

$F$ -field,  $f(x) \in F[x]$  irreducible  $\Rightarrow E = F[x]/(f(x))$  is a field

relabel  $x$  into  $\alpha$  in definition of  $E$  and keep  $x$  as a formal variable.  $E \supset F$  (extension of  $F$ )

$E = F[\alpha]/(f(\alpha))$  (Later!)  $E$  is a vector space over  $F$  with basis  $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ ,  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ ,  $\deg f = n$

$\alpha$  direction, grow our field

all maps are inclusions  $\hookrightarrow$

$E = F[\alpha]/(f(\alpha)) \hookrightarrow E[x]$



$F$

$F \hookrightarrow F[x]$

$x$  direction, form polynomials

$f(x)$  factors over  $E$ ,  $f(\alpha) = 0$  in  $E \Rightarrow$   
 $x - \alpha \mid f(x)$  in  $E[x]$   
 $f(x) = (x - \alpha)g(x)$ ,  $g(x) \in E[x]$   
 $\deg g = n - 1$

$g(x)$  has complicated coefficients (in  $E$ , not in  $F$ )

Examples:

1)  $F = \mathbb{R}$ ,  $f(x) = x^2 + 1$   $E = \mathbb{R}[\alpha]/(\alpha^2 + 1) \cong \mathbb{C}$  (relabel  $\alpha \mapsto i$ ,  $\mathbb{C} \cong \mathbb{R}[i]/(i^2 + 1)$ )  
 $i^2 = -1$   
 In  $\mathbb{C}$  can factor  $f(x) = x^2 + 1 = (x + i)(x - i)$   
 coefficients in  $\mathbb{C}$ , not in  $\mathbb{R}$

2)  $F = \mathbb{Q}$ ,  $f = x^2 - 2$ ,  $E = \mathbb{Q}[\alpha]/(\alpha^2 - 2)$  since  $E \subset \mathbb{R}$  (can realize  $E$  inside  $\mathbb{R}$ ) can take  $\alpha = \sqrt{2}$   
 $x^2 - 2 = (x - \alpha)(x + \alpha) = (x - \sqrt{2})(x + \sqrt{2})$   
 irr/ $\mathbb{Q}$  factors in  $E$  factors in  $\mathbb{R}$   $E \rightarrow \mathbb{R}$   
 $\alpha \mapsto \sqrt{2}$   $F \subset E \subset \mathbb{R}$

3)  $F = \mathbb{F}_2 = \mathbb{Z}/2$   $\{0, 1 \mid 1+1=0\}$   $f = x^2 + x + 1$   $E = \mathbb{F}_4 = \mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1)$   
 $\alpha^2 = \alpha + 1 = \alpha^2$   
 $x^2 + x + 1 = (x + \alpha)(x + \alpha + 1)$  roots of  $f$  in  $\mathbb{F}_4 = \{\alpha, \alpha + 1\}$   
 factors in  $\mathbb{F}_4$   $\mathbb{F}_4 \cong \mathbb{C}_3$

4) Degree 3 example  $F = \mathbb{Q}$ ,  $f = x^3 - 2$ ,  $E = \mathbb{Q}[\alpha]/(\alpha^3 - 2)$ ,  $x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$   
 (irr/ $\mathbb{Q}$ , will see soon) field  $g(x) \uparrow$   
 $\omega = e^{2\pi i/3}$  3rd root of 1  $K = E[\beta]/(\beta^2 + \alpha\beta + \alpha^2)$  irr in  $E$   
 in  $K$ ,  $x^3 - 2 = (x - \alpha)(x - \beta)(x - \beta^2\alpha^{-1})$   $\beta \mapsto e^{2\pi i/3}\sqrt[3]{2}$   
 $\alpha \mapsto \sqrt[3]{2}$

