Algebra. Lec 15 . Algebraic extensions

Lang. Chap V

Algebraic Extension

A **vector space** over $\mathbb{F}$ is a set V with two operations, **addition** carrying $V \times V$ into V and **scalar multiplication** carrying $\mathbb{F} \times V$ into V, with the following properties:

(i) the operation of addition, written $+$, satisfies

(a) $v_1 + (v_2 + v_3) = (v_1 + v_2) + v_3$ for all v_1, v_2, v_3 in V (associative law),
(b) there exists an element 0 in V with $v + 0 = 0 + v = v$ for all v in V,
(c) to each v in V corresponds an element $-v$ in V such that $v + (-v) = (-v) + v = 0$,
(d) $v_1 + v_2 = v_2 + v_1$ for all v_1 and v_2 in V (commutative law);

abelian Group.

(ii) the operation of scalar multiplication, written without a sign, satisfies

(a) $a(bv) = (ab)v$ for all v in V and all scalars a and b,
(b) $1v = v$ for all v in V and for the scalar 1;

(iii) the two operations are related by the distributive laws

(a) $a(v_1 + v_2) = av_1 + av_2$ for all v_1 and v_2 in V and for all scalars a,
(b) $(a + b)v = av + bv$ for all v in V and all scalars a and b.

E. field. (ring. comm. division).

$F \subseteq E$. F subfield of E.

We say E is an. ext of F , we may view E as a vector space $/F$

if $\dim_F E < \infty$. E: finite ext. $/F$
if not. finite. E: infinite ext $/F$

- $F \subseteq E$. $\alpha \in E$. is said to be <u>algebraic</u> over F

  if. $a_0, \dots, a_n \in F$. not all zero

  s.t. $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$

<u>Rmk</u>. not algebraic. = transcedental

- $F \subseteq E$. $\alpha \in E$. transcedental $/F$

  $F[x] \xrightarrow{\sim} F[\alpha]$ as rings

Rmk $F \subseteq E \ni \alpha$

α : alg/F

Consider $F[x] \xrightarrow{\varphi} E$, $x \mapsto \alpha$ $\quad \varphi|_F = \mathrm{id}_F$. φ. ring hom

$\because$ α : alg/F $\quad$ $\ker(\varphi)$. nontrivial. ideal of $\underbrace{F[x]}_{\text{PID}}$

$\Rightarrow \ker(\varphi) = \langle p(x) \rangle$, may assume $p(x)$ has leading coff. 1.

Claim $p(x)$. irreducible

Pf if not. $p(x) = a(x) b(x)$

$\Rightarrow p(\alpha) = a(\alpha) b(\alpha) = 0 \in E$ $\quad$ say $a(\alpha) = 0$

$\langle a(x) \rangle \subseteq \ker(\varphi) = \langle p(x) \rangle \subsetneq \langle a(x) \rangle$ $\quad$ $\times$

$F[x]/\ker(\varphi) = F[x]/(p(x)) \overset{\text{as rings}}{\simeq} F[\alpha]$

for $F[x]$ is (ED) PID.

$\Rightarrow (p(x))$ is prime $\quad \Rightarrow F[\alpha]$ domain

$p(x)$ = uniquely determined by α.

= the irreducible polynomial of α.

= $\mathrm{Irr}(\alpha, F, x)$

Rmk E. ext of F is said to be algebraic

if every elem. in E is alg/F

Prop 1.1 E: finite extension /F.

$\Rightarrow$ E: alg ext /F.

Pf. $\alpha \in E$ $\alpha \neq 0$. consider $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$. for some n

$\downarrow$

can not be lin. indep /F for all n.

$\exists$ a lin relation for $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ for some n.

$(a_0 1 + a_1 \cdot \alpha + \dots + a_{n-1}\alpha^{n-1} = 0.$ $a_i \in F$. not all zero)

$\therefore$ α : alg /F $\square$

Rmk. $\exists$ E: alg ext /F s.t. $\dim_F E$ not finite

Example.

$$\mathbb{Q} \subseteq \underset{\text{dim}=2}{\mathbb{Q}(\sqrt{2})} \subset \underset{\text{dim}=3}{\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})} \subset \underset{\text{dim}=4}{\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[5]{2})} \subset \cdots$$

$\downarrow$ alg $\quad \downarrow$ alg $\quad \downarrow$ alg

Prop 1.2 $k \subseteq F \subseteq E$. denote $\dim_F E = [E:F]$

$\Rightarrow$ $[E:k] = [E:F][F:k]$

Pf. $\{\alpha_i\}$. basis of F/k

$\{\beta_j\}$. basis of E/F

$\Rightarrow \{\alpha_i\beta_j\}$. basis of E/k.

def. $k \subseteq E$. $\alpha \in E$

$k(\alpha) \triangleq$ the smallest. subfield of E containing k and α

$$k(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; f(x), g(x) \in k[x] \right\}$$

$g(\alpha) \neq 0$.

rational field

check. $k \in \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; f(x). g(x) \in k[x] \right\}$

$\alpha \in \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; f(x)\ g(x) \in k[x] \right\}$

$\Rightarrow k(\alpha) \subseteq$ RHS

Any subfield of E containing k. α. containing RHS   why ?

need to generate a field !

Prop. 1.4. α : alg$/k$. . $k \subseteq E \ni \alpha$

$\Rightarrow k(\alpha) = k[\alpha]$ $k(\alpha)$ algebraic $/k$ ✓

and. $k(\alpha)$. finite $/k$.

$$[k(\alpha):k] = \deg \operatorname{Irr}(\alpha, k, x)$$

$\mathbb{R}[i] = \mathbb{R}(i)$. field.

$\mathbb{R}[i]$ finite $/\mathbb{R}$. and.

$p(x) = i^2+1$ is prime

$\Rightarrow$ max

$\Rightarrow \mathbb{R}[i]/(i^2+1)$. is field.

$\quad \parallel$

$\quad \mathbb{C}$.

---

pf

$p(x) = \operatorname{Irr}(\alpha, k, x)$

let. $f(x) \in k[x]$ be st. $f(\alpha) \neq 0$.

$\Rightarrow p(x) \nmid f(x)$

$\Rightarrow (p(x)) + (f(x)) = k[x]$ $\quad$ ($p(x)$ is prime $\Rightarrow$ $p(x)$ is max $\Rightarrow (p(x)) + (f(x)) = k[x]$)

$\exists\, g(x).\ h(x).\quad g(x)p(x) + h(x)f(x) = 1. \in k[x]$

$\Rightarrow g(\alpha)p(\alpha) + h(\alpha)f(\alpha) = 1$

$\qquad\qquad \parallel$

$\qquad h(\alpha)f(\alpha)$ $\quad \therefore f(\alpha)$ invertible in $k[\alpha]$

$\Rightarrow k[\alpha]$, is a field.

$\downarrow$

include k and α

$\Rightarrow k[\alpha] = k(\alpha)$

$d = \deg p(x)$

$\Rightarrow \{1, \alpha, \cdots, \alpha^{d-1}\}$ lin. indep. $/k$ $\quad$ (otherwise. $\exists\, g(x).\ g(\alpha)=0.\ \deg g < d$ $\longrightarrow\!\!\!\!\!\!\times$)

let $f(\alpha) \in k[\alpha]$

$f(x) = q(x)p(x) + r(x) \quad \deg r(x) < d$.

$f(\alpha) = r(\alpha)$. $\therefore$ $\{1, \alpha, \dots, \alpha^{d-1}\}$ generates $k[\alpha]$ as a vector space$/k$

$$\Rightarrow \dim_k k[\alpha] = d = \deg \mathrm{Irr}(\alpha, k, x) \qquad \square$$

Rmk. E, F : ext$/k$

E, F. contained in some field L.

$EF \triangleq$ the smallest subfield of L containg E and F.

(Composition of E and F)

Rmk. $k \subseteq E$. $\alpha_1, \dots, \alpha_n \in E$

$k(\alpha_1, \dots, \alpha_n)$ the smallest subfield of E containing $k, \alpha_1, \dots, \alpha_n$

claim. $k(\alpha_1, \dots, \alpha_n) = \left\{ \dfrac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \;\middle|\; \begin{array}{l} f, g \in k[x_1, \dots, x_n] \\ g(\alpha_1, \dots, \alpha_n) \neq 0 \end{array} \right\}$

def. $k \subseteq E$

we say E is finitely generated over k

if $\exists$ a finite family of elements $\alpha_1, \dots, \alpha_n$.

s.t. $E = k(\alpha_1, \dots, \alpha_n)$.

$\mathbb{Q}(\pi)$. infinite

but finite gen.

Prop 1.5 E. finite extension of k

$\Longrightarrow$ E finitely gen. over k

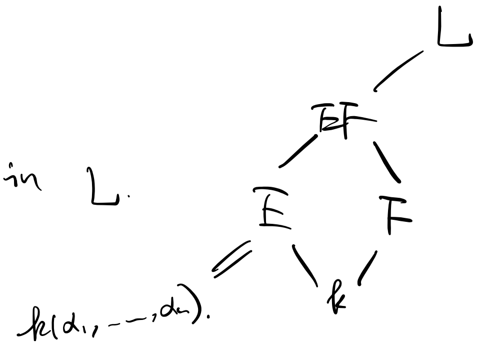
Pf. Let $\{\alpha_1, \dots, \alpha_n\}$ be a basis of E as vector space$/k$

then. $k(\alpha_1, \dots, \alpha_n) = E$ $\square$

Rmk. $E = k(\alpha_1, \dots, \alpha_n)$. finitely gen.

F: ext$/k$.

$E.F.$ contained in L.



$\Rightarrow$ $EF = F(\alpha_1, \dots, \alpha_n)$. $\Rightarrow$ the translation of E to F.

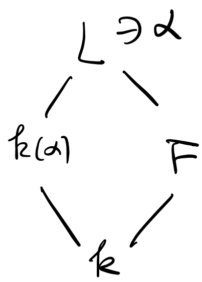
or also the lifting of E to F.

- α. alg$/k$

F: ext of k $\Longrightarrow$ α: alg $/F$

$k(\alpha)$. F. contained in L

for $k(\alpha) F = F(\alpha)$
$\shortparallel$
$F[\alpha]$ a field.



$\Downarrow$

Rmk $k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1, \ldots, \alpha_n)$

α_i : alg $/k$ $\forall i = 1, \ldots, n$.

$\Rightarrow \alpha_{i+1}$ alg over $k(\alpha_1, \ldots, \alpha_i)$

Prop. 1.6 $E = k(\alpha_1, \ldots, \alpha_n)$. finitely gen. $/k$.

α_i : alg $/k$ $i = 1, \ldots, n$

$\Rightarrow E$: finite algebraic $/k$.

Pf. $k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1, \ldots, \alpha_n)$

$\alpha_1 : \text{alg}/k$ $\alpha_2 : \text{alg}/k(\alpha_1)$

finite finite

$\Rightarrow E = k(\alpha_1, \ldots, \alpha_n)$ finite over k

$\Rightarrow E$ is alg $/k$ $\square$

Let. $\mathcal{C}$ be a certain class of extension. $F \subseteq E$

$\mathcal{C}$ is called **distinguished** if

① $k \subset F \subset E$ $k \subset E$ in $\mathcal{C}$ $\Leftrightarrow$ $k \subset F$ and. $F \subset E$ in $\mathcal{C}$

② if $k \subset E$ is in $\mathcal{C}$, if $k \subset F$ be any ext, E, F contained in L

$\Rightarrow F \subset EF$ in $\mathcal{C}$

③. $k\subset F$. $k\subset E$ in $\mathcal{C}$ $\Rightarrow$ $k\subset EF$ in $\mathcal{C}$.

$E\cdot F$ contained in some L

$$\begin{tikzcd} E \arrow[d, dash, "\text{in } \mathcal{C}"] \\ F \arrow[d, dash, "\text{in } \mathcal{C}"] \\ k \end{tikzcd} \quad \text{in } \mathcal{C} \qquad \begin{tikzcd} & EF & \\ E \arrow[ur, dash] & & F \arrow[ul, dash, "\text{in } \mathcal{C}."'] \\ & k \arrow[ul, dash, "\text{in } \mathcal{C}"] \arrow[ur, dash] & \end{tikzcd} \qquad \begin{tikzcd} & EF \arrow[d, dash, "\text{in } \mathcal{C}"] & \\ E \arrow[ur, dash] & & F \arrow[ul, dash] \\ & k \arrow[ul, dash, "\text{in } \mathcal{C}"] \arrow[ur, dash, "\text{in } \mathcal{C}."'] & \end{tikzcd}$$

① + ② $\Rightarrow$ ③

Prop. 1.7. The class of alg. extension is distinguished.

The class of fin. extension is distinguished.

Pf. <u>finite ext. class.</u>

①. obvionse.

②. $$\begin{tikzcd} & EF & \\ E \arrow[ur, dash] & & F \arrow[ul, dash] \\ & k \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

E/k. finite. $\Rightarrow$ $E = k(\alpha_1, \dots, \alpha_n)$ (prop 1.5)

$\therefore EF = F(\alpha_1, \dots, \alpha_n)$ finitely gen $/F$

α_i : alg $/F$

$\Rightarrow$ EF. finite $/F$

<u>algebraic ext class</u>

① $k\subset F\subset E$

if E: algebraic $/k$. $\Rightarrow$ F: alg $/k$ (by def.)

E: alg $/k$.

Conversely E/F alg. F/k alg.

$\alpha \in E$. $a_n\alpha^n + \cdots + a_0 = 0$ $\quad a_i \in F$, $a_n \neq 0$.

$F_0 = k(a_0, \dots, a_n)$

$\Rightarrow \underbrace{k \subset F_0}_{\text{finite}} \underbrace{\subset F_0(\alpha)}_{\text{finite}}$

$\Rightarrow F_0(\alpha)$ finite$/k$

$\therefore \alpha$: alg$/k$

②. $k \subset E$. alg$/k$

$$\begin{tikzcd}
 & EF & \\
E \arrow[ur, Rightarrow, "\text{in } \mathcal{C}."'] \arrow[ur, dash] & & F \arrow[ul, dash] \\
 & k \arrow[ul, dash, "\text{inc}"] \arrow[ur, dash] &
\end{tikzcd}$$

$\alpha \in E$ $\quad \alpha$: algebraic$/k$

$$\begin{tikzcd}
 & EF. & \\
k(\alpha) \arrow[ur, dash] & & F \arrow[ul, dash] \\
 & k \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

$\Rightarrow$ α. algebraic$/F$

$\Rightarrow$ $F(\alpha)$ algebraic$/F$

$\Rightarrow$ EF algebraic$/F$