May 7

Normal extensions $K \subset L$

Defn: Every poly $f \in K[x]$ with a root in L splits over L

Example: If $K \subset L$ is the splitting field of a polynomial $f \in K[x]$, then it's normal.

Ex: • $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ not normal

b/c $x^3 - 2 \in \mathbb{Q}[x]$ has a root in $\mathbb{Q}(\sqrt[3]{2})$ but doesn't split

• $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$ $\omega = e^{2\pi i/3}$

$= \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ is normal!

Suppose $K \subset K(\alpha)$. Is this normal?

Let $f =$ min poly of α

Then $K \subset K(\alpha)$ normal $\iff$ f splits over $K(\alpha)$

If $K \subset K(\alpha_1, \ldots, \alpha_n) = L$

Let $f_i =$ min poly of α_i

Then $K \subset L$ is normal

$\iff$ each f_i splits/L

(B/c then L is splitting field $f_1 f_2 \cdots f_n$)

Two notions for $K \subset L$

① separable

② normal

Example: $K \subset L$ normal, not separable

$$K = \mathbb{F}_p(t) \subset \mathbb{F}_p(t^{1/p}) = L = K(\alpha)$$

If $\alpha = t^{1/p}$, then $\alpha^p = t$

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

Claim: $\alpha = t^{1/p} \in \mathbb{F}_p(t^{1/p})$ is not separable

Its min poly is

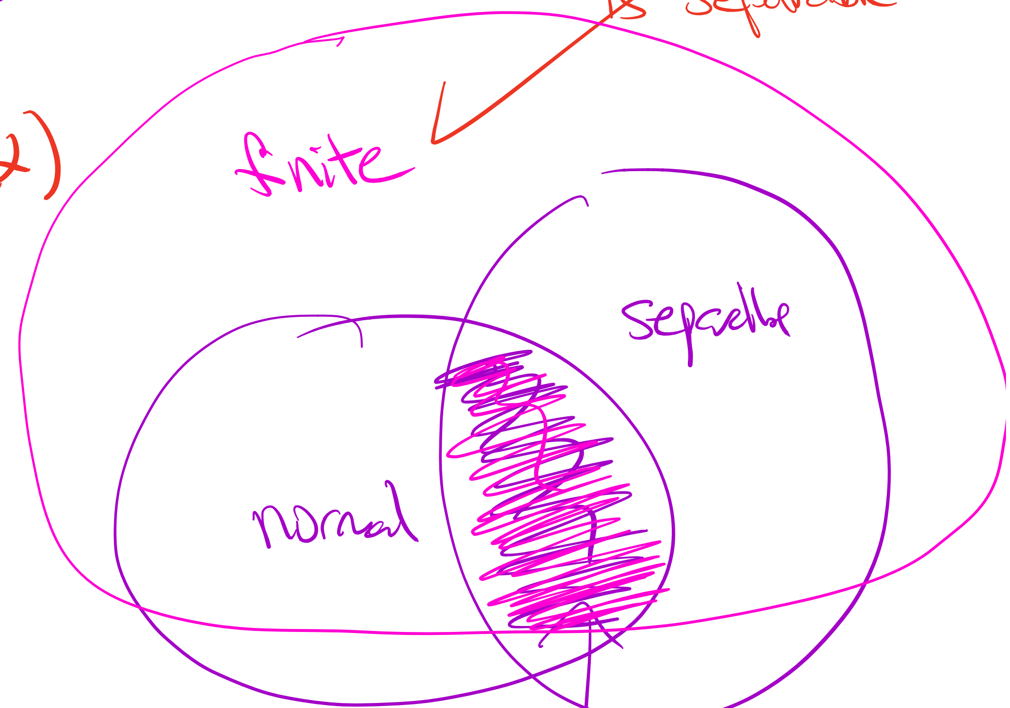
$$x^p - t = (x-\alpha)^p$$

Freshman dream

Example: $K \subset L$ separable, not normal

$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ not normal ✓

is separable ✓



Galois = finite + normal + separable

Recall

$K \subset L$ finite field ext

Defn. • Say $\alpha \in L$ is separable$/K$ if its min. poly has no repeated roots in its splitting field

• $K \subset L$ separable if all $\alpha \in L$ are separable$/K$.

Facts

① If $\text{char}(K) = 0$, then any field ext $K \subset L$ is separable

② Let $p = \text{char}(K) > 0$. If every element $\alpha \in K$ has a p^{th} root in K, then any field ext $K \subset L$ is separable

---

The characteristic of any field is 0 or a prime integer.

$($ $\mathbb{Z} \longrightarrow K$, $1 \mapsto 1$

Reason:

An irred poly $f(x) \in K[x]$ has not repeated roots $\Longleftrightarrow$ f and f' are rel. prime

In $\text{char} = 0$, if $\deg(f) = d$ then $\deg(f') = d-1$. Since f is irred, f & f' are rel. prime.

Skip.

We won't actually need it

You could use ② to show $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ is separable.

Finite field p prime

$\mathbb{F}_p$ every element $\alpha \in \mathbb{F}_p$ satisfies $\alpha^p = \alpha$

Why? $|\mathbb{F}_p^\times| = p-1 \rightsquigarrow \alpha^{p-1} = 1$ for $\alpha \neq 0$.

In part., α is p^{th} root of α.

Thm There exists a unique field $\mathbb{F}_{p^n}$ with p^n elements where

- p is a prime
- $n > 0$ is pos. integer.
- Moreover, $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$.
- And $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ is finite, normal and separable.

① Uniqueness Let K be a field with p^n elements.

Every element $\alpha \in K$ satisfies

$$\alpha^{p^n} = \alpha$$

Why? $|K^\times| = p^n - 1$

$\rightsquigarrow$ K splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$

Use uniqueness of splitting fields.

$K = \{\alpha_1, \alpha_2, \dots, \alpha_{p^n}\}$

each α_i is a root of $x^{p^n} - x$.

$$\rightsquigarrow x^{p^n} - x = \prod_{i=1}^{p^n} (x - \alpha_i)$$

Thm There exists a unique field $\mathbb{F}_{p^n}$ with p^n elements where

- p is a prime
- $n > 0$ is pos. integer.

- Moreover, $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$.
- And $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ is finite, normal and separable.

Existence

Let K be the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$

Need to show: $\#K = p^n$

Know: $\mathbb{F}_p \subset K$ of degree m

$\rightsquigarrow \#K = p^m$ for $m \leq n$

Need to show: $m = n$.

Also know: every element $\alpha \in K$ satisfies $\alpha^{p^n} = \alpha$

$\rightsquigarrow \alpha$ is a root of

$f(x) = x^{p^n} - x$

$$K = \{\underbrace{\alpha_1, \alpha_2, \ldots, \alpha_{p^m}}_{\text{all roots of } f(x)}\}$$

Not only is $\alpha_i^{p^n} = \alpha_i$, $|K^\times| = p^m - 1$

$\alpha_i^{p^m} = \alpha_i$

Each α_i is a root of

$x^{p^m} - x$.

$\rightsquigarrow x^{p^m} - x \mid x^{p^n} - x$

$\leadsto\; x^{p^n}-1 = (x^{p^m}-1)\underbrace{(x^{(p^m-1)(a-1)} + x^{(p^m-1)(a-2)} + \cdots + x^{p^m-1} + 1)}_{h}$

where $(p^n-1) = (p^m-1)\cdot a$

has no roots in K

Plug in α

But K splitting field of $x^{p^n}-x$

Get contradiction if $\deg(h) > 0$

Missing detail! Know $K^\times = \mathbb{Z}/p^m-1$ is cyclic !

general fact.

$\Rightarrow \exists\, \alpha \in K^\times$ of order p^m-1

$\Rightarrow$ min poly of α is $x^{p^m}-x$

Since α is also a root of $x^{p^n}-x$, get $x^{p^m}-x \mid x^{p^n}-x$

$\Rightarrow m \leq n$ and more...