May 3

Today

- separable field ext
- finite fields

Separable

Let $K \subset L$ be a field ext

Defn We say that an element $\alpha \in L$ is separable/K if it is algebraic and its min polynomial has distinct roots.

Defn We say $K \subset L$ is separable if every $\alpha \in L$ is separable over K.

Ex: $\mathbb{R} \subset \mathbb{C}$ $\quad i \in \mathbb{C}$ separable

Why? min poly $= x^2+1 = (x-i)(x+i)$ distinct

Ex: $\mathbb{F}_p(t) \subset \mathbb{F}_p(t^{1/p})$

$K = \mathbb{F}_p(t)$, $\quad \mathbb{F}_p(t^{1/p}) = K[x]/(x^p-t)$

If $\alpha = t^{1/p}$, its min poly is $f(x) = x^p - t$

But $f = x^p - t$ factors in $\mathbb{F}_p(t^{1/p})$

as
$$x^p - t = (x-\alpha)^p$$

$\Rightarrow$ $\alpha = t^{1/p}$ is not separable

Finite fields

THM • For each prime p and each pos. integer $n > 0$, there exists unique field $\mathbb{F}_{p^n}$ with p^n elements.

• Moreover, $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ is the splitting field of
$$x^{p^n} - x \in \mathbb{F}_p[x]$$

$\mathbb{F}_{p^n} \cong (\mathbb{F}_p)^n \leftarrow$ n dim'l vector space

as vector spaces (not as rings!)

Another characterization of separability

Lemma: Let K be a field.
Let $f(x) \in K[x]$.
If $f(x)$ and $f'(x)$ are rel. prime
then $f(x)$ is separable.

Rmk:

- Say $f(x)$ is seperable if it has distinct roots in a splitting field
- $f'(x)$ = derivative of $f(x)$
  (Explicitly, $f(x) = a_n x^n + \cdots + a_0$
  $f'(x) = n \cdot a_n x^{n-1} + \cdots + a_1$)
- f & g rel. prime $\Longleftrightarrow$
  $\nexists h$ of deg ≥ 1 w/ $h \mid f$, $h \mid g$

Usual laws apply:
product rule, —

PF: If $f(x)$ were not separable,
then factor
$$f(x) = (x-\alpha)^2 g(x)$$
(Here $\alpha \in L$ & $g \in L$ where $K \subset L$ is a splitting field of f)
Then
$$f'(x) = 2(x-\alpha) g(x) + (x-\alpha)^2 g'(x)$$
$$= (x-\alpha)\left(2g(x) + (x-\alpha)g'\right)$$
$\Longrightarrow f$ & f' are not ~~not~~ rel. prime

Cor: If K is char $= 0$,
then any irred $f(x) \in K[x]$ is separable.

PF: Write $f(x) = a_n x^n + (\text{lower terms})$ $\boxed{a_n \neq 0}$
$$f'(x) = \underbrace{n \cdot a_n}_{\text{not zero}} x^{n-1} + (\text{lower terms})$$
$\Longrightarrow f'$ is non-zero poly of deg $n-1$
$\Longrightarrow f$ & f' rel prime

Cor: If K is char $= 0$, then any irred $f(x) \in K[x]$ is separable.

Cor If K char $= 0$, then any field ext $K \subset L$ is separable.

Pf Let $\alpha \in L$. Let $f(x) \in K[x]$ be its min poly.
Cor $\Rightarrow$ $f(x)$ is sep
$\Rightarrow$ α is sep.

Ex: $\mathbb{F}_p(t) \subset \mathbb{F}_p(\underset{\alpha}{\underset{\shortparallel}{t^{1/p}}})$

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

$f'(x) = \cancel{p \cdot x^{p-1}} - 0 = 0$

Ex: $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})^{=K}$ separable $/\mathbb{Q}$

min poly $x^3 - 2$ does not split in K

Let $\mathbb{F}_{p^n}$ be the splitting field of
$f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$

Claim: $f(x)$ is separable.

Pf: $f'(x) = p^n x^{p^n - 1} - 1$
$= -1$
$\Rightarrow f$ & f' are rel prime ✓

Cor $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ is separable

Pf: Pick $\alpha \in \mathbb{F}_{p^n}$

Claim $\alpha^{p^n} = \alpha \in \mathbb{F}_{p^n}$

Why? $\mathbb{F}_{p^n}^\times$ mult. gp of order $p^n - 1$

Cor $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ is separable

Pf: Pick $\alpha \in \mathbb{F}_{p^n}$

Claim $\alpha^{p^n} = \alpha \in \mathbb{F}_{p^n}$

Why? $\mathbb{F}_{p^n}^{\times}$ mult. gp of order $p^n - 1$

Group theory $\Rightarrow$

$$\alpha^{p^n - 1} = 1 \in \mathbb{F}_{p^n}^{\times}$$

$$\Rightarrow \alpha^{p^n} = \alpha \in \mathbb{F}_{p^n}$$

$\Rightarrow$ α is a root of

$$f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$$

The min poly of α divides f

Since f is sep, so is α.