Lecture 13: Conjugate Elements and the Isomorphism Extension Theorem

MAT205 Abstract Algebra II

Ma, Jia-Jun

Xiamen University Malaysia

Motivation: Lifting Isomorphisms Along Algebraic Extensions

The universal property of the algebraic closure gave: every algebraic extension E/F admits an F-embedding $E \hookrightarrow \overline{F}$ — a field embedding σ with $\sigma|_F = \mathrm{id}_F$.

Question. What if F itself carries an automorphism, or more generally an isomorphism $\sigma : F \to F'$? Can σ be lifted to an embedding $E \to \overline{F'}$?

Answer (today). Yes — the isomorphism extension theorem. Two consequences:

- the full uniqueness of algebraic closures (the universal property handled only $\sigma = \mathrm{id}_F$);
- a way to count F-automorphisms by counting conjugate roots — the starting point of Galois theory.

Recall: Minimal Polynomial

For α algebraic over F, the set $I_\alpha = \{\, f \in F[x] : f(\alpha) = 0 \,\}$ is a nonzero ideal of the PID $F[x]$, generated by a unique monic polynomial — the *minimal polynomial* $m_\alpha \in F[x]$.

It is the monic polynomial of least degree vanishing at α, and is irreducible (else $F(\alpha) \cong F[x]/(m_\alpha)$ would have zero divisors).

Minimal-polynomial theorem (used throughout). With $n = \deg m_\alpha$,

$$F(\alpha) \cong F[x]/(m_\alpha), \qquad F\text{-basis } 1, \alpha, \ldots, \alpha^{n-1}, \qquad [F(\alpha) : F] = n.$$

Definition: Conjugate Elements

Let E/F be a field extension and $\alpha, \beta \in E$ both algebraic over F.

Definition. α and β are *conjugate over* F if their minimal polynomials agree:

$$m_\alpha = m_\beta \quad \text{in } F[x].$$

Equivalently, α and β are roots of the same monic irreducible $p \in F[x]$ (necessarily $p = m_\alpha = m_\beta$).

Examples: Conjugate Elements

- $\sqrt{2}$ and $-\sqrt{2}$ over $\mathbb{Q}$ — roots of $x^2 - 2$.
- i and $-i$ over $\mathbb{R}$ — roots of $x^2 + 1$.
- $\sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2}$ over $\mathbb{Q}$, with $\omega = e^{2\pi i/3}$ — roots of $x^3 - 2$.
- $a + bi$ and $a - bi$ over $\mathbb{R}$ for $b \neq 0$ — classical complex conjugates, roots of $x^2 - 2ax + (a^2 + b^2)$.

Non-example. $\sqrt{2}$ and $\sqrt{3}$ are not conjugate over $\mathbb{Q}$: their minimal polynomials $x^2 - 2$ and $x^2 - 3$ differ.

Lemma: Minimal Polynomial Under Base Change

Setup. $F \subseteq M$ a tower of fields; α algebraic over F (in some extension of M).

Lemma. α is algebraic over M, and

$$[M(\alpha) : M] \;\leq\; [F(\alpha) : F].$$

Equality holds iff $m_{\alpha,F}$ remains irreducible as an element of $M[x]$.

Proof: Minimal Polynomial Under Base Change

$m_{\alpha,F} \in F[x] \subseteq M[x]$ vanishes at α, so α is algebraic over M, with a minimal polynomial $m_{\alpha,M} \in M[x]$.

$m_{\alpha,M}$ generates the ideal $\{\, g \in M[x] : g(\alpha) = 0 \,\}$ of the PID $M[x]$. Since $m_{\alpha,F}$ lies in it, $m_{\alpha,M} \mid m_{\alpha,F}$, hence $\deg m_{\alpha,M} \leq \deg m_{\alpha,F}$.

By the minimal-polynomial theorem, $[F(\alpha) : F] = \deg m_{\alpha,F}$ and $[M(\alpha) : M] = \deg m_{\alpha,M}$. Combining gives $[M(\alpha) : M] \leq [F(\alpha) : F]$. $\square$

Examples: Base Change

Equality. $F = \mathbb{Q}$, $M = \mathbb{Q}(i)$, $\alpha = \sqrt{2}$. Here $x^2 - 2$ stays irreducible over $\mathbb{Q}(i)$ (as $\sqrt{2} \notin \mathbb{Q}(i)$), so

$$[M(\alpha) : M] = 2 = [F(\alpha) : F].$$

Strict. $F = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt{2})$, $\alpha = \sqrt{2}$. Now $\alpha \in M$, so $m_{\alpha,M} = x - \sqrt{2}$ and

$$[M(\alpha) : M] = 1 < 2 = [F(\alpha) : F].$$

Theorem: Conjugation Isomorphism

Conventions. An F-*homomorphism* $\varphi : E_1 \to E_2$ is a ring homomorphism with $\varphi|_F = \mathrm{id}_F$; an F-*isomorphism* is bijective, an F-*embedding* injective.

Theorem. Let α, β be conjugate over F. There is a unique F-isomorphism

$$\psi_{\alpha,\beta} : F(\alpha) \to F(\beta), \qquad \psi_{\alpha,\beta}(\alpha) = \beta.$$

Explicit formula. With $n = \deg m_\alpha$,

$$\psi_{\alpha,\beta}\big(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}\big) = c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1}.$$

Proof: Conjugation Isomorphism (existence)

The minimal-polynomial theorem gives canonical F-isomorphisms, by evaluation:

$$\varphi_\alpha : F[x]/(m_\alpha) \xrightarrow{\sim} F(\alpha), \qquad \varphi_\beta : F[x]/(m_\beta) \xrightarrow{\sim} F(\beta).$$

Conjugacy means $m_\alpha = m_\beta$ in $F[x]$, so the source rings are equal:
$F[x]/(m_\alpha) = F[x]/(m_\beta)$.

Set $\psi_{\alpha,\beta} := \varphi_\beta \circ \varphi_\alpha^{-1}$. A composite of F-isomorphisms is an F-isomorphism.

Proof: Conjugation Isomorphism (tracking, uniqueness)

Tracking α. $\varphi_\alpha^{-1}(\alpha) = x + (m_\alpha)$ and $\varphi_\beta(x + (m_\beta)) = \beta$, so $\psi_{\alpha,\beta}(\alpha) = \beta$.

General element. φ_α^{-1} sends $\xi = c_0 + \cdots + c_{n-1}\alpha^{n-1}$ to $h(x) + (m_\alpha)$ with $h = c_0 + \cdots + c_{n-1}x^{n-1}$; then φ_β sends it to $h(\beta)$ — the explicit formula.

Uniqueness. Any F-homomorphism $\psi : F(\alpha) \to F(\beta)$ is F-linear on the basis $1, \alpha, \ldots, \alpha^{n-1}$, so the single value $\psi(\alpha) = \beta$ determines ψ termwise: $\psi = \psi_{\alpha,\beta}$. □

Theorem: Isomorphism Extension

Setup. $\sigma : F \to F'$ a field isomorphism; $\overline{F'}$ an algebraic closure of F' (Steinitz's theorem); E/F an algebraic extension.

Theorem. σ extends to a field embedding

$$\tau : E \hookrightarrow \overline{F'}, \qquad \tau|_F = \sigma.$$

Slogan. Any isomorphism of base fields lifts to an embedding of an algebraic extension into any chosen algebraic closure of the codomain.

Isomorphism Extension: Specializations

Polynomial-side action. For $p = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$, write $\sigma_* p = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n \in F'[x]$.

Take $F = F'$, $\sigma = \mathrm{id}_F$, $\overline{F'} = \overline{F}$: recovers the universal property of the algebraic closure.

Take $E = F(\alpha)$, $\sigma = \mathrm{id}_F$: the extension sends α to a root of m_α in $\overline{F}$ — the conjugation isomorphism $\psi_{\alpha,\beta}$ followed by $F(\beta) \hookrightarrow \overline{F}$.

Proof: The Zorn Argument (poset, chains)

Step 1 (Poset).

$$\mathcal{P} = \{\, (K, \tau_K) : F \subseteq K \subseteq E,\ \tau_K : K \to \overline{F'} \text{ embedding},\ \tau_K|_F = \sigma \,\},$$

ordered by $(K_1, \tau_1) \leq (K_2, \tau_2)$ iff $K_1 \subseteq K_2$ and $\tau_2|_{K_1} = \tau_1$.

Step 2 (Upper bounds). For a chain $\{(K_i, \tau_i)\}$, set $K_\infty = \bigcup_i K_i$ (a subfield of E, algebraic over F) and $\tau_\infty(x) = \tau_i(x)$ for $x \in K_i$. Well-defined: if $x \in K_i \subseteq K_j$ then $\tau_j|_{K_i} = \tau_i$. So $(K_\infty, \tau_\infty) \in \mathcal{P}$ bounds the chain.

Proof: The Zorn Argument (maximal element)

Step 3 (Zorn). $\mathcal{P}$ has a maximal element $(K_{\max}, \tau_{\max})$.

Step 4. Suppose $K_{\max} \subsetneq E$. Pick $\alpha \in E \setminus K_{\max}$; it is algebraic over $K_{\max}$ (a witness $g \in F[x] \subseteq K_{\max}[x]$ exists). Let $m \in K_{\max}[x]$ be its minimal polynomial over $K_{\max}$.

Apply $\tau_{\max}$ to the coefficients of m: the image $m^{\tau_{\max}} \in \overline{F'}[x]$ is nonconstant ($\tau_{\max}$ injective), so it has a root $\beta \in \overline{F'}$ ($\overline{F'}$ algebraically closed).

Proof: The Zorn Argument (contradiction)

Define $\tau' : K_{\max}(\alpha) \to \overline{F'}$ extending $\tau_{\max}$ by $\tau'(\alpha) = \beta$ — that is, $\tau'(h(\alpha)) = h^{\tau_{\max}}(\beta)$ for $\deg h < \deg m$.

Well-defined: the only h with $\deg h < \deg m$ and $h(\alpha) = 0$ is $h = 0$ (minimality of m). Then τ' is a ring homomorphism, injective, with $\tau'|_F = \sigma$.

So $(K_{\max}(\alpha), \tau') \in \mathcal{P}$ strictly extends $(K_{\max}, \tau_{\max})$ — contradicting maximality. Hence $K_{\max} = E$, and $\tau_{\max} : E \to \overline{F'}$ is the required extension. □

Corollary: Lifting Conjugations

Corollary. Let E/F be algebraic and $\alpha, \beta \in \overline{F}$ conjugate over F. The conjugation isomorphism $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ extends to an embedding $E \to \overline{F}$.

Proof. Apply the isomorphism extension theorem with base fields $F(\alpha), F(\beta)$, base isomorphism $\psi_{\alpha,\beta}$, and codomain closure $\overline{F'} = \overline{F}$. $\square$

Corollary: Uniqueness of the Algebraic Closure

Corollary. Let $\sigma : F \to F'$ be an isomorphism, with algebraic closures $\overline{F}, \overline{F'}$. Then σ extends to an isomorphism

$$\overline{F} \xrightarrow{\sim} \overline{F'}.$$

Taking $F = F'$ and $\sigma = \mathrm{id}_F$ recovers uniqueness of $\overline{F}$. For general σ: isomorphic base fields have isomorphic algebraic closures.

Application: $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$

Any $\mathbb{Q}$-automorphism σ sends $\sqrt{2}$ to a root of x^2-2, so $\sigma(\sqrt{2}) \in \{\pm\sqrt{2}\}$; likewise $\sigma(\sqrt{3}) \in \{\pm\sqrt{3}\}$ — at most 4 automorphisms.

Each sign choice is realized: extend $\mathrm{id}_{\mathbb{Q}}$ to $\mathbb{Q}(\sqrt{2})$ by $\sqrt{2} \mapsto \pm\sqrt{2}$ (lifting conjugations), then to $\mathbb{Q}(\sqrt{2},\sqrt{3})$ by $\sqrt{3} \mapsto \pm\sqrt{3}$. Hence

$$\left|\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})\right| = 4 = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}].$$

This equality of automorphism count and degree is the starting point of Galois theory.

Definition: Index of a Field Extension

Let E/F be finite algebraic. For an embedding $\iota : F \to A$ into an algebraically closed field A, set

$$\{E : F\}_\iota := \#\{\text{ embeddings } \tau : E \to A \text{ with } \tau|_F = \iota\}.$$

We show next that this count is independent of ι and A; the common value is the *index* $\{E : F\}$.

Relation to automorphisms. Taking ι the inclusion $F \hookrightarrow \overline{F}$, every F-automorphism of E is an embedding $E \to \overline{F}$ fixing F, so $|\mathrm{Aut}(E/F)| \leq \{E : F\}$.

Theorem: The Index Is Well-Defined

Theorem. For finite algebraic E/F, the count $\{E : F\}_\iota$ is the same for every embedding $\iota : F \to A$ into an algebraically closed field A. Write $\{E : F\}$ for this common value.

So the index counts extensions into *any* algebraically closed field over F — it does not depend on the choice. In particular it may be computed inside a single algebraic closure $\overline{F}$ as $\#\{F\text{-embeddings } E \to \overline{F}\}$.

Proof: The Index Is Well-Defined

Let $\iota : F \to A$ and $\iota' : F \to A'$ be embeddings into algebraically closed fields. The elements of A algebraic over $\iota(F)$ form an algebraic closure $\overline{\iota(F)} \subseteq A$; likewise $\overline{\iota'(F)} \subseteq A'$.

Any extension $\tau : E \to A$ of ι has $\tau(E)$ algebraic over $\iota(F)$ (E/F algebraic), so $\tau(E) \subseteq \overline{\iota(F)}$ — the extensions of ι into A are the extensions into $\overline{\iota(F)}$, and likewise for ι'.

By the uniqueness corollary, $\iota' \circ \iota^{-1} : \iota(F) \to \iota'(F)$ extends to an isomorphism $\lambda : \overline{\iota(F)} \to \overline{\iota'(F)}$ with $\lambda \circ \iota = \iota'$. Then $\tau \mapsto \lambda \circ \tau$ bijects the extensions of ι with those of ι', so the counts agree. $\square$

Index of a Simple Extension

Proposition. For α algebraic over F,

$$\{F(\alpha) : F\} = \#\{\text{ distinct roots of } m_\alpha \text{ in } \overline{F}\,\} \leq \deg m_\alpha = [F(\alpha) : F].$$

Proof. An F-embedding $\tau : F(\alpha) \to \overline{F}$ is determined by $\tau(\alpha)$, and $m_\alpha(\alpha) = 0$ forces $m_\alpha(\tau(\alpha)) = 0$: so $\tau(\alpha)$ is a root of m_α. Conversely each root β gives the embedding $\psi_{\alpha,\beta}$.

So embeddings correspond bijectively to the distinct roots of m_α in $\overline{F}$ — at most $\deg m_\alpha$ of them (root bound), and $\deg m_\alpha = [F(\alpha) : F]$. □

Theorem: Product Formula for the Index

Theorem. For a tower $F \subseteq K \subseteq E$ of finite algebraic extensions,

$$\{E : F\} = \{E : K\} \cdot \{K : F\}.$$

A multiplicative law for embedding counts, parallel to the tower law for degrees. This is the tool that reduces the degree bound to simple extensions.

Proof: Product Formula

Fix an algebraic closure $\overline{F}$ and restrict embeddings to K:

$$\rho : \{\, E \to \overline{F} \,\} \longrightarrow \{\, K \to \overline{F} \,\}, \qquad \tau \longmapsto \tau|_K,$$

a map whose codomain has $\{K : F\}$ elements.

Fix $\sigma : K \to \overline{F}$. The embeddings τ with $\tau|_K = \sigma$ are exactly the extensions of σ to E. Since σ embeds K into the algebraically closed $\overline{F}$, well-definedness gives their number as $\{E : K\}$ — the same for every σ (so ρ is onto).

Summing over the $\{K : F\}$ values of σ, $\{E : F\} = \{K : F\} \cdot \{E : K\}$. □

Theorem: Degree Bound on Embeddings and Automorphisms

Theorem. For every finite algebraic extension E/F, the index is finite and

$$|\mathrm{Aut}(E/F)| \leq \{E : F\} \leq [E : F].$$

Proof. Write $E = F(\alpha_1, \ldots, \alpha_r)$ and form the tower $F = K_0 \subseteq \cdots \subseteq K_r = E$ with $K_i = K_{i-1}(\alpha_i)$. Iterating the product formula and the simple-extension count,

$$\{E : F\} = \prod_{i=1}^{r} \{K_i : K_{i-1}\} \leq \prod_{i=1}^{r} [K_i : K_{i-1}] = [E : F]$$

by the tower law. Each factor is finite. □

Examples: Embeddings versus Automorphisms

Sharp. $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$: $|\mathrm{Aut}| = 4 = \{E : F\} = [E : F]$ — all three coincide.

Asymmetric. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$: there are 3 embeddings into $\overline{\mathbb{Q}}$ (one per root of $x^3 - 2$), but $|\mathrm{Aut}| = 1$ — the roots $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ are non-real, so not in $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$.

So the index can reach the degree while the automorphism count falls short: E need not contain all conjugates of its own elements.

Characteristic 0: Index Equals Degree

In characteristic 0, every irreducible $p \in F[x]$ has $\deg p$ distinct roots in $\overline{F}$ (since $\gcd(p, p') = 1$, as $p' \neq 0$). So the simple-extension count gives $\{F(\alpha) : F\} = [F(\alpha) : F]$, and by the product formula and tower law

$$\{E : F\} = [E : F] \quad \text{for every finite algebraic } E/F.$$

E.g. $\{\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\} = 4$ and $\{\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\} = 3$, each equal to the degree — though $|\mathrm{Aut}|$ need not be. The property responsible for sharpness in general is *separability*.

Definition: Separable Polynomial

Definition. A nonzero $p \in F[x]$ is *separable* if it has no repeated root in $\overline{F}$ — equivalently, in $p = c\prod_i (x-\alpha_i)^{e_i}$ over $\overline{F}$, all $e_i = 1$.

Lemma (derivative test). A nonzero $p \in F[x]$ is separable iff

$$\gcd(p, p') = 1 \quad \text{in } F[x].$$

Proof: Derivative Test ($\Rightarrow$)

Suppose p has a repeated root $\alpha \in \overline{F}$: $p = (x-\alpha)^2 q$ in $\overline{F}[x]$.

Differentiate:

$$p' = (x-\alpha)\big(2q + (x-\alpha)q'\big)\,,$$

so $(x-\alpha) \mid \gcd(p, p')$ in $\overline{F}[x]$.

The gcd over $F[x]$ equals the gcd over $\overline{F}[x]$ (the Euclidean algorithm runs over either ring), so $\gcd(p, p') \neq 1$ in $F[x]$ too. $\square$

Proof: Derivative Test ($\Leftarrow$)

Suppose $d = \gcd(p, p')$ has $\deg d \geq 1$. Then d has a root $\alpha \in \overline{F}$, with $p(\alpha) = p'(\alpha) = 0$.

Write $p = (x - \alpha)q$ in $\overline{F}[x]$; then $p' = q + (x - \alpha)q'$, so $p'(\alpha) = q(\alpha) = 0$.

Hence $(x - \alpha) \mid q$, so $(x - \alpha)^2 \mid p$: a repeated root. $\square$

Definition: Separable Extension; Characterization

Definition. α algebraic over F is *separable* if m_α is separable; E/F is *separable* if every $\alpha \in E$ is separable over F.

Theorem. For a finite algebraic extension E/F,

$$\{E : F\} = [E : F] \quad \Longleftrightarrow \quad E/F \text{ is separable.}$$

Proof: Separable $\Rightarrow$ Index = Degree

Build a tower $F = K_0 \subset \cdots \subset K_r = E$ with $K_{i+1} = K_i(\alpha_{i+1})$.

Each α_{i+1} is separable over K_i (its minimal polynomial over K_i divides that over F, and a divisor of a separable polynomial is separable). So a separable minimal polynomial of degree $[K_{i+1} : K_i]$ has that many distinct roots: $\{K_{i+1} : K_i\} = [K_{i+1} : K_i]$.

By the product formula and tower law,

$$\{E : F\} = \prod_i \{K_{i+1} : K_i\} = \prod_i [K_{i+1} : K_i] = [E : F].$$

$\square$

Proof: Index = Degree ⇒ Separable

Contrapositive: suppose some $\alpha \in E$ is inseparable, so m_α has fewer than $\deg m_\alpha$ distinct roots: $\{F(\alpha) : F\} < [F(\alpha) : F]$.

By the product formula and the degree bound $\{E : F(\alpha)\} \leq [E : F(\alpha)]$,

$$\{E : F\} = \{E : F(\alpha)\}\,\{F(\alpha) : F\} < [E : F(\alpha)]\,[F(\alpha) : F] = [E : F].$$

So $\{E : F\} < [E : F]$. Contrapositively, equality forces E/F separable. □

Theorem: Characteristic 0 Implies Separable

Theorem. If $\operatorname{char} F = 0$, every algebraic extension E/F is separable.

Proof. Let m_α be irreducible of degree $n \geq 1$. The leading term x^n differentiates to nx^{n-1} with $n \neq 0$, so $\deg m'_\alpha = n - 1$ and $m'_\alpha \neq 0$.

Now $d = \gcd(m_\alpha, m'_\alpha)$ divides the irreducible m_α, but $\deg d \leq n - 1 < n$, so $d = 1$. By the derivative test m_α is separable. $\square$

Inseparable Example (char p): Setup

Let $F = \mathbb{F}_p(t)$ (rational functions over $\mathbb{F}_p$), and $\alpha \in \overline{F}$ a p-th root of t ($\alpha^p = t$).
Consider $f = x^p - t \in F[x]$.

Root. $f(\alpha) = \alpha^p - t = 0$.

Single root. In $\overline{F}[x]$, by the Frobenius binomial ($\binom{p}{k} \equiv 0 \pmod{p}$ for $1 \le k \le p-1$),

$$f = x^p - \alpha^p = (x - \alpha)^p$$

— one root α, multiplicity p.

Inseparable Example: Irreducibility of $x^p - t$

Suppose $f = gh$ in $F[x]$ with g, h nonconstant. By the single-root factorization, $g = (x - \alpha)^k$ in $\overline{F}[x]$ for some $1 \leq k \leq p - 1$.

Its constant term $(-\alpha)^k = (-1)^k \, t^{k/p}$ must lie in $F = \mathbb{F}_p(t)$.

But $t^{k/p} \notin \mathbb{F}_p(t)$: it would make $t^k = (t^{k/p})^p$ a p-th power in $\mathbb{F}_p(t)$, impossible since t^k has t-degree k with $1 \leq k \leq p - 1$, not divisible by p. Contradiction — so f is irreducible and $m_\alpha = f$.

Inseparable Example: Inseparability and Index

Inseparable. $f' = p\,x^{p-1} = 0$ in characteristic p, so $\gcd(f, f') = f \neq 1$. By the derivative test, $m_\alpha = f$ is inseparable.

Index. Each embedding $F(\alpha) \to \overline{F}$ sends α to a root of f; there is only α. So

$$\{F(\alpha) : F\} = 1 < p = [F(\alpha) : F].$$

Perfect Fields

Definition. F is *perfect* if every algebraic extension of F is separable.

- Characteristic-0 fields are perfect (the characteristic-0 theorem).
- Finite fields are perfect (the Frobenius map $x \mapsto x^p$ is surjective).
- The prototypical *imperfect* field is $\mathbb{F}_p(t)$, by the example above.

Proof: Finite Fields Are Perfect

Let F be finite, $\operatorname{char} F = p$. The Frobenius map $\varphi : F \to F$, $\varphi(x) = x^p$, is a ring homomorphism, injective (it is a field map), hence surjective (F finite): every element of F is a p-th power.

Let $f \in F[x]$ be irreducible. If f were inseparable, then $\gcd(f, f') \neq 1$; as f is irreducible this forces $f \mid f'$, and $\deg f' < \deg f$ gives $f' = 0$. So only exponents divisible by p occur: $f = \sum_i a_i x^{pi}$. Writing $a_i = b_i^p$,

$$f = \sum_i b_i^p \, x^{pi} = \Big(\sum_i b_i \, x^i \Big)^p,$$

contradicting irreducibility. Hence every irreducible over F is separable, i.e. F is perfect. $\square$