Q20:

20.

Proposition 7. *For every n there exists an irreducible polynomial of degree n in $\mathbb{F}_p[x]$.*

Proof. Suppose we fix some arbitrary n.
We know there exists some finite field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$.
Note that $Q19$ gave us that $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ for some $\alpha \in \mathbb{F}_{p^n}$.
Furthermore, $Q2$ gave us that $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ and thus $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n$.
Hence, we know that the degree of α over $\mathbb{F}_p$ is n.
By definition, the minimal polynomial $f(x) \in \mathbb{F}_p[x]$ for α is degree n.
Furthermore, we know that minimal polynomials are irreducible.
Therefore, for arbitrary n, we have found an irreducible polynomial of degree n in $\mathbb{F}_p[x]$. □

Q21:

21.

Proposition 8. *The* ***Frobenius map*** $\Phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ *given by* $\Phi : \alpha \mapsto \alpha^p$ *is an automorphism of order* n.

Proof. Observe $\Phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and thus is by definition an automorphism if it is an isomorphism.
We will first show that Φ is a homomorphism.
Preserves Addition:
Suppose $x, y \in \mathbb{F}_{p^n}$.
Note for Freshman's Dream that $\mathbb{F}_{p^n}$ has characteristic p.
Then, we have

$$\begin{aligned}\Phi(x+y) &= (x+y)^p \\ &= x^p + y^p \text{ (by Freshman's Dream Theorem)} \\ &= \Phi(x) + \Phi(y)\end{aligned}$$

and thus Φ preserves addition.
Preserves Multiplication:
Suppose $x, y \in \mathbb{F}_{p^n}$.

$$\begin{aligned}\Phi(xy) &= (xy)^p \\ &= x^p y^p \text{ (as multiplication is commutative)} \\ &= \Phi(x)\Phi(y)\end{aligned}$$

and thus Φ preserves multiplication.
To show that Φ is bijective, it suffices to show that Φ is invertible.
If Φ has order n, then Φ must be invertible as then $\Phi^{n-1} = \Phi^{-1}$.
To show Φ^n is the identity automorphism, suppose we take some $x \in \mathbb{F}_{p^n}$.
We want to show $\Phi^n(x) = x$.
Evidently $\Phi^n(x) = x^{p^n}$.
However, we know that $|\mathbb{F}_{p^n}^\times| = p^n - 1$ as every element but 0 is a unit, and hence the order of x divides $p^n - 1$.
This gives us that $x^{p^n - 1} = 1$.
Hence $x^{p^n-1}x = x$ and therefore $x^{p^n} = x$.
We have successfully shown that $\Phi^n(x) = x$ for arbitrary x, and therefore Φ^n is the identity automorphism.
Hence, we have that the order of Φ divides n.
Suppose for contradiction that $|\Phi| < n$ and let $k = |\Phi|$.
Then Φ^k is the identity automorphism and by definition for all $x \in \mathbb{F}_{p^n}$ we have $x^{p^k} = x$, which implies $x^{p^k} - x = 0$.
However $x^{p^k} - x$ is a degree p^k polynomial, and thus having p^n roots with $k < n$ is a contradiction.
Therefore, we know that Φ has order n, by our previous argument Φ is bijective, and thus Φ is an automorphism on $\mathbb{F}_{p^n}$. $\square$

Q23:

Q23.

Since E and F are fields, $E \cap F$ is also a field.

Suppose $a, b \in E \cap F$, then $a, b \in E, F$ and so $a-b, \frac{a}{b} \in E, F$ and $a-b, \frac{a}{b} \in E \cap F$.

Thus, $E \cap F$ is a subfield of $GF(p^n), E, F$ and so $|E \cap F| = p^k$ where $k \mid r$, $k \mid s$ and $k \mid n$.

We claim $k = \gcd(r, s)$. We know that $GF(p^{\gcd(r,s)}) \subseteq GF(p^r)$ and $GF(p^{\gcd(r,s)}) \subseteq GF(p^s)$, so $GF(p^{\gcd(r,s)}) \subseteq E \cap F$. and so $\gcd(r, s) \mid k$. Since $k \mid r$, $k \mid s$, $k = \gcd(r, s)$.

Thus, the order of $E \cap F$ is p^k where $k = \gcd(r,s)$.

23.

Proposition 9. *Let E and F be subfields of $\mathbb{F}_{p^n}$. If $|E| = p^r$ and $|F| = p^s$, then the order of $E \cap F$ is $p^{\gcd(r,s)}$.*

Proof. Suppose E, F are subfields of $\mathbb{F}_{p^n}$ such that $|E| = p^r$ and $|F| = p^s$.
As $E \cap F$ is a subfield of E, it must be true that $E \cap F = \mathbb{F}_{p^k}$ for some k such that $k \mid r$ by Theorem 22.7.
Similarly, as $E \cap F$ is a subfield of F, it must be true that $k \mid s$.
Then $k \mid r$ and $k \mid s$ implies $k \mid \gcd(r, s)$.
As $E \cap F$ is by definition the largest possible shared subfield between E and F, this implies $k = \gcd(r, s)$ and therefore $|E \cap F| = p^{\gcd(r,s)}$. □