Apr 30

Recall

- splitting field
- We showed splitting fields exist and are unique.

Defn We say $K \subset L$ is a **normal** field extension if for every irred poly $f(x) \in K[x]$ such that $f(x)$ has a root in L, then every root of $f(x)$ is in L

Ex: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ normal

$x^2 - 2 \in \mathbb{Q}[x]$

$\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ & so is $-\sqrt{2}$

But need to check it for every irred. poly

Here $h(x) = (x^2+1)(x-\sqrt{2})$

does have $\sqrt{2}$ as a root but well are not rational

Prop Any splitting field is normal

Pf: Let $K \subset L$ be the splitting field of $f(x) \in K[x]$

Let $g(x) \in K[x]$ irred and $\alpha \in L$ a root of $g(x)$.

Need to show: All roots of $g(x)$ are in L.

It's not true in general that $g \mid f$. Would be easy otherwise

Let $L \subset L'$ be splitting of $g(x) \in K[x] \cap L[x]$

Need to show: if α, α' roots of g then $\alpha \in L \iff \alpha' \in L$

Picture

$K \subset L \subset L'$

α, α'

Prop Any splitting field is normal

Pf: Let $K \subset L$ be the splitting field of $f(x) \in K[x]$

Let $g(x) \in K[x]$ irred and $\alpha \in L$ a root of $g(x)$.

Need to show: All roots of $g(x)$ are in L.

It's not true in general that $g \mid f$. Would be easy otherwise

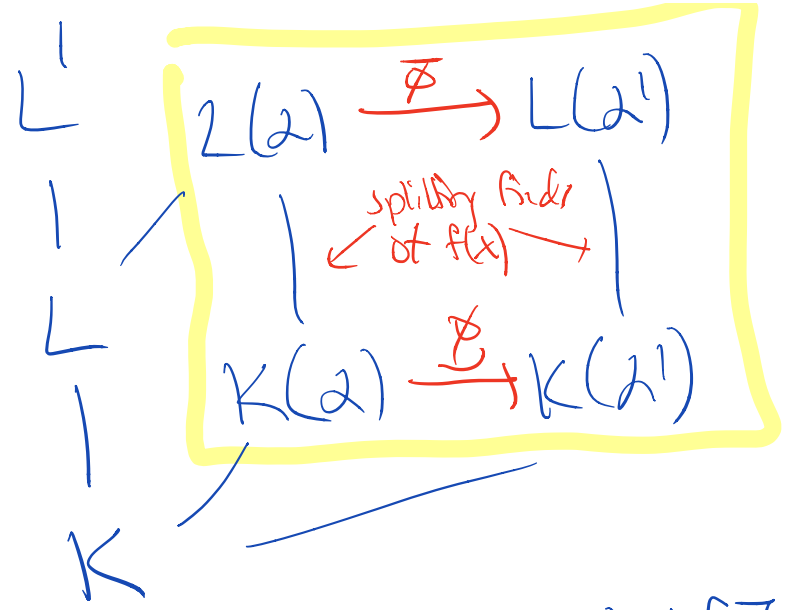
Let $L \subset L'$ be splitting of $g(x) \in K[x]$

Need to show: if α, α' roots of g then $\alpha \in L \Leftrightarrow \alpha' \in L$

Picture

$$K \subset L \subset L'$$

α, α'



- Since α, α' roots of $g(x) \in K[x]$ irred
  $g(x) = \min$ poly of α
  $= \min$ poly of α'
  $K(\alpha) \cong K[x]/(g(x)) \cong K(\alpha')$
  $\Rightarrow \exists$ isom $\phi: K(\alpha) \to K(\alpha')$ over K.
- L splitting field of $f(x) \in K[x]$
  $\Rightarrow L(\alpha)$ splitting field of $f(x) \in K(\alpha)[x]$
  $L(\alpha')$ $K(\alpha')[x]$
- By uniqueness of splitting field $\exists$ isom ϕ extending ϕ
- Therefore $|L(\alpha):L| = |L(\alpha'):L|$

$\alpha \in L \Leftrightarrow |L(\alpha):L| = 1 \Leftrightarrow |L(\alpha'):L| = 1 \Leftrightarrow \alpha' \in L$ ✓

Positive characteristic

Let K be a field

There is a ring homomorphism

$\phi : \mathbb{Z} \longrightarrow K$

$n \longmapsto \underbrace{1+\cdots+1}_{n \text{ times}}$ $n>0$

$0 \longmapsto 0$

$n \longmapsto -(\underbrace{1+\cdots+1}_{|n| \text{ times}})$ $n<0$

Ex: $\mathbb{Z} \to \mathbb{Q}$, $\mathbb{Z} \to \mathbb{C}$ } injective] char = 0

$\mathbb{Z} \to \mathbb{F}_p = \mathbb{Z}/p$, $p \mapsto 0$ char = p

(not injective)

The kernel

$\ker(\phi) \subset \mathbb{Z}$ is a prime ideal

$\Rightarrow \exists$ prime p s.t. $\ker(\phi) = (p)$

The characteristic of K is p,

the smallest pos. integer such that

$p = \underbrace{1+\cdots+1}_{p \text{ times}} = 0 \in K$

Nice feature of pos. characteristic

Lemma: Let K be a field of char $= p$.

Then for all $x, y \in K$,

$$(x+y)^p = x^p + y^p$$

Proof uses $p \mid \binom{p}{i}$ for $i = 1, \dots, p-1$

Rmk: If $\mathrm{char}(K) = p$

$\mathbb{F}_p \subset K$ is a subfield

(Because $(p) = \ker(\mathbb{Z} \to K)$

1st isom $\Rightarrow \mathbb{Z}/p \hookrightarrow K$

$\mathbb{F}_p$

Cor: If K is a finite field (i.e. $\#K$ is finite), then $\#K = p^n$ for some prime p and some $n \geq 1$.

Pf: Know $\mathrm{char}(K) =$

$\Rightarrow \mathbb{F}_p \subset K$ field ext

In particular, K is a vector space over $\mathbb{F}_p$. It is finite dim'l.

As vect. spaces, $K \cong \mathbb{F}_p^n$ (not a field) for some n

$\Rightarrow \#K = p^n$

number of elements of the set K

An example of a field in pos. char that is not a finite field.

Ex: $\mathbb{F}_p(x)$ field

Consider $\mathbb{F}_p(x) \subset \mathbb{F}_p(x^{1/p})$, where $\mathbb{F}_p(x) = \mathbb{F}_p(x)[y]/(y^p - x)$

$x^{1/p}$ = pth root of x

If $\alpha = x^{1/p}$, its min poly is

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

Over $\mathbb{F}_p(x^{1/p})$, we have

$$f(y) = (y - \alpha)^p$$

Roots are not distinct!

Weird

Defn • $K \subset L$ field ext

• $\alpha \in L$

Say $\alpha \in L$ **separable** if roots of its min poly are distinct

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

Ex: $\mathbb{F}_p(x) \subset \mathbb{F}_p(x^{1/p})$ **not** separable