Algebra. Lec 16 Algebraic closure.

①

$$\begin{tikzcd} E \arrow[r, hook, "\tau"] & L \\ F \arrow[u, "\text{inc}"] \arrow[r, "\sigma"'] & L \arrow[u, "\text{id}"'] \end{tikzcd}$$

emb

same as

$$\begin{tikzcd} E \arrow[dr, hook, "\tau.\ \text{emb}"] & \\ F \arrow[u, "\text{inc}"] \arrow[r, hook, "\sigma"', "\text{emb}"] & L \end{tikzcd}$$

σ. injective field hom (not inclusion).

τ. injective field hom

We say $\tau: E \hookrightarrow L$ is an embedding of E over F if $\tau|_F = \sigma$

embedding = injective field hom.

②.

$$\begin{tikzcd} E \arrow[r, hook, "\tau"] & L \\ & F \arrow[ul, "\text{inc}"] \arrow[u, "\text{inc}"'] \end{tikzcd}$$

emb.

$\tau|_F = \text{inclusion}.$

Rmk $f(x) \in F[x]$ $\alpha \in E$. a root of $f(x)$

$f(x) = a_0 + \cdots + a_n x^n$. $a_i \in F$

$\therefore 0 = a_0 + \cdots + a_n \alpha^n \in E$

if τ extends σ as above diagram.

$$0 = \tau(0) = \tau(f(\alpha)) = \sigma(a_0) + \sigma(a_1)(\tau(\alpha)) + \cdots + \sigma(a_n)(\tau(\alpha))^n.$$

$$\underset{\text{write as}}{=\!=} a_0^\sigma + a_1^\sigma(\tau\alpha) + \cdots + a_n^\sigma(\tau\alpha)^n.$$

$\therefore \tau(\alpha)$ is a root of $f^\sigma(x) = a_0^\sigma + a_1^\sigma x + \cdots + a_n^\sigma x^n$.

Lem. 2.1 E : alg ext. $/k$

$$\begin{array}{ccc} E & \xrightarrow[\text{injection}]{\sigma} & E \\ & \nwarrow_{\text{inclusion}} \quad k \quad \nearrow_{\text{inclusion}} & \end{array}$$

$\sigma: E \to E$. an. embedding of E into E over k (injective hom).

$(\sigma|_k = id_k)$

$\Rightarrow \sigma$: isomorphism.

Pf. want to show . σ: injective.

let $\alpha \in E$. $p(x) = Irr(\alpha, k, x)$.

$E' = k$(all roots of $p(x)$ laying in E) $\subseteq E$.

$\therefore E'$ fin. gen $/k$. and every generators is algebraic $/k$.

why?

$\overset{\text{Lem. 1.6.}}{\Longrightarrow}$ E' : finite ext$/k$

σ: (a root of $p(x)$ in E) $\xrightarrow{\text{by Rmk.}}$ (a root of $p(x)$ in E).

$\Rightarrow f^{\sigma}(x) = a_0^{\sigma} + a_1^{\sigma} x + \cdots + a_n^{\sigma} x^n$.
$= a_0 + a_1 x + \cdots + a_n x^n$.

$\Rightarrow \sigma : \underset{vs/k}{E'} \hookrightarrow \underset{vs/k}{E'}$ injective

Now regard σ as a k-homorphism. of vector space

(i.e. linear transf $E' \to E'$ E' : vs$/k$)

$\therefore [\sigma(E') : k] = [E' : k]$ $\overset{\text{有限维}}{\Rightarrow}$ $\sigma(E') = E' \ni \alpha$.

$\therefore \sigma$ surjective $\square$

Rmk. E, F ext$/k$ contained in some larger field L.

$E[F]$ = the ring gen. by F over E $= \{a_1b_1 + \cdots + a_nb_n \mid a_i \in E,\ b_j \in F\} = F[E]$

EF : quotient field of $E[F] = F[E]$ (or we can say EF is the field of quotients of these elements).

Lem 2.2. E_1, E_2 : ext$/k$ contained in E

$$\sigma : E \overset{\text{emb.}}{\hookrightarrow} L$$

$$\Rightarrow \sigma(E_1E_2) = \sigma(E_1)\sigma(E_2)$$

pf. $$\sigma\left(\frac{a_1b_1 + \cdots + a_nb_n}{a_1'b_1' + \cdots + a_m'b_m'}\right) = \frac{a_1^\sigma b_1^\sigma + \cdots + a_n^\sigma b_n^\sigma}{a_1'^\sigma b_1'^\sigma + \cdots + a_m'^\sigma b_m'^\sigma}$$ is the elem of $\sigma(E_1)\sigma(E_2)$

and is surjective.

prop. 2.3 k. field. $f \in k[x]$. $\deg f \geq 1$

$\Rightarrow \exists$ an ext E of k. in which f have a root.

Pf. may assume. $f(x) = p$: irred. in $k[x]$

$$\sigma : k[x] \longrightarrow k[x]/(p(x))$$

$$x \longmapsto \sigma(x) = \xi = x + (p(x))$$

$$p(x) \longmapsto 0 = (p(x))^\sigma = p^\sigma(x^\sigma) = p^\sigma(\xi)$$

$(\sigma|_k)$ $\sigma : k \longrightarrow k[x]/(p(x))$ (PID; irred $\Rightarrow$ max $\Rightarrow$ $k[x]/(p(x))$ field.) injective field hom

k: field
ideal of $f = \{0\}$ or k

$\ker(\sigma)$: ideal of k. $\Rightarrow$ $\ker(\sigma) = \{0\}$.
$\ker(\sigma) \neq k$

i.e. $\sigma : k \xhookrightarrow{\text{emb.}} F = k[x]/(p(x))$ s.t. $p^\sigma(x)$ has a root ξ in F

now, we still don't get a root for $p(x)$
but $p^\sigma(x)$. next we do the ext.

extension

now $\tilde{\sigma} : (F - \sigma k) \sqcup k \longrightarrow F$

$$\begin{tikzcd} E \arrow[r, hook, "\tilde{\sigma}"] & F \\ k \arrow[u, hook] \arrow[r, hook, "\text{emb.}"', "\sigma"] & F \arrow[u, "\text{id}"'] \end{tikzcd}$$

$$\left.\begin{array}{l} \tilde{\sigma}|_k = \sigma \\ \tilde{\sigma}|_{F-\sigma k} = \text{id} \end{array}\right) \quad \tilde{\sigma} : \text{bijection as sets}$$

on E. define a field structure.

$$\begin{cases} xy \triangleq \tilde{\sigma}^{-1}(\tilde{\sigma}(x)\,\tilde{\sigma}(y)) \\ x+y \triangleq \tilde{\sigma}^{-1}(\tilde{\sigma}(x)+\tilde{\sigma}(y)) \end{cases} \Rightarrow E \text{ is a field. } \quad k \subseteq E.$$

$\Rightarrow$ $\tilde{\sigma}$ $E \xrightarrow{\sim} F$.

now : $p(\tilde{\sigma}^{-1}(\xi)) \longrightarrow p^\sigma(\xi) = 0$

$\Rightarrow$ $p(\tilde{\sigma}^{-1}(\xi)) = 0$. by isomorphism $\square$

Cor 2.4 k: field

$f_1, \dots, f_n \in k[x]$. $\deg f_i \geq 1$

$\Rightarrow$ $\exists$ an ext E of k. in which f_i has a root in E

def A field L is called algebraically closed.

if every polynomial in $L[x]$ has a root in L

Thm 2.5 k field. $\exists$ an alg closed field containing k.

pf. First construct E_1/k, s.t. every polynomial in $k[x]$ degree ≥ 1. has a root in E_1

Δ tricky

(Artin) $\forall f \in k[x]$ $\deg f \geq 1$ $\xrightarrow{\text{associate a formal variable.}}$ X_f

S: the set of all X_f.

Form the polynomial ring $k[S]$

Claim. $I = (f(X_f) \mid X_f \in S)$. : ideal of $k[S]$

$\rightarrow$ I is not the unit ideal (proper. i.e. $\neq k[S]$)

pf of claim if $g_1 f_1(X_{f_1}) + \cdots + g_n f_n(X_{f_n}) = 1$.

$g_i \in k[S]$. write $X_{f_i} = X_i$

$\Rightarrow \sum_{i=1}^{n} g_i(x_1, \ldots, x_N) f_i(x_i) = 1$

variables may include $X_1 \sim X_n$ and more

write as $X_{n+1} \ldots X_N$.

$N \geq n$.

let F : finite ext $/k$. in which $f_1, \dots, f_n$ have a root. α_i

let $\alpha_i = 0$ for $i = n+1 \dots N$.

Substitue α_i for x_i in our relation

$$\Downarrow$$

$$\sum_{i=1}^{n} g_i(\alpha_1, \dots, \alpha_N) f_i(\alpha_i) = 0 = 1 \quad \divideontimes$$

$\square$ of claim.

$\therefore I = (f(x_f) \mid x_f \in S) \subset \underset{\text{some max.}}{\underline{m}} \subset k[S]$

$$\sigma : k[S] \longrightarrow k[S]/\underline{m}$$

$$(k \longrightarrow \sigma k)$$

$$f(x_f) \longmapsto f^{\sigma}(\underline{\sigma x_f}) = 0$$

$$I \subset \underline{m}.$$

$\Rightarrow$ let $f \in k[x]$, $\deg f \geq 1$. f^{σ} has a root in $k[S]/\underline{m}$. which is ext of σk.

$\therefore$ By similar argument as in prop 2.3

we have E_1 : ext$/k$. s.t. every $f(x) \in k[x]$ has a root in E_1

Inductively. $k \subset E_1 \subset E_2 \dots \subset E_n \subset$

all $f \in E_1[x]$ has a root in E_2

$\sim$ $E_2[x]$ $\sim$ in E_3 ...

Let E = union of all E_n

$\Rightarrow E$, a field $\because x, y \in E \Rightarrow x, y \in E_n$ for some n

$\Rightarrow xy \in E_n \subset E$, $x+y \in E_n \subset E$.

: every polynomial in $E[x]$, thus its coff in E_n for some n.

$\Rightarrow$ have a root $\subset E_{n+1} \subset E$

$\Rightarrow E$ is alg closed $\square$.

Cor 2.6 k : field.

Then $\exists$ an ext k^a, which is algebraic over k and algebraically closed.

pf by Thm. 2.5. $\exists$ E: ext of k E. alg closed.

let k^a = union of all <u>subextension</u> of E. alg$/k$.

$k^a = \bigcup_{\substack{k \in F \subset E \\ F: \text{alg}/k}} F = \{\alpha \in E \mid \alpha: \text{alg}/k\}$

up to E ?

$\Rightarrow k^a$. alg over k.

we already have k^a: alg$/k$.

if $\alpha \in E$. α: alg$/k^a$ then $\Rightarrow \alpha$: alg$/k$. (Prop 1.7).

$f \in k^a[x] \subset E$. $\deg f \geq 1$ then f has a root $\alpha \in E$.

$\therefore \alpha$ alg$/k^a$. $\Rightarrow \alpha$ alg$/k^a$

$\Rightarrow \alpha \in k^a$

$\Rightarrow k^a$ alg closed. $\square$

k. field.

$\sigma : k \xrightarrow{\text{emb.}} L$. L is alg closed.

E: ext of k.

Want to study the extension of σ to E/k

Let $E = k(\alpha)$, α: alg $/k$. $p(x) = \mathrm{Irr}(\alpha, k, x)$.

$$P(x) \longrightarrow p^\sigma(x) \in \sigma k[x] \subseteq L \qquad \exists \beta \in L.\ p^\sigma(\beta) = 0$$

define an extension of σ

$$\tilde{\sigma} : E = k(\alpha) = k[\alpha] \hookrightarrow L$$

$$f(\alpha) \longmapsto f^\sigma(\beta)$$

$$0 = p(\alpha) \longmapsto p^\sigma(\beta) = 0$$

well-defined ? $g(\alpha) = f(\alpha) \Rightarrow (g-f)(\alpha) = 0$.

$\Rightarrow p(x) \mid (g-f)(x)$

$p^\sigma(x) \mid (g^\sigma - f^\sigma)(x) \Rightarrow g^\sigma(\beta) = f^\sigma(\beta)$

$\Rightarrow \tilde{\sigma}$. homomorphism. extending σ

Prop 2.7. $\sigma : k \xrightarrow{\text{emb}} L$ L. alg closed

$\tilde{\sigma} : E = k(\alpha) = k[\alpha] \longrightarrow L$

α. alg $/k$.

(The number of extension) $\leq \deg \mathrm{Irr}(\alpha, k, x)$.

(distinct roots of $p(x)$ in L) $\qquad \| \qquad \deg p(x)$.

Thm. 2.8 k: field. $\sigma: k \overset{\text{emb}}{\hookrightarrow} L$. L alg closed.

E: alg ext$/k$.

$\Rightarrow \exists$ an extension of σ to embedding of E into L

$$\begin{tikzcd} E \arrow[dr, "\exists \tilde{\sigma}"] & \\ k \arrow[u, hook, "\text{inc}"] \arrow[r, hook, "\sigma", "\text{emb.}"'] & L \end{tikzcd}$$

alg

alg closed

即. 任何 alg ext 都能 embedding 到 alg closed 中去

If moreover E is alg closed. L: alg$/\sigma k$.

$\Rightarrow$ any such ext $\tilde{\sigma}: E \hookrightarrow L$. is an iso

Pf or thm 2.8

$$S = \{ (F, \tau) \mid E \supseteq F \supseteq k, \ \tau: F \overset{\text{emb.}}{\hookrightarrow} L \ \ \tau|_k = \sigma \}.$$

S: nonempty for $(k, \sigma) \in S$.

(F, τ). $(F', \tau') \in S$

we write $(F, \tau) \leq (F', \tau')$ if $F \subseteq F'$. and $\tau'|_F = \tau$.

If we have a chain in S.

i.e. $(F_1, \tau_1) \leq (F_2, \tau_2) \leq (F_3, \tau_3) \leq \cdots$

let $F = \bigcup F_i \Rightarrow$ a field contained in E

$\}$

$\tau|_{F_i} = \tau_i$ (definition of τ.

Then. $(F, \tau) \in S$. $\therefore (F, \tau)$ is upper bound of the chain.

By Zone's Lemma $\exists$ a max elem in S. say $(K, \lambda) \in S$. $\lambda|_K = \sigma$

<u>claim</u>. $K = E$

<u>pf of claim</u>: if not. $K \subsetneq E \Rightarrow \exists \alpha \in E . \alpha \notin K$.

$$\begin{tikzcd} K \arrow[r, hook, "\lambda"] \arrow[d, hook] & L \\ K(\alpha) \arrow[ur] \arrow[d, hook] & \\ E & \end{tikzcd}$$

$\exists \tilde{\lambda}$ (by prop. 2.7) $\Rightarrow (K(\alpha), \tilde{\lambda}) \geq (K, \lambda)$ $\times$

Moreover part

now:

$$\begin{tikzcd} \text{alg closed } E \arrow[dr, hook, "\tilde{\sigma}"] & \\ k \arrow[u, dash, "\text{alg}"] \arrow[r, hook, "\sigma"'] & L . \text{ alg closed.} \end{tikzcd}$$

$$\begin{tikzcd} L \\ \tilde{\sigma}E \arrow[u, dash, "\text{alg}"] \\ \sigma k \arrow[u, dash, "\text{alg}"] \arrow[uu, bend left, dash, "\text{alg}"] \end{tikzcd}$$

$\tilde{\sigma}E$: alg closed. $\Rightarrow L = \tilde{\sigma}E$.

why? alg ext of alg closed. is itself.

pf. if $L \neq \tilde{\sigma}E$

$\exists \alpha \in L - \tilde{\sigma}E$. α. alg $/\sigma E$

$\exists p(x) \in (\sigma E)[x]$. st. $p(\alpha) = 0$. $\Rightarrow \alpha \in \sigma E$. $\times$

Cor 2.9 k. field. E, E' alg $/k$

Assume E, E' : alg closed.

$\Rightarrow \exists\, \tau : E \hookrightarrow E'$. inducing id on k. $\Rightarrow$ k^a unique.

Rmk. k^a : algebraic closure of k. unique up to iso.

or $\bar{k}$

Rmk $\mathbb{Q} \subset \mathbb{Q}^a \subseteq \mathbb{C}$ alg closed.

$$\mathbb{Q}^a = \{ x \in \mathbb{C} \mid x : \text{alg}/\mathbb{Q} \}.$$

$\mathbb{Q}$: countable $\Rightarrow$ $\mathbb{Q}^a$ countable

Pf. polynomial $\in \mathbb{Q}[x]$

$$\begin{pmatrix} \text{roots of} \\ a_1x + a_0 \end{pmatrix} \begin{pmatrix} \text{roots of} \\ a_2x^2 + a_1x + a_0 \end{pmatrix} \cdots \qquad \text{all countable}$$

Countable union of countable sets.