Today: Algebraic closure & seperable extensions

Algebraic closure

Def: F: field. An alg. ext. $\overline{F}/F$ is an alg. closure of F if every poly. $f \in F[x]$ splits over $\overline{F}$.

This always exists (Prop. 30), and is unique (Prop. 31)

Def: A field F is alg. closed if $\overline{F} = F$.

Prop 29: An alg. closure is alg. closed

Intuition: $\overline{F} = F(\text{all roots to all polys in } F[x])$

Proof: Similar to creating $F(\text{root of } f)$, but uses Zorn's Lemma

Fundamental Thm. of Alg.: $\mathbb{C}$ is alg. closed

Pf: Later

Cor 32: $\overline{\mathbb{Q}} \subseteq \mathbb{C}$

---

§13.5: Separable Extensions

Inseparability: the problem that (usually) doesnt happen

Let $f(x) \in F[x]$, and let K be a splitting field for F.

Def: Over K,

$$f(x) = (x-\alpha_1)^{n_1} \cdots (x-\alpha_k)^{n_k} \qquad \begin{matrix} \alpha_1, \ldots, \alpha_k \text{ distinct} \\ n_i \geq 1 \end{matrix}$$

n_i: multiplicity of α_i

α_i is a $\begin{cases} \text{multiple root if } n_i > 1 \\ \text{Simple root if } n_i = 1 \end{cases}$

f is separable if it has no multiple roots.

When does f have multiple roots?

Def (no calculus derivative):

The derivative of

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$$

is

$$Df(x) := D_x f(x) = n a_n x^{n-1} + \cdots + 2a_2 x + a_1 \in F[x]$$

Prop 33: α is a mult. root of f $\iff$ α is a root of $f(x)$ and $D_x f(x)$

$\Rightarrow$: Over $\bar{K}$,

$$f(x) = (x-\alpha)^2 g(x)$$

$$Df(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 D_x g(x)$$ has α as a root.

$\Leftarrow$ Over $\bar{K}$,

$$f(x) = (x-\alpha)h(x)$$

$$Df(x) = h(x) + (x-\alpha)Dh(x),$$

so α must be a root of $h(x)$, so a mult. root of $f(x)$.

Corollary: $f(x)$ is separable $\Leftrightarrow$ $\gcd(f(x), D_x f(x)) = 1$

When are polys. separable?

Prop: All irred. polys. over

(a) a field of char 0 (Cor. 34)

(b) a finite field (Prop. 37)

are separable

Furthermore, roots of distinct irred. polys. are distinct (Prop 9), so in these cases, only way to get multiple roots is to have more than 1 of the same irred. factor.

Are all irred. polys. irreducible?

No. Consider $F = \mathbb{F}_2(t)$ i.e. the field of rat'l fns. in t w/

coeffs. in $\mathbb{F}_2$. Let

$$f(x) = x^2 - t$$

Over its splitting field,

$$f(x) = (x+\sqrt{t})(x-\sqrt{t}) = (x+\sqrt{t})^2,$$

so f is not separable. But it is irreducible since $\sqrt{t} \notin F$.

Pf of a):

$$f(x) \in F[x] \text{ irred. of deg } n$$

Then $\gcd(f, Df)$ is a poly in $F[x]$ of degree $\leq \deg Df = n-1$.
Since f is irred, this must be 1.

Why can't we use this proof in char. p?

Ans: derivative could be 0.

$$f(x) = a_m x^{mp} + a_{m-1} x^{(m-1)p} + \cdots + a_1 x^p + a_0 = g(x^p) \text{ where}$$

$$g(x) = a_m x^m + \cdots + a_1 x + a_0$$

Prop 35: Suppose Char $F = p$. The pth power map:

$$\left.\begin{aligned} F &\xrightarrow{\varphi} F \\ a &\mapsto a^p \end{aligned}\right\} \text{ Frobenius endomorphism}$$

is an inj. field endomorphism. When F is finite, φ is also surj., so every elt. of F is a pth power.

Pf: Compute that

$$(a+b)^p = a^p + b^p$$
$$(ab)^p = a^p b^p$$

Pf of b): If f inseparable, $\exists g \in F[x]$ s.t. $f(x) = g(x^p)$, so

$$f(x) = g(x^p) = a_m x^{mp} + a_{m-1} x^{(m-1)p} + \cdots + a_1 x^p + a_0$$
$$= (b_m x^m)^p + (b_{m-1} x^{m-1})^p + \cdots + (b_1 x)^p + b_0^p$$
$$= \underbrace{(b_m x^m + \cdots + b_1 x + b_0)^p}_{\text{reducible! Contradiction}}$$

use Frobenius endomorphism

Def: A field F is called <u>perfect</u> if

- char $F = 0$; or
- char $F = p$, and every elt. of F is a pth power

Cor: Every irred. poly. over a perfect field is separable

Cor (Prop 38): Let char $F = p$, $f(x) \in F[x]$ irred. $\exists!$ irred. separable poly. $f_{sep}(x) \in F[x]$, $k \geq 0$ s.t. $p(x) = p_{sep}(x^{p^k})$

Pf: If f not separable, $f(x) = f_1(x^p)$, $f_1 \in F[x]$. Then f_1 is sep. or $f_1(x) = f_2(x^p)$.

Def: The separable degree $\deg_s f(x) = \deg f_{sep}(x)$

The inseparable degree $\deg_i f(x) = p^k$

$\deg f = \deg_s f \cdot \deg_i f$

E.g.: $F = \mathbb{F}_2(t)$

a) $f(x) = x^2 - t$ $\quad f_{sep}(x) = x - t$

$\deg_s f = 1 \quad \deg_i f = 2$

b) $f(x) = x^{2^m} - t$ $\quad f_{sep}(x) = x - t$

$\deg_s f = 1 \quad \deg_i f = 2^m$

c) $(x^{p^2} - t)(x^p - t)$ is inseparable, but not irred.,

so no f_{sep}, $\deg_s$, $\deg_i$ possible