Modern Algebra

Chapter V. Fields and Galois Theory

V.5. Finite Fields—Proofs of Theorems

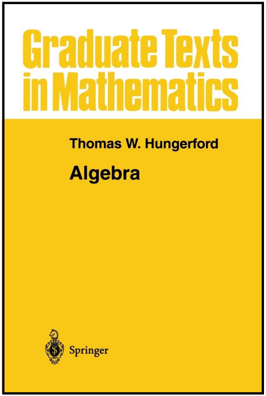

Table of contents

Theorem V.5.1

Theorem V.5.1. Let F be a field and let P be the intersection of all subfields of F. Then P is a field with no proper subfields. If $\text{char}(F) = p$ (where p is prime), then $P \cong \mathbb{Z}_p$. If $\text{char}(F) = 0$ then $P \cong \mathbb{Q}$.

Proof. Note that every subfield of F must contain 0 and 1_F. Since P is the intersection of all subfields of F then P has no proper subfields. Clearly P contains all elements of the form $m1_F = 1_F + 1_F + \cdots + 1_F$ (m times) for $m \in \mathbb{N}$; replace 1_F with -1_F if $m \in \mathbb{Z}$ with $m < 0$).

Theorem V.5.1

Theorem V.5.1. Let F be a field and let P be the intersection of all subfields of F. Then P is a field with no proper subfields. If $\text{char}(F) = p$ (where p is prime), then $P \cong \mathbb{Z}_p$. If $\text{char}(F) = 0$ then $P \cong \mathbb{Q}$.

Proof. Note that every subfield of F must contain 0 and 1_F. Since P is the intersection of all subfields of F then P has no proper subfields. Clearly P contains all elements of the form $m1_F = 1_F + 1_F + \cdots + 1_F$ (m times) for $m \in \mathbb{N}$; replace 1_F with -1_F if $m \in \mathbb{Z}$ with $m < 0$). By Theorem III.1.9(i), the map $\varphi : \mathbb{Z} \to P$ given by $m \mapsto m1_F$ is a ring homomorphisms with kernel (n) where $n = \text{char}(F)$ (this is valid for $n \geq 0$). Since P is a field then it has no zero divisors (see the second Remark on page 116) then by Theorem III.1.9(iii), if $n \neq 0$ then n is prime.

Theorem V.5.1

Theorem V.5.1. Let F be a field and let P be the intersection of all subfields of F. Then P is a field with no proper subfields. If $\mathrm{char}(F) = p$ (where p is prime), then $P \cong \mathbb{Z}_p$. If $\mathrm{char}(F) = 0$ then $P \cong \mathbb{Q}$.

Proof. Note that every subfield of F must contain 0 and 1_F. Since P is the intersection of all subfields of F then P has no proper subfields. Clearly P contains all elements of the form $m1_F = 1_F + 1_F + \cdots + 1_F$ (m times) for $m \in \mathbb{N}$; replace 1_F with -1_F if $m \in \mathbb{Z}$ with $m < 0$). By Theorem III.1.9(i), the map $\varphi : \mathbb{Z} \to P$ given by $m \mapsto m1_F$ is a ring homomorphisms with kernel (n) where $n = \mathrm{char}(F)$ (this is valid for $n \geq 0$). Since P is a field then it has no zero divisors (see the second Remark on page 116) then by Theorem III.1.9(iii), if $n \neq 0$ then n is prime.

Theorem V.5.1

Theorem V.5.1. Let F be a field and let P be the intersection of all subfields of F. Then P is a field with no proper subfields. If $\text{char}(F) = p$ (where p is prime), then $P \cong \mathbb{Z}_p$. If $\text{char}(F) = 0$ then $P \cong \mathbb{Q}$.

Proof (continued). If $n = p$ (prime) then $\mathbb{Z}_p \cong \mathbb{Z}/(p) = \mathbb{Z}/\text{Ker}(\varphi)$. By the First Isomorphism Theorem (Corollary III.2.10), we then have that $\mathbb{Z}_p \cong \mathbb{Z}/\text{Ker}(\varphi) \cong \text{Im}(\varphi) \subset P$. Since $\mathbb{Z}_p$ is a field and P has no proper subfields, we must have $\mathbb{Z}_P \cong \text{Im}(\varphi) = P$. If $n = 0$, then $\varphi : \mathbb{Z} \to P$ is one to one (a monomorphism) and by Corollary III.4.6 there is a unique monomorphism of fields $\overline{\varphi} : \mathbb{Q} \to P$ (where $\mathbb{Q}$ is the field of quotients of $\mathbb{Z}$). As above, using the First Isomorphism Theorem, $\mathbb{Q} \cong \text{Im}(\overline{\varphi}) = P$. □

Theorem V.5.1

Theorem V.5.1. Let F be a field and let P be the intersection of all subfields of F. Then P is a field with no proper subfields. If $\text{char}(F) = p$ (where p is prime), then $P \cong \mathbb{Z}_p$. If $\text{char}(F) = 0$ then $P \cong \mathbb{Q}$.

Proof (continued). If $n = p$ (prime) then $\mathbb{Z}_p \cong \mathbb{Z}/(p) = \mathbb{Z}/\text{Ker}(\varphi)$. By the First Isomorphism Theorem (Corollary III.2.10), we then have that $\mathbb{Z}_p \cong \mathbb{Z}/\text{Ker}(\varphi) \cong \text{Im}(\varphi) \subset P$. Since $\mathbb{Z}_p$ is a field and P has no proper subfields, we must have $\mathbb{Z}_P \cong \text{Im}(\varphi) = P$. If $n = 0$, then $\varphi : \mathbb{Z} \to P$ is one to one (a monomorphism) and by Corollary III.4.6 there is a unique monomorphism of fields $\overline{\varphi} : \mathbb{Q} \to P$ (where $\mathbb{Q}$ is the field of quotients of $\mathbb{Z}$). As above, using the First Isomorphism Theorem, $\mathbb{Q} \cong \text{Im}(\overline{\varphi}) = P$. □

Corollary V.5.2

Corollary V.5.2. If F is a finite field, then $\mathrm{char}(F) = p \neq 0$ for some prime p and $|F| = p^n$ for some $n \in \mathbb{N}$.

Proof. As in the proof of Theorem V.5.1, by Theorem III.1.9(iii), F has prime characteristic $p \neq 0$. Since F is a finite dimensional vector space over its prime subfield $\mathbb{Z}_p$ (since F is finite itself), then by Theorem IV.2.4 [which we may have skipped] we have $F \cong \mathbb{Z}_P \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ (n summands) and hence $|F| = p^n$. □

Corollary V.5.2

Corollary V.5.2. If F is a finite field, then $\text{char}(F) = p \neq 0$ for some prime p and $|F| = p^n$ for some $n \in \mathbb{N}$.

Proof. As in the proof of Theorem V.5.1, by Theorem III.1.9(iii), F has prime characteristic $p \neq 0$. Since F is a finite dimensional vector space over its prime subfield $\mathbb{Z}_p$ (since F is finite itself), then by Theorem IV.2.4 [which we may have skipped] we have $F \cong \mathbb{Z}_P \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ (n summands) and hence $|F| = p^n$. □

Theorem V.5.3

Theorem V.5.3. If F is a field and G is a finite subgroup of the multiplicative group of nonzero elements of F, then G is a cyclic group. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.

Proof. If G is a nontrivial finite multiplicative subgroup of field F, then G is abelian and so by the Fundamental Theorem of Finitely Generated Abelian Groups (theorem II.2.1), $G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}$ (in additive notation) where $m_1 > 1$ and $m_1 \mid m_2$, $m_2 \mid m_2$, ..., $m_{k-1} \mid m_k$.

Theorem V.5.3

Theorem V.5.3. If F is a field and G is a finite subgroup of the multiplicative group of nonzero elements of F, then G is a cyclic group. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.

Proof. If G is a nontrivial finite multiplicative subgroup of field F, then G is abelian and so by the Fundamental Theorem of Finitely Generated Abelian Groups (theorem II.2.1), $G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}$ (in additive notation) where $m_1 > 1$ and $m_1 \mid m_2$, $m_2 \mid m_2$, ..., $m_{k-1} \mid m_k$. So $m_k(\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}) = 0$ (that is, $m_k z = 0$ for all $z \in \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}$). Since G is a multiplicative group, then $g^{m_k} = 1_F$ for all $g \in G$. That is, every $u \in G$ is a root of the polynomial $x^{m_k} - 1_F \in F[x]$.

Theorem V.5.3

Theorem V.5.3. If F is a field and G is a finite subgroup of the multiplicative group of nonzero elements of F, then G is a cyclic group. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.

Proof. If G is a nontrivial finite multiplicative subgroup of field F, then G is abelian and so by the Fundamental Theorem of Finitely Generated Abelian Groups (theorem II.2.1), $G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}$ (in additive notation) where $m_1 > 1$ and $m_1 \mid m_2$, $m_2 \mid m_2, \ldots, m_{k-1} \mid m_k$. So $m_k(\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}) = 0$ (that is, $m_k z = 0$ for all $z \in \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}$). Since G is a multiplicative group, then $g^{m_k} = 1_F$ for all $g \in G$. That is, every $u \in G$ is a root of the polynomial $x^{m_k} - 1_F \in F[x]$. By Theorem III.6.7, this polynomial has at most m_k distinct roots in F. So G must contain at most m_k elements. Therefore, $|G| = m_1 m_2 \cdots m_k$ implies $k = 1$ and $G \cong \mathbb{Z}_{m_1}$. □

Theorem V.5.3

Theorem V.5.3. If F is a field and G is a finite subgroup of the multiplicative group of nonzero elements of F, then G is a cyclic group. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.

Proof. If G is a nontrivial finite multiplicative subgroup of field F, then G is abelian and so by the Fundamental Theorem of Finitely Generated Abelian Groups (theorem II.2.1), $G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}$ (in additive notation) where $m_1 > 1$ and $m_1 \mid m_2$, $m_2 \mid m_2$, $\ldots$, $m_{k-1} \mid m_k$. So $m_k(\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}) = 0$ (that is, $m_k z = 0$ for all $z \in \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}$). Since G is a multiplicative group, then $g^{m_k} = 1_F$ for all $g \in G$. That is, every $u \in G$ is a root of the polynomial $x^{m_k} - 1_F \in F[x]$. By Theorem III.6.7, this polynomial has at most m_k distinct roots in F. So G must contain at most m_k elements. Therefore, $|G| = m_1 m_2 \cdots m_k$ implies $k = 1$ and $G \cong \mathbb{Z}_{m_1}$. □

Corollary V.5.4

Corollary V.5.4. If F is a finite field, then F is a simple extension of its prime subfield $\mathbb{Z}_p$; that is, $F = \mathbb{Z}_p(u)$ for some $f \in F$. (Notice Hungerford's comment on page 279 that we do not distinguish between $P \cong \mathbb{Z}_p$ and $P = \mathbb{Z}_p$ in term of the prime subfield.)

Proof. By Theorem V.5.3, the multiplicative group of nonzero elements of F form a (finite) cyclic group. Let u be a generator of this multiplicative group. Since $\mathbb{Z}_p \subset F$ and $u \in F$, then $\mathbb{Z}_p(u) \subset F$.

Corollary V.5.4

Corollary V.5.4. If F is a finite field, then F is a simple extension of its prime subfield $\mathbb{Z}_p$; that is, $F = \mathbb{Z}_p(u)$ for some $f \in F$. (Notice Hungerford's comment on page 279 that we do not distinguish between $P \cong \mathbb{Z}_p$ and $P = \mathbb{Z}_p$ in term of the prime subfield.)

Proof. By Theorem V.5.3, the multiplicative group of nonzero elements of F form a (finite) cyclic group. Let u be a generator of this multiplicative group. Since $\mathbb{Z}_p \subset F$ and $u \in F$, then $\mathbb{Z}_p(u) \subset F$. Also, $0_F \in \mathbb{Z}_p$ and the powers of u generate all nonzero elements of F, so $\mathbb{Z}_p(u) = F$. □

Corollary V.5.4

Corollary V.5.4. If F is a finite field, then F is a simple extension of its prime subfield $\mathbb{Z}_p$; that is, $F = \mathbb{Z}_p(u)$ for some $f \in F$. (Notice Hungerford's comment on page 279 that we do not distinguish between $P \cong \mathbb{Z}_p$ and $P = \mathbb{Z}_p$ in term of the prime subfield.)

Proof. By Theorem V.5.3, the multiplicative group of nonzero elements of F form a (finite) cyclic group. Let u be a generator of this multiplicative group. Since $\mathbb{Z}_p \subset F$ and $u \in F$, then $\mathbb{Z}_p(u) \subset F$. Also, $0_F \in \mathbb{Z}_p$ and the powers of u generate all nonzero elements of F, so $\mathbb{Z}_p(u) = F$. □

Lemma V.5.5

Lemma V.5.5. If F is a field of characteristic p and if $r \geq 1$ is an integer, then the map $\varphi : F \to F$ given by $u \mapsto u^{p^r}$ is a $\mathbb{Z}_p$-monomorphism of fields. If F is finite, then φ is a $\mathbb{Z}_p$-automorphism of F.

Proof. First, we show that φ is a field homomorphism. Let $u, v \in F$. Then

$$\begin{aligned} \varphi(uv) &= (uv)^{p^r} = u^{p^r} v^{p^r} \text{ since } F \text{ is a field} \\ &= \varphi(u)\varphi(v). \end{aligned}$$

By Exercise III.1.11 (The Freshman's Dream), $(u \pm v)^{p^r} = u^{p^r} \pm v^{p^r}$ and so $\varphi(u + v) = (u + v)^{p^r} = u^{p^r} + v^{p^r} = \varphi(u) + \varphi(v)$. So φ is a field homomorphism.

Now $\varphi(1_F) = a_F^{p^r} = 1_F$, so each element of $\mathbb{Z}_p$, being of the form $1_F + 1_F + \cdots + 1_F$, is fixed by φ, as claimed.

Lemma V.5.5

Lemma V.5.5. If F is a field of characteristic p and if $r \geq 1$ is an integer, then the map $\varphi : F \to F$ given by $u \mapsto u^{p^r}$ is a $\mathbb{Z}_p$-monomorphism of fields. If F is finite, then φ is a $\mathbb{Z}_p$-automorphism of F.

Proof. First, we show that φ is a field homomorphism. Let $u, v \in F$. Then

$$\begin{aligned} \varphi(uv) &= (uv)^{p^r} = u^{p^r} v^{p^r} \text{ since } F \text{ is a field} \\ &= \varphi(u)\varphi(v). \end{aligned}$$

By Exercise III.1.11 (The Freshman's Dream), $(u \pm v)^{p^r} = u^{p^r} \pm v^{p^r}$ and so $\varphi(u+v) = (u+v)^{p^r} = u^{p^r} + v^{p^r} = \varphi(u) + \varphi(v)$. So φ is a field homomorphism.

Now $\varphi(1_F) = a_F^{p^r} = 1_F$, so each element of $\mathbb{Z}_p$, being of the form $1_F + 1_F + \cdots + 1_F$, is fixed by φ, as claimed.

Lemma V.5.5 (continued)

Lemma V.5.5. If F is a field of characteristic p and if $r \geq 1$ is an integer, then the map $\varphi : F \to F$ given by $u \mapsto u^{p^r}$ is a $\mathbb{Z}_p$-monomorphism of fields. If F is finite, then φ is a $\mathbb{Z}_p$-automorphism of F.

Proof (continued). We only need to show that φ is one to one. If $\varphi(u) = \varphi(v)$ then $u^{p^r} = v^{p^r}$ or $u^{p^r} - v^{p^r} = 0$ or $(u - v)^{p^r} = 0$ by "The Freshman's Dream." Since F is a field then it has no zero divisors and hence $u - v = 0$ or $u = v$. Therefore, φ is one to one and $\varphi : F \to F$ is a $\mathbb{Z}_p$-monomorphism.

Since $\varphi : F \to F$ is one to one, if F is finite then φ must also be onto and φ is a $\mathbb{Z}_p$-automorphism of F. □

Lemma V.5.5 (continued)

Lemma V.5.5. If F is a field of characteristic p and if $r \geq 1$ is an integer, then the map $\varphi : F \to F$ given by $u \mapsto u^{p^r}$ is a $\mathbb{Z}_p$-monomorphism of fields. If F is finite, then φ is a $\mathbb{Z}_p$-automorphism of F.

Proof (continued). We only need to show that φ is one to one. If $\varphi(u) = \varphi(v)$ then $u^{p^r} = v^{p^r}$ or $u^{p^r} - v^{p^r} = 0$ or $(u - v)^{p^r} = 0$ by "The Freshman's Dream." Since F is a field then it has no zero divisors and hence $u - v = 0$ or $u = v$. Therefore, φ is one to one and $\varphi : F \to F$ is a $\mathbb{Z}_p$-monomorphism.

Since $\varphi : F \to F$ is one to one, if F is finite then φ must also be onto and φ is a $\mathbb{Z}_p$-automorphism of F. □

Proposition V.5.6

Proposition V.5.6. Let p be a prime and $n \geq 1$ an integer. Then F is a finite field with p^n elements if and only if F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

Proof. (1) If $|F| = p^n$, then the multiplicative group of nonzero elements of F has order $p^n - 1$. Hence every nonzero $u \in F$ satisfies $u^{p^n} - 1 = 1_F$ (see also the proof of Corollary V.5.3 for details). Thus every nonzero $u \in F$ is a root of $x(x^{p^n-1} - 1_F) = x^{p^n} - x \in \mathbb{Z}_p[x]$ as well.

Proposition V.5.6

Proposition V.5.6. Let p be a prime and $n \geq 1$ an integer. Then F is a finite field with p^n elements if and only if F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

Proof. (1) If $|F| = p^n$, then the multiplicative group of nonzero elements of F has order $p^n - 1$. Hence every nonzero $u \in F$ satisfies $u^{p^n} - 1 = 1_F$ (see also the proof of Corollary V.5.3 for details). Thus every nonzero $u \in F$ is a root of $x(x^{p^n-1} - 1_F) = x^{p^n} - x \in \mathbb{Z}_p[x]$ as well. Since $0 \in F$ is also a root of $x^{p^n} - x$, then $s^{p^n} - x$ has p^n distinct roots in F (namely, 0 and the $p^n - 1$ nonzero elements of F as shown above).

Proposition V.5.6

Proposition V.5.6. Let p be a prime and $n \geq 1$ an integer. Then F is a finite field with p^n elements if and only if F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

Proof. (1) If $|F| = p^n$, then the multiplicative group of nonzero elements of F has order $p^n - 1$. Hence every nonzero $u \in F$ satisfies $u^{p^n} - 1 = 1_F$ (see also the proof of Corollary V.5.3 for details). Thus every nonzero $u \in F$ is a root of $x(x^{p^n - 1} - 1_F) = x^{p^n} - x \in \mathbb{Z}_p[x]$ as well. Since $0 \in F$ is also a root of $x^{p^n} - x$, then $s^{p^n} - x$ has p^n distinct roots in F (namely, 0 and the $p^n - 1$ nonzero elements of F as shown above). Now $x^{p^n} - x$ has exactly p^n roots by Theorem III.6.7 and by the Factor Theorem (Theorem III.6.6) it splits over F. Since the roots of $x^{p^n} - x$ are precisely the elements of F, then F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

Proposition V.5.6

Proposition V.5.6. Let p be a prime and $n \geq 1$ an integer. Then F is a finite field with p^n elements if and only if F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

Proof. (1) If $|F| = p^n$, then the multiplicative group of nonzero elements of F has order $p^n - 1$. Hence every nonzero $u \in F$ satisfies $u^{p^n} - 1 = 1_F$ (see also the proof of Corollary V.5.3 for details). Thus every nonzero $u \in F$ is a root of $x(x^{p^n - 1} - 1_F) = x^{p^n} - x \in \mathbb{Z}_p[x]$ as well. Since $0 \in F$ is also a root of $x^{p^n} - x$, then $s^{p^n} - x$ has p^n distinct roots in F (namely, 0 and the $p^n - 1$ nonzero elements of F as shown above). Now $x^{p^n} - x$ has exactly p^n roots by Theorem III.6.7 and by the Factor Theorem (Theorem III.6.6) it splits over F. Since the roots of $x^{p^n} - x$ are precisely the elements of F, then F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

Proposition V.5.6 (continued)

Proof (continued). (2) Now suppose F is a splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. Then since $\text{char}(F) = \text{char}(\mathbb{Z}_p) = p$, we have that the derivative $f'(x) = p^n x^{p^n - 1} - 1 = -1$ and so f and f' are relatively prime in $F[x]$. By Theorem III.6.10(ii), f has no multiple roots in F and so f has p^n distinct roots in F. Let $\varphi : F \to F$ be the monomorphism of Lemma V.5.5 with $r = n$, where $\varphi(u) = u^{p^n}$. Then $u \in F$ is a root of $f(x) = x^{p^n} - x$ if and only if $\varphi(u) = u$.

Proposition V.5.6 (continued)

Proof (continued). (2) Now suppose F is a splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. Then since $\text{char}(F) = \text{char}(\mathbb{Z}_p) = p$, we have that the derivative $f'(x) = p^n x^{p^n - 1} - 1 = -1$ and so f and f' are relatively prime in $F[x]$. By Theorem III.6.10(ii), f has no multiple roots in F and so f has p^n distinct roots in F. Let $\varphi : F \to F$ be the monomorphism of Lemma V.5.5 with $r = n$, where $\varphi(u) = u^{p^n}$. Then $u \in F$ is a root of $f(x) = x^{p^n} - x$ if and only if $\varphi(u) = u$. Now since φ is a homomorphism, then $u, v \in E$ we have $\varphi(uv) = \varphi(u)\varphi(v) = uv$ and $\varphi(u + v) = \varphi(u) + \varphi)v) = u + v$, so E is closed under $+$ and $\cdot$ (and $0, 1_F \in E$), so E is a subfield of F and E is of order p^n. So $E \subset F$.

Proposition V.5.6 (continued)

Proof (continued). (2) Now suppose F is a splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. Then since $\text{char}(F) = \text{char}(\mathbb{Z}_p) = p$, we have that the derivative $f'(x) = p^n x^{p^n-1} - 1 = -1$ and so f and f' are relatively prime in $F[x]$. By Theorem III.6.10(ii), f has no multiple roots in F and so f has p^n distinct roots in F. Let $\varphi : F \to F$ be the monomorphism of Lemma V.5.5 with $r = n$, where $\varphi(u) = u^{p^n}$. Then $u \in F$ is a root of $f(x) = x^{p^n} - x$ if and only if $\varphi(u) = u$. Now since φ is a homomorphism, then $u, v \in E$ we have $\varphi(uv) = \varphi(u)\varphi(v) = uv$ and $\varphi(u + v) = \varphi(u) + \varphi)v) = u + v$, so E is closed under $+$ and $\cdot$ (and $0, 1_F \in E$), so E is a subfield of F and E is of order p^n. So $E \subset F$. Also, φ fixes $\mathbb{Z}_p$ elementwise and so $\mathbb{Z}_p \subset E \subset F$. Now F is a splitting field of $f(x) = x^{p^n} - x$ and so $F = \mathbb{Z}_p(E) \subset E$ (since E contains $\mathbb{Z}_p$). That is, $F = E$ and F is a finite field or order p^n. □

Proposition V.5.6 (continued)

Proof (continued). (2) Now suppose F is a splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. Then since $\text{char}(F) = \text{char}(\mathbb{Z}_p) = p$, we have that the derivative $f'(x) = p^n x^{p^n - 1} - 1 = -1$ and so f and f' are relatively prime in $F[x]$. By Theorem III.6.10(ii), f has no multiple roots in F and so f has p^n distinct roots in F. Let $\varphi : F \to F$ be the monomorphism of Lemma V.5.5 with $r = n$, where $\varphi(u) = u^{p^n}$. Then $u \in F$ is a root of $f(x) = x^{p^n} - x$ if and only if $\varphi(u) = u$. Now since φ is a homomorphism, then $u, v \in E$ we have $\varphi(uv) = \varphi(u)\varphi(v) = uv$ and $\varphi(u + v) = \varphi(u) + \varphi)v) = u + v$, so E is closed under $+$ and $\cdot$ (and $0, 1_F \in E$), so E is a subfield of F and E is of order p^n. So $E \subset F$. Also, φ fixes $\mathbb{Z}_p$ elementwise and so $\mathbb{Z}_p \subset E \subset F$. Now F is a splitting field of $f(x) = x^{p^n} - x$ and so $F = \mathbb{Z}_p(E) \subset E$ (since E contains $\mathbb{Z}_p$). That is, $F = E$ and F is a finite field or order p^n. □

Corollary V.5.8

Corollary V.5.8. If K is a finite field and $n \in \mathbb{N}$, then there exists a simple extension field $F = K(U)$ of K such that F is finite and $[F : K] = n$. Any two n-dimensional extension fields of K are K-isomorphic.

Proof. Given K of order p^r (this must be the order of K by Corollary V.5.2), let F be a splitting field of $f(x) = x^{p^{rn}} - x$ over K. By Proposition V.5.6, every $u \in K$ satisfies $u^{p^r} = u$ and it follows inductively (by repeatedly raising both sides to the p^r power) that $u^{p^{r^n}} = u$ for all $u \in K$.

Corollary V.5.8

Corollary V.5.8. If K is a finite field and $n \in \mathbb{N}$, then there exists a simple extension field $F = K(U)$ of K such that F is finite and $[F : K] = n$. Any two n-dimensional extension fields of K are K-isomorphic.

Proof. Given K of order p^r (this must be the order of K by Corollary V.5.2), let F be a splitting field of $f(x) = x^{p^{rn}} - x$ over K. By Proposition V.5.6, every $u \in K$ satisfies $u^{p^r} = u$ and it follows inductively (by repeatedly raising both sides to the p^r power) that $u^{{p^r}^n} = u$ for all $u \in K$. Now we have $\mathbb{Z}_p \subset K \subset F$ where F is a splitting field of f over K, so by Exercise V.3.3 F is a splitting field of f over $\mathbb{Z}_p$. The proof of Proposition V.5.6 shows that F consists of precisely the p^{nr} distinct roots of f (namely, the set E in the proof).

Corollary V.5.8

Corollary V.5.8. If K is a finite field and $n \in \mathbb{N}$, then there exists a simple extension field $F = K(U)$ of K such that F is finite and $[F : K] = n$. Any two n-dimensional extension fields of K are K-isomorphic.

Proof. Given K of order p^r (this must be the order of K by Corollary V.5.2), let F be a splitting field of $f(x) = x^{p^{rn}} - x$ over K. By Proposition V.5.6, every $u \in K$ satisfies $u^{p^r} = u$ and it follows inductively (by repeatedly raising both sides to the p^r power) that $u^{{p^r}^n} = u$ for all $u \in K$. Now we have $\mathbb{Z}_p \subset K \subset F$ where F is a splitting field of f over K, so by Exercise V.3.3 F is a splitting field of f over $\mathbb{Z}_p$. The proof of Proposition V.5.6 shows that F consists of precisely the p^{nr} distinct roots of f (namely, the set E in the proof). Now with the dimension of F over K as $[F : K]$, then since $|K|$ is finite then the number of vectors in F (treated as a vector space over K) is $|K|^{[F:K]}$; that is, $p^{nr} = |F| = |K|^{[F:K]} = (p^r)^{[F:K]}$. Whence $[F : K] = n$. Corollary V.5.4 implies that F is a simple extension of its prime subfield and hence of K.

Corollary V.5.8

Corollary V.5.8. If K is a finite field and $n \in \mathbb{N}$, then there exists a simple extension field $F = K(U)$ of K such that F is finite and $[F : K] = n$. Any two n-dimensional extension fields of K are K-isomorphic.

Proof. Given K of order p^r (this must be the order of K by Corollary V.5.2), let F be a splitting field of $f(x) = x^{p^{rn}} - x$ over K. By Proposition V.5.6, every $u \in K$ satisfies $u^{p^r} = u$ and it follows inductively (by repeatedly raising both sides to the p^r power) that $u^{p^{r^n}} = u$ for all $u \in K$. Now we have $\mathbb{Z}_p \subset K \subset F$ where F is a splitting field of f over K, so by Exercise V.3.3 F is a splitting field of f over $\mathbb{Z}_p$. The proof of Proposition V.5.6 shows that F consists of precisely the p^{nr} distinct roots of f (namely, the set E in the proof). Now with the dimension of F over K as $[F : K]$, then since $|K|$ is finite then the number of vectors in F (treated as a vector space over K) is $|K|^{[F:K]}$; that is,
$p^{nr} = |F| = |K|^{[F:K]} = (p^r)^{[F:K]}$. Whence $[F : K] = n$. Corollary V.5.4 implies that F is a simple extension of its prime subfield and hence of K.

Corollary V.5.8 (continued)

Corollary V.5.8. If K is a finite field and $n \in \mathbb{N}$, then there exists a simple extension field $F = K(U)$ of K such that F is finite and $[F : K] = n$. Any two n-dimensional extension fields of K are K-isomorphic.

Proof (continued). If F_1 is another extension field of K with $[F_1 : K] = n$, then

$$\begin{aligned} [F_1 : \mathbb{Z}_p] &= [F_1 : K][K : \mathbb{Z}_p] \text{ by Theorem V.1.2} \\ &= n[K : \mathbb{Z}_p] = nr \end{aligned}$$

since $[K : \mathbb{Z}_p] = r$ because $|K| = p^r$ (as argued above for F as a vector space over finite K). Whence, as above, $F_1| = |\mathbb{Z}_p|^{[F_1:\mathbb{Z}_p]} = p^{nr}$. By Proposition V.5.6, F_1 is a splitting field of $x^{p^{nr}} = x$ over $\mathbb{Z}_p$ and hence (by Exercise V.3.3) is a splitting field over K. By Corollary V.3.9, F and F_1 are K-isomorphic. □

Corollary V.5.8 (continued)

Corollary V.5.8. If K is a finite field and $n \in \mathbb{N}$, then there exists a simple extension field $F = K(U)$ of K such that F is finite and $[F : K] = n$. Any two n-dimensional extension fields of K are K-isomorphic.

Proof (continued). If F_1 is another extension field of K with $[F_1 : K] = n$, then

$$\begin{aligned} [F_1 : \mathbb{Z}_p] &= [F_1 : K][K : \mathbb{Z}_p] \text{ by Theorem V.1.2} \\ &= n[K : \mathbb{Z}_p] = nr \end{aligned}$$

since $[K : \mathbb{Z}_p] = r$ because $|K| = p^r$ (as argued above for F as a vector space over finite K). Whence, as above, $F_1| = |\mathbb{Z}_p|^{[F_1:\mathbb{Z}_p]} = p^{nr}$. By Proposition V.5.6, F_1 is a splitting field of $x^{p^{nr}} = x$ over $\mathbb{Z}_p$ and hence (by Exercise V.3.3) is a splitting field over K. By Corollary V.3.9, F and F_1 are K-isomorphic. □

Proposition V.5.10

Proposition V.5.10. If F is a finite dimensional extension field of a finite field K, then F is finite and is Galois over K. The Galois group $\mathrm{Aut}_K(F)$ is cyclic.

Proof. Let $\mathbb{Z}_p$ be the prime subfield of K (which is guaranteed to exist by Theorem V.5.1 and Corollary V.5.2). Then F is finite dimensional over $\mathbb{Z}_p$ since, by Theorem V.1.2, $[F : \mathbb{Z}_p] = [F : K][K : \mathbb{Z}_p]$.

Proposition V.5.10

Proposition V.5.10. If F is a finite dimensional extension field of a finite field K, then F is finite and is Galois over K. The Galois group $\mathrm{Aut}_K(F)$ is cyclic.

Proof. Let $\mathbb{Z}_p$ be the prime subfield of K (which is guaranteed to exist by Theorem V.5.1 and Corollary V.5.2). Then F is finite dimensional over $\mathbb{Z}_p$ since, by Theorem V.1.2, $[F : \mathbb{Z}_p] = [F : K][K : \mathbb{Z}_p]$. Let $[F : \mathbb{Z}_p] = n$ and then (treating F as an n-dimensional vector space over finite field $\mathbb{Z}_p$, as discussed in the proof of Corollary V.5.8) $|F| = p^n$. By the proof of Proposition V.5.6, F is a splitting field over $\mathbb{Z}_p$ of $f(x) = x^{p^n} - x$ (the set E in the proof) and hence be Exercise V.3.2 is a splitting field of f over K. Also, all roots of f are distinct (see the proof of Proposition V.5.6).

Proposition V.5.10

Proposition V.5.10. If F is a finite dimensional extension field of a finite field K, then F is finite and is Galois over K. The Galois group $\mathrm{Aut}_K(F)$ is cyclic.

Proof. Let $\mathbb{Z}_p$ be the prime subfield of K (which is guaranteed to exist by Theorem V.5.1 and Corollary V.5.2). Then F is finite dimensional over $\mathbb{Z}_p$ since, by Theorem V.1.2, $[F : \mathbb{Z}_p] = [F : K][K : \mathbb{Z}_p]$. Let $[F : \mathbb{Z}_p] = n$ and then (treating F as an n-dimensional vector space over finite field $\mathbb{Z}_p$, as discussed in the proof of Corollary V.5.8) $|F| = p^n$. By the proof of Proposition V.5.6, F is a splitting field over $\mathbb{Z}_p$ of $f(x) = x^{p^n} - x$ (the set E in the proof) and hence be Exercise V.3.2 is a splitting field of f over K. Also, all roots of f are distinct (see the proof of Proposition V.5.6). By Theorem (the (iii)⇒(i) part) F is Galois over K. The map $\varphi : F \to F$ given by $u \mapsto u^p$ is a $\mathbb{Z}_p$-automorphism by Lemma V.5.5 (with $r = 1$). Since φ^n maps $u \mapsto n^{p^n} = u$ then φ^n is the identity on F.

Proposition V.5.10

Proposition V.5.10. If F is a finite dimensional extension field of a finite field K, then F is finite and is Galois over K. The Galois group $\mathrm{Aut}_K(F)$ is cyclic.

Proof. Let $\mathbb{Z}_p$ be the prime subfield of K (which is guaranteed to exist by Theorem V.5.1 and Corollary V.5.2). Then F is finite dimensional over $\mathbb{Z}_p$ since, by Theorem V.1.2, $[F : \mathbb{Z}_p] = [F : K][K : \mathbb{Z}_p]$. Let $[F : \mathbb{Z}_p] = n$ and then (treating F as an n-dimensional vector space over finite field $\mathbb{Z}_p$, as discussed in the proof of Corollary V.5.8) $|F| = p^n$. By the proof of Proposition V.5.6, F is a splitting field over $\mathbb{Z}_p$ of $f(x) = x^{p^n} - x$ (the set E in the proof) and hence be Exercise V.3.2 is a splitting field of f over K. Also, all roots of f are distinct (see the proof of Proposition V.5.6). By Theorem (the (iii)⇒(i) part) F is Galois over K. The map $\varphi : F \to F$ given by $u \mapsto u^p$ is a $\mathbb{Z}_p$-automorphism by Lemma V.5.5 (with $r = 1$). Since φ^n maps $u \mapsto n^{p^n} = u$ then φ^n is the identity on F.

Proposition V.5.10 (continued)

Proposition V.5.10. If F is a finite dimensional extension field of a finite field K, then F is finite and is Galois over K. The Galois group $\text{Aut}_K(F)$ is cyclic.

Proof (continued). No lower power k of φ can be the identity, or else the polynomial $x^{p^k} - x$ would have p^n distinct roots in F where $p^k < p^n$, contradicting Theorem III.6.7. By the Fundamental Theorem of Galois Theory (Theorem V.2.5(i)) $|\text{Aut}_{\mathbb{Z}_p} F| = [F : \mathbb{Z}_p] = n$, and since $\varphi \in \text{Aut}_{\mathbb{Z}_p} F$ is an element of order n then φ must generate $\text{Aut}_{\mathbb{Z}_p} F$ and $\text{Aut}_{\mathbb{Z}_p} F$ is cyclic. Since $\mathbb{Z}_p \subset K$ then $\text{Aut}_K F$ is a subgroup of $\text{Aut}_{\mathbb{Z}_p} F$ and so $\text{Aut}_K F$ is cyclic by Theorem I.3.5. □

Proposition V.5.10 (continued)

Proposition V.5.10. If F is a finite dimensional extension field of a finite field K, then F is finite and is Galois over K. The Galois group $\text{Aut}_K(F)$ is cyclic.

Proof (continued). No lower power k of φ can be the identity, or else the polynomial $x^{p^k} - x$ would have p^n distinct roots in F where $p^k < p^n$, contradicting Theorem III.6.7. By the Fundamental Theorem of Galois Theory (Theorem V.2.5(i)) $|\text{Aut}_{\mathbb{Z}_p} F| = [F : \mathbb{Z}_p] = n$, and since $\varphi \in \text{Aut}_{\mathbb{Z}_p} F$ is an element of order n then φ must generate $\text{Aut}_{\mathbb{Z}_p} F$ and $\text{Aut}_{\mathbb{Z}_p} F$ is cyclic. Since $\mathbb{Z}_p \subset K$ then $\text{Aut}_K F$ is a subgroup of $\text{Aut}_{\mathbb{Z}_p} F$ and so $\text{Aut}_K F$ is cyclic by Theorem I.3.5. □