(a) Let \( K \) be a field of char \( p \).

Clearly \( (xy)^p = x^py^p \) for any \( x, y \in K \).

Hence, \( \sum_{k+l=p} \frac{p!}{k!l!} x^k y^l = x^p + x^p = x^p + \sum_{k+l=p} \frac{p!}{k!l!} x^k y^l \).

We know \( \frac{p!}{l!} \in \mathbb{Z} \), but since \( k, l < p \), we can interpret this as \( \ell \cdot l! \) where \( p, p-1, \ell \) are prime fields (all integers between 1 and \( p-1 \) are invertible in \( \mathbb{Z}/p\mathbb{Z} \)). So \( \frac{p!}{l!} = 0 \) in \( \mathbb{Z}/p\mathbb{Z} \) and

\[(x+y)^p = x^p + y^p.
\]

In \( \mathbb{Z}/p\mathbb{Z} \), have \( 1^p = 1 \), so by linearity \( \left( \begin{array}{cccc} 1 & \ldots & 1 \end{array} \right)^p = 1^p + \ldots + 1^p \).

Cor: \( 0^p = 0 \), and if \( x \in (\mathbb{Z}/p\mathbb{Z})^* \) then \( x^p = 1 \) (Lagrange’s thm).

So \( x^p = x \).

Remark: In \( \mathbb{F}_p(t) \) image of Frobenius is \( \mathbb{F}_p(t) \).

\[ (a_0 + a_1 t + \ldots + a_p t^p)^p = a_0^p + a_1^p t^p + \ldots + a_p^p t^{p^p} \]

(b) \( x^{p+1} = (x^p)^p \), i.e. the map \( x \mapsto x^p \) is \( \mathbb{F}_p \) linear.

\[ \xi(x) = x^p \]

\( \xi \) is a composition and power.

(c) By the pigeonhole principle, \( \xi \) is surjective if \( K \) is finite.

(d) Let \( K/F_p \) be algebraic, let \( \alpha \in K \). Then \( \alpha \) is algebraic over \( F_p \), so \( [F_p(\alpha) : F_p] < \infty \) so \( F_p(\alpha) \) is a finite field.
(it has \( p^{[F_p(a) : F_p]} \) elements). Now \( F_p(a) \) is the Frobenius map of \( F_p(a) \), by part (c) that is surjective, so there is \( \beta \in F_p(a) \) s.t. \( p^\beta = a \). Then \( \lambda \in \text{Image of } F_p \).

Ideas: dim\( F_p \) may be infinite, but any particular element lies in a finite-dimensional piece of \( K \).

(2) \( \mathbb{Z}/(\mathbb{Z}/n\mathbb{Z})^+ \) the elements of order dividing \( d \) of \( (\mathbb{Z}/n) \) are those \( x \) s.t. \( d \cdot x \equiv 0 \pmod{n} \), i.e. the multiples of \( \frac{n}{d} \).

So \( \mathbb{Z}/(\mathbb{Z}/n\mathbb{Z})^+ \) has exactly \( d \) elements of order dividing \( d \) (thought: use the conclusion; check what a cyclic \( G \) is like).

So conditions for any \( d \mid n \), \( G \) has at most as many elements of order dividing \( d \) as \( C_d \).

Prove claim (c) by induction. If \( n=1 \), nothing to prove.

Suppose for any \( m \mid n \), if \( G \) has order \( m \), at most \( d \) elements of order \( d \) for \( d \mid m \) then \( G \triangleleft C_m \).

Now let \( d \mid n \), ask: how many elements of order \( d \) does \( G \) have? Suppose this is positive, let \( x \) be such an element. Then \( \langle x \rangle \leq G \) is isomorphic to \( C_d \).

So has \( d \) elements of order dividing \( d \) so it has all \( d \) elements of order \( 1d \) in \( G \). So all elements of order exactly \( d \) are in \( \langle x \rangle \), so \( G \) has exactly as many such elements as \( C_d \) and \( C_n \).
Conclusion: for any abelian $G$ has no elements of order 1, or exactly as many as $C_n$. But every element of $G$ has order dividing $n = \#G = \#C_n$, so $G$ has as many elements of order as $C_n$. Apply to $d = n$ to get $G \subset C_n$

$$n = \sum_{d \mid n} \#C_d \leq \sum_{d \mid n} \#G_d = n$$

term-by-term

Conclude $F$ is a field, $G \subset F^*$ is finite, elements of $G$ of order $d$ satisfy $x^d = 1$, and $x^d - 1 \in \mathbb{F}[x]$ has at most $d$ roots. \(\Rightarrow\) $G$ is cyclic.

**Example:** $G \subset \mathbb{C}^*$ is finite. The every $z \in G$ has $|z| = 1$.

Otherwise $z$ has infinite order since $|z^n| \to \infty$ as $n \to \infty$.

Also, any $z \in \mathbb{C} \cdot 2\pi i$. (if $z^d = 1$, $z = \frac{2\pi i}{d}$.

Taking logarithms, $G \subset \mathbb{Q}/\mathbb{Z}$. Note: $\frac{a}{d}$ with $(a,d) = 1$ generates $\frac{1}{d} \mathbb{Z}/d\mathbb{Z}$ in $\mathbb{Q}/\mathbb{Z}$ also if $a \in \mathbb{Z}$, $\frac{1}{d} \mathbb{Z}/d\mathbb{Z}$

(3) Consider $x^2 - x \in \mathbb{F}_p[x]$, $g = p^e$.

(a) $\partial(x^q - x)$: $q \cdot x^{q-1} - 1 = -1$ so no root of $x^q - x$ is a root of $\partial(x^q - x)$ so it’s separable.

(i.e. in the splitting field, $x^q - x$ has $q$ distinct roots)

(b) Let $F$ be a field with $9$ elements.
Then $F$ has char $p$, $F^* \cong \mathbb{Z}/(p-1)$, so every non-zero $\alpha \in F$ has $\alpha^{q-1} = 1$, so $\alpha^2 = \alpha$.

- Every $\alpha \in F$ is a root of $x^q - x$.

So $F$ consists of the roots of $x^q - x$, and in particular is generated by them.

(c) Since splitting fields are unique up to isomorphism, fields with $q$ elements are unique up to $\text{GF}(q)$-isomorphism.

If $F_q$ exists, it's the splitting field of $x^q - x$.  Maybe:  (1) the splitting field has fewer than $q$ elements?  [Ruled out by separability of $x^q - x$]

(2) The splitting field has more than $q$ elements?

Let $F$ be the splitting field of $x^q - x$ over $\text{GF}(p)$.

Then map $\phi(x) \mapsto x^q$ is an automorphism of $F$ (1)(c).

The set $K = \{ x \in F \mid \phi(x) = x \}$ is a subfield containing

the roots of $x^q - x$: closed under $+$, $\cdot$, since $\phi$ is

a monomorphism (Corollary).

\[ \phi(x + \beta \cdot \gamma) = \phi(x) + \phi(\beta) \phi(\gamma) = x + \phi(\gamma) \]

if $x, \beta, \gamma \in K$, if $\phi$ then $\phi(\beta) \phi(\gamma) = \phi(1) = 1$

\[ \phi(\beta \cdot \gamma) = \phi(\beta) \cdot \phi(\gamma) \]

$\phi(\beta^{-1}) = \beta^{-q}$.

So $x^q - x$ splits in $K$, and hence $K = F$.

$\Rightarrow F$ consists exactly of the $q$ distinct roots of $x^q - x$, $\text{GF}(q)$.
5. If $K$ has order $q$, $K$ is the splitting field of $x^q - x$ over $F_p$, hence over $F_q$, so $K/F_q$ is normal.
Every $\alpha \in K$ is a root of the separable polynomial $x^q - x$.

6. (a) $\alpha$ is algebraic over $K$, then finitely many fields between $K$, $K(\alpha)$.
Let $K \subseteq M \subseteq K(\alpha)$ be a subfield, let $m_\alpha \in M[x]$ be the minimal polynomial of $\alpha$.
Think of $m_\alpha$ as a poly. in $K(\alpha)[x]$.
Certainly, $M = K(\text{coefficients of } m_\alpha) \supseteq K$.
What is $m_\alpha$? It must be a divisor of $m_\alpha$.
Because $m_\alpha \in M[x]$. But $m_\alpha$ is irreducible in $M[x]$.
So also in $M[x]$.

Idea: If $f$ irreducible in $K[x]$ it's irreducible over any subfield (containing the coeffs).

So $m_\alpha = m_\alpha$.

Reflection: if map $M \to m_\alpha$ fails to be injective then have $\tilde{M} \subseteq M$ with $m_\tilde{M} = m_\alpha$.

But: $[K(\alpha) : M] = \deg m_\alpha = \deg m_\tilde{M} = [K(\alpha) : \tilde{M}]$.
So $[M : \tilde{M}] = 1$, and $M = \tilde{M}$.

(if $\alpha$ transcendental over $K$, $K(\alpha(t)) \subsetneq K(t)$ all distinct)
If \( L \neq \mathbf{K}(\alpha) \) add \( \alpha_2, \alpha_3, \ldots \), if can't stop get any more subfields. Total deg \( L:K \) finite by mul in tower.

(3) By induction enough to show \( K(\alpha, \beta) = K(\beta) \)

Consider the elements \( \alpha + \lambda \beta, \alpha \in K \)

no two of them belong to same subfield.

\( \sqrt{2} + i \sqrt{3} \)

\( n \quad \text{proper} \)

If \( \alpha + \lambda \beta \) and \( \alpha + \mu \beta \) \( \in M \)

then \( (\alpha - \mu) \beta \in M \Rightarrow \beta \in M \).

then \( \alpha \in M \).

\( \Rightarrow \) at most finitely many \( \alpha \in K \) if \( K(\alpha, \lambda \beta) \neq K(\beta) \)

\( \Rightarrow K \) finite) for almost all \( \alpha \in K \), \( K(\alpha + \lambda \beta) = K(\beta) \).