Algebraic closure and transcendent extensions.

Definition. A field extension K of F is called an algebraic closure (resp. separable closure)
(代数闭包) (可分闭包)

if ① K/F is an algebraic extension (resp. algebraic separable extension)

② Every polynomial (resp. separable polynomial) $f(x) \in F[x]$ splits completely in K.

· Typically, we write F^{alg} or $\bar{F}$ for algebraic closure, F^{sep} for separable closure

Subtlety: (1) did not state existence
(2) did not say any "minimality" > will prove later

Note: If E/F is the splitting field of $f(x) \in F[x]$
then $E \hookrightarrow F^{alg}$. If $f(x)$ is separable $\Rightarrow E \hookrightarrow F^{sep}$

So "algebraic closure" contains any splitting field of F

Definition A field K is called algebraically closed if all polynomials in $K[x]$ splits
($\Leftrightarrow$ the only irreducible polynomials in $K[x]$ are linear & constant ones
$\Leftrightarrow$ K has no nontrivial algebraic extension.)

A field K is called separably closed if all nontrivial algebraic extensions are inseparable.

Proposition (1) An algebraic closure of an algebraically closed field K is just K.
(b/c $\forall a \in K^{alg}$ is the zero of a polynomial in $K[x] \Rightarrow a \in K$ ✓)

(2) A separable closure of a separably closed field K is just K. ✓

(3) If $\bar{F}$ is an algebraic closure of F, then $\bar{F}$ is algebraically closed.

Proof of (3): Suppose α is algebraic over $\bar{F}$. WTS $\alpha \in \bar{F}$

Consider $m_{\alpha,\bar{F}}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ minimal polynomial of α over $\bar{F}$.

$$\left.\begin{array}{l} F(\alpha, a_{n-1}, \cdots, a_0) \\ \quad | \quad \text{finite} \\ F(a_{n-1}, \cdots, a_0) \\ \quad | \quad \text{finite} \\ F \end{array}\right\} \Rightarrow \alpha \text{ is the zero of a polynomial in } F \Rightarrow \alpha \in \bar{F}$$

Theorem (1) Any field F is contained in an algebraically closed field K (proof see notes)

(2) If $F \subseteq K$ with K algebraically closed, then

$\bar{F} := \{x \in K ;\ x \text{ algebraic over } F\}$ is an algebraic closure of F

$F^{sep} := \{x \in K ;\ x \text{ algebraic \& separable over } F\}$ is a separable closure of F.

(3) Algebraic closure is unique up to isomorphisms (not a canonical isom.)

Proof. (2) By definition, $\bar{F}/F$ is an algebraic extension.

Every polynomial $f(x) \in F[x]$ splits completely in K, so $f(x)$ splits over $\bar{F}$.

Same argument works for F^{sep}

(3) If $F \hookrightarrow \bar{F}$, $F \hookrightarrow \bar{F}'$ $\rightsquigarrow$ extension $\eta : \bar{F} \hookrightarrow \bar{F}'$

$\Rightarrow \bar{F}'$ is an algebraic extension of $\eta(\bar{F})$

But $\eta(\bar{F})$ is algebraically closed $\Rightarrow \eta(\bar{F}) = \bar{F}'$. ✓

Transcendence extension.

Definition (1) Let K/F be a field extension. A subset $\{\alpha_1, \cdots, \alpha_n\} \subseteq K$ is algebraically independent over F (在F上代数无关), if there is no nonzero polynomial $f(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$ such that $f(\alpha_1, \cdots, \alpha_n) = 0$.

This gives rise to $\eta : F(x_1, \cdots, x_n) \longrightarrow K$

$$p(\underline{x})/q(\underline{x}) \longmapsto p(\underline{\alpha})/q(\underline{\alpha}).$$

(2) A transcendence base (超越基) for K/F is a maximal subset of K which is algebraically independent $/F$.

This is equivalent to $\alpha_1, \cdots, \alpha_n$ algebraically independent $/F$

and $K/F(\alpha_1, \cdots, \alpha_n)$ is algebraic

Theorem The extension K/F has a transcendence base and any two transcendence bases of K/F have the same cardinality.

Proof: Existence of transcendence base follows from Zorn's lemma.

Need to show that $\#\{\text{an algebraic indep set}\} \leq \#\{\text{a transcendence basis}\}$

First finite case, $\{\beta_1, \cdots, \beta_m\}$ $\quad$ $\{\alpha_1, \cdots, \alpha_n\}$

(Replace the condition $\{\alpha_1, \cdots, \alpha_n\}$ being a transcendence basis by $K/F(\alpha_1, \cdots, \alpha_n)$ algebraic)

- If $\{\beta_1, \cdots, \beta_m\} \subseteq \{\alpha_1, \cdots, \alpha_n\} \Rightarrow m \leq n$.
- For $\beta_1 \rightsquigarrow \alpha_1, \cdots, \alpha_n, \beta_1$ are algebraically dependent $\rightsquigarrow f(\alpha_1, \cdots, \alpha_n, \beta_1) = 0$

$\exists$ some α_i where the coeffs is nontrivial, say α_1

K / algebraic $F(\alpha_1, \cdots, \alpha_n, \beta_1)$ finite $\Rightarrow K/F(\alpha_2, \cdots, \alpha_n, \beta_1)$ is algebraic

$F(\alpha_1, \cdots, \alpha_n)$ $\quad$ $F(\alpha_2, \cdots, \alpha_n, \beta_1)$ $\quad$ Done by exchange argument.

Infinite transcendence base case: Zorn's lemma.

Definition. The cardinality of a transcendence base for K/F is called the transcendence degree for K/F (超越次數)

Note: $\mathbb{Q}(\pi)$ is isomorphic to $\mathbb{Q}(t)$.

Caveat: If $\{\alpha_1, \cdots, \alpha_n\}$ and $\{\alpha_1', \cdots, \alpha_n'\}$ are transcendence bases,

in general, $F(\alpha_1, \cdots, \alpha_n) \neq F(\alpha_1', \cdots, \alpha_n')$

E.g. $\mathbb{Q}(x^2) \subseteq \mathbb{Q}(x)$.

Proposition Let t be a transcendental variable over F.

If $p(t), q(t) \in F[t]$ be relatively prime polynomials that are not both constant,

then $[F(t) : F\left(\frac{p(t)}{q(t)}\right)] = \max\left(\deg p(x), \deg q(x)\right)$

Proof: Writing $y = \frac{p(t)}{q(t)}$, the minimal polynomial of t over $F(y)$ is

$$p(t) - y \cdot q(t) = 0 \quad \text{or} \quad q(t) - \frac{1}{y} p(t) = 0. \quad \square$$

Definition. An extension K/F is called **purely transcendent** if $K \simeq F(\alpha_1, \cdots, \alpha_n)$.

Question. How to describe general K/F? Integral version?

E.g. $F(x)\left(\sqrt{x^3+x}\right) \supseteq F[x,y]/(y^2 - x^3 - x)$ General $K \supseteq \cdots$ ← a good one?

$F(x) \supseteq F[x]$ $\quad$ $F(\alpha_1, \cdots, \alpha_n) \supseteq F[\alpha_1, \cdots, \alpha_n]$

See this geometrically?

Basic idea: $U \subseteq \mathbb{C}^n$ open $\longleftrightarrow$ $\mathcal{O}(U) = \{\text{holomorphic functions on } U\}$

$x \in U \rightsquigarrow \mathfrak{m}_x = \{f \in \mathcal{O}(U),\ f(x) = 0\}$

$\mathcal{O}(U)/\mathfrak{m}_x \simeq \mathbb{C}$ so $\mathfrak{m}_x$ is a maximal.

(A function f on U can be evaluated at every point of U.)

- Let k = an algebraically closed field (e.g. $k = \mathbb{C}$)
- space k^n $\longleftrightarrow$ polynomial ring $k[x_1, \cdots, x_n]$
  - A polynomial f evaluated at $(a_1, \cdots, a_n)$ is $f(a_1, \cdots, a_n)$

So each $\underline{a} = (a_1, \cdots, a_n) \in k^n \rightsquigarrow$ maximal ideal $\mathfrak{m}_{\underline{a}} = (x_1 - a_1, \cdots, x_n - a_n)$.

Hilbert Nullstellensatz (weak form) Assume that k is algebraically closed.

Every maximal ideal of $k[x_1, \cdots, x_n]$ is of the form $(x_1 - a_1, \cdots, x_n - a_n)$

There's a bijection $\{\text{maximal ideals of } k[x_1,\cdots,x_n]\} \longleftrightarrow k^n$

· Some commutative algebra.

* R = a commutative ring $\supseteq I$ ideal.

Define the radical of I to be $\sqrt{I} = \{f \in R \mid f^m \in I \text{ for some } m\} \supseteq I$

check that $\sqrt{I}$ is an ideal:

① if $f, g \in \sqrt{I} \Rightarrow f^m, g^n \in I \Rightarrow (f+g)^{m+n-1} = f^m \cdot a + g^n \cdot b \in I. \Rightarrow f+g \in \sqrt{I}.$

② $\forall\, a \in R,\ f \in \sqrt{I} \Rightarrow f^m \in I \Rightarrow (af)^m = a^m f^m \in I \Rightarrow af \in \sqrt{I}.$

Definition. An ideal $I \subseteq R$ is called radical if $I = \sqrt{I}$.

Fact: If $\mathfrak{p}$ is a prime ideal s.t. $I \subseteq \mathfrak{p} \Rightarrow \sqrt{I} \subseteq \mathfrak{p}$ (same for $\mathfrak{p}$ maximal.)

Proof: If $a \in \sqrt{I} \Rightarrow a^n \in I \subseteq \mathfrak{p}$ for some $n \in \mathbb{N}$

$\Rightarrow a \in \mathfrak{p}$. □

Picture: Subsets of k^n $\longleftrightarrow$ ideals of $k[x_1,\cdots,x_n]$

$Z \longmapsto I(Z) = \{f \in k[x_1,\cdots,x_n] \mid f(z)=0\ \forall z \in Z\}$

$= \bigcap_{z \in Z} m_z.$

$Z(I) := \{a \in k^n \mid f(a)=0\ \forall f \in I\} \longmapsto I$

$Z(f) := \{a \in k^n \mid f(a)=0\} \longmapsto f \in k[x_1,\cdots,x_n]$

So if $I = (f_1,\cdots,f_m)$, then $Z(I) = Z(f_1) \cap \cdots \cap Z(f_m)$

Definition. An algebraic subset (or a variety) of k^n is a subset of the form $Z(I)$ for some ideal $I \subseteq k[x_1,\cdots,x_n]$

Hilbert Nullstellensatz (strong form) There is a one-to-one correspondence

$$\{\text{Algebraic subsets of } k^n\} \longleftrightarrow \{\text{radical ideals of } k[x_1, \dots, x_n]\}$$
$$Z \longmapsto I(Z)$$

<u>Basic philosophy</u>: Algebraic subsets of k^n = "good spaces"

$$\updownarrow$$

$\mathcal{O}(Z) := k[x_1, \dots, x_n] / I(Z)$ = "functions on Z" because all functions in $I(Z)$ do not change the values on Z.

Maximal ideals of $\mathcal{O}(Z) \longleftrightarrow$ maximal ideals m of $k[x_1, \dots, x_n]$ s.t. $I(Z) \subseteq m$

$\longleftrightarrow \underline{a} \in k^n$ s.t. $m_{\underline{a}} \supseteq I(Z)$

($m_{\underline{a}}$ = precisely polys vanishes at $\underline{a}$)

$\longleftrightarrow \underline{a} \in k^n$ s.t. $I(Z)$ vanishes at $\underline{a}$

$\longleftrightarrow \underline{a} \in Z$.

So points on $Z \longleftrightarrow$ maximal ideal of $\mathcal{O}(Z)$