}_{p^n}^{\times}| = p^n - 1$, we get that $\alpha^{p^n-1} = 1$, so $m \mid p^n - 1$ as desired.

We assume $m \mid p^n - 1$. Then for some $\beta \in \mathbb{F}_{p^n}$ by Theorem 10.16, we get that $o(\beta) = |\mathbb{F}_{p^n}^{\times}| = p^n - 1$. This implies that $\mathbb{F}_{|\ltimes} = \{0, \beta, \cdots, \beta^{p^n-1}\}$. Since $m \mid p^n - 1$, there exist some integer q where $mq = p^n - 1$. Since $q \leq p^n - 1$, $\beta^q \in \mathbb{F}_{p^n}$. Note that $(\beta^q)^m = \beta^{p^n-1}$, so $o(\beta^q) \mid m$. Suppose $o(\beta^q) < m$ and let $d = o(\beta^q)$, this implies that $\beta^{qd} = 1$. However, $qd < qm = p^n - 1$, so this contradicts $o(\beta)$'s minimality. Hence, it must be that $o(\beta^q) = m$. $\square$

(b) **Claim:** $\Phi_m(x)$ splits completely in $\mathbb{F}_{p^d}$.

Since $d = o_m(p)$, we get that $m \mid p^d - 1$. By the result of the proof from Theorem 10.7, if $d \mid |\mathbb{F}_{p^n}^{\times}|$, then the number of elements in $\mathbb{F}_{p^n}$ with order exactly d is $\phi(d)$. Since $m \mid m$, there exist $\phi(m)$ elements with order m. Hence, for each of the $\phi(m)$ elements β with $o(\beta) = m$, we get that $\Phi_m(\beta) = 0$ from HW7(b). $\Phi_m(x)$ is degree $\phi(m)$ with $\phi(m)$ distinct roots. By Corollary 9.7, $\Phi_m(x)$ is divisible by the product of $\phi(m)$ linear polynomials, so it splits completely in $\mathbb{F}_{p^n}$. $\square$

Claim: Irreducible polynomial factors of $\Phi_m(x)$ in $\mathbb{F}_p$ has degree d.

Let $f(x)$ be an irreducible polynomial factor of $\Phi_m(x)$ in $\mathbb{F}_p$ with degree k. Since $f(x)$ is a factor of $\Phi_m(x)$, which splits completely in $\mathbb{F}_{p^d}$. $f(x)$ must also split completely and shares roots with $\Phi_m(x)$. Earlier, we showed that all roots of $\Phi_m(x)$ has order m. Hence, there is a root α of $f(x)$ where $o(\alpha) = m$.

By Theorem 9.23, $f(x)$ is factor of $x^{p^k} - x$ in $\mathbb{F}_p$ since $k \mid k$. Since there is a natural way to $\mathbb{F}_p$ in $\mathbb{F}_{p^d}$, we note that $f(x)$ is a factor of $x^{p^k} - x$ in $\mathbb{F}_{p^d}$ and consequently, $\alpha^{p^k} - \alpha = 0$ and that $\alpha^{p^k-1} = 1$. Since $o(\alpha) = m$, $p^k \equiv 1 \pmod{m}$ and $d \mid k$.

Meanwhile, from Theorem 9.21, there exist a homomorphism $\mathbb{F}_p[x]/(f(x)) \to \mathbb{F}_{p^d}$ is the same as giving the root α in $\mathbb{F}_{p^d}$. Since $\mathbb{F}_p[x]/(f(x))$ is a field with order p^k, from Theorem 10.1 (d), this homomorphism implies that $k \mid d$. Since $k \mid d$ and $d \mid k$, we get that $k = d$ as desired. $\square$

Since $\Phi_m(x)$ is a monic polynomial, it can be written as a product of irreducible polynomials as quoted from Example 9.15. Since each irreducible polynomial factor is degree d and $\Phi_m(x)$ is degree $\phi(m)$, it must be that there exists $\phi(m)/d$ irreducible polynomial factors for $\Phi_m(x)$. $\square$

(c) We assume p is not a square mod q. We first note that by Euler Criterion, we get that $\phi(m) = q - 1$. Meanwhile, $(\frac{p}{q}) = -1 \equiv p^{(q-1)/2} \pmod{q}$. This implies $d \nmid (q-1)/2$. We also note that $1 \equiv p^{q-1} \pmod{q}$, so $d \mid q - 1$. Since $dr = q - 1$, it follows that $d(r/2) = (q-1)/2$. $(r/2) \notin \mathbb{Z}$ or else $d \mid (q-1)/2$. This implies that r is odd. Since $q - 1$ is even from q being an odd prime, it follows that d must be even.

We assume d is even and r is odd. Since $rd = q - 1$, we note that $r/2 \notin \mathbb{Z}$ and that $d \nmid (q-1)/2$. This implies that $p^{(q-1)/2} \not\equiv 1 \pmod{q}$. However, $p^{q-1} \equiv 1 \pmod{q}$ by Fermat's Last Theorem, so $p^{(q-1)/2} \equiv -1 \pmod{q}$. By Corollary 11.3, p is a quadratic non-residue mod q, so p is not a square mod q. $\square$

3. (a) For any $a_i \in F$, we re-organize $f(x)$ to $(x-a_i)\prod_{\substack{k=1\\k\neq i}}^{n}(x-a_k)$. We note that:

$$f'(x) = (x-a_i)(\prod_{\substack{k=1\\k\neq i}}^{n}(x-a_k))' + 1\cdot\prod_{\substack{k=1\\k\neq i}}^{n}(x-a_k) = \prod_{\substack{k=1\\k\neq i}}^{n}(x-a_k)$$

Within the product of $f(a_i)$, there exists i instances where $i > k$. We correct this by applying $(-1)^i f'(a_i)$ to get that:

$$(-1)^i f'(a_i) = \prod_{k=1}^{i-1}(a_k - a_i)\cdot\prod_{k=i+1}^{n}(a_i - a_k)$$

We then note that for any $1 \leq i < j \leq n$, $(a_i - a_j)$ is a factor in the products of $(-1)^i f'(a_i)$ and $(-1)^j f'(a_j)$. Hence, we note that the product of all such $(-1)^i f'(a_i)$ is equal to:

$$\begin{aligned}\prod_{i=1}^{n}(-1)^i f'(a_i) &= (-1)^{1+\cdots+n}\prod_{i=1}^{n} f'(a_i)\\ &= (-1)^{n(n-1)/2}\prod_{1\leq i<j\leq n}(a_i-a_j)^2\\ &= \triangle f\end{aligned}$$

as desired. □

(b) Let $f(x) = x^8 + x^2 + 1$. We note that $f'(x) = 8x^7 + 2x = 2x(4x^6+1)$ We then note that if $f(x)$ splits completely in F, it must have 8 roots because $\deg f = 8$. We apply the altered calculation of the determinant from (a) and consider that $(-1)^(8\cdot 7/2) = (-1)^{28} = 1$. Thus:

$$\triangle f = \prod_{i=1}^{8} f'(a_i) = 2^8\cdot\prod_{i=1}^{8} a_i\cdot\prod_{i=1}^{8} 4a_i^6 + 1$$

Claim (Vieta): If a polynomial $f(x)$ splits completely and is monic. Then $f(0)$ is equal to product of its roots times $(-1)^{\deg f}$.

Let us assume $f(x) = (x-a_1)\cdots(x-a_k)$ with degree k. Then $f(0) = (-a_1)\cdots(-a_k) = (-1)^k\cdot a_1\cdots a_k$. □

With Vieta, we note that $f(0) = 1$, so by Vieta, we get that $(-1)^8\prod_{i=1}^{8} a_i = \prod_{i=1}^{8} a_i = 1$. Thus, we can simplify $\triangle f$ into:

$$\triangle f = 2^8\cdot\prod_{i=1}^{8} 4a_i^6 + 1$$

We also then note that for any root a_i, $a_i^8 + a_i^2 + 1 = 0$, so $a_i^6 = -(1 + 1\cdot a_i^{-2})$ Thus:

$$\begin{aligned}\triangle f &= 2^8\cdot\prod_{i=1}^{8} -4(1+1\cdot a_i^{-2}) + 1\\ &= 2^8\cdot\prod_{i=1}^{8} -4 - 4\cdot a_i^{-2} + 1\\ &= 2^8\cdot\prod_{i=1}^{8} -a_i^{-2}\prod_{i=1}^{8} 3a_i^2 + 4\end{aligned}$$

We note that $\prod_{i=1}^8 -a_i^{-2} = (\prod_{i=1}^8 a_i)^{-2} = 1^{-2} = 1$, so:

$$\triangle f = 2^8 \cdot \prod_{i=1}^{8} 3a_i^2 + 4$$

We then note that $f(x)$ is an even polynomial as all of its powers are even. Hence, $f(-x) = f(x)$. This means that the negation of each of the roots are also roots. Hence, we can pair each of the roots $a_1, \cdots, a_8$ into $b_1, \cdots, b_4, -b_1, \cdots, -b_4$, which gives us the follow since $(-b_i)^2 = b_i^2$:

$$\triangle f = 2^8 \cdot (\prod_{i=1}^{4} 3b_i^2 + 4)^2$$

We now denote a new polynomial $g(x) = x^4 + x + 1 \in F[x]$. Because $f(x) = (x^2 - b_1^2) \cdots (x^2 - b_4^2)$ and that $f(x) = g(x^2)$, we get that $g(x) = (x - b_1^2) \cdots (x - b_4^2)$. Hence, it splits completely and it has 4 roots.

Hence, let $h(x) = 3^4 \cdot (((x-4)/3)^4 + ((x-4)/3) + 1)$ and $h(x) \in F[x]$. Note that $char(F) \neq 3$, so we can divide by 3. We also note that:

$$\begin{aligned} h(x) &= 3^4 \cdot ((x-4)/3 - b_1^2) \cdots ((x-4)/3 - b_4^2) \\ &= ((x-4) - 3b_1^2) \cdots ((x-4) - 3b_4^2) \\ &= (x - (3b_1^2 + 4)) \cdots (x - (3b_4^2 + 4)) \end{aligned}$$

Thus, $h(x)$ is monic and splits completely. We expand to get $h(x) = (w-4)^4 + 27(w-4) + 81$. We then calculate $h(0) = 256 - 108 + 81 = 229$. We apply Vieta to get that $(-1)^4 \prod_{i=1}^4 3b_i^2 + 4 = 229$ as they are roots of $h(x)$. Hence, we substitute it in and get that for $charF \neq 3$:

$$\triangle f = 2^8 \cdot 229^2$$

And we are done. $\square$

(c) By contradiction, $f(x) = x^8 + x^2 + 1$ is irreducible in $\mathbb{F}_p[x]$ for some prime p. Let p be one such prime. Since $f(x)$ is a monic irreducible polynomial in $\mathbb{F}_p[x]$, by Q1(b), we can factor $f(x)$ in $\mathbb{F}_p[x]/(f(x))$ as:

$$f(x) = \prod_{i=0}^{8-1} (x - \alpha^{p^i})$$

We also note that:

$$\triangle f = \prod_{0 \leq i < j \leq 7} (\alpha^{p^i} - \alpha^{p^j})^2$$

From (b), $\triangle f = 2^8 \cdot 229^2$. However, this looks very similar to the β defined in HW1(d) where:

$$\beta = \prod_{0 \leq i < j \leq 7} (\alpha^{p^i} - \alpha^{p^j})$$

Hence, $\beta = 2^4 \cdot 229$. Since $2^4 \cdot 229 = 2^4 \cdot 229 \cdot 1$, $\beta \in \mathbb{F}_p$. However, from HW1(d), $\beta \in \mathbb{F}_p$ if and only if $\deg f$ is odd. Clearly, $\deg f$ is not odd, so we reached a contradiction. Thus, $f(x)$ is reducible in $\mathbb{F}_p[x]$ for any prime p. $\square$