Field Extensions

Point of view for studying fields:

* prime fields: $\mathbb{F}_p$, $\mathbb{Q}$ smallest possible fields
* build new fields from the known ones: $\mathbb{Q}(i)$, $\mathbb{Q}(\alpha)$ for α a root of some irreducible polynomial

$\mathbb{Q}(x) := \mathrm{Frac}(\mathbb{Q}[x])$ "transcendental extensions"

Definition The characteristic (特征) of a field F, denoted by $\mathrm{char}(F)$, is

- the smallest possible integer p s.t. $p \cdot 1_F = 0$ if such p exists
- 0, otherwise.

Note: If $\mathrm{char}(F) > 0$, it must be a prime number $p > 0$

(b/c If $\mathrm{char}(F) = m \cdot n$ for $m, n \in \mathbb{N} \Rightarrow mn = 0$ in $F \Rightarrow$ either m or n is zero in F.)

Definition The prime field (素域) of a field F is the smallest field of F containing 1_F

$$= \begin{cases} \mathbb{F}_p & \text{if } \mathrm{char}(F) = p > 0 \\ \mathbb{Q} & \text{if } \mathrm{char}(F) = 0 \end{cases}$$

Notation If $F \subseteq K$ is a subfield of a field, we say that K is a field extension (域扩张) of F.

Sometimes, we call F the base field (基域)

Any field E such that $F \subseteq E \subseteq K$ is called an intermediated field (中间域)

We often write

$$\begin{matrix} K \\ | \\ E \\ | \\ F \end{matrix} \quad \text{or} \quad K/E/F$$

Note: $F \subseteq K$ makes K an F-vector space

Definition. The degree (次数) of the field extension K/F is $[K:F] = \dim_F(K)$

The extension is finite / infinite if $[K:F]$ is.

↑ compare to the index of groups

Theorem. Let $F \subseteq E \subseteq K$ be fields. Then $[K:F] = [K:E][E:F]$

Proof: Put $[K:E]=n$, $[E:F]=m$

$$[K:F]\left(\begin{array}{c} K \\ | \\ E \\ | \\ F \end{array}\right)\begin{array}{l}[K:E]=n \\ \\ [E:F]=m\end{array}$$

Let $\beta_1, \cdots, \beta_n$ be an E-basis of K; $\alpha_1, \cdots, \alpha_m$ be an F-basis of E

Then $\forall x \in K$ can be written as

$$a_1\beta_1 + \cdots + a_n\beta_n \quad \text{for } a_i \in E$$

and each a_j can be written as a sum $a_j = c_{1j}\alpha_1 + \cdots + c_{mj}\alpha_m$ with $c_{ij} \in F$

Then we have $x = \sum c_{ij}\alpha_i\beta_j$

This shows that $\{\alpha_i\beta_j\}_{\substack{i=1,\cdots,m \\ j=1,\cdots,n}}$ form an F-basis of K.

Conversely, we show that $\{\alpha_i\beta_j\}$ is F-linearly independent.

Suppose $c_{ij} \in F$ are given so that $\sum_{i,j} c_{ij}\alpha_i\beta_j = 0$

Then $\sum_j \underbrace{\left(\sum_{i=1}^{m} c_{ij}\alpha_i\right)}_{\in E} \cdot \beta_j = 0$

Since $\beta_1, \cdots, \beta_n$ are E-linearly independent $\Rightarrow \sum_{i=1}^{m} c_{ij}\alpha_i = 0$

As $\alpha_1, \cdots, \alpha_m$ are F-linearly independent $\Rightarrow$ each $c_{ij} = 0$. $\square$

Example: $\mathbb{Q}(\sqrt[6]{2}) = \left\{ a_0 + a_1 \cdot 2^{\frac{1}{6}} + \cdots + a_5 \cdot 2^{\frac{5}{6}} \mid a_i \in \mathbb{Q} \right\}$

$$\text{degree} = 6 \left(\begin{array}{c} \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}\right)\begin{array}{l}\text{so, has degree 3.} \\ \\ \text{degree} = 2\end{array}$$

Lemma. All homomorphisms between fields are injective!

For field E, F, every homomorphism $\eta: F \to E$ is injective,

and thus realizes E as a field extension of $\eta(F)$.

Proof: $\ker\eta$ is an ideal of F: (0) or F

But our convention is $\eta(1_F) = 1_E \neq 0_E \Rightarrow \ker\eta = (0) \Rightarrow \eta$ is injective.

Construction of field extensions

F field, $p(x) \in F[x]$ an irreducible polynomial of degree n.

Then $(p(x))$ is a prime ideal $\Rightarrow$ maximal

$\Rightarrow K := F[x]/(p(x))$ is a field, containing F.

Setting $\theta := x \bmod (p(x))$

Then $K = \{a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} \mid a_0, a_1, \cdots, a_{n-1} \in F\}$

need to show that every polynomial $a(x)$ can be written uniquely as $a(x) = q(x)\cdot p(x) + r(x)$ with $\deg r < n$

Then $a(x) \equiv r(x) \bmod (p(x)$

So $\dim_F K = [K:F] = n$.

i.e. K is the field extension of F of deg n, determined by $p(x)$.

Lemma: Equation $p(z) = 0$ has a zero in K

Proof: Say $p(x) = c_0 + c_1x + \cdots + c_nx^n \in F[x]$

Then $p(\theta) = c_0 + c_1\theta + \cdots + c_n\theta^n \equiv c_0 + c_1x + \cdots + c_nx^n \equiv 0 \bmod (p(x))$

So θ is a "tautological zero" of $p(z)$ in K.

Examples: ① $\mathbb{R}[x]/(x^2+1) \xrightarrow{\simeq} \mathbb{C}$

$\eta_1 : ax+b \longmapsto ai+b$

$\eta_2 : ax+b \longmapsto -ai+b$

We view $\mathbb{R}[x]/(x^2+1)$ as an "abstract extension" of $\mathbb{R}$

it has two "realizations" η_1, η_2 to be isomorphic to $\mathbb{C}$.

② $K = \mathbb{Q}[x]/(x^3-2)$

"Realization 1" $r_1 : K \hookrightarrow \mathbb{R}$ $\quad K \simeq r_1(K)$

$x \longmapsto \sqrt[3]{2}$

"Realization 2" $r_2, r_3 : K \hookrightarrow \mathbb{C}$

$r_2(x) = e^{2\pi i/3} \cdot \sqrt[3]{2}$, $r_3(x) = e^{4\pi i/3} \cdot \sqrt[3]{2}$

• $r_1(K)$, $r_2(K)$ are different "field extensions" of $\mathbb{Q}$, but they are isomorphic abstractly.

③ $K = \mathbb{F}_2[x]/(x^2+x+1)$ is a field extension of $\mathbb{F}_2$ of deg 2

So $\#K = 4$, a field of 4 elements

Definition Let K be a field extension of F, and let $\alpha_1, \cdots, \alpha_n \in K$

$F(\alpha_1, \cdots, \alpha_n)$:= smallest subfield of K containing F,

called the field generated by $\alpha_1, \cdots, \alpha_n$

If $K = F(\alpha)$ for some $\alpha \in K$, we say that K/F is a simple extension (单扩张)

If $K = F(\alpha_1, \cdots, \alpha_n)$, we say that K/F is finitely generated

Remark: $F(\alpha_1, \alpha_2) = (F(\alpha_1))(\alpha_2)$

Theorem. Let K/F be a field extension and let $\alpha \in K$. We have a dichotomy: (二选一)

Either (1) $1, \alpha, \alpha^2, \cdots$ are linearly independent over F,

in this case $F(\alpha) \simeq F(x) := \mathrm{Frac}(F[x])$;

Or (2) $1, \alpha, \alpha^2, \cdots$ are linearly dependent over F,

then there exists a unique monic polynomial $m_\alpha(x) = m_{\alpha,F}(x)$,

called the minimal polynomial of α over F (α在F上的极小多项式),

that is irreducible over F, and $m_\alpha(\alpha) = 0$

Moreover, $F(\alpha) \simeq F[x]/(m_\alpha(x))$ and $[F(\alpha):F] = \deg m_\alpha(x)$

Proof: Case 1: $\varphi : F[x] \longrightarrow K$ is an injective homomorphism

$f(x) \longmapsto f(\alpha)$

This clearly extends to a homomorphism $\varphi : F(x) := \mathrm{Frac}(F[x]) \longrightarrow K$ and is injective

$f(x)/g(x) \longmapsto f(\alpha)/g(\alpha)$

Its image is $F(\alpha) \simeq F(x)$

Case 2: $\varphi : F[x] \longrightarrow K$ not injective

$f(x) \longmapsto f(\alpha)$

Then $\ker \varphi = (p(x))$ is a prime ideal $\Rightarrow$ maximal ideal (may take $p(x)$ to be monic)

(This $p(x)$ is the minimal polynomial of α: the nonzero poly with minimal degree in $\ker \varphi$.)

$F(\alpha) = \mathrm{Im}\,\varphi \simeq F[x]/(p(x))$

Definition In the above theorem, case 1 $\Rightarrow$ say α is transcendental over F (在F上超越)

case 2 $\Rightarrow$ say α is algebraic over F (在F上代数)

We say the extension K/F is algebraic if every element α of K is algebraic over F

(i.e. $[F(\alpha):F]$ finite.)

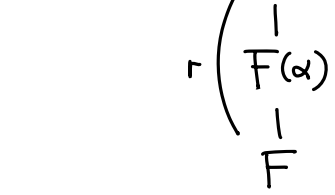
Theorem The following are equivalent for a field extension K/F

(1) K/F is finite

(2) K/F is finitely generated + algebraic

Proof: (1) $\Rightarrow$ (2) K/F is finite, so K is generated over F by basis elements

$\forall \alpha \in K$, $1, \alpha, \cdots, \alpha^r$ are linearly dependent $/F \Rightarrow \alpha$ algebraic $/F$



Cor: $[F(\alpha):F] \mid [K:F]$.

(2) $\Rightarrow$ (1). Slightly later....

Lemma $K/E/F$ (tower $K \supseteq E \supseteq F$). Given field extensions $K/E/F$, and $\alpha \in K$

$\deg(m_{\alpha,E}(x)) \leq \deg(m_{\alpha,F}(x))$. In fact $m_{\alpha,E}(x) \mid m_{\alpha,F}(x)$ in $E[x]$

Proof: Since $m_{\alpha,F}(\alpha) = 0$, so $m_{\alpha,F}(x) \in (m_{\alpha,E}(x))$ in $E[x]$. $\square$

Corollary. $[E(\alpha) : E] \leq [F(\alpha) : F]$

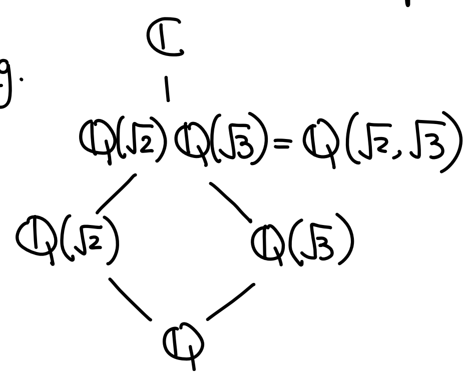
$$[E(\alpha):E] = \deg m_{\alpha,E}(x), \qquad [F(\alpha):F] = \deg m_{\alpha,F}(x)$$

Definition. Let K/F be a field extension and $F \subseteq E_i \subseteq K$ (for $i = 1, 2$) be intermediate fields

Define $E_1E_2 :=$ minimal field that contains both E_1 and E_2

↑ called the composite (复合) of E_1 and E_2

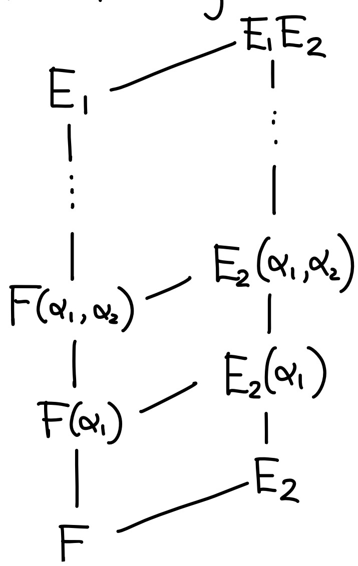
E.g.



Corollary Let E_1, E_2 be two intermediate fields in the field extension K/F, s.t. $[E_i/F] < +\infty$

Then $[E_1E_2 : F] \leq [E_1 : F][E_2 : F]$

Proof: As E_1 is a finite extension of F; write $E_1 = F(\alpha_1, \cdots, \alpha_n)$



$[E_2(\alpha_1) : E_2] \leq [F(\alpha_1) : F]$

$[E_2(\alpha_1, \alpha_2) : E_2(\alpha_1)] \leq [F(\alpha_1, \alpha_2) : F(\alpha_1)]$

$\cdots$

Take product $\Rightarrow [E_1E_2 : E_2] \leq [E_1 : F]$

Proof of Theorem (2) $\Rightarrow$ (1) $\quad K = F(\alpha_1, \cdots, \alpha_n) = F(\alpha_1) \cdots F(\alpha_n)$

$\Rightarrow [K:F] \le [F(\alpha_1):F] \cdots [F(\alpha_n):F]$ $\square$

Corollary Suppose in a field extension K/F, $\alpha, \beta \neq 0 \in K$ are algebraic $/F$

Then $\alpha \pm \beta$, $\alpha \cdot \beta$, α/β are all algebraic over F

(b/c they all lie in $F(\alpha,\beta)$, which is finite $/F$.)

So $\{\alpha \in K;\ \alpha$ algebraic over $F\}$ is a subfield of K,

called the algebraic closure of F in K (F在K中的代数闭包).

Example: $\mathbb{C}/\mathbb{Q} \rightsquigarrow \{\alpha \in \mathbb{C};\ \alpha$ algebraic over $\mathbb{Q}\} =: \mathbb{Q}^{alg}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

$\Updownarrow$

α is the zero of a polynomial $f(x) \in \mathbb{Q}[x]$

Theorem. If K/E and E/F are both algebraic extensions, then K/F is algebraic.

Proof: Let $\alpha \in K$; its minimal polynomial $m_\alpha(x)$ over E

$\| $

$x^n + c_{n-1}x^{n-1} + \cdots + c_0$

Each c_i is algebraic over F.

So
$$\begin{array}{l} F(c_0, \cdots, c_{n-1}, \alpha) \\ \quad | \quad \text{) deg } n \\ F(c_0, \cdots, c_{n-1}) \\ \quad | \quad \text{) finite} \\ F \end{array}$$

$\Rightarrow F(\alpha) \subseteq F(c_0, \cdots, c_{n-1}, \alpha)$ ↑ finite $/F$

So $[F(\alpha):F] < \infty$