Corollary 10.7 Let F, F' be finite fields with $|F| = |F'|$. Then $F \cong F'$.

Proof By Corollary 10.5 we have $|F| = |F'| = p^n$ for some prime number p and some $n \geq 1$. Moreover, the prime fields $F_p, F_{p'}$ of F, F' satisfy $F_p \cong \mathbb{Z}_p \cong F_{p'}$ by Theorem 10.4. By Theorem 10.6 and using uniqueness of splitting fields up to isomorphism, we have

$$F \cong \text{splitting field of } x^{p^n} - x \in F_p[x]$$
$$\cong \text{Splitting Field of } x^{p^n} - x \in F_{p'}[x] \cong F'. \qquad \square$$

We have shown that if a field with p^n elements exists, then it is unique up to isomorphism. We now show that such a field does indeed exist.

Theorem 10.8 Let F be a field with $|F| = p^n$ for some prime number p and $n \geq 1$. Then there exists an extension field E of F with $[E:F] = m$ for every $m \in \mathbb{Z}_{\geq 1}$.

Proof Let $f(x) = x^{p^{nm}} - x \in F[x]$. Let E be the splitting field of f over F. Let $\alpha \in E$ be a root of f. Since $f'(x) = p^{nm} x^{p^{nm}-1} - 1 = -1 \neq 0$ (because $\text{char}(F) = p$), we have that α is a simple root of f by Lemma 9.5. Consider the set

$$E' = \{ r \in E \mid f(r) = 0 \}.$$

Since $\deg(f) = p^{nm}$ and f has no multiple roots, we have $|E'| = p^{nm}$. We claim that E' is a subfield of E. Indeed, let $\alpha, \beta \in E'$. Then $\alpha^{p^{nm}} = \alpha$, $\beta^{p^{nm}} = \beta$ and

$$(\alpha+\beta)^{p^{nm}} \overset{\text{Exercise}}{=\!=} \alpha^{p^{nm}} + \beta^{p^{nm}} = \alpha + \beta \implies f(\alpha+\beta) = 0 \Rightarrow \alpha + \beta \in E'$$
$$(-\alpha)^{p^{nm}} \overset{\text{Exercise}}{=\!=} -(\alpha^{p^{nm}}) = -\alpha \implies f(-\alpha) = 0 \Rightarrow -\alpha \in E'$$

$(\alpha\beta)^{p^{mn}} = \alpha^{p^{mn}}\beta^{p^{mn}} = \alpha\beta \Rightarrow f(\alpha\beta)=0 \Rightarrow \alpha\beta \in E'$

if $\alpha \neq 0$, $(\alpha^{-1})^{p^{mn}} = (\alpha^{p^{mn}})^{-1} = \alpha^{-1} \Rightarrow f(\alpha^{-1})=0 \Rightarrow \alpha^{-1} \in E'$.

Hence E' is a field with $|E'| = p^{mn}$ and F splits in E'. Since $E' \subseteq E$ and by minimality of the splitting field E we have $E = E'$. Let $[E:F] = x$. Then $|E| = (p^n)^x$ and so

$$p^{mn} = |E'| = |E| = (p^n)^x = p^{nx}$$

implies $x = m$ as required. □

Corollary 10.9. For every prime number p and every integer $n \geq 1$, there exists a unique field with p^n elements up to isomorphism.

Proof. Existence follows by Theorem 10.8 (put $n=1$, $m=n$). Uniqueness follows by Corollary 10.7.

Notation 10.10 By Corollaries 10.5 and 10.9 it follows that we have a correspondence

$$\left\{\begin{array}{l}\text{Finite fields}\\ \text{up to isomorphism}\end{array}\right\} \xleftrightarrow{1:1} \{p^n \in \mathbb{Z} \mid p \text{ prime}, n \geq 1\}$$

We denote by $GF(p^n)$ the unique up to isomorphism field with p^n elements. The notation stands for Galois Fields which is what finite fields are usually called.

Recall. Let G be a finite group.

(1) Let $g \in G$. The order of g, denoted $o(g)$, is the smallest n such that $g^n = 1$. Since $g^{|G|} = 1$, we have that $o(g)$ is finite. Also, if $g^k = 1$, then $o(g) \mid k$ and so $o(g) \mid |G|$.

(2) The exponent of G, denoted $e(G)$ is the smallest n such that $g^n = 1$ $\forall g \in G$. In other words,

$$e(G) = \operatorname{lcm}\{o(g) \mid g \in G\}.$$

(Example: $e(\mathbb{Z}_4) = 4$, $e(\mathbb{Z}_2 \times \mathbb{Z}_2) = 2$). In particular, $e(G) \mid |G|$.

(3) If G is abelian, then $\exists g \in G$ with $o(g) = e(G)$.

Indeed, in this case $G \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}}$ for some prime numbers $p_1, \ldots, p_n$, and integers $r_1, \ldots, r_n \geq 1$. Then one sees that

$$o(1, \ldots, 1) = \operatorname{lcm}(p_1^{r_1}, \ldots, p_n^{r_n}) = \operatorname{lcm}(e(\mathbb{Z}_{p_1^{r_1}}), \ldots, e(\mathbb{Z}_{p_n^{r_n}})) = e(G).$$

(4) It follows that if G is abelian, then

$$G \text{ is cyclic} \iff e(G) = |G|.$$

Indeed, assume first that G is cyclic. Then $\exists g \in G$ with $o(g) = |G|$. Then $|G| \leq e(G)$ by definition of $e(G)$. By (2) we have $e(G) \mid |G|$ so we conclude that $|G| = e(G)$.

For the other direction, assume $|G| = e(G)$. By (3) there exists $g \in G$ with $o(g) = e(G) = o(G)$. Then (g) is a subgroup of G with order $o(g) = |G|$ and so $(g) = G$ and G is cyclic.

Theorem 10.11. Let F be a field. Then the multiplicative group $F^* = F \setminus \{0\}$ is cyclic if and only if F is finite.

Proof. ($\Leftarrow$) By (4) above it is enough to show $e(F^*) = |F^*|$. Since $\alpha^{e(F^*)} = 1 \ \forall \alpha \in F^*$, we have that every $\alpha \in F^*$ is a root of $x^{e(F^*)} - 1 \in F[x]$. Hence this polynomial has at least $|F^*|$ roots. Since it has at most $e(F^*)$ roots, we obtain $|F^*| \leq e(F^*)$. But $e(F^*) \mid |F^*|$ and so $e(F^*) = |F^*|$.

($\Rightarrow$) Let $F^* = (\alpha)$ and assume to a contradiction that $|F^*| = \infty$.

Case 1: $\operatorname{char}(F) \neq 2$. Then $-1 \in F^*$ and $-1 \neq 1$. Since $(-1)^2 = 1$, -1 has finite order. But $-1 \in F^* = (\alpha) \Rightarrow -1 = \alpha^r$ for some $r \in \mathbb{Z} \Rightarrow \alpha^r$ has finite order $\Rightarrow \alpha$ has finite order, contradicting $(\alpha) = F^*$ being infinite.

Case 2: $\operatorname{char}(F) = 2$. Then $F_p \cong \mathbb{Z}_2$ is the prime field of F.

Then

$$F = F^* \cup \{0\} = \langle\alpha\rangle \cup \{0\} \subseteq F_p(\alpha) \Rightarrow F_p(\alpha) = F$$
$$F_p \subseteq F \Rightarrow F_p(\alpha) \subseteq F(\alpha) = F$$

We have $F_p \cong \mathbb{Z}_2 = \{0,1\}$. Since $o(\alpha) = \infty$, we have $\alpha \neq 1$ and so $0 \neq \alpha - 1 \overset{\text{char}(F)=2}{=\!=} \alpha + 1 \in F^* = \langle\alpha\rangle$. Hence $1 + \alpha = \alpha^r$ for some $r \in \mathbb{Z} \setminus \{0\}$. Let

$$F_p[x] \ni f(x) = \begin{cases} x^r - x - 1, & \text{if } r > 0, \\ x^{-r} + x^{-r+1} - 1, & \text{if } r < 0. \end{cases}$$

Then α is a root of $f(x)$ and so α is algebraic over F_p. Hence

$[F_p(\alpha) : F_p]$ = degree of minimal polynomial of α over $F_p = d \geq 1$.

Hence $|F| = |F_p(\alpha)| = |F_p|^d = p^d$, contradicting $|F| \geq |F^*| = \infty$.

It follows that $|F^*| < \infty$ and so $|F| = |F^*| + 1 < \infty$. ∎