Week 9

Constructing fields "from bottom up" start with F

Tomorrow: constructing fields "from top down" start with $F \subseteq E$ (big field)

Proposition: Suppose F is a field and $f(x) \in F[x]$ is irreducible

Then let $E = F[x]/\langle f(x)\rangle$ and let $\alpha = x + \langle f(x)\rangle \in E$

Then

1. E is a field
2. The composition $F \underset{\text{injection}}{\hookrightarrow} F[x] \underset{\text{surjection}}{\twoheadrightarrow} F[x]/\langle f(x)\rangle = E$ — the whole thing is an injection
3. As an F-vector space, the set $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a basis for E where $n = \deg(f)$

   $\Rightarrow E = \{c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1} : c_j \in F\}$

4. The field injection $F \hookrightarrow E$ induces a ring injection

   $F[x] \hookrightarrow E[x]$

   we identify $f(x) \in F[x]$ with its image in $E[x]$

   then $f(\alpha) = 0$ in E

5. For mult. in E:

   given $\beta, \gamma \in E$ to compute $\beta\gamma$ (and write it in terms of the basis)

option #1: Use division

write $\beta = g(x) + \langle f(x)\rangle$ $\quad \gamma = h(x) + \langle f(x)\rangle$

then $\beta\gamma = g(x)h(x) + \langle f(x)\rangle$

Divide this product by $f(x)$ to get remainder $r(x)$

$\Rightarrow \beta\gamma = r(x) + \langle f(x)\rangle = r(\alpha)$

option #2: Stick with α's

write $\beta = \underbrace{c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1}}_{g(\alpha)}$ $\quad \gamma = \underbrace{d_0 + d_1\alpha + \dots + d_{n-1}\alpha^{n-1}}_{h(\alpha)}$

multiply $\beta\gamma = c_0d_0 + (c_0d_1 + c_1d_0)\alpha + \dots + c_{n-1}d_{n-1}\alpha^{2n-2}$

then use $\underbrace{\text{key property}}_{f(\alpha)=0}$ to reduce all powers $\geq n$

Ex: 1 $f(x) = x^2 - 2$ in $\mathbb{Q}[x]$

irred in $\mathbb{Q}[x]$? Yes

$E = \mathbb{Q}[x]/\langle x^2-2\rangle = \{c_0 + c_1\alpha : c_0, c_1 \in \mathbb{Q}\}$ and $\alpha^2 - 2 = 0 \Rightarrow \alpha^2 = 2$

Do NOT write $\alpha = \sqrt{2}$

lets multiply two random elements

$\beta = 3+5\alpha \qquad \gamma = 1+10\alpha$

option #1: $\beta = 3+5x + \langle x^2-2\rangle \qquad \gamma = 1+10x + \langle x^2-2\rangle$

multiply $(3+5x)(1+10x) = 3+35x+50x^2$

$\beta\gamma = 3+35x+50x^2 + \langle x^2-2\rangle = 3+35\alpha+50\alpha^2$

Divide

$$\begin{array}{r} 50 \\ x^2-2 \enclose{longdiv}{50x^2+35x+3} \\ 50x^2+0x-100 \\ \hline 35x+103 \end{array}$$

$\Rightarrow \quad \beta\gamma = 103+35x+\langle x^2-2\rangle$
$= 103+35\alpha$

option #2: $\beta\gamma = (3+5\alpha)(1+10\alpha)$
$= 3+35\alpha+50\alpha^2$ and $\alpha^2 = 2$
$= 103+35\alpha$

example 2: $f(x) = x^2+1$ in $\mathbb{R}[x]$

Q: irred. in $\mathbb{R}[x]$?

A: no real roots, so yep

$E = \mathbb{R}[x]/\langle x^2+1\rangle = \{c_0+c_1\alpha : c_0, c_1 \in \mathbb{R}\}$ key property $\alpha^2+1=0$ in E

compare to $\mathbb{C} = \{a+bi : a, b \in \mathbb{R}\}$ with $i^2 = -1$

Ex: 3: $f(x) = x^2+1$ in $\mathbb{Q}[x]$

irred in $\mathbb{Q}[x]$

$\rightarrow E' = \mathbb{Q}[x]/\langle x^2+1\rangle = \{c_0+c_1\alpha : c_0, c_1 \in \mathbb{Q}\}$ with $\alpha^2+1=0$

and $E' \cong \mathbb{Q}(i) = \mathrm{Frac}(\mathbb{Q}[i])$ $\quad \not\cong \mathbb{C}$

Ex 4: $f(x) = x^3-2$ in $\mathbb{Q}[x]$

irred: Yep (Eisenstein $p=2$)

$E = \mathbb{Q}[x]/\langle x^3-2\rangle = \{c_0+c_1\alpha+c_2\alpha^2 : c_1, c_2, c_0 \in \mathbb{Q}\}$

$\alpha^3 - 2 = 0 \qquad \alpha^3 = 2$

Ex 5: $f(x) = x^3-2$ in $\mathbb{R}[x]$

irred.? no, $\sqrt[3]{2}$ is a root of this $\quad x-\sqrt[3]{2}$ is a factor of $f(x)$

Example of mult in Ex 4:

$\beta = 1+3\alpha^2 \quad \gamma = 3+\frac{5}{2}\alpha$

$$\beta\gamma = (1+3\alpha^2)(3+\tfrac{5}{2}\alpha)$$
$$= 3+\tfrac{5}{2}\alpha+9\alpha^2+\tfrac{15}{2}\alpha^3$$

use $\alpha^3 = 2$

$$= 3+\tfrac{5}{2}\alpha+9\alpha^2+\tfrac{15}{2}2$$
$$= 18+\tfrac{5}{2}\alpha+9\alpha^2$$

Ex 6: $f(x) = x^2+x+1$ in $\mathbb{Z}_2[x]$

irred? Yes

$$E = \mathbb{Z}_2[x]/\langle x^2+x+1\rangle = \{c_0+c_1\alpha : c_0, c_1 \in \mathbb{Z}_2\}$$

with $\alpha^2+\alpha+1 = 0$

$= \{0, 1, \alpha, 1+\alpha\}$ four elements

Ex: $(1+\alpha)(1+\alpha) = 1+\underbrace{2\alpha}_{=0}+\alpha^2 = 1+\alpha+1$ $\quad (\alpha^2 = -\alpha-1 = \alpha+1)$

$= \alpha$

Today: Top down field construction

Start with: field hom. $F \hookrightarrow E$

and element $\alpha \in E$

There is a field L with the following universal property

① $F \hookrightarrow L \hookrightarrow E$ ("intermediate" field)

② $\alpha \in L$

③ L is the "smallest" such field

Construction (unhelpful)

let $F' \subseteq E$ be the image of F in E

then $L = \bigcap_{\substack{F' \subseteq M \subseteq E \\ \alpha \in M}} M$ would do it, so L is smallest sub-field of E that contains F and α

Notation: we call that field "F adjoin α" and denote

$F(\alpha)$

Ex 1 $\mathbb{Q} \to \mathbb{R}$

$\frac{1}{2} \in \mathbb{R}$ and $\mathbb{Q}(\frac{1}{2}) = \mathbb{Q}$ b/c $\frac{1}{2} \in \mathbb{Q}$ already

Ex 2: $\mathbb{Q} \to \mathbb{R}$ $\quad \sqrt{2} \in \mathbb{R}$ and $\mathbb{Q}(\sqrt{2})$ = smallest subfield containing $\mathbb{Q}$ and $\sqrt{2}$

More generally, for any subset $S \subseteq E$, still define

$F(S)$ = smallest subfield of E with F and S

Ex 3: $\mathbb{Q} \to \mathbb{R}$ $\quad \sqrt{2}, \sqrt{3} \in \mathbb{R} \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$ = smallest subfield of $\mathbb{R}$ containing $\sqrt{2}, \sqrt{3}, \mathbb{Q}$

can show $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$ (can do it one at a time)

more surprising $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$

Q: What does $F(\alpha)$ look like?

"Clever idea" Given $F \hookrightarrow E$ and $\alpha \in E$

look @ $ev_\alpha : F[x] \to E$

$p(x) \mapsto p(\alpha)$

FACT: recall our notation $\operatorname{im}(ev_\alpha) = F[\alpha] = \{c_0 + c_1\alpha + \dots + c_n\alpha^n : c_j \in F\}$

$F[\alpha]$ is the smallest sub-ring of E that containing F and α

(integral domain!)

Consequence: $\operatorname{Frac}(F[\alpha])$ = smallest subfield of E that contains F and α

Notice: 1) ev_α injective $\iff$ the only polynomial with $p(\alpha)=0$ is zero polynomial

↳ we say α is <u>transcendental</u> over F if α is not the root of any nonzero polynomial

($\iff$ ev_α is injective)

<u>Transcendental case</u>: Suppose $F \hookrightarrow E \ni \alpha$ and α transcendental over F

then ① $F(\alpha) = \operatorname{Frac}(F[\alpha])$

② α transcendental over $F \Rightarrow \operatorname{Ker}(ev_\alpha)$ trivial $\Rightarrow \underbrace{F[\alpha]}_{\operatorname{im}(ev_\alpha)} \cong \underbrace{F[x]}_{\text{domain}}$

$F(\alpha) \cong \operatorname{Frac}(F(\alpha)) = F(x) = \left\{ \frac{f(x)}{g(x)} : f,g \in F[x],\ g \neq 0 \right\}$

Ex 4: Fact: π and e are transcendental over $\mathbb{Q}$

$$\mathbb{Q}(\pi) = \left\{ \frac{c_0 + c_1\pi + c_2\pi^2 + \dots + c_n\pi^n}{d_0 + d_1\pi + d_2\pi^2 + \dots + d_n\pi^n} : c_i, d_i \in \mathbb{Q} \right\} \cong \mathbb{Q}(x)$$

$$\mathbb{Q}(e) = \left\{ \frac{c_0 + c_1 e + \dots + c_n e^n}{d_0 + d_1 e + \dots + d_n e^n} : c_i, d_j \in \mathbb{Q} \right\} \cong \mathbb{Q}(x)$$

Case 2: ev_α not injective $\iff \operatorname{Ker}(ev_\alpha)$ nontrivial

$\iff$ there are nonzero polynomials $p(x) \in F[x]$ with $p(\alpha)=0$

$\iff$ Def: α is <u>algebraic</u> over F if there is some nonzero $p(x) \in F[x]$ such that $p(\alpha)=0$

Ex 5: $\alpha = \sqrt{2}$ in $\mathbb{Q}$: root of $x^2 - 2 = f(x) \in \mathbb{Q}[x]$

for $\alpha = \sqrt{2}$ over $\mathbb{R}$: root of $x^2 - \sqrt{2} \in \mathbb{R}[x]$

better/smaller root of $g(x) = x - \sqrt{2} \in \mathbb{R}[x]$

Suppose $\alpha \in E$ alg over F

① $F(\alpha) = \text{Frac}(F[\alpha])$

② 1^{st} isomorphism thm.

$$ev_\alpha : F[x] \to F$$

$$\Rightarrow F[\alpha] = \text{im}(ev_\alpha) \simeq F[x] / \ker(ev_\alpha)$$

③ $F[x]$ is a Euclidean domain $\Rightarrow$ PID

$\Rightarrow \ker(ev_\alpha)$ is principle $\Rightarrow \ker(ev_\alpha) = \langle p(x) \rangle$

so $p(\alpha) = 0$ and if $f \in F[x]$ with $f(\alpha) = 0$, then $f(x) = g(x) p(x)$ for some $g(x) \in F[x]$

Let us choose the unique <u>monic</u> polynomial generator, call it the <u>minimal polynomial for α over F</u>

denote $m_{\alpha, F}(x) \in F[x]$ easy exercise: irreducible in $F[x]$

<u>So</u> $F[\alpha] \simeq F[x] / \langle m_{\alpha,F}(x) \rangle$ already a field! (from yesterday)

so $F(\alpha) \simeq F[x] / \langle m_{\alpha,F}(x) \rangle$ (Know that the elements look like)

$F(\alpha) = \{ c_0 + c_1 \alpha + \dots + c_{n-1} \alpha^{n-1} : c_i \in F \}$ where $n = \deg(m_{\alpha,F}(x))$

<u>Ex 6</u>: $\sqrt{2}$ over $\mathbb{Q}$ root of $f(x) = x^2 - 2$

$x^2 - 2$ irreducible over $\mathbb{Q}[x]$? yes

$\Rightarrow m_{\sqrt{2}, \mathbb{Q}}(x) = x^2 - 2$

$\mathbb{Q}(\sqrt{2}) = \{ c_0 + c_1 \sqrt{2} : c_0, c_1 \in \mathbb{Q} \}$

Ex 7: $\sqrt[4]{2}$ over $\mathbb{Q}$ $f(x) = x^4 - 2 \in \mathbb{Q}[x]$

$x^4 - 2$ irreducible? yes (Eisenstein)

$\Rightarrow \mathbb{Q}(\sqrt[4]{2}) = \{ c_0 + c_1 \sqrt[4]{2} + c_2 (\sqrt[4]{2})^2 + c_3 (\sqrt[4]{2})^3 : c_1, c_0, c_2, c_3 \in \mathbb{Q} \}$

Ex 8: $\sqrt[4]{2}$ over $\mathbb{Q}(\sqrt{2})$?

root of $f(x) = x^4 - 2$

f irred in $\mathbb{Q}(\sqrt{2})$? no. $x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2})$

but we don't have $\sqrt[4]{2}$ in $\mathbb{Q}(\sqrt{2})$, $m_{\sqrt[4]{2}, \mathbb{Q}(\sqrt{2})}(x) = x^2 - \sqrt{2}$

For a field extension $F \hookrightarrow E$, if we view E as an F vector space the dimension of E as an F vector space is called the <u>degree</u> of E over F and is denoted $[E:F]$

We say, the extension is <u>finite</u> if $[E:F]<\infty$ (danger: finite field extension does not mean both fields are finite)

Ex: $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2})$ $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2 \Rightarrow$ finite

$\mathbb{Q} \hookrightarrow \mathbb{Q}(\pi)$ $[\mathbb{Q}(\pi):\mathbb{Q}]=\infty$ ($\{1,\pi,\pi^2,\dots\}$ is lin. independent b/c π transcendental over $\mathbb{Q}$)

$\mathbb{Q} \hookrightarrow \mathbb{R}$ is infinite extension

We say the extension is <u>algebraic</u> over F if every $\alpha \in E$ is algebraic over F

<u>Ex</u>: $\underset{\text{algebraic}}{\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3})}$ vs. $\mathbb{Q} \hookrightarrow \mathbb{R}$ not algebraic

we say the extension is simple if there is some $\alpha \in E$ such that $E=F(\alpha)$

(Usually: $F \hookrightarrow F(\alpha) \hookrightarrow E$)

Ex: $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3})$ b/c $\mathbb{Q}(\sqrt{2}+\sqrt{3})$

<u>What we know</u>: For $F \hookrightarrow E$ and $\alpha \in E$ alg/F with minimal poly $m_{\alpha,F}(x)$

$$\begin{tikzcd}
E \ni \alpha \\
F(\alpha) \cong F[x]/\langle m_{\alpha,F}(x)\rangle \arrow[u] \\
F \arrow[u]
\end{tikzcd}$$

(smallest subfield of E containing α, F)

So: $\mathcal{B}=\{1,\alpha,\dots,\alpha^{n-1}\}$ $n=\deg(m_{\alpha,F}(x))$ is a basis for $F(\alpha)$

$F(\alpha)=\{c_0+c_1\alpha+\dots+c_{n-1}\alpha^{n-1} : c_i \in F\}$

key prop. $m_{\alpha,F}(\alpha)=0$ $[F(\alpha):F]=\deg(m_{\alpha,F}(x))$

Corollary: If α_1,α_2 are roots of same minimal poly $f(x)$

then $F(\alpha_1) \cong F(\alpha_2)$

$$\begin{array}{ccc} F(\alpha_1) & \cong & F(\alpha_2) \\ \wr\wr & & \parallel \\ F[x]/\langle f(x)\rangle & & F[x]/\langle f(x)\rangle \end{array}$$

Ex: $\mathbb{Q}(\sqrt[4]{3}) \cong \mathbb{Q}(i\sqrt[4]{3})$ b/c both root of $f(x)=x^4-3$ over $\mathbb{Q}$

Computing degrees of extensions:

<u>The tower law</u>: If $F \hookrightarrow E$ and $E \hookrightarrow D$ are finite field extensions

then $[D:F]=[D:E][E:F]$

$$\begin{tikzcd}
D \\
E \arrow[u] \\
F \arrow[u]
\end{tikzcd}$$

If $\{\alpha_1, \dots, \alpha_n\}$ is a basis for E/F and $\{\beta_1, \dots, \beta_m\}$ is a basis for D/E then $\{\alpha_i \beta_j : 1 \le i \le n, 1 \le j \le m\}$ basis for D/F

Ex: ① $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2}, i)$

$\mathbb{Q}(\sqrt{2}, i)$ — i is a root of $f(x) = x^2+1$ monic irred. over $\mathbb{Q}(\sqrt{2})$ enough to have no roots in $\mathbb{Q}(\sqrt{2})$ roots are $\pm i \in \mathbb{C} \Rightarrow \pm i \notin \mathbb{Q}(\sqrt{2}) \Rightarrow$ no roots

$\uparrow_2$ basis $\{1, i\}$

$\mathbb{Q}(\sqrt{2})$ — $x^2 - 2 = m_{\sqrt{2},\mathbb{Q}}(x)$ basis: $\{1, \sqrt{2}\}$

$\uparrow_2$

$\mathbb{Q}$

basis for whole thing is $\{1, \sqrt{2}, i, \sqrt{2}i\}$

Ex ②: $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$

$\mathbb{Q}(\sqrt[3]{2})$ root of $x^3 - 2$ irred.? enough to show no roots

It is possible to show none of the roots are in $\mathbb{Q}(\sqrt{2})$

$\uparrow$

$\mathbb{Q}(\sqrt{2})$ basis $\{1, \sqrt{2}\}$

$\uparrow_2$

$\mathbb{Q}$

alternative approach:

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

$\uparrow_?$ $\sqrt{2}$ root of $f(x) = x^2 - 2$

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

$\uparrow$

$\mathbb{Q}$ — $m_{\sqrt[3]{2},\mathbb{Q}}(x) = x^3 - 2$

the last result told us that the degree of the whole thing is a multiple of 2

so this has to be a degree 2 extension

<u>Minimal polynomials</u>: For an element $\alpha \in E$, alg over F, it minimal polynomial of F is the unique $f(x) \in F[x]$

1) $f(\alpha) = 0$ 2) f is monic 3) f irreducible over $F[x]$

Note if $f(x)$ is any nonzero poly with $f(\alpha) = 0$, then min poly for α over F is one of the irreducible factors over $F[x]$

note that (3) is equivalent to $\deg(f) = [F(\alpha) : F]$

Ex: ③ $\alpha = \sqrt{3} + \sqrt{2}i$ over $\mathbb{Q}$

<u>Ad hoc method</u>: start with $\alpha = \sqrt{3} + \sqrt{2}i$

Do stuff (field operations) until you get only powers of α and rationals

$(\alpha - \sqrt{3})^2 = (\sqrt{2}i)^2 \Rightarrow \alpha^2 - 2\sqrt{3} + 3 = -2$

$(\alpha^2+5)^2 = (2\sqrt{3}\alpha)^2$

$\alpha^4 + 10\alpha^2 + 25 = 12\alpha^2$

$\alpha^4 - 2\alpha^2 + 25 = 0$ so $f(\alpha)=0$ $\quad f(x) = x^4 - 2x^2 + 25 \in \mathbb{Q}[x]$

Option 1: To conclude this is min poly

$\mathbb{Q}(\sqrt{2}, \sqrt{3}i) \overset{*}{=} \mathbb{Q}(\sqrt{2}+\sqrt{3}i)$

$2 \uparrow$

$\mathbb{Q}(\sqrt{3})$ $\quad$ so degree of extension is 4 so

$2 \uparrow$ $\quad$ $[\mathbb{Q}(\sqrt{3}+\sqrt{2}i) : \mathbb{Q}] = 4$ so $f(x)$ is minimal

$\mathbb{Q}$

Linear algebra method:

Have a basis for $\mathbb{Q}(\sqrt{3}, \sqrt{2}i)$ over $\mathbb{Q}$

$B = \{\underset{v_1}{1}, \underset{v_2}{\sqrt{3}}, \underset{v_3}{\sqrt{2}i}, \underset{v_4}{\sqrt{6}i}\}$

Idea: The $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ must be a $\mathbb{Q}$ linearly dependent set $c_0 1 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 + c_4\alpha^4 = 0$ for some $c_i \in \mathbb{Q}$

write each of the 5 elements $1, \alpha, \alpha^2, \dots, \alpha^4$ in terms of basis

$1 = 1v_1$ $\quad [1] = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

$\alpha = 0v_1 + 1v_2 + 1v_3 + 0v_4 = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$

Then compute null space of the matrix $([1], [\alpha], [\alpha^2], [\alpha^3], [\alpha^4])$