

lect 9

Field extensions + wrap up

$$\begin{array}{c} \underline{F} \subset \underline{E} \\ \downarrow \psi \\ \underline{\alpha} \end{array}$$

field extension

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

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}\}$$

char p from last time.

$$\begin{array}{c} F \subset E \\ \downarrow \alpha \end{array}$$

$$\begin{array}{c} \underline{ev}_\alpha: F[x] \rightarrow \underline{E} \\ \underline{f(x)} \mapsto \underline{f(\alpha)} \end{array}$$

$F[\alpha]$  - smallest subfield of  $E$

contains both  $F$  and  $\alpha$ .

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

$$a_n \alpha^n + \dots + a_0 \in E, \text{ not in } F.$$

$F[\alpha]$  - polyn

$$\alpha \in E$$

subring, all polyn. in  $\alpha$  with coeff. in  $F$ .

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

$x$  unrelated to  $E$ ,  $\alpha \in E$  - congruence relation on  $x$  in  $E$

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

free case, no rel's on  $\alpha$  in  $E$

$$1) \ker ev_\alpha = \{0\}$$

$ev_\alpha$  - injective.  $\downarrow E$ .

subring of  $E$

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

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

not a field.

$$R \xrightarrow{\psi} S$$

$\psi$  inj.

$$\psi(R) = R$$

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

$$\downarrow ev_\alpha$$

$$x \mapsto \alpha.$$

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

$\mathbb{Q} \subset \mathbb{R}$  most el's  $\alpha$  of  $\mathbb{R}$  are transcendental ( $\mathbb{Q}$ )  
 $\begin{matrix} \mathbb{Q} \\ \parallel \\ \mathbb{F} \end{matrix}$   $\begin{matrix} \mathbb{R} \\ \parallel \\ \mathbb{E} \end{matrix}$   
 Countable      Uncountable

if  $\alpha$  not transcendental.  
 $\Rightarrow$  some polyn. rel'n of  $\alpha$ .

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

$\uparrow$   
 $\mathbb{Q}$

only countably many such polynomials

$\Rightarrow$  only countably many roots

subring field  
 $\alpha \quad \mathbb{F}[\alpha] \subset \mathbb{E}$

$\mathbb{Q} \quad \sqrt{2} \quad \pi, e$

no polyn. relations on  $\alpha$

subring is integral domain.

$$\frac{\mathbb{F}[\alpha]}{\cap} \begin{matrix} \hookrightarrow \\ \rightarrow \end{matrix} \mathbb{E}$$

frac. field  $\mathbb{F}(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \mid \frac{f}{g} \sim \frac{f'}{g'} \right\}$ .

int. domain  $\mathbb{F}[x] \xrightarrow{ev_\alpha} \mathbb{E}$        $f(x) \mapsto f(\alpha)$   
 $\cap$   
 field  $\mathbb{F}(x) \xrightarrow{ev_\alpha} \mathbb{E}$

$\mathbb{F}[x] \xrightarrow{ev_\alpha} \mathbb{E}$        $\text{Im } ev_\alpha = \text{subring of } \mathbb{E}$   
 $x \mapsto \alpha$

case 1)  $\text{Im } ev_\alpha \cong \mathbb{F}[\alpha]$ , here is  $\{\emptyset\}$ .

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

$S$  is a lin. indep set of vectors in  $E$ .

(think of  $E$  as a vect. space over  $F$ ).

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

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

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

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

$$f(\alpha) = 0. \quad \alpha \text{ root of } f \text{ in } E.$$

field of fr

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

polyn. no rel.

$F \subset E, \alpha$

$\nearrow$   $\ker ev_\alpha = \{0\}$   
 $\alpha$  is transcendental  
 (no relations)

$\searrow$   $\alpha$  is algebraic

$F \subset F[x] \subset F(\alpha) \subset E$   
 $\{1, \alpha, \alpha^2, \dots\}$   
 $\infty$ -dim vect. space /  $F$   
 in  $E$ .  
 $E$  is an infinite extension

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

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

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

$$\frac{p(x) \in F[x]}{U}$$

$$a_i \in F. \quad \ker ev_\alpha$$

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

$$f(\alpha) = 0 \Leftrightarrow$$

$$\begin{array}{ccc} x & \longmapsto & \alpha \\ F[x] & \longrightarrow & E \end{array}$$

$$f \in \ker ev_\alpha \Leftrightarrow$$

$$f = p(x)q(x) \text{ some } q.$$

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

$$\begin{array}{ccc} F[x] & \xrightarrow{ev_\alpha} & E \\ \downarrow & \dashrightarrow & \leftarrow \text{ev}_\alpha \\ & & F[x]/(p(x)) \end{array}$$

$\alpha$  generates a copy of  $\frac{F[x]}{(p(x))}$  in  $E$ .

$$\underbrace{1, \alpha, \alpha^2, \dots, \alpha^{n-1}}_{\substack{\uparrow \\ \text{lin. indep. / } F}} \quad \alpha^n = -a_{n-1}\alpha^{n-1} - \dots - a_0$$

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

$$\frac{F[x]}{(p(x))} \cong \text{Im } \nu_\alpha$$

$$F[x] \longrightarrow E \ni \underbrace{\text{Im } \nu_\alpha}_{\substack{\uparrow \\ \text{"small"}}} \cong \frac{F[x]}{(p(x))}$$

$\text{Im } \nu_\alpha$  is a subfield of  $E$ ,

since  $p(x)$  is irreducible.

$p(x) = q(x)r(x) \Rightarrow q(x), r(x)$  are 0-divisors

$$\text{in } \frac{F[x]}{(p)} \quad q(\alpha), r(\alpha) \quad q(\alpha)r(\alpha) = 0 \text{ in } E$$

contradiction w/  $E$  a field.

$\Rightarrow \text{Im } \nu_\alpha$  is a subfield of  $E$ .

$$\text{Im } \nu_\alpha \cong \frac{F[x]}{(p)}$$

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

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

smallest field contains  $F, \alpha$

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

$$F \subset \frac{F[x]}{(p)} = \underline{F(\alpha)} \subset E \quad \begin{matrix} \uparrow \text{ } \{1, \alpha, \alpha^2, \dots\} & \text{f. fractions} \\ \text{proper} & \end{matrix}$$

$$\left. \begin{array}{l} \alpha \text{ transcendental} \\ \alpha \text{ algebraic} \end{array} \right\} \begin{array}{l} F \subset F[\alpha] \subset F(\alpha) \subset E \\ F \subset F[\alpha] = F(\alpha) \subset E \\ \text{lin. dep. } \alpha^n \end{array}$$

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

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

$$p = \text{irr}(\alpha, F) \quad F \subset E \stackrel{\alpha}{\Rightarrow}$$

monic,  $\deg p = \deg$  of extension  $F \subset F(\alpha)$   
 $\parallel$   
 $F[\alpha]$

Example 1)  $x^2 - 2 = \text{irr}(\sqrt{2}, \mathbb{Q})$

$$F[x]$$

$$\mathbb{Q}[x] \rightarrow \mathbb{R}$$

$$x \mapsto \sqrt{2}$$

$$x^2 \mapsto 2$$

$$x^2 - 2 \mapsto 0$$

irred over  $\mathbb{Q}$

$\cap$   
 lies in  $\mathbb{R}$

$$\frac{x^2 - 2}{\parallel}$$

$$\text{irr}(\sqrt{2}, \mathbb{Q})$$

$$\text{irr}(\sqrt{2}, \mathbb{R}) = x - \sqrt{2}$$

$$\text{Im } \text{ev}_{\sqrt{2}} = \mathbb{Q}(\sqrt{2})$$

$(1, \sqrt{2})$  basis of

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

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

$$x^3 - 2 = 0$$

$\cap$   
 no roots in  $\mathbb{Q}$

$$\mathbb{Q} \subset \mathbb{R}$$

$$\sqrt[3]{2}$$

algebraic

$$x^3 - 2 \in \text{ker } \text{ev}_{\sqrt[3]{2}}$$

Prop (degree f-l, Rothman lemma 49)

If  $\underline{F} \subset \underline{B} \subset \underline{E}$ ,  $[E:B]$ ,  $[B:F]$  finite degree.  $\Rightarrow$

$[E:F]$  is finite and

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

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

$[E:B]$  or  $[B:F]$

of extension

$\hat{\text{deg}}$

$\Rightarrow E/F$  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  $\alpha \in E$

$$\begin{array}{l}
 \text{basis } \{\alpha_1, \dots, \alpha_m\} \quad E/B \quad [E:B]=m \\
 \text{basis } \{\beta_1, \dots, \beta_n\} \quad B/F \quad [B:F]=n \\
 \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \dim_F E = \infty \\
 \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \text{lin. indep.} \\
 \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} F \subset B \subset E \\
 \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} F \subset F[\alpha] \subset E \\
 \left. \begin{array}{l} \\ \\ \\ \end{array} \right\} (E:F) = nm
 \end{array}$$

$$\underline{S} = \{ \alpha_i \beta_j \mid 1 \leq i \leq m, 1 \leq j \leq n \} \quad \text{--- basis } E/F$$

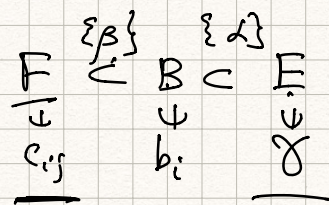
1)  $S$  spans  $E$  as  $F$ -vector space

$$\gamma = \sum_{i=1}^m b_i \alpha_i, \quad \underline{b_i} \in B$$

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

„ $\alpha_i \beta_j$ “

$$\gamma = \sum_{i,j} c_{ij} \beta_j \alpha_i \Rightarrow \{ \alpha_i \beta_j \} = S \text{ spans } E \text{ as } F\text{-vector space}$$



2) Linear independence. Assume otherwise

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

$$\downarrow \quad \begin{array}{ccc}
 b_i & = & \sum_j c_{ij} \beta_j \\
 \uparrow & & \uparrow \\
 B & & F \quad B
 \end{array}$$

$$\sum_{i=1}^m b_i \alpha_i = 0 \Rightarrow b_i = 0.$$

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

□.

Example (Rotman, ex. 201).

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

$\begin{array}{ccc} \text{F} & \text{B} & \text{E} \\ \cdot & \text{B} & \cdot \\ & \text{B} & \cdot \end{array}$

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

$$\text{irr}(\sqrt{3}, \mathbb{Q}(\sqrt{2}))$$

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

$$x^2 - 3$$

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

exercise

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

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

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

$$\underline{x^2 - 3}$$

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

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

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

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

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

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

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

$$\alpha = \sqrt{2} + \sqrt{3}$$

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

$$\text{claim } \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$$\alpha^2 \in \mathbb{Q}(\alpha)$$

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

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

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

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

$$\underline{\sqrt{3} + \sqrt{2}} \in \mathbb{Q}(\alpha)$$

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

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \quad \leftarrow \text{deg } 4$$

$\alpha$  - algebraic

$$\mathbb{Q}(\alpha) = \mathbb{Q}[x] / (p(x)) \quad \leftarrow \text{deg } 4$$

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

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

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

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

$$p(x) = x^4 - 10x^2 + 1$$

monic, deg 4,  $\alpha$  as a root.

$$\mathbb{Q}(\alpha) = \mathbb{Q}[x] / (x^4 - 10x^2 + 1)$$

does not factor over  $\mathbb{Q}$ .

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

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

$$\binom{p}{0} = 1, \quad \binom{p}{p} = 1$$

$$\mathbb{F}_p \subset \mathbb{R} \ni a, b$$

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

$$(ab)^p = a^p b^p$$

Frobenius endomorphism

$$F_r : R \rightarrow R$$

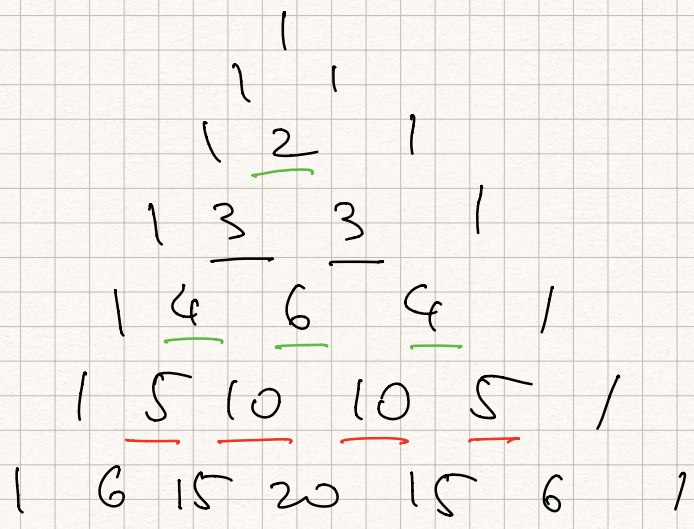
$$\mathcal{Z}_p \quad \mathcal{Z}_p(a) = a^p$$

any homomorphism from  $R$  to itself. sometimes it's bijective.

then  $\mathcal{Z}_p$  is an automorphism (symmetry).



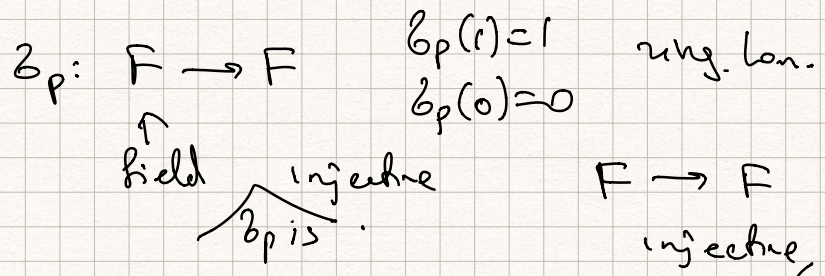
$p=5$   
 $\binom{5}{i} \equiv 0 \pmod{5}$   
 $i=1, \dots, 4$



$p=3$   
 $p=2$   
 $\binom{3}{1}, \binom{3}{2} \equiv 0 \pmod{3}$   
 $(a+b)^4 = a^4 + b^4 \pmod{2}$   
 over  $\mathbb{F}_2$

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

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



$F \rightarrow F$   
 injective,  $F$  finite  
 $\Rightarrow \sigma_p$  is bijjective

it's an automorphism.

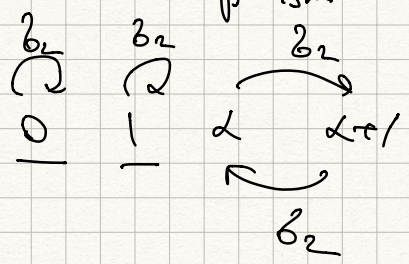
$\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$

$$\mathbb{F}_4 \cong \mathbb{F}_2[x] / \langle x^2 + x + 1 \rangle$$

$p=2$

- $0 \mapsto 0$
- $1 \mapsto 1$
- $\alpha \mapsto \alpha^2 = \alpha + 1$
- $\alpha + 1 \mapsto (\alpha + 1)^2 = \alpha^2 + 1 = \alpha + 1 + 1 = \alpha$

Free automorphism



$$\mathbb{F}_p \subset F.$$

$$\zeta_p(1) = 1$$

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

$$\zeta_p(a) = a^p \equiv a \pmod{p}$$

Fermat's  
little  
theorem

{ Any <sup>finite</sup> field  $F \supset \mathbb{F}_p$  has Frobenius  
auto morphism  $\zeta_p(a) = a^p \quad \forall a \in F$