Propn If K/F, L/F are extensions, K is algebraically closed, L/F is algebraic, Then $\exists$ an embedding

$$\begin{tikzcd} L \arrow[rr, hook] & & K \\ & F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

(of extensions).

Corollaries: ① if $\bar{F}$ is an algebraic closure of F then $\bar{F}$ contains a copy of any algebraic extension of F.

② Any two algebraic closures of F are isomorphic (over F)

$$\begin{tikzcd} K_1 \arrow[rr, hook, "\varphi"] & & K_2 \\ & F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

proof: φ exists, $K_2/\varphi(K_1)$ is algebraic, So $K_2 = \varphi(K_1)$ since $\varphi(K_1)$ is algebraically closed.

③ If K is an algebraically closed extension of F, then $\exists$ embedding $\bar{F} \hookrightarrow K$, so alg. closure is minimal algebraically closed extension of F.

Proof of Propn By Zorn Lemma.

Let $\mathcal{L}$ be the set of embeddings $E \longrightarrow K$ over F, where $L/E/F$. $\mathcal{L} \neq \phi$ since $(F \longrightarrow K) \in \mathcal{L}$.

We say that $(E_1 \xrightarrow{\varphi_1} K) \leq (E_2 \xrightarrow{\varphi_2} K)$ if $E_1 \subseteq E_2$ and $\varphi_1 = \varphi_2|_{E_1}$.

if $\mathcal{C}$ is a chain in $\mathcal{L}$, put $E = \bigcup_{\alpha \in \Lambda} E_\alpha$, $\varphi(u) = \varphi_\alpha(u)$ if $u \in E_\alpha$.

$\mathcal{C} = \{E_\alpha \xrightarrow{\varphi_\alpha} K : \alpha \in \Lambda\}$

α, Put $E = \bigcup_{\alpha\in\Lambda} E_\alpha$, $\varphi(u) = \varphi_\alpha(u)$ if $u \in E_\alpha$.

$\{E_\alpha \xrightarrow{\varphi_\alpha} K : \alpha \in \Lambda\}$

Then $E \xrightarrow{\varphi} K$ is an upper bound of $\mathcal{C}$.

Zorn's lemma implies $\exists$ max'l $E \xrightarrow{\varphi} K$.

Claim: $E = L$.

if not, let $\alpha \in L \setminus E$.

α is algebraic over F so over E.

Let $f = m_{\alpha, E}$.

The pol-l $\varphi(f)$ splits in K,

So it has a root. Let β be a root of $\varphi(f)$.

Then $\exists$ extension $\tilde{\varphi}$ of φ,

$$E(\alpha) \xrightarrow{\tilde{\varphi}} K(\beta) = K$$

and this contradicts maximality of φ. $\square$

$f \in F[x]$, $\deg f = n$, # roots of f in K/F ?

In some extension (in the splitting field of f),

f has n roots (counting multiplicities.

$f(x) = (x-\alpha_1)^{m_1} \cdot \dots \cdot (x-\alpha_k)^{m_k}$, $\quad m_1 + \cdots + m_k = n$.

<u>Def</u> f is separable if it has exactly deg f roots in its splitting field. (no multiple roots).

- f has a multiple root α iff $f'(\alpha) = 0$, that is,

  iff f & f' have a common root,

  iff $\gcd(f, f') \neq 1$ (in $F[x]$, although it doesn't depend on F).

- If f is irreducible, may f be inseparable?

  f is irr-le: $\overset{\text{if}}{}$ f is inseparable iff $f' = 0$

  This is possible if char $F = p \neq 0$.

  for $f(x) = x^p - 1 \in \mathbb{F}_p[x]$, $f' = 0$.

  $ \overset{\parallel}{(x-1)^p}$.

If char $F = p$, $f' = 0$ iff $f(x) = g(x^p)$.

So an irreducible f is inseparable iff $f(x) = g(x^p)$, $g \in F[x]$

<u>Def</u> α is separable over F if $m_{\alpha F}$ is separable.

K/F is separable if $\forall \alpha \in K$ is separable.

F is perfect if $\forall$ its algebraic extension is separable.
(if $\forall$ irr-le pol-l from $F[x]$ is seperable)

Let $F = \mathbb{F}_p(t)$ - rational fns over $\mathbb{F}_p$.

Let $f(x) = x^p - t$. Then $f' = 0$.

$F =$ field of fractions of $\mathbb{F}_p[t]$.

eisenstein criterion:

$f = a_n x^n + \cdots + a_0$,

prime p s.t. $p \nmid a_n$, $p \mid a_i \ \forall i < n$, $p^2 \nmid a_0$,

then f is irreducible.

t is prime in $\mathbb{F}_p[t]$, so f is irreducible over $\mathbb{F}_p[t]$,

and by Gauss's lemma, f is irreducible over F.

Let α be a root of f.

$\alpha^p = t$, $\alpha = \sqrt[p]{t}$, in $F(\alpha)$, $f(x) = (x-\alpha)^p$.

If $\operatorname{char} F = p$, then $(a+b)^p = a^p + b^p$.

So α is a multiple root of f.

If $\operatorname{char} F = p$, $\Phi : F \longrightarrow F$, $a \mapsto a^p$ is a hom-sm.

it's called the Frobenius Endomorphism.

Φ may not be surjective: eg when $F = \mathbb{F}_p(t)$.

$\Phi(u(t)) = u(t^p)$. Φ is not surjective.

$t \mapsto t^p$

$a \mapsto a^p = a$.

if F is finite, Φ is surj. b.c. it's injective ($F/\mathbb{F}_p$ is a fdvs).

Then Φ is the Frobenius Automorphism.

Theorem F is perfect iff its FA is surjective.

of finite characteristic