Corollary V.5.2. If \( p \) is a prime field, then \( \text{char}(F) \neq 0 \).

Proof. As in the proof of Theorem V.5.1, by Corollary III.1.9((II)), \( F \) has prime \( p \) and \( |F| = p \) for some \( n \in \mathbb{N} \).

Theorem V.5.1. Let \( F \) be a field and let \( p \) be the intersection of all subfields of \( F "). Since \( p \) is prime, then \( 0 \neq d = \prod_{i=1}^{m} (x - a_i) \) for some \( m \in \mathbb{N} \).

Remark on page II.10: Since \( F \) is a field, then \( F \) has zero divisors (see the second homomorphism theorem kernel (K) for \( F \)). This is valid for the map \( \phi : \mathbb{Z} \rightarrow \phi(\mathbb{Z}) \) where \( \phi \) is a ring homomorphism, and hence (by Theorem II.8((II))), the map \( \phi : \mathbb{Z} \rightarrow \phi(\mathbb{Z}) \) is an endomorphism of \( \mathbb{Z} \).

Proof. Note that every subfield of \( F \) is finite, since \( p \) is prime. Therefore, \( F \) is a field with no proper subfields. It follows that \( \text{char}(F) \neq 0 \) and \( d = \prod_{i=1}^{m} (x - a_i) \) for some \( a_i \in \mathbb{F} \).
Since 0 = (n) + (n) = (n + n) + (n) = (n + (n + n)) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n + (n + n)) + (n) + (n) = (n +s}
are $\mathbb{F}$-isomorphic.

Exercise V.3.3: $F$ is a splitting field over $K$. By Corollary V.3.9, $F$ and $E$ are $d_F \mathbb{Z}$ fields of $x^r \in \mathbb{K}$, and hence $d = |d_F \mathbb{Z}| = |E| = \frac{n!}{|d_F \mathbb{Z}|}$. Hence, $|d_F \mathbb{Z}|$ is the number of vectors in $F$ that is, $|F : K|$, then $|F : K|$ is finite if and only if $F$ is a splitting field of $x^r \in \mathbb{K}$.

Proposition V.3.5: $F$ is a splitting field of $x^r \in \mathbb{K}$ over $\mathbb{K}$. Then, $|d_F \mathbb{Z}|$ is a splitting field of $x^r \in \mathbb{K}$, and hence $F$ is finite if and only if $F$ is a splitting field of $x^r \in \mathbb{K}$.

Corollary V.5.8: Every $\mathbb{F}$-isomorphic field $\mathbb{K}$ contains a splitting field of $x^r \in \mathbb{K}$.

Corollary V.5.6: Every $\mathbb{F}$-isomorphic field $\mathbb{K}$ contains a splitting field of $x^r \in \mathbb{K}$.

Proof (continued): Let $\mathbb{K}$ be a splitting field of $x^r \in \mathbb{K}$. Then, $|d_F \mathbb{Z}|$ is a splitting field of $x^r \in \mathbb{K}$, and hence $F$ is finite if and only if $F$ is a splitting field of $x^r \in \mathbb{K}$.
Proposition 5.10 (continued)

If $F$ is a finite dimensional extension field of a finite cyclic field $K$, then $F$ is finite and is Galois over $K$. The Galois group Aut$_F(K)$ is cyclic.

Proof. Let $\mathbb{Z}^d$ be the prime subfield of $K$ (which is guaranteed to exist by Proposition V.5.10). If $F$ is a finite dimensional extension field of a finite cyclic field $K$.