Thm: If F is a field and if L_1, L_2 are both alg. closures of F, then $L_1 \cong L_2$.

Pf: Let $\mathcal{S}$ $\neq \phi$ be the collection of all nonzero field homs.

$\tau: K_1 \to L_2$, where $F \subseteq K_1 \subseteq L_1$.

Partial order on $\mathcal{S}$: $\tau_1 \leq \tau_2$ if τ_2 extends τ_1.

Suppose $\{\tau_i : K_i \to L_2\}$ is a chain in $\mathcal{S}$.

Define $K = \cup K_i$, and define $\tau: K \to L_2$ by

$\tau(\alpha) = \tau_i(\alpha)$, $\forall \alpha \in K_i$. Then τ is an upp. bd. for the chain.

By Zorn's lemma, $\exists$ max elem $\tilde{\tau}: \tilde{K} \to L_2$.

Claims:

i) $\tilde{K} = L_1$: If not then $\exists$ poly. in $F[x]$ which doesn't split completely in $\tilde{K}[x]$

$\Rightarrow \exists f \in \tilde{K}[x]$, irred., $\deg f \geq 2$.

Then f has a root α_1 in L_1, $\tilde{\tau}(f)$ is irred. in $\tilde{\tau}(\tilde{K})[x]$ and has a root α_2 in L_2, and (by a thm from before), $\tilde{\tau}$ extends to an isom from $\tilde{K}(\alpha_1) \to \tilde{\tau}(\tilde{K})(\alpha_2)$, which contradicts the maximality of $\tilde{\tau}$.

ii) $\tilde{\gamma}$ is onto : Apply the same argument from i) to $\tilde{\gamma}^{-1}$.

Conclusion: $L_1 \cong L_2$. ☒

Thm (Fund. thm. of Algebra): $\mathbb{C}$ is algebraically closed.

Pf: Let $f \in \mathbb{C}[z]$, $\deg f \geq 1$. Suppose f has no roots in $\mathbb{C}$

$f(z) = a_n z^n + \cdots + a_1 z + a_0$, $a_0, \ldots, a_n \in \mathbb{C}$, $n \geq 1$, $a_n \neq 0$.

Then $h(z) = \dfrac{1}{f(z)}$ is entire function.

But $h(z) \to 0$ as $|z| \to \infty$

$\Rightarrow h(z)$ is bounded

$\Rightarrow h(z)$ is constant (by Liouville's thm.)

$\Rightarrow h(z) = 0$

Contradiction. ☒

Tale of Ω_p:

$$\begin{array}{l} \mathbb{C} = \overline{\mathbb{R}},\ |\cdot|_\infty \\ 2 \,\big|\ \text{algebraic closure} \\ \mathbb{R},\ |\cdot|_\infty \\ \big|\ \text{completion} \\ \mathbb{Q},\ |\cdot|_\infty \end{array}$$

$$\begin{array}{l} \Omega_p,\ |\cdot|_p \ \text{(turns out to be algebraically closed)} \\ \big|\ \text{completion} \\ \overline{\mathbb{Q}_p},\ |\cdot|_p \\ \infty \,\big|\ \text{algebraic closure} \\ \mathbb{Q}_p,\ |\cdot|_p \\ \big|\ \text{completion} \\ \mathbb{Q},\ |\cdot|_p \end{array}$$

Def:
$|\cdot|_p : \mathbb{Z} \to \mathbb{Z}[\frac{1}{p}]$,

$n \in \mathbb{Z}$, $n = p^\alpha \cdot m$, $(m,n) = 1$, $|n|_p := p^{-\alpha}$, $|0|_p = 0$.

$|\cdot|_p : \mathbb{Q} \to \mathbb{Z}[\frac{1}{p}]$, $|\frac{a}{b}|_p := \frac{|a|_p}{|b|_p}$.

Finite fields

Thm: If $|F| < \infty$ then $|F| = p^n$ for prime p, $n \in \mathbb{N}$.

Pf: F is a finite dim v.s. over it's prime subfield $\mathbb{F}_p$.

$[\mathbb{F}_p : F] = n$. ∎

Def: Suppose $f \in F[x]$, $f(x) = \sum_{i=0}^{n} a_i x^i$,

define $(D_x f) \in F[x]$ by

$$(D_x f)(x) = \sum_{i=1}^{n} i a_i x^{i-1}.$$

Facts (HW): $D_x(f+g) = D_x f + D_x g$

$D_x(fg) = (D_x f) g + f \cdot (D_x g)$.

Lemma: If $f \in F[x]$ has a repeated root α iff α is also a root of $D_x f$.

Pf: Suppose $f(x) = (x-\alpha)^n g(x)$, $n \geq 2$ (over some spl. fld.)

Then $(D_x f)(x) = n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n (D_x g)(x)$

$\Rightarrow D_x f(\alpha) = 0$.

On the other hand, suppose $f(\alpha) = (D_x f)(\alpha)$.

Write $f(x) = (x-\alpha) h(x)$. Then

$D_x f(x) = h(x) + (x-\alpha)(D_x h)(x)$, so

$0 = D_x f(\alpha) = h(\alpha) \Rightarrow (x-\alpha)^2 \mid f(x)$. $\boxtimes$

Def: $f \in F[x]$ is separable if it factors as a product of distinct linear factors over a spl. fld.

Lem: $\forall f \in F[x]$,

$$\gcd(f, D_x f) = 1 \Leftrightarrow f \text{ is separable.}$$

Pf: follows from Lemma above. $\boxtimes$

Thm: $\forall p$ prime, $n \in \mathbb{N}$, $\exists$ a unique field of order p^n, up to isom.

Pf: Existence: Let K be the spl. field over $\mathbb{F}_p$ of the poly. $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.

Since $(D_x f)(x) = p^n x^{p^n - 1} - 1 = -1 \in \mathbb{F}_p[x]$, the roots of f in K are distinct.

Suppose α, β are roots of f in K. Then

$$f(\alpha - \beta) = (\alpha - \beta)^{p^n} - (\alpha - \beta)$$
$$= \alpha^{p^n} - \beta^{p^n} - (\alpha - \beta)$$
$$= f(\alpha) - f(\beta) = 0,$$

and, if $\beta \neq 0$,

$$f\left(\frac{\alpha}{\beta}\right) = \left(\frac{\alpha}{\beta}\right)^{p^n} - \left(\frac{\alpha}{\beta}\right) = \frac{\alpha}{\beta} - \frac{\alpha}{\beta} = 0.$$

So the collection of p^n roots of f is a field, which implies that $|K| = p^n$.

Uniqueness: Suppose $K/\mathbb{F}_p$ is a field of order p^n. Then $|K^\times| = p^n - 1 \Rightarrow \forall \alpha \in K$, $\alpha^{p^n} = \alpha$, so K is the spl. field of $f(x)$ above, which is unique up to isom. $\blacksquare$