lect 9   Field extensions + wrap up char p from last time.

$\underline{F} \subset \underline{E}$ field extension
$ \underline{\overset{\cup\!\!|}{\alpha}}$

$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R} \subset \mathbb{C}$

$\phantom{\mathbb{Q} \subset} \overset{\shortparallel}{\mathbb{Q}[\sqrt{2}]} = \{a+b\sqrt{2}\}$

$F \subset E$
$ \overset{\cup\!\!|}{\alpha}$

$\underline{F(\alpha)}$ - smallest subfield of E contains both F and α.

$\underline{F[\alpha]}$ - polyn.

$\underline{ev_\alpha} : F[x] \longrightarrow E$

$f(x) \longmapsto \overset{\cup\!\!|}{f(\alpha)}$

$a_n x^n + \ldots + a_0 \quad a_i \in F$

$a_n \alpha^n + \ldots + a_0 \in E$, not in F.

$\alpha \in E$

subring, all polyn. in α coeff in F.

$\mathrm{Im}\ ev_\alpha = \underline{F[\alpha]} \subset \underline{E}$

x unrelated to E, $\alpha \in E \rightsquigarrow$ can get relation on α in E

$\underline{\ker ev_\alpha} \subset F[x]$ ideal

free case, no rel's on α in E

1) $\underline{\ker ev_\alpha = \{0\}}$. ev_α - injective. $\alpha \in E$.

$f \in F[x]$, $f \neq 0 \Rightarrow f(\alpha) = 0$

subring of E

$\underline{E} \supset \mathrm{Im}\ ev_\alpha \simeq F[x] \subset E$

not a field.

$R \xrightarrow{\varphi} S$

φ inj.

$\varphi(R) \simeq R$

$F[x] \xrightarrow[ev_\alpha]{\text{isom}} \underline{F[\alpha]} \subset E$

$x \longmapsto \alpha.$

α is transcendental over F (no rel's on α in E with coeff. in F).

$$\begin{tikzcd} \mathbb{Q} \arrow[d, phantom, "\shortparallel"] \arrow[r, phantom, "\subset"] & \mathbb{R} \arrow[d, phantom, "\shortparallel"] \\ F & \underline{E} \end{tikzcd}$$

countable   uncountable

most el's α of $\mathbb{R}$ are transcendental / $\mathbb{Q}$.

if α not transcendental.

$\Rightarrow$ some polyn. rel'n of α.

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

$\uparrow$ $\mathbb{Q}$ $\longrightarrow$

only countab'y many such polynomials

$\Rightarrow$ only countably many roots

$\underline{\pi, e}$

subring   field

α $F[\alpha] \subset E$ $\mathbb{Q}$ $\sqrt{2}$ $\pi, e.$

no polyn. relations on α

subring is integral domain.

$$\begin{tikzcd} \underline{F[\alpha]} \arrow[r, hook] & \underline{E} \\ \underline{F(\alpha)} \arrow[u, phantom, "\cap"] \arrow[ur, dashed] \end{tikzcd}$$

frac. field $F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; \frac{f}{g}\frac{r}{r} \sim \frac{f}{g} \right\}.$

$$\begin{tikzcd} F[x] \arrow[r, "ev_\alpha"] & \underline{E} \\ F(x) \arrow[u, phantom, "\cap"] \arrow[ur, "\widetilde{ev}_\alpha"'] \end{tikzcd}$$

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

int. domain

field.

$$\begin{tikzcd} F[x] \arrow[r, "ev_\alpha"] & \underline{E} \\ x \arrow[r, mapsto] & \alpha \end{tikzcd}$$

$\mathrm{Im}\, ev_\alpha$ - subring of E.

case 1) $\mathrm{Im}\, ev_\alpha \simeq F[\alpha]$, ker is $\{0\}$.

$S = \{1, \alpha, \alpha^2, \alpha^3 \dots \}$ no relations on these elements with coefficients in F are possible in E.

S' is a lin. indep set of vectors in E.
(think of E as a vect. space over F).

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

lin. dep. on vectors $1, \alpha, \alpha^2, \dots \alpha^n$

$ev_\alpha : F[x] \to E$ has nontrivial kernel

$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in F[x]$

$f(\alpha) = 0$. α root of f in E.

$\ker ev_\alpha \subset (f)$

$\ker ev_\alpha = \{0\}$

$F \subset E, \alpha$ $\nearrow$ α is transcendental (no relations)

$F \subset E, \alpha$ $\searrow$ α is algebraic

$\ker ev_\alpha \neq 0$ $\ker ev_\alpha = (p)$

$p(x)$ - monic $\deg p = n$

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

$p(\alpha) = 0$ $\forall f \in F[x]$

$$\begin{tikzcd} x \arrow[r, mapsto] & \alpha \\ F[x] \arrow[r] & E \end{tikzcd}$$

$f(x) \mapsto 0 = f(\alpha)$

$$\begin{tikzcd} F[x] \arrow[r, "ev_\alpha"] \arrow[d] & E \\ F[x]/(p(x)) \arrow[ur, dashed] & \overline{ev_\alpha} \arrow[l, dashed] \end{tikzcd}$$

field of fr

polyn., no rel.

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

$\{1, \alpha, \alpha^2, \dots\}$

∞-dim vect. space$/F$ in E.

E is an infinite extension

$p(x) \in F[x]$

$\cup$

$\ker ev_\alpha$

$a_i \in F$.

$f(\alpha) = 0 \iff$

$f \in \ker ev_\alpha \iff$

$f = p(x)q(x)$

some q.

α generates a copy of $\underbrace{F(x)/(p(x))}$ in E.

$\underbrace{1, \alpha, \alpha^2, \dots}_{\uparrow}$ $\alpha^n = -a_{n-1}\alpha^{n-1} - \dots - a_0$

$\alpha^n \in \langle 1, \alpha, \dots \alpha^{n-1} \rangle$.

lin. indep/F , $\alpha^n \in F \cdot 1 + F \cdot \alpha + \dots + F\alpha^{n-1}$

$$F[x]/\underline{(p(x))} \simeq \mathrm{Im}\, ev_\alpha$$

$$F[x] \longrightarrow E \ni \underline{\mathrm{Im}\, ev_\alpha} \simeq \underset{\substack{\uparrow \\ \text{"small"}}}{F[x]}/(p(x))$$

$\mathrm{Im}\, ev_\alpha$ is a subfield of E,

Since $p(x)$ $\underline{\text{is irreducible}}$.

$p(x) = q(x) r(x) \Rightarrow q(x), r(x)$ are 0-divisors in $F(x)/(p)$. $q(\alpha), r(\alpha)$ $\quad q(\alpha) r(\alpha) = 0$ in E

contradiction with E a field.

$\Rightarrow \mathrm{Im}\, ev_\alpha$ is a subfield of E.

$\mathrm{Im}\, ev_\alpha \simeq F[x]/\underset{\nearrow}{(p)}$

monic, coeff in $\underline{F}$, lowest degree among such polynomials f , $\underline{f(\alpha) = 0}$.

$F \subset \underset{\substack{| \\ \text{smallest field contains } F, \alpha}}{F(\alpha)} \subset E$

in case 2) $F[\alpha] = F(\alpha)$.

$F \subset \underline{F[\alpha]} = \underline{\underline{F(\alpha)}} \subset E$ $\quad 1, \alpha, \alpha^2 \dots \quad$ f. fractions $\quad$ proper

$$\left\{ \begin{array}{ll} \alpha \text{ transcendental} & F \subset F[\alpha] \subset F(\alpha) \subset E \\ \alpha \text{ algebraic} & F \subset F[\alpha] = F(\alpha) \subset E \\ & 1, \alpha, \dots \alpha^n \text{ - lin. dep} \end{array} \right]$$

$F[\alpha]$ - "small" fin. dim vect. space $/F$.

$[F[\alpha] : F] = n = \deg p$.

$p = \operatorname{irr}(\alpha, \underline{F})$ $\qquad F \subset \overset{\substack{\alpha \\ \in}}{E}$

$\overset{\uparrow}{\text{monic}}$, $\deg p =$ deg of extension $F \subset \underset{\substack{\| \\ F[\alpha]}}{F(\alpha)}$.

<u>Example</u> 1) $x^2 - 2 = \operatorname{irr}(\sqrt{2}, \mathbb{Q})$ $\qquad \mathbb{Q} \subset \underset{\substack{\ni \\ \sqrt{2}}}{\mathbb{R}}$

$F[x]$

$\mathbb{Q}[x] \longrightarrow \mathbb{R}$ $\qquad x \longmapsto \sqrt{2}$

$x^2 \longmapsto 2 \qquad \underset{\substack{\in \\ \ker ev_{\sqrt{2}}}}{x^2 - 2} \longrightarrow 0$

irred over $\mathbb{Q}$

$\underline{x^2 - 2}$ no roots

$\|$

$\operatorname{irr}(\sqrt{2}, \mathbb{Q})$ $\qquad \operatorname{Im} ev_{\sqrt{2}} \simeq \mathbb{Q}(\sqrt{2})$

$\operatorname{irr}(\sqrt{2}, \underline{\mathbb{R}}) = x - \sqrt{2}$ $\qquad (1, \sqrt{2})$ basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

2) $\operatorname{irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ $\qquad \mathbb{Q} \subset \underset{\substack{\ni \\ \sqrt[3]{2}}}{\mathbb{R}}$

$x^3 - 2 = 0$ $\qquad$ ↑ no roots in $\mathbb{Q}$ $\qquad$ algebraic

$x^3 - 2 \in \ker ev_{\sqrt[3]{2}}$

<u>Prop</u> (degree f-la, Rotman lemma 49)

If $F \subset B \subset E$, $[E:B]$, $[B:F]$ finite degree $\Rightarrow$

$[E:F]$ is finite and

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

$[B:F] =$ dim of B as F-vect. space

$[E:B]$ or $[B:F]$ $\underset{\deg}{\infty}$ extension $\Rightarrow E/F$ ∞ degree.

(Remark: if $F \subset E$ has finite degree, all el's of E are algebraic over F) | if $F \subset E$ has a transcendental $\alpha \in E$

basis $\{\alpha_1 \dots \alpha_m\}$ E/B $[E:B]=m$

basis $\{\beta_1 \dots \beta_n\}$ B/F $[B:F]=n$

$$F \overset{\{\beta\}}{\subset} B \overset{\{\alpha\}}{\subset} E$$

$$F \overset{\{\alpha\beta\}}{\subset} E \qquad [E:F]=nm$$

$\dim_F E = \infty$

$1, \alpha, \alpha^2 \dots$

lin. indep

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

$$\underline{S} = \{ \underline{\alpha_i \beta_j} \mid 1 \le i \le m, 1 \le j \le n \}. \leftarrow \text{basis } E/F$$

1) S spans E as F-vect. space

$$\gamma = \sum_{i=1}^{m} b_i \alpha_i \ , \underline{b_i} \in B \qquad \begin{array}{ccccc} & n & & m & \\ \underline{F} & \overset{\{\beta\}}{\subset} & B & \overset{\{\alpha\}}{\subset} & \underline{E} \\ \Psi & & \Psi & & \Psi \\ \underline{c_{ij}} & & b_i & & \underline{\gamma} \end{array}$$

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

$$\gamma = \sum_{i,j} c_{ij} \underbrace{\beta_j \alpha_i}_{} \overset{\alpha_i \beta_i}{=} \Rightarrow \{\alpha_i \beta_j\} = S \text{ spans } E$$

as F-vector space

2) linear independence. Assume otherwise

$$(*) \sum_{i,j} c_{ij} \alpha_i \beta_j = 0 \quad \text{some } c_{ij} \in F.$$

$$\underset{B}{\overset{\cap}{b_i}} = \sum_j \underset{F}{\overset{\cap}{c_{ij}}} \underset{B}{\overset{\cap}{\beta_j}}$$

$\downarrow$

$$\sum_{i=1}^{m} \underset{B}{\overset{\cap}{b_i}} \alpha_i = 0 \Rightarrow b_i = 0.$$

$$\Rightarrow \sum_{j=1}^{n} \underset{F}{\overset{\cap}{c_{ij}}} \underset{B}{\overset{\cap}{\beta_j}} = 0. \quad \leftarrow \text{lin. indep } /F. \qquad \Rightarrow c_{ij} = 0$$

□.

Example (Rotman, ex. 20).

$$\underset{F}{\mathbb{Q}} \overset{2}{\subset} \underset{\underset{B}{\|}}{\mathbb{Q}(\sqrt{2})} \overset{\textcircled{2}}{\subset} \underset{\underset{E}{\|}}{\mathbb{Q}(\sqrt{2},\sqrt{3})}$$

$[E:F] =$
$[E:B][B:F] =$
$= 2\,2 = 4.$

$\mathrm{irr}(\sqrt{3}, \mathbb{Q}(\sqrt{2}))$ $\qquad \mathrm{irr}(\sqrt{3}, \mathbb{Q}) = \underline{x^2-3}$

$\|$

x^2-3 or $\underline{\sqrt{3}} \in \underline{\mathbb{Q}(\sqrt{2})}.$ $\qquad$ exercise

$\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$

$\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ $\qquad \sqrt{3} = a + b\sqrt{2} \quad a, b \in \mathbb{Q}.$

$\underline{\underline{x^2-3}}$ $\qquad \underline{3} = (a+b\sqrt{2})^2 = \underline{a^2+2b^2} + \underline{2ab}\underline{\sqrt{2}}$

$[\underline{\mathbb{Q}(\sqrt{2},\sqrt{3})} : \underline{\mathbb{Q}(\sqrt{2})}] = 2$

basis is $(1, \sqrt{3})$

basis of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$.

$\{1, \sqrt{2}\}$ $\qquad \{1, \sqrt{3}\}$

$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ - basis of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$.

$\alpha = \sqrt{2}+\sqrt{3}$ $\qquad \underline{\alpha}^2 = (\sqrt{2}+\sqrt{3})^2 = \underline{5+2\sqrt{6}}. \Rightarrow \underline{\sqrt{6}} \in$

Claim $\mathbb{Q}(\alpha) \underset{\subset}{=} \mathbb{Q}(\sqrt{2}, \sqrt{3})$ $\qquad \alpha^2 \in \mathbb{Q}(\alpha)$

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

$1, \alpha = \sqrt{2}+\sqrt{3}, \sqrt{6}$

$\underline{\sqrt{6}}\,\underline{\alpha} = \sqrt{6}(\sqrt{2}+\sqrt{3}) = \sqrt{12}+\sqrt{18} = \underline{2\sqrt{3}+3\sqrt{2}} \in \underline{\mathbb{Q}(\alpha)}$

$\underline{\sqrt{3}+\sqrt{2}}$

$\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha).$

$$\left.\begin{array}{l}\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\alpha) \\ 3\sqrt{2}+2\sqrt{3} \in \mathbb{Q}(\alpha)\end{array}\right\} \Rightarrow \sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha).$$

$\underline{\mathbb{Q}(\alpha)} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. ← deg 4

α – algebraic $\mathbb{Q}(\alpha) \simeq \mathbb{Q}[x]/(p(x))$ ← deg 4.

$\alpha^2 = 5+2\sqrt{6}$ $\alpha^2 - 5 = \underline{2\sqrt{6}}$

$\alpha^4 - 10\alpha^2 + 25 = 24$. $\alpha^4 - 10\alpha^2 + 1 = 0$

↑ monic, deg 4, α as a root.

$p(x) = x^4 - 10x^2 + 1$ ⟵

$\mathbb{Q}(\alpha) \simeq \mathbb{Q}[x]/(x^4 - 10x^2 + 1)$. ← does not factor over $\mathbb{Q}$.

$(a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + b^p$. p-prime

$\binom{p}{i} = 0$ in $\mathbb{F}_p$ $\Rightarrow$ $(a+b)^p = a^p + b^p$.
$1 \le i \le p-1$

$\binom{p}{0} = 1$, $\binom{p}{p} = 1$ $\mathbb{F}_p \subset R \ni a, b$
$(a+b)^p = a^p + b^p$
$(ab)^p = a^p b^p$

Frobenius endomorphism

$Fr : R \to R$ ↖ any homomorphism from R to itself.
σ_p $\sigma_p(a) = a^p$ sometimes it's bijective.

Then σ_p is an automorphism (symmetry).

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad \underline{2} \quad 1 \\
1 \quad \underline{3} \quad \underline{3} \quad 1 \\
1 \quad \underline{4} \quad \underline{6} \quad \underline{4} \quad 1 \\
1 \quad \underline{5} \quad \underline{10} \quad \underline{10} \quad \underline{5} \quad 1 \\
1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1
\end{array}
$$

$p=3$

$p=2$

$\binom{3}{1}, \binom{3}{2} \equiv 0 \ (\text{mod } 3)$

$(a+b)^4 = a^4 + b^4$
mod 2
over $\mathbb{F}_2$

$p=5$

$\binom{5}{i} \equiv 0$
mod 5
$i=1,..,4$

$(a+b)^p = a^p + b^p$ $\quad$ $(a+b)^{p^2} = a^{p^2} + b^{p^2}$

$\mathbb{F}_p \subset F \leftarrow$ finite field

$\sigma_p : F \to F$ $\quad$ $\sigma_p(1)=1$ $\quad$ ring. hom.
$\sigma_p(0)=0$

$\uparrow$
field

σ_p is injective.

$F \to F$
injective, F finite
$\Rightarrow \sigma_p$ is bijective

it's an automorphism.

$\mathbb{F}_4$ $\quad 0, 1, \alpha, \alpha+1$ $\qquad$ $\mathbb{F}_4 \simeq \mathbb{F}_2[\alpha]/\underline{(\alpha^2+\alpha+1)}$

$p=2$

$0 \mapsto 0$

$1 \mapsto 1$

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

$\alpha+1 \mapsto (\alpha+1)^2 = \alpha^2+1 = \alpha$

Frob. automorphism

$$\begin{tikzcd}
\underline{0} \arrow[loop above, "\sigma_2"] & \underline{1} \arrow[loop above, "\sigma_2"] & \alpha \arrow[r, bend left, "\sigma_2"] & \alpha+1 \arrow[l, bend left, "\sigma_2"]
\end{tikzcd}$$

$\mathbb{F}_p \subset F$. $\sigma_p(1) = 1$

$a \in \mathbb{F}_p$ $\sigma_p(a) = a$

$\sigma_p(a) = a^p \equiv a \pmod{p}$ Fermat's little thm

Any finite field $F \supset \mathbb{F}_p$ has Frobenius
automorphism $\sigma_p(a) = a^p \quad \forall a \in F$