Splitting Fields

Recap: $p(x) \in F[x]$ irred. How to find a field where $p(x)$ has a root? $F[x]$ PID and p irred. $\Rightarrow$ (p) prime So (p) is maximal.

$F[x]/(p(x)) := K$ is a field.

in K, we have $p([x])$

$= [p(x)] = 0.$

The natural projection $\pi : F[x] \to F[x]/(p(x))$

$\pi(F) \cong F.$

We view K as an extension of

F by identifying F w/ it's
iso copy in K.

Do this inductively, i.e. Keep adjoining roots of irred. factors until you get a field extension K/F containing all roots of f(x), so that

$$f(x) = (x-r_1)\cdots(x-r_n) \in K[x].$$

Def: A field K/F is a splitting field of f if:

- $f(x) = (x-r_1)\cdots(x-r_n) \in K[x]$
- no intermediate extension between F and K has this property.

Big Thm: if K, K' splitting fields of $f \in F[x]$. Then

$K \cong K'$ via $\sigma : K \to K'$

w/ $\sigma(F) = F$.

Also: algebraically closed fields.

K is called alg. closed if for all $f \in K(x)$, f factors into linear terms in $K[x]$.

K/F is an alg. closure of F if K is alg. closed extension of F.

- Every F has an alg. closure $\overline{F}/F$.

Ex:

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

  roots are $\pm i$.

Splitting field over $\mathbb{Q}$ is $\mathbb{Q}(i)$.

Splitting field over $\mathbb{Q}(i)$ is $\mathbb{Q}(i)$.

- $(x^2-2)(x^2-3) \in \mathbb{Q}[x]$

  roots $\pm\sqrt{2}, \pm\sqrt{3}$

Splitting field contains $\sqrt{2}, \sqrt{3}$

$\Rightarrow$ contains $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

other conjugate is also

Clear

$\Rightarrow$ $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is splitting field.

over $\mathbb{Q}$.

Similarly see $\mathbb{Q}(\sqrt{2},\sqrt{3})$

is S.f. over $\mathbb{Q}(\sqrt{2})$.

- $x^4+4 \in \mathbb{Q}[x]$

$$x^4+4 = (x^2+2x+2)(x^2-2x+2)$$

roots: $\pm 1 \pm i$

Splitting field: $\mathbb{Q}(i)$.

$f \in F[x]$ w/ roots

$r_1, \dots, r_n$.

$F(r_1, \dots, r_n)$ ← btwn the roots

In general, there are alg. relations

Ex: What is the degree of S.f. of $x^4 - 10x^2 + 1$ over $\mathbb{Q}$?

$r = x^2$ $\qquad r^2 - 10r + 1 = 0$

$r^2 = 5 \pm 2\sqrt{6}$ $\qquad \alpha = 5 + 2\sqrt{6}$

$r = \pm\sqrt{5 \pm 2\sqrt{6}}$ $\qquad \beta = 5 - 2\sqrt{6}$

S.f. $\mathbb{Q}(\sqrt{\alpha}, \sqrt{\beta})$

Are there any algebraic relations between $\sqrt{\alpha}$ and $\sqrt{\beta}$?

$\alpha\beta = 1$ so $\beta = 1/\alpha$

So s.f. is $\mathbb{Q}(\sqrt{\alpha})$. What is $[\mathbb{Q}(\sqrt{\alpha}) : \mathbb{Q}]$?

$\alpha = 5 + 2\sqrt{6}$

$\mathbb{Q}(\sqrt{\alpha})$

$1 \leq 2$

$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{6})$

$1 \quad 2$

$\mathbb{Q}$

$\sqrt{\alpha}$ is root of $X^2 - (5+2\sqrt{6})$

$\in \mathbb{Q}(\alpha)[X]$.

degree of top extension is 2

$\Longleftrightarrow \sqrt{\alpha} \notin \mathbb{Q}(\alpha)$.

$\sqrt{\alpha} \in \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{6})$

$\sqrt{\alpha} = a + b\sqrt{6} \quad a, b \in \mathbb{Q}$

$5 + 2\sqrt{6} = a^2 + 6b^2 + 2ab\sqrt{6}$

$$\begin{cases} 5 = a^2 + 6b^2 \\ 1 = ab \end{cases}$$

$a = \frac{1}{b}$ $\qquad 5 = \frac{1}{b^2} + 6b^2$

$\Rightarrow \quad 6b^4 - 5b^2 + 1 = 0$

So b is rational root of

$x^4 - 5x^2 + 1$. Can check

directly via rational root test

that this has no rational

roots

$\Rightarrow$ no sol^n to system

$\Rightarrow \quad \sqrt{a} \notin \mathbb{Q}(a)$.

$\Rightarrow \quad [\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 4.$

Ex: $p(x) = x^4 - 2 \in \mathbb{Q}[x]$

p has roots

$$\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i$$

Splitting field is $\mathbb{Q}(\sqrt[4]{2}, i)$

$\subseteq$

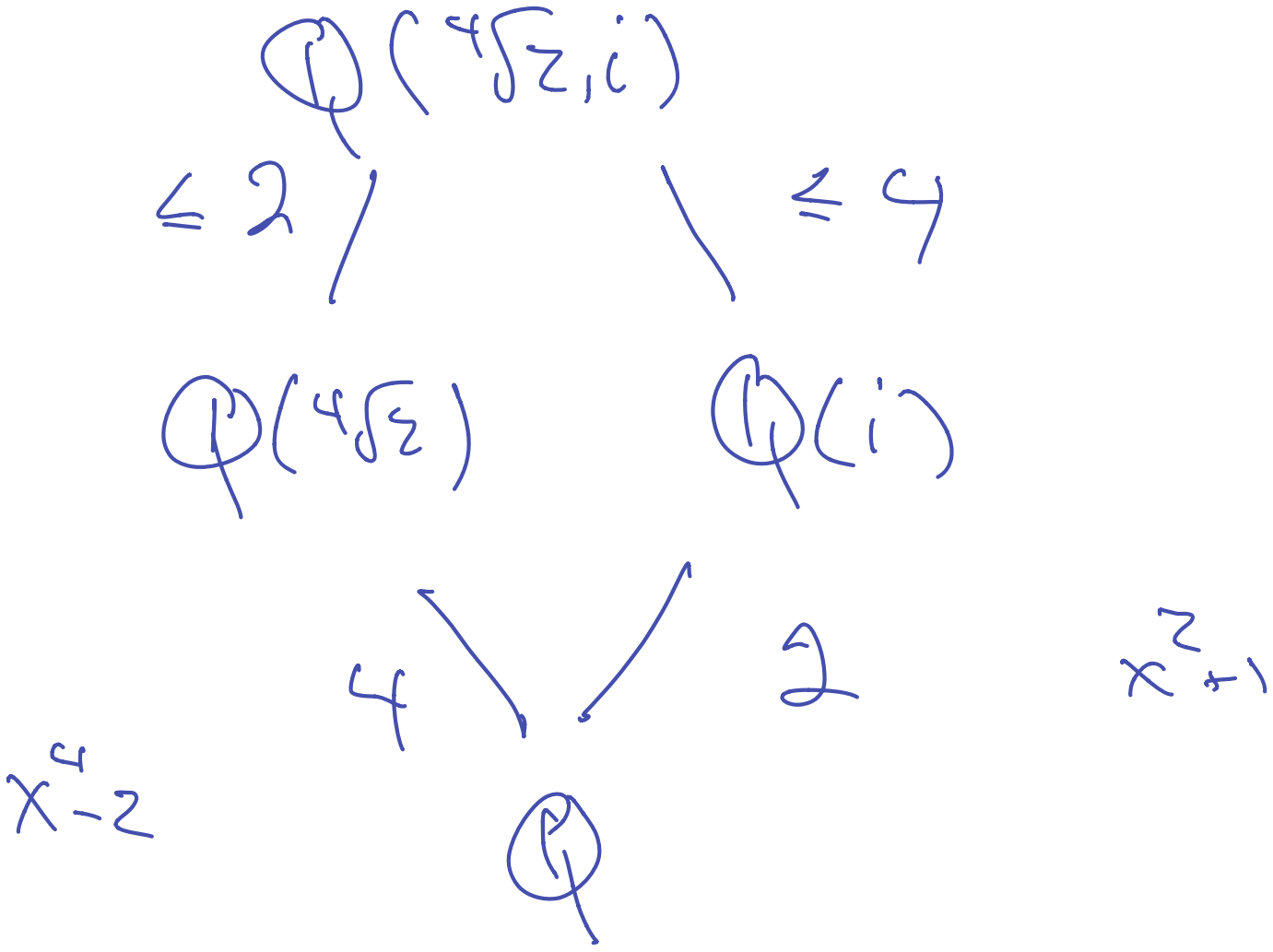
S.f. contains

$\sqrt[4]{2}, \sqrt[4]{2}i \Rightarrow$

contains $\frac{\sqrt[4]{2}i}{\sqrt[4]{2}} = i.$

$\Rightarrow$ contains

$\mathbb{Q}(\sqrt[4]{2}, i)$.



$$\left[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})\right] = 2$$

b/c $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$

and $i \notin \mathbb{R}$.

So $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ has

degree 8.

What is a S.f. of $x^4 - 2$ over $\mathbb{F}_3$?

First, factor over $\mathbb{F}_3[x]$.

Can see no roots in $\mathbb{F}_3$ by inspection. So if factors, must be two quadratics.

Irred. quadratic in $\mathbb{F}_3[x]$:

- x^2+x+1
- x^2+x+2
- x^2+2x+2

$$x^4-2 = (x^2+x+2)(x^2+2x+2)$$

note that if σ is a root of a quadratic in some field, then the other root is also contained in field.

Let α be a root of x^2+x+2. β be a root of x^2+2x+2.

$\mathbb{F}_3(\alpha, \beta)$. Note: 2α is a root of x^2+2x+2

sf is $\mathbb{F}_3(\alpha)$ and $\mathbb{F}_3(\alpha)/\mathbb{F}_3$ has degree 2.

Note: $\mathbb{F}_3(\alpha)$ is a field of size $3^2 = 9$.

Things I didn't have time for:

if F is alg closed then F must be infinite. If $a_1, \ldots, a_n$ are elements of F, then $(x-a_1)\cdots(x-a_n)+1$ has no roots in F, $\Rightarrow\Leftarrow$.

F alg closed.

$$\left\{\begin{matrix}\text{points of} \\ F\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{maximal} \\ \text{ideals} \\ \text{of } F[x]\end{matrix}\right\}$$

$$a \longleftrightarrow (x-a)$$

In general

$$\left\{\begin{matrix}\text{Points of} \\ F^n\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{maximal} \\ \text{ideals of} \\ F[x_1,\dots,x_n]\end{matrix}\right\}$$

$$(a_1,\dots,a_n) \longleftrightarrow (x_1-a_1,\dots,x_n-a_n)$$

"Weak Nullstellensatz"

Ex: $x^3+x^2+1 \in \mathbb{F}_2[x]$

is irred b/c no root in $\mathbb{F}_2$. Let α be a root in an extension field

$\mathbb{F}_2(\alpha)$ $\quad \alpha^3+\alpha^2+1=0$

$\Big| 3 \quad \Rightarrow \alpha^3 = \alpha^2+1$

$\mathbb{F}_2$

The map $\sigma: \mathbb{F}_2[x] \to \mathbb{F}_2[x]$ given by $\sigma(p) = p^2$

is a ring hom. b/c Squaring is additive in field of char 2 and $c^2 = c$ for $c \in \mathbb{F}_2$.

In fact, we have

$$p(x)^2 = p(x^2).$$

$$p(\alpha)^2 = 0 \implies p(\alpha^2) = 0$$

$$p(\alpha^2)^2 = 0 \implies p(\alpha^4) = 0$$

Roots: $\alpha, \alpha^2, \alpha^4 = \alpha \cdot \alpha^3$

$$= \alpha, \alpha^2, \alpha^2 + \alpha + 1$$

So $\mathbb{F}_2(\alpha)$ is a s.f. of x^3+x^2+1 over $\mathbb{F}_2[x]$.