## Contact:

Email: tsmits@math.ucla.edu

OH: Tues. 11:30 - 12:30
Th. 5:30 - 6:30

Website: can get to via CCLE.

## Field Extensions

$L/F$ $\quad \begin{array}{c} L \\ | \\ F \end{array}$ is a field extension

if $F \subset L$ are both fields.
($F$ subfield of $L$)

Main point: $L$ is an $F$-vector space via multiplication.

The degree of $L$ over $F$

$$[L:F] := \dim_F L.$$

The characteristic of a field $F$ is the smallest pos integer $n$ s.t.

$$n \cdot 1 = 0.$$

$\mathrm{char}(F) = 0$ if no such $n$ exists

if $\mathrm{Char}(F) > 0$ then $\mathrm{char}(F) = p$ for some prime $p$.

Ex: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ char $0$

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ finite char $p$

$\mathbb{F}_p(t)$ = rational functions in $t$

infinite field of char p.

$L/F$ $\alpha \in L$. $\alpha$ is algebraic
if $p(\alpha) = 0$ for some $p \in F[x]$.

$L/F$ is algebraic if all elts
are algebraic.

Otherwise, extension is transcendental.

Lecture Recap: $\alpha$ algebraic

- $\exists!$ monic irred. $m_\alpha \in F[x]$
with $m_\alpha(\alpha) = 0$ called minimal poly.
of $\alpha$.

- $m_\alpha(x) \mid p(x)$ for any $p(x) \in F[x]$ w/ $p(\alpha) = 0$.

$F(\alpha) =$ F-span of $\alpha$.

if $\alpha \in L$, $L/F$, then $F(\alpha)$ is smallest subfield of $L$ containing $F$ and $\alpha$.

- $[F(\alpha):F] =$ deg $m_\alpha = n$.

Basis is given by

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

Ex: • $\mathbb{C} = \mathbb{R}(i)$

$m_i = x^2+1 \in \mathbb{R}[x]$

$\mathbb{C}$ has basis $\{1, i\}$ as an $\mathbb{R}$-v.s.

• $\mathbb{Q}(\sqrt{2})$ $\quad m_{\sqrt{2}} = x^2-2 \in \mathbb{Q}[x]$

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

basis $\{1, \sqrt{2}\}$.

if we view $\sqrt{2} \in \mathbb{R}$

$m_{\sqrt{2}} = x - \sqrt{2} \in \mathbb{R}[x]$

i.e. $\mathbb{R}(\sqrt{2}) = \mathbb{R}$.

• For any $n>0$, $x^n-2 \in \mathbb{Q}[x]$ is Eisenstein at 2 $\Rightarrow$ irred.

$[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$

basis $\{1, \sqrt[n]{2}, \sqrt[n]{4}, \ldots\}$

---

How to compute minimal polynomial?

- Algebraic manipulations
- Use linear algebra.

$\alpha \in L/F$

$T_\alpha : L \to L$ F-linear map

$x \mapsto \alpha x$

Turns out that

$m_\alpha = m_{T_\alpha}$ (in the linear algebra sense)

In particular, $m_{T_\alpha} \mid c_{T_\alpha}$

so we can quickly get candidate minimal polynomials.

Ex: $\mathbb{C}/\mathbb{R}$ $\alpha = 2+3i$

What is $m_\alpha$?

$$\alpha - 2 = 3i$$
$$(\alpha-2)^2 = -9$$

$\alpha^2 - 4\alpha + 13 = 0$

$m_\alpha \mid x^2 - 4x + 13 \in \mathbb{R}[x]$

irred b/c no real root

$\Longrightarrow$

$m_\alpha = x^2 - 4x + 13.$

Alt: let's compute $T_\alpha$.

$\mathbb{C}/\mathbb{R}$ has basis $\{1, i\}$

$T_\alpha(1) = \alpha = 2 + 3i$

$T_\alpha(i) = \alpha i = -3 + 2i$

$$[T_\alpha] = \begin{pmatrix} 2 & -3 \\ 3 & 2 \end{pmatrix}$$

$C_{T_\alpha} = x^2 - 4x + 13.$

Same as before shows

$C_{T_\alpha}$ is irred w/ $\alpha$ as a root

$\implies$ equals $m_\alpha$.

In particular, this computation shows that

$$[\mathbb{R}(\alpha):\mathbb{R}] = 2$$

$$2\left(\begin{array}{l} \mathbb{C} \\ \mid \\ \mathbb{R}(\alpha) \\ \mid \cdot 2 \\ \mathbb{R} \end{array}\right.$$

i.e. $\mathbb{R}(\alpha) = \mathbb{C}$

as expected.

Ex: $\alpha = 1 + \sqrt[3]{2} + \sqrt[3]{4}$

What is the degree of $\mathbb{Q}(\alpha)/\mathbb{Q}$?

$m_\alpha$?

View $\alpha \in \mathbb{Q}(\sqrt[3]{2})$.

$$\begin{tikzcd} \mathbb{Q}(\sqrt[3]{2}) \arrow[d, dash] \\ \mathbb{Q}(\alpha) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has degree 3 b/c $x^3 - 2 \in \mathbb{Q}[x]$ is irred.

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ over $\mathbb{Q}$.

What is $T_\alpha$?

$$T_\alpha(1) = \alpha = 1 + \sqrt[3]{2} + \sqrt[3]{4}$$

$$T_\alpha(\sqrt[3]{2}) = 2 + \sqrt[3]{2} + \sqrt[3]{4}$$

$$T_\alpha(\sqrt[3]{4}) = 2 + 2\sqrt[3]{2} + \sqrt[3]{4}$$

$$[T_\alpha] = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}$$

$$c_{T_\alpha} = x^3 - 3x^2 - 3x - 1$$

Note $c_{T_\alpha}$ has an Eisenstein translate at 1, i.e.

$c_{T_\alpha}(x+1)$ is Eisenstein

So $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ b/c found irred. poly of degree 3 that kills $\alpha$ (i.e. $c_{T_\alpha} = m_\alpha$ !)

and in particular,

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2})$$

Not obvious how to show equality without a degree argument.

---

Examples I didn't get to in discussion:

$$\begin{array}{c} L \\ | \\ K \\ | \\ F \end{array}$$

tower of fields

$$[L:F] = [L:K][K:F]$$

Ex: $\mathbb{Q}(\sqrt[6]{2})$

$$6\left\{\begin{array}{c} \mathbb{Q}(\sqrt[6]{2}) \\ \big|\ 3 \\ \mathbb{Q}(\sqrt{2}) \\ \big|\ 2 \\ \mathbb{Q} \end{array}\right.$$

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

$m_{\sqrt[6]{2}} = x^6 - 2 \in \mathbb{Q}[x]$

$\Rightarrow [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3.$

Note $\sqrt[6]{2}$ is a root of

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

$\Rightarrow$ equals min. poly of $\sqrt[6]{2}$ over $\mathbb{Q}(\sqrt{2})$

(b/c has same degree as min. poly!)

Not immediately clear that $x^3 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$ is irred.

This shows how field theory can show polynomials are irred.

<u>Ex:</u> $\alpha$ root of $x^3 - 6x^2 + 9x + 3 \in \mathbb{Q}[x]$

Eisenstein at 3

$$\begin{array}{c} \mathbb{Q}(\alpha) \\ \Big| \, 3 \\ \mathbb{Q} \end{array}$$

Note $\sqrt{2} \notin \mathbb{Q}(\alpha)$

b/c $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

and $2 \nmid 3$.

Showing $\sqrt{2}$ isn't in the span of $\{1, \alpha, \alpha^2\}$ directly is hard!!

Ex: $\alpha = \sqrt{3+2\sqrt{2}}$ what is $[\mathbb{Q}(\alpha):\mathbb{Q}]$?

$\alpha^2 = 3+2\sqrt{2} \implies \alpha$ is root of
$x^2-(3+2\sqrt{2}) \in \mathbb{Q}(\sqrt{2})[x]$

$\mathbb{Q}(\alpha)$

$|\ \leq 2$

$\mathbb{Q}(\sqrt{2})$

$|\ 2$

$\mathbb{Q}$

So $\mathbb{Q}(\alpha)/\mathbb{Q}$ has degree 2 or 4.

Top ext^n has degree 1 $\iff$
$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2})$, i.e. $\alpha \in \mathbb{Q}(\sqrt{2})$.

Want to solve

$\alpha = a + b\sqrt{2}$ $\quad a, b \in \mathbb{Q}$

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

$\Rightarrow \begin{cases} 3 = a^2 + 2b^2 \\ 1 = ab \end{cases}$

take $a = b = 1$.

Note that $(1+\sqrt{2})^2 = 3 + 2\sqrt{2}$ is indeed true, so actually we have $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2})$

so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.

Note: $\alpha$ satisfies $\alpha^4 - 6\alpha^2 + 1 = 0$ by manipulation. What we did show $x^4-6x^2+1$ is

reducible in $\mathbb{Q}[x]$. Not at

all obvious!