Extension fields (Friedman & splitting fields, Rotman) lecture 9

$F \subset E$ field extension $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{R} \subset \mathbb{C}$

subfield field

$F \subset E$, choose $\alpha \in E$. Have a homomorphism $ev_\alpha : F[x] \to E$

$f(x) \longmapsto f(\alpha)$

$\mathrm{Im}\, ev_\alpha = F[\alpha]$ is a subring of E.

$ev_\alpha(f(x)) = f(\alpha)$

smallest subring that contains both F and α; integral domain since a subring of a field.

2 cases:

1) $\ker ev_\alpha = \{0\}$ injective map. if $f \in F[x]$, $f \neq 0 \Rightarrow f(\alpha) \neq 0$.

α is transcendental over F.

Example $\mathbb{Q} \subset \mathbb{R}$
Most real numbers, including π and e are transcendental over $\mathbb{Q}$
(only countably many real #'s are algebraic, not transcendental over $\mathbb{Q}$)

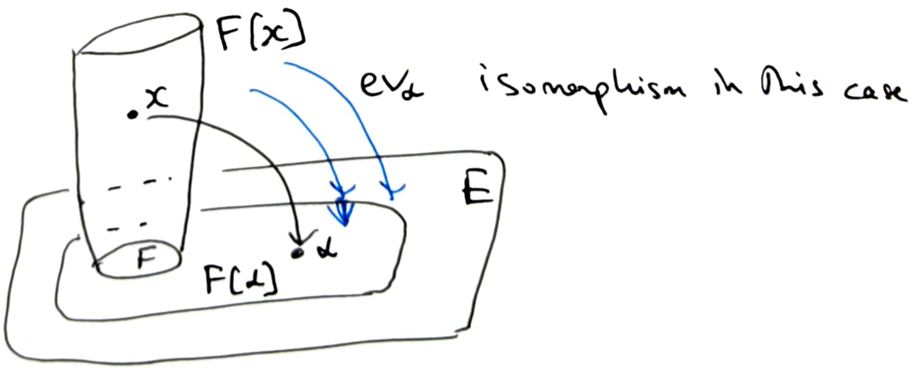
$\Rightarrow \mathrm{Im}\, ev_\alpha \simeq F[x]$

$F[\alpha] \simeq F[x]$

not a field

$F[x] \xrightarrow{\text{isomorphism}} F[\alpha] \subset E$

$x \longmapsto \alpha$



injective homomorphism

$F[x] \xrightarrow{ev_\alpha} E$

extends to a homomorphism

$F(x) \xrightarrow{\widetilde{ev}_\alpha} E$ of the field of fractions $F(x) = \mathrm{Frac}(F[x])$

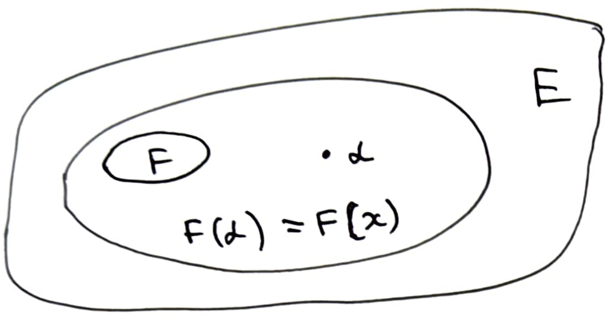
$\frac{f(x)}{g(x)} \in F(x)$ usual manipulation, coefficients in F $\qquad \frac{f(x)\cancel{r(x)}}{g(x)\cancel{r(x)}} = \frac{f(x)}{g(x)}$.

subfield

$F(x)$ is a field $\Rightarrow \widetilde{ev}_\alpha$ is injective, $F(x) \xrightarrow{\widetilde{ev}_\alpha} F(\alpha) \subset E$

Each transcendental element $\alpha \in E$ (transcendental over F)

generates a copy of $F(x)$, field of rational functions over F, in E



$F \subset F[\alpha] \subset F(\alpha) \subset E$

$\uparrow$

already infinite-dimensional over F

basis $\{1, \alpha, \alpha^2, \dots\}$ all powers of α

2) $\ker ev_\alpha \neq \{0\}$. $\exists$ a nonzero polynomial $f \in F[x]$, $f(\alpha) = 0$.

α is <u>algebraic</u> over F.

<u>Proposition</u> Let $F \subset E$ field extension, $\alpha \in E$ algebraic over F.

Then $\ker ev_\alpha = (p)$, $p \in F[x]$ an irreducible polynomial.

If $f \in F[x]$, $f(\alpha) = 0 \Rightarrow p \mid f$.

$ev_\alpha : F[x] \to E$ induces an isomorphism $\widehat{ev}_\alpha : F[x]/(p(x)) \longrightarrow F[\alpha]$

$\widehat{ev}_\alpha(x + (p)) = \alpha$. $F[\alpha] = \mathrm{Im}\, ev_\alpha$ is a field

<u>Proof</u> $\ker ev_\alpha$ is a nonzero ideal, principal.

By 1st isom theorem get induced isomorphism

$\widehat{ev}_\alpha : F[x]/\ker ev_\alpha \to F[\alpha]$, $F[\alpha] \cong F[x]/\ker ev_\alpha$

$x \xmapsto{ev_\alpha} \alpha$

$x + \ker ev_\alpha \xmapsto{\widehat{ev}_\alpha} \alpha$

$F[\alpha]$ integral domain $\Rightarrow$

$F[x]/\ker ev_\alpha$ integral domain

$\Rightarrow \ker ev_\alpha$ is a prime ideal $\Rightarrow$ max ideal

$\ker ev_\alpha = (p)$ $p \in F[x]$ irreducible

$f(\alpha) = 0 \iff f \in \ker ev_\alpha \iff p \mid f$

$F \subset E$ extension field, $\alpha \in E$ algebraic over F.

Define $F(\alpha) = F[\alpha]$.

$F(\alpha)$ is a subfield of E, smallest subfield that contains both F & α

α is "free" over F, no relations

$F \subset E, \alpha$ → α is transcendental, $F \subset F[\alpha] \subset F(\alpha) \subset E$ ← large field, $\simeq$ rational functions $\dfrac{f(\alpha)}{g(\alpha)}$.

→ α is algebraic, $F \subset F[\alpha] = F(\alpha) \subset E$

$F \subset F(\alpha)$ finite degree extension

$(p) = \ker ev_\alpha$

Can choose monic p.

denote $p = irr(\alpha, F)$

$p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ $\quad a_i \in F$

↑ monic

$\deg p(x) = n \Rightarrow \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a basis of field $F(\alpha)$

$[F(\alpha) : F] = n$

$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$ in E

lowest degree relation on α in E.

<u>lemma</u> (Friedman, lemma 1.4)

$F \subset E$ extension field, $\alpha \in E$. Suppose $p \in F[x]$ is an irreducible monic polynomial s.t. $p(\alpha) = 0$. Then $p = irr(\alpha, F)$.

<u>Example</u> 1) $x^2 - 2 = irr(\sqrt{2}, \mathbb{Q})$.

↑ monic, irreducible, $p(\sqrt{2}) = \sqrt{2}^2 - 2 = 0$.

$irr(\alpha, F)$ depends on F $\quad irr(\sqrt{2}, \mathbb{Q}(\sqrt{2})) = x - \sqrt{2}$

2) $irr(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$. no roots in $\mathbb{Q}$, since $\sqrt[3]{2}$ is irrational

3) $\sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \Rightarrow irr(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = x^2 - 3 = irr(\sqrt{3}, \mathbb{Q})$.

↑ exercise

<u>Prop</u> (degree formula, Rotman Lemma 49)

If $F \subset B \subset E$ fields, $[E:B]$, $[B:F]$ finite $\Rightarrow [E:F]$ is finite and

$$[E:F] = [E:B][B:F].$$

<u>Proof</u> $\{\alpha_1 \dots \alpha_m\}$ basis E/B, $\{\beta_1 \dots \beta_n\}$ basis B/F.

We'll show that $S = \{\beta_j \alpha_i \mid 1 \le i \le m,\ 1 \le j \le n\}$ is a basis of E/F.

1) S spans E. $\gamma \in E \Rightarrow \gamma = \sum_{i=1}^{m} b_i \alpha_i$, $b_i \in B$

$b_i = \sum_{j=1}^{n} c_{ij} \beta_j \Rightarrow$

$$\begin{array}{ccccc} F & \subset & B & \subset & E \\ \downarrow & & \downarrow & & \downarrow \\ c_{ij} & & b_i & & \gamma \end{array}$$

$\gamma = \sum_{i,j} c_{ij} \beta_j \alpha_i$.

2) Linear independence. Assume otherwise,

$$\begin{array}{cc} F & B \\ \downarrow & \downarrow \end{array}$$

$\sum c_{ij} \beta_j \alpha_i = 0$ for some $c_{ij} \in F$. $\Rightarrow b_i := \sum c_{ij} \beta_j \in B$.

$\{\alpha_i\}$ independent over B, $\sum_i \underset{\underset{B}{\cap}}{b_i} \alpha_i = 0 \Rightarrow b_i = 0\ \forall i$

$\Rightarrow \sum_j c_{ij} \beta_j = 0\ \forall i$, β_j independent $/F$ $\Rightarrow c_{ij} = 0.\ \forall i,j$ $\square$.

Example (Rotman, example 20, p. 54)

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$$
$$\underset{F}{\shortparallel} \qquad\qquad \underset{B}{\shortparallel} \qquad\qquad \underset{E}{\shortparallel}$$

$\sqrt{3}$ algebraic over $\mathbb{Q}$, $\mathrm{irr}(\sqrt{3}, \mathbb{Q}) = x^2 - 3 \Rightarrow \sqrt{3}$ algebraic over B.

$\mathrm{irr}(\sqrt{3}, B) \mid x^2 - 3. \Rightarrow [E : \mathbb{Q}(\sqrt{2})] \leq 2$

$[E : \mathbb{Q}(\sqrt{2})] = 2$, since $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

if $\sqrt{3} = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$ $\Rightarrow 3 = a^2 + 2ab\sqrt{2} + 2b^2 \Rightarrow$ since $\sqrt{2}$ is irrational come to contradiction

$\Rightarrow [E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$

$\alpha = \sqrt{2} + \sqrt{3}$. $\quad \alpha^2 = (\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6} \quad \alpha^2 - 5 = 2\sqrt{6}$

$\alpha^4 - 10\alpha^2 + 25 = 24 \qquad \underbrace{\alpha^4 - 10\alpha^2 + 1 = 0}_{\text{degree } 4.}$ will show soon that this polynomial is irr/$\mathbb{Q}$

$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset E$, $\quad \mathrm{irr}(\alpha, \mathbb{Q})$ has degree 4. $\Rightarrow E = \mathbb{Q}(\alpha)$

Alternative: $\mathbb{Q}(\alpha)$ contains 1, $\alpha = \sqrt{2} + \sqrt{3}$, $\alpha^2 = 5 + 2\sqrt{6} \Rightarrow \sqrt{6} \in \mathbb{Q}(\alpha)$

$\Rightarrow \sqrt{6}\alpha = 3\sqrt{2} + 2\sqrt{3} \in \mathbb{Q}(\alpha)$: $\sqrt{2} + \sqrt{3}, 3\sqrt{2} + 2\sqrt{3} \in \mathbb{Q}(\alpha) \Rightarrow$ any $\mathbb{Q}$-lin. comb. of $\sqrt{2}, \sqrt{3}$ $\in \mathbb{Q}(\alpha) \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. $\Rightarrow \mathrm{irr}(\alpha, \mathbb{Q})$ has degree 4, as claimed

$$\mathrm{irr}(\alpha, \mathbb{Q}) = \alpha^4 - 10\alpha^2 + 1.$$

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

1 8 28 56 70 56 28 8 1

9 36 84 126 126 84 36 9 1

— even

= div by 3

~ div. by 5

w div. by 7.

$$(a+b)^p = a^p + b^p \pmod p$$

$$\binom{p}{i} \equiv 0 \mod p \quad i = 1, 2, \dots, p-1$$

$\mathbb{F}_p \subset R \leftarrow$ commutative ring $\Rightarrow (a+b)^p = a^p + b^p$ in R

Fr or $\phi_p : R \longrightarrow R$ $\quad \phi_p(a) = a^p$ is a ring homomorphism $R \to R$ (endomorphism)

$\phi_p(a+b) = \phi_p(a) + \phi_p(b)$

$\phi_p(ab) = \phi_p(a)\phi_p(b)$

Exercise: if $F \supset \mathbb{F}_p$ is a finite field, Frobenius endomorphism $\phi_p : F \to F$ is bijective (an automorphism).