Lecture 15:

Last time:

Thm: Any $f(x) \in F[x]$ has a splitting field K where $[K:F] < (\deg f)!$.

Addendum: Suppose K, K' are splitting fields for $f(x) \in F[x]$. Then $\exists$ an isom $\psi: K \to K'$ with $\psi|_F = id_F$.

Pf: See text, think $F(\alpha) \cong F[x]/m_{F,\alpha}(x)$

Algebraically closed: Every poly in $K[x]$ has a root in K. ($\Rightarrow$ it splits completely)

Ex: $\mathbb{C}$ (by Fund. Thm of Algebra)

$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is alg over } \mathbb{Q}\}$

Non Ex: $\mathbb{Q}, \mathbb{R}$

Pf: Suppose $f(x) \in \overline{\mathbb{Q}}[x]$. Let $\alpha \in \mathbb{C}$ be a root of f. Then $\overline{\mathbb{Q}}(\alpha)/\overline{\mathbb{Q}}$ is alg. and $\overline{\mathbb{Q}}/\mathbb{Q}$ is $\Rightarrow \overline{\mathbb{Q}}(\alpha)/\mathbb{Q}$ is alg $\Rightarrow \alpha \in \overline{\mathbb{Q}}$.

Fund Thm of Algebra (Gauss 1816)

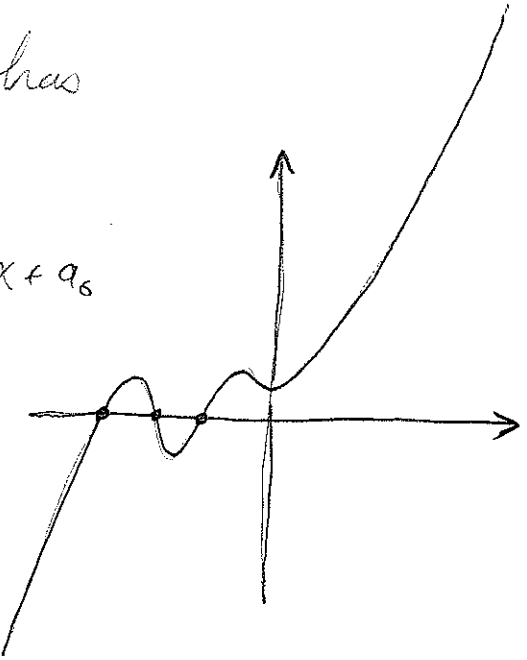
Every $f(x) \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.

All proofs use some analysis/topology. Minimum is two consequences of the Intermediate Value Thm:

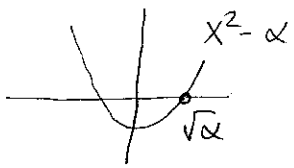
① Every odd degree poly in $\mathbb{R}[x]$ has a root in $\mathbb{R}$.

$$f(x) = x^{d} + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \qquad (d \text{ odd})$$

is neg for $x \ll 0$ and pos for $x \gg 0$



② Every pos α in $\mathbb{R}$ has a square root.



[Will use Galois Theory to finish the job later, purely anal/top proofs are really more natural
Cf. Milnor, Topology from a differentiable viewpoint.]

Def: K is an algebraic closure of F if K/F is algebraic and K is algebraically closed.

Ex: $\overline{\mathbb{Q}}/\mathbb{Q}$ **Non Ex:** $\mathbb{C}/\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$

Thm: Any field F has an alg. closure.

Pf: See text, think adding in roots ad infinitum (i.e. use Zorn's Lemma) ▨

Q: What is the alg. closure of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$?

$f(x) \in F[x]$ monic. Over the splitting field of f, have

$$f(x) = (x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_n)^{k_n} \leftarrow \text{multiplicity}$$

with α_i distinct. If $k_i = 1$, then α_i is a simple root otherwise, is a mult. root.

$f(x)$ is separable if all are simple

Ex: x^2+1, x^2-1 in $\mathbb{Q}[x]$

Non Ex: x^2+2x+1 in $\mathbb{Q}[x]$

Interesting example: $x^2 + t \in \mathbb{F}_2(t)[x]$

is ↑ rat'l functions.

(a) Irreducible (Eisenstein with ideal (t))

(b) Let α be a root in the splitting field, so $\alpha^2 = t$. Then

$$(x-\alpha)^2 = x^2 - 2\alpha x + t = x^2 + t.$$

So doesn't have a simple root

Goal Thm: If F has char 0 or is finite, then every $f(x) \in F[x]$ is separable.

For $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ in $F[x]$

set $f'(x) = n a_n x^n + (n-1) a_{n-1} x^{n-2} + \cdots + 2 a_2 x + a_1$

[The derivative is also in $F[x]$, but is formal as the limiting notions used to define the der. in calc may make no sense here. Has usual props.]

$$(f+g)' = f' + g' \quad \text{and} \quad (fg)' = f'g + fg'.$$

Lemma 1: $f(x) \in F[x]$ has a mult root α iff α is also a root of $f'(x)$.

Lemma 2: $f(x) \in F[x]$ is separable iff $\gcd(f(x), f'(x)) = 1$ in $F[x]$.

Ex: ① $f(x) = x^2 + 1$ in $\mathbb{Q}[x]$

$f'(x) = 2x \Rightarrow$ separable

② $f(x) = x^2 + 2x + 1$ in $\mathbb{Q}[x]$

$f'(x) = 2x + 2 = 2(x+1) \Rightarrow \gcd(f, f'(x)) = (x+1)$.

③ $f(x) = x^2 + t$ in $\mathbb{F}_2(t)[x]$

$f'(x) = 2x = 0$

Pf of Lemma 1: Consider $g(x) = f(x - \alpha)$. Then a mechanical check gives that $g'(x) = f'(x - \alpha)$. So can assume $\alpha = 0$. Then

$g(x) = x^k h(x)$ where $h(x)$ has a non-zero const term.

Then

$$g'(x) = kx^{k-1}h(x) + \underbrace{x^k h'(x)}_{0 \text{ at } x=0}$$

(x^{k-1}: $\neq 0$ at $x=0$)

Thus

$$g'(0) = \begin{cases} 0 & k > 1 \\ h(0) & k = 1. \end{cases}$$

∎

Proof of Lemma 2: Need to show for $p, q \in F[x]$

$\gcd(p(x), q(x)) = 1 \iff$ p, q have no common roots in an ext. where they split completely.

($\Rightarrow$) Clear

($\Leftarrow$) If α is common root, then $m_{F,\alpha}(x)$ must divide p and q.

∎