

If  $L/K$  is a field extension

$$\alpha_1, \dots, \alpha_n \in L$$

$K(\alpha_1, \dots, \alpha_n)$   $\leftarrow$  smallest subfield of  $L$   
containing  $K, \alpha_1, \dots, \alpha_n$ .

Note:  $K(\alpha_1, \alpha_2, \dots, \alpha_n) = K(\alpha_1)(\alpha_2, \dots, \alpha_n)$   
 $= (K(\alpha_1)(\alpha_2))(\alpha_3, \dots, \alpha_n)$ .

I a set  $\alpha_i \in L \quad i \in I$   $\vdots$   
Then  $K(\alpha_i \mid i \in I)$ .

IF  $L = K(\alpha_1, \dots, \alpha_n)$  for  $\alpha_1, \dots, \alpha_n \in L$ .  
then  $L$  is finitely generated over  $K$ .

IF  $[L:K] < \infty$   $L$  is a finite extension  
of  $K$ .

Example  $K(x)/K$  is not finite  
 $\downarrow$  but it is finitely generated

Field of rational  
functions in the variable  $x$  over  $K$ .

$L/K$  is algebraic if every  $\alpha \in L$   
is algebraic over  $K$ .  
(transcendental otherwise).

Theorem  $L/K$  is finite ( $[L:K] < \infty$ )

if and only if  $L/K$  is finitely generated and algebraic.

Main lemma: If  $L/K$  is finite, then  $L/K$  is algebraic.

Other main lemma: If  $M/L/K$  then  $[M:K] = [M:L][L:K]$ .

→ Proof Let  $\alpha \in L$   $d = [L:K]$ .

$1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^d$

$d+1$  vectors in  $d$ -dim space.

There is a non-trivial linear dependence.

$$a_0 \cdot 1 + a_1 \alpha + a_2 \alpha^2 + \dots + a_d \alpha^d = 0$$

$a_i \in K$ .

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_d x^d$$

This is a non-zero polynomial w/coeff in  $K$

$$f(\alpha) = 0 \quad \text{So } \alpha \text{ is algebraic.}$$

Theorem:

If  $K$  is a field and

$f$  is a non-constant polynomial over  $K$

Then  $\exists$  an extension  $L/K$  s.t.:

$f$  has a root in  $L$ .

Proof:  $K[x]$  is a PID

Take an irreducible factor  
 $g(x)$  of  $f(x)$ .

$L = K[x]/g(x)$  is a field

Claim:  $\bar{y}$  for the image of  $y$   
in  $L$ , then

$\bar{y}$  is a root of  $F(x) \in L[x]$

Need to check  $F(\bar{y}) = 0$  in  $L$

$$f(x) = g(x)h(x).$$

$$f(\bar{y}) = g(\bar{y})h(\bar{y}).$$

$\hat{L}$  suffice to show this  
is zero.

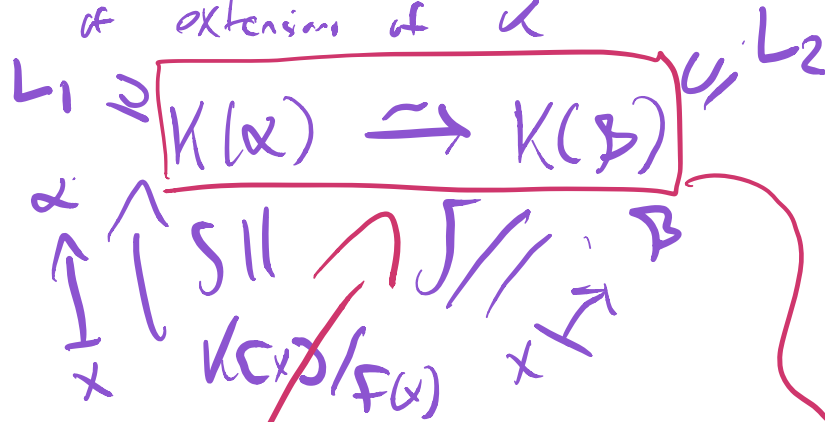
$$g(\bar{y}) \in L = K[x]/g(x).$$

$$\overline{a(x)} \stackrel{\text{def}}{=} a(x) \text{ mod } g(x)$$

$$0 + 0 + \dots + 0 = 0.$$

Uniqueness statement: If  $L_1/K$   $L_2/K$   
 $\alpha \in L_1$   $\beta \in L_2$  are both  
 roots of  
 an irreducible  $f(x) \in K[x]$ ,

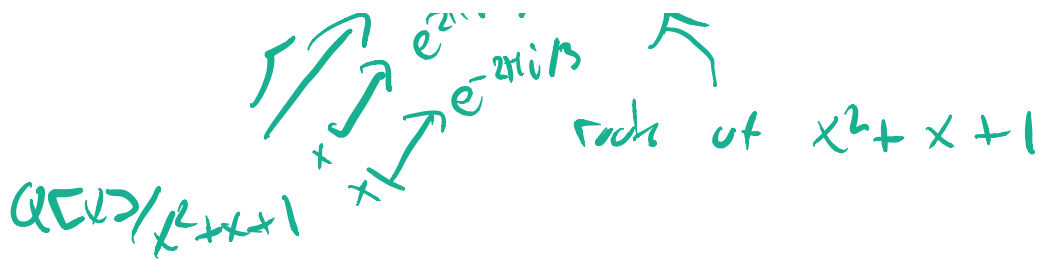
then there is an isomorphism  
 of extensions of  $K$



This isomorphism  
 is not typically  
 unique. But  
 now it is explicit in  
 terms of the  
 extra data.

The unique isomorphism sends  $\alpha$  to  $\beta$ .

Example  $K(\alpha) \cong K(\beta)$   $\Rightarrow e^{2\pi i/3} =$



Remark: If  $f \in K[x]$   $L_1/K$   $L_2/K$   
 are extensions. Then any  
 $\psi: L_1 \rightarrow L_2$  s.t.  $\psi|_K = \text{Id}$ ,  
 sends roots of  $f$  in  $L_1$  to  
 roots of  $f$  in  
 $L_2$ .

If  $\alpha \in L_1$  is a root of  $f$

$$f = a_0 + a_1x + \dots + a_dx^d$$

$a_i \in K$ .

$$\begin{aligned}
 \psi(f(\alpha)) &= \psi(a_0 + a_1\alpha + \dots + a_d\alpha^d) \\
 &= \psi(a_0) + \psi(a_1)\psi(\alpha) + \dots + \psi(a_d)\psi(\alpha)^d \\
 &= a_0 + a_1\psi(\alpha) + \dots + a_d\psi(\alpha)^d \\
 &= f(\psi(\alpha))
 \end{aligned}$$

$$\text{if } f(\alpha) = 0 \quad f(\psi(\alpha)) = \psi(f(\alpha)) = \psi(0) = 0.$$

Bootstrap: Splitting field.

If  $f \in K[x]$

then an extension  $L/K$  is  
a splitting field for  $f$   
if

(1)  $f$  factors into degree 1 polynomials  
in  $L[x]$ .

(2) If  $\alpha_1, \dots, \alpha_s$  are  
the roots of  $f$ . ( $s \leq \deg f$ )  
Then  $L = K(\alpha_1, \dots, \alpha_s)$ .

Theorem: Splitting fields exist and  
any 2 are isomorphic as  
extensions of  $K$ .

Proof: For existence - suffices to construct  
an extension satisfying (1)  
then take sub ext. generated by  
roots.  
Do by induction on degree.

Note: If  $L/K$  is a splitting field  
for  $f$  then  $[L:K] \leq (\deg f)!$

Given a field  $K$ , is there an extension  $L/K$  s.t.  
any  $f \in K[x]$  splits into linear factors in  $L[x]$ ?

Theorem/dfn: There exist such an extension which furthermore algebraic over  $K$  and such an extn is unique up to isomorphism.

(Such an  $L$  is called an algebraic closure of  $K$ ).

Proof

- 1) Construct an extension where all polynomials split.
- 2) Show that the subset of elements algebraic over  $K$  is a field.
- 3) Build up uniqueness from splitting field uniqueness.

Part 2: Claim if  $L/K$  then

$$L^{ab} \subseteq L$$

$= \{ \alpha \in L \mid \alpha \text{ is algebraic over } K \}$   
is a subfield.

Need to check, e.g., if  $\alpha, \beta$  are algebraic then so is  $\alpha + \beta$   $\leftarrow$   
 $\alpha\beta$   $\leftarrow$   $-\alpha$ .

Note If  $f(\alpha) = 0$   $g(\beta) = 0$   
It's not clear  $\exists h$   $h(\alpha + \beta) = 0$ .  
 $\Rightarrow \alpha^1, \dots$   
 $\alpha + \beta \in K(\alpha, \beta)$

$$K \subseteq K(\alpha) \subseteq K(\alpha, \beta)$$

$\uparrow$  finite extension       $\swarrow$  finite extension.

so  $K(\alpha, \beta)/K$  is finite

$$[K(\alpha, \beta) : K] \leq [K(\alpha) : K][K(\beta) : K].$$

finite  $\Rightarrow$  algebraic.



Example: Every polynomial in  $\mathbb{C}[X]$   
splits by Liouville's theorem.

-  $\mathbb{C}/\mathbb{Q}$  is a field extension  
 $\overline{\mathbb{Q}} := \mathbb{C}^{\text{alg}}$  is an algebraic  
closure of  $\mathbb{Q}$ .