域论：(Dummit 目录) Lib. 代数(超越)扩张定义；域论basic复习，

def: K is field containing field F, K是F的field extension. 记为 K/F (K over F)
实际上 every field 是某 prime field 的 extension

def: degree (也叫 relative deg, index) of K/F, 记为 $[K:F] = \dim_F K$,
the dimension of K as vector space over F

Prop P512: $\varphi: F \to F'$ is homomorphism of field; then $\varphi = 0$ 或 φ is injective
即 $\text{img}(\varphi) = 0$ 或 $\text{img}(\varphi) \cong F$

若 $\exists b \in F'$ $b = \varphi(x) = \varphi(y)$, $\varphi(xy^{-1}) = e$
即WTS: $\varphi(e) = e$, 也就是 $e \in F$ $\varphi(1_{e \in F}) = e \in F'$

P513: { Lem0: ring homomorphism 的 kernel 是一个 ideal, kernel 指 $f(x) = 0$ 的原像
Lem1: I 为 R 的 ideals, R commutative 人 R is a field $\Leftrightarrow$ R 的 ideal 仅有 0 和 R, 即 $I = 0$ 或 $I = R$
且有1

"$\Rightarrow$" R is field, 每个元素均 unit
I 为 ideals, 设 I, 证毕. $(r) = R$ since $\forall r \in R$ $\exists t = r^{-1}$ s.t. $r = rt \in (r)$ $\Rightarrow I = R$
$(r) \subseteq I$ since I ideals
即证 I 证毕. I 中只有 0. $I = 0$.
"$\Leftarrow$" 即反证 R not field, $\exists a \in R$ not a unit
consider $I = (a) \neq 0$, $1 \notin (a) = R$ 即 $\forall r \in R$, $r = ax$ some $x \in R$, let $r = 1$ 即可

$\therefore$ 由以上可知, F is a field, ideals in F 仅有 0 和 F

回到 $\varphi: F \to F'$, 若非 $0 \to 0$
$\ker\varphi = \{x \in F : \varphi(x) = 0\} = 0$ 或 F, since it's ideals
设 $\varphi(1) = 1$, $\varphi(a) = 1 \Rightarrow \varphi(a-1) = 0$ { 设 a 可以取 F 中的零元, $\varphi = 0$ 即 $\ker\varphi = F$
$\ker\varphi = 0$, $a = 1$ 说明 φ 只有 e $\varphi(e) = e$ then inj

def(recall): ring homomorphism $\varphi: R_1 \to R_2$ 要满足加法和乘法
{ $\varphi(e) = \varphi(e)$ $e = 0$ 和 1. (加法e和乘法e)
$\varphi(x+y) = \varphi(x) + \varphi(y)$
$\varphi(xy) = \varphi(x) \cdot \varphi(y)$
$\ker\varphi$ for 0 是 ideals $\Rightarrow$ 这在 R_1 is field 时 $\ker\varphi = 0$ 或 R_1

Thm. P512, F is field, $p(x) \in F[x]$ irreducible, $\Rightarrow$ $\exists$ field K 含有 an isomorphic copy of F, in which $p(x)$ has a root.
(identify F with this iso copy shows that: $\exists$ extension of F where $p(x)$ has root)

consider $K = F[x]/(p(x))$

- $F[x]$ 为 PID ($I \subseteq F[x]$, $I = (g)$ for g with smallest deg in I) (ED)
  $p(x)$ irreducible in PID, then $(p(x))$ prime $\overset{PID}{\Leftrightarrow}$ maximal (各种路径可推)
- F is field, $(p(x))$ maximal $\Leftrightarrow$ $F[x]/(p(x))$ is field
- irr $\xrightarrow{UFD}$ prime $\xrightarrow{D}$ maximal $\overset{PID}{\Leftrightarrow}$ primal
- irr $\overset{ID}{\Leftarrow}$ maximal
- consider $\varphi: F[x] \to F[x]/(p(x))$ and $\varphi|_F \neq 0$
  $f(x) \mapsto f(x)+(p(x))$

  lem: field homomorphism injective or zero $\Rightarrow \varphi|_F$ injective

  $\therefore \varphi|_F(F) \cong F$, 即 $F[x]/(p(x))$ 中有与 F isomorphic 的域 …①
- in $F[x]/(p(x))$, ($\forall \varphi$ homo 不定) $p(\varphi(x)) = \varphi(p(x)) = p(x)+(p(x)) = (p(x))$

  and: $(f+(p(x)))+(g+(p(x))) = f+(p(x))$ iff $g \in (p(x))$; $(p(x))$ is the "zero" in $F[x]/(p(x))$

  $\therefore p(\varphi(x)) = 0$, $p(x)$ has a root $\varphi(x)$ in $F[x]/(p(x))$ …②

①+② $\Rightarrow$ $F[x]/(p(x))$ 为使 irreducible $p(x) \in F[x]$ 有 root 的, F 的 field extension

Rmk: • field extension 后形式可不同. 如 numerical $F \longrightarrow$ polynomial $F[x]/(p(x))$

• 例: x^2+1 在 $F = \mathbb{R}$ 中无根, irreducible, $\mathbb{R} \to \mathbb{C}$, $x^2+1=0$ has root i in $\mathbb{C}$

存在性由上方定理决定

Pf: Thm: F is field, $p(x) \in F[x]$, $p(x)$ irreducible; K is extension of F containing a root α of $p(x)$, $F(\alpha)$ is the subfield of K generated over F by α; then: $F(\alpha) \cong F[x]/(p(x))$

Rmk: 上个定理证了, 含 irr $p(x)$ 的域 F 可以扩张成含 $p(x)$ root 的域; 域可以扩成 $F[x]/(p(x))$

here WTS: 扩法不唯一, 但每种 field extension 之间 isomorphic ($F(\alpha)$ 也取了一种扩法)

bzd

- consider $\varphi: F[x] \to F(\alpha) \subseteq K$ (ring homomorphism)
  $f(x) \mapsto f(\alpha)$ → $F(\alpha)$ 可以用 $f(\alpha)$ 含取到, since $\exists f=1, \exists f=x$

  $\ker\varphi = \{f(x): f(\alpha)=0\} = (p(x))$

  $\therefore \varphi(F[x]) \cong F[x]/(p(x))$ then $\varphi(F[x])$ is also field (已证过 $F[x]/p(x)$ 是) …①

  (*): surjective
- $F \in F[x]$. $\varphi(F) = F \subseteq \varphi(F)$

  $F[x]$: 所有以 F 中元素作为系数的多项式. $x \in F[x]$ $\therefore \alpha \in \varphi(F[x])$ …②

①+② $\Rightarrow$ $\varphi(F[x])$ 符合条件, 且 isomorphic to …; $\varphi(F[x]) = F(\alpha)$ here

(没什么用吧): 补(*): $\phi: F[x]/(p(x)) \to F(\alpha)$

ϕ is field homomorphism, $\phi \neq 0$ $\therefore \phi$ injective

由 $F(\alpha)$ 形式, ϕ surjective

Thm: $F \subseteq E$; E, F is field, $\alpha \in E \setminus F$

(1): α transcendental. $F(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} : f, g \in F[x], g \neq 0\}$

(2): α algebraic, $F(\alpha) \cong F[x]/(m(x))$; $m(\alpha)=0$, $m \mid f \ \forall f(\alpha)=0$

Q consider: $F(\alpha) = \{f(\alpha) : f \in F[x]\}$ 这个式子为啥是恒等的

$\{\frac{f(\alpha)}{g(\alpha)} : f, g \in F[x], g \neq 0\}$ 不相等?

pf: 考虑 $\theta : F[x] \to F(\alpha)$

$f \mapsto f(\alpha)$

θ is surjective, $\mathrm{im}(\theta) = F(\alpha)$

$\ker(\theta) = \{f \in F[x] : f(\alpha)=0\} \overset{记}{=} I$, I is ideal

$\therefore F(\alpha) \cong F[x]/I$

(1): 由 $f \in F[x]$, $f \neq 0$, $f(\alpha)=0$, $\therefore I = \{0\}$

$F(\alpha) \cong F[x]/\{0\} = F[x]$

⇐ algebraic定义为 $\exists f \neq 0 \in F[x]$. $f(\alpha)=0$

(2): $F(\alpha) \cong F[x]/\{f \in F[x] : f(\alpha)=0\}$

$f \in F[x]$, $f(\alpha)=0 \Rightarrow m_{\alpha F} \mid f$, $\therefore f \in (m_{\alpha F}(x))$

即 $F(\alpha) \cong F[x]/(m(x))$, $m(x)$ 为 α 在 F 中的最小多项式

例1: (Thm): $\mathbb{F}_3[x]/(x^2+1) \cong \mathbb{F}_3[x]/(x^2+x+2)$, $\mathbb{F} = \{1, 2, 3\}$

$\begin{cases} \mathbb{F}_3[x]/(x^2+1) \cong \mathbb{F}_3(\alpha_1), & \alpha_1 = \pm i \\ \mathbb{F}_3[x]/(x^2+x+2) \cong \mathbb{F}_3(\alpha_2), & \alpha_2 = \frac{-1 \pm \sqrt{7}i}{2} \end{cases}$

在 $\mathbb{F}_3$ 的扩域 $\mathbb{C}$ 中, 找到两个 α_1, α_2; $\alpha_1 \alpha_2$ algebraic over $\mathbb{F}_3$

$\begin{cases} \deg(\mathbb{F}_3(\alpha_1)) = \deg(\alpha_1 \text{在} \mathbb{F}_3 \text{上的最小多项式}) = \deg(x^2+1) = 2 \\ \deg(\mathbb{F}_3(\alpha_2)) = \deg(x^2+x+2) = 2 \end{cases}$

$\therefore \mathbb{F}_3(\alpha_1) = \{a_0 + a_1\alpha_1 : a_0, a_1 \in \mathbb{F}_3\}$, $\mathbb{F}_3(\alpha_2) = \{a_0 + a_1\alpha_2 : a_0, a_1 \in \mathbb{F}_3\}$

then $\exists \theta : \mathbb{F}_3(\alpha_1) \to \mathbb{F}_3(\alpha_2)$, θ isomorphism

$1 \mapsto 1$

$\alpha_1 \mapsto \alpha_2$

Prop: Lib $\forall n \in \mathbb{Z}^+$, $\exists$ irr polynomial $p(x)$ of deg n, in $\mathbb{F}_p[x]$ p prime, 改成 p^r 也一样

先考虑 $n=2$, 有 p^2 多项式长成 $x^2+bx+a = p(x)$

$p(x)$ reducible: $x^2+bx+a = \begin{cases} (x+a_0)(x+a_0) & \cdots \text{至多 } p \text{ 种} \\ (x+a_1)(x+a_2) \ a_1 \neq a_2 & \cdots \frac{1}{2}p(p-1) \text{种} \end{cases}$

$p + \frac{1}{2}p(p-1) < p^2$ 小还有irr的

- lem: irreducible & root

  $\mathbb{F}$ is a field. $f \in \mathbb{F}[x]$, $\deg(f) \geq 2$, f is irreducible in $\mathbb{F}[x]$, f has no roots in $\mathbb{F}$

  $\deg(f) = 2$ 或 3, f has no roots in $\mathbb{F}$, then f irreducible in $\mathbb{F}[x]$

  ⇓

  没有一阶项 $ax+b$ ($a \neq 0$)

  $\deg(f) = 2$ or 3. $f = f_1 \times f_2$, $f_1 = c$, $f_2 = f$, $\exists c^{-1}$

  反例: $\deg(f) = 4$, $f = (x^2+1)(x^2+1)$

- recall definition of $\mathbb{F}[x]/(p(x)) = \{ f(x) + (p(x)) : f(x) \in \mathbb{F}[x] \}$

  $f(x) \bmod (p(x))$ in Dummit,

- 我的笔记本 P21: $p(x) \in \mathbb{F}[x]$, $\mathbb{F}$ is field, then

  (1) $p(x)$ irreducible $\Leftrightarrow$ (2) $I = (p(x))$ is maximal ideal of $\mathbb{F}[x]$

  $\Leftrightarrow$ (3) $\mathbb{F}[x]/(p(x))$ is field

- $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a PID

  设 I is ideal of $\mathbb{F}[x]$, $I \neq 0$, $g \in I$ 且 g 在 I 中有最小的 degree

  设 g is const, $\forall f \in \mathbb{F}[x]$, $f = (fg^{-1})g \in I$, $\therefore I = \mathbb{F}[x] = (g)$

  设 $\deg(g) \geq 1$, $\forall h(x) \in I$, $\exists \deg(r) < \deg(g)$, $r \neq 0$: $h(x) = q(x) \cdot g(x) + r$ (Division algorithm)

  $\therefore r = h(x) - q(x) \cdot g(x) \in I$, 与 g 在 I 中具有最小的值矛盾

  $\therefore r \neq 0$

  $\therefore h(x) = q(x) \cdot g(x) \in (g(x))$. 即 $I \subseteq (g(x))$ then $I = (g(x))$

  ⇓ 这段证明同样适用于所有 $\mathbb{F}$ is field (即 Division 适用)

P255: R is commutative, then ideal P is a prime ideal in R

$\Leftrightarrow$ the quotient ring R/P is an integral domain 含1. 无0因子. 交换

$R/P = \{ r+P : r \in R \}$, 乘法单位元 $1+P$, 加法零元 P

$\Leftarrow$: 设 $xy \in P$; $x \notin P$, $y \notin P$, then $(x+P)(y+P) = xy+P = P$ then $xy \in P$, $x \notin P$, $y \notin P$, 矛盾 x, y 为0因子. 矛盾

$\Rightarrow$: 同上 R/P 无0因子, let $r \in P$ 含1. given commutative, $\therefore R/P$: ID

Coro: R commutative, ∀ maximal ideal of R is prime ideal

引理: M is maximal ideal, ③⇔ R/M is a field: then ID

① ⇕ the only ideal of R/M is 0 or R/M ⇕ ②

②在前面证过

③: ⇐ for r+M, ∃ s+M s.t. (r+M)(s+M) = rs+M = 1+M

∴ ∀ r∈R, ∃ s s.t. sr∈M

设 M⊊I; take i∈I, i∉M, ∃ j s.t. ji = m∈M, ji∈I

② ⇐ 对于 r+M, (r+M)(s+M) = rs+M = 1+M

r(s-1)∈M ∀r.

∴ s-1 = m some m∈M, s+M = 1+m+M = 1+M 乘法之

R/M field, then ∀ r+M, ∃ s+M, s.t. rs+M = 1+M

即 rs = 1+m', m'∈M

∴ 设 M⊆I, ∀ i∈I, ∃ ji = 1+m', m∈M, (这里设i∉M, 上面的 r,s 也是设了不在M中得出的)

∴ 1 = ji - m'∈I, then ∀ r∈R, r·1∈I ∴ I=R

∴ M is maximal

⇒: 即证反证. 即 ∀r, ∃ sr = 1+m'

M is maximal, ∴ ∃ r∉M, r+M∈R/M } ... (*)

∴ rR+M = R

⇒ 或者说: r∉M (r)+M=R

即 1∈R, ∃ rs∈(r), 1 = rs+M

∴ 不在M内 ⇒ unit

for 1∈R, then ∃ s∈R, m∈M, rs+m=1 即 (r+M)^{-1} = (s+M)

(在M内: 对于R/M是"0")

M 和 N 均为 maximal ideal of R

then: 若 M∩N ≠ ∅, M∪N = R

pf: M, ideal, N ideal ⇒ M∪N ideal 且 M∪N ≠ M } ⇒ M∪N = R

M is maximal

Thm: (degree of extension) $p(x)\in F[x]$. irr polynomial of degree n; $K=F[x]/(p(x))$

let $\theta = x \bmod (p(x)) \in K$, then $1, \theta, \theta^2, \cdots \theta^{n-1}$ are basis for K as vector space over F

(即: $[K:F]=n$, $K=\{a_0+a_1\theta+\cdots a_{n-1}\theta^{n-1} = a_i\in F\}$, consists of 为 polynomials of degree $<n$ in θ)

- lem: $F[x]$ is ED, > PID > UFD

$F[x]$ is ED 必存在除法.

Span: let $a(x)\in F[x]$, then $\exists\ q, r\in F[x]$, $\deg r < \deg p = n$, s.t: $a(x) = q(x)p(x)+r(x)$

$a(x) \bmod (p(x)) = r(x) \bmod (p(x))$

即 $\forall a\in F[x]$. $a \bmod (p(x))$ 所以用 deg $<n$ 的多项式表示

∴ the image of $1, x, x^2, \cdots x^{n-1}$ 即 $1, \theta, \theta^2, \cdots \theta^{n-1}$ span the vector space over F

independent: if $\exists\ b_0, \cdots b_{n-1}\in F$, not all zeros: $b_0+b_1\theta+\cdots b_{n-1}\theta^{n-1}=0$

代入 $\theta = x \bmod (p(x))$: $b_0+b_1x+\cdots+b_{n-1}x^{n-1} \equiv 0 \pmod{p(x)}$

$p \mid (b_0+b_1x+\cdots+b_{n-1}x^{n-1})$ 矛盾

∴ $\theta = x \bmod (p(x))$: $1\ \theta\ \theta^2, \cdots \theta^{n-1}$ is basis, $[K:F]=n$

Rmk: $K = F[x]/(p(x)) = \{f+(p(x)) : f\in F[x]\}$ 等于 $\{f \bmod (p(x)) : f\in F[x]\}$

coro 7: P318 $p(x)\in F[x]$, $\deg(p)=n$, $F(\alpha)=\{a_0+a_1\alpha+a_2\alpha^2+\cdots a_{n-1}\alpha^{n-1} : a_0\cdots a_{n-1}\in F\} \subseteq K$

{ Th6 中证过 $F(\alpha) \cong F[x]/(p(x))$
Thm 中证明 $[K:F]=n$, 即 $K = F[x]/(p(x))$ n 维

∴ $\alpha\in F(\alpha)$. α 张成的空间为 $1, \alpha, \alpha^2, \cdots \alpha^{n-1}$; (1 可以生成 F)

Rmk: $F(\alpha)$ 不要把 α 理解为函数, α 是一个元素, 可以理解为 x; 因为 $\alpha\notin F$, 比如 $\mathbb{R}=\mathbb{Z}$, $\alpha=i$, $p(x)=x^2+1$

- recall Th6: $\varphi: F[x] \to F(\alpha)\subseteq K$
  $f(x) \mapsto f(\alpha)$
  $\ker\varphi = \{f : f(\alpha)=0\} = \{(p(x))\}$; $\operatorname{im}\varphi = F(\alpha)$, $f=1$ 生成 F, $f=x$ 生成 α

P320: Prop 9: α is algebraic over F, ① $\exists$ unique monic irr polynomial $m_{\alpha,F}(x)\in F[x]$, $m_{\alpha,F}(\alpha)=0$.

② then $f\in F[x]$ has root $\alpha \Leftrightarrow m_{\alpha,F}(x) \mid f$, 称 $m_{\alpha,F}(x)$ 为最小多项式 这个均可作为最小的定义

proof: α algebraic ∴ 故 $\exists$ monic poly $p\in F[x]$, $p(\alpha)=0$.

- let $g(x)\in F[x]$ g monic and $g(\alpha)=0$. 取这样的 g 中 degree 最小的

if g is reducible ∴ $g(x)=f_1(x)\cdot f_2(x)$, f_1, f_2 均不可逆说明 $\deg f_i > 0$. then $\deg f_i < \deg g$

∴ g should irr in $F[x]$, $\Rightarrow m_{\alpha,F}$ exist.

- $f \in F[x]$, $f(a)=0$.

  $F[x]$ is ED, 存在除法 $\exists q, r \in F[x]$, $\deg r < \deg g$ s.t. $f(x)=q(x)g(x)+r(x)$

  $f(a)=q(a)g(a)+r(a)=0$ $\therefore r(a)=0$ 与 deg 最小矛盾

  $\therefore r \equiv 0$, 即 $f=qg$ 让 $f(a)=0$.

  另一方向 $f=qg$, then $f(a)=0$ obv

- 假设 g 不唯一, g_1, g_2 满足

  then $g_1 \mid g_2$, $g_2 \mid g_1$, $\therefore g_2 = g_1$ $\Rightarrow$ unique Rmk: a 不一定在下中的!

HW10.3: $a = e^{2\pi i/p} \in \mathbb{R}$, $a^p=1$ $\therefore x^p-1 \big|_{x=a} = 0$ (p odd prime)

then $m_{a,F} \mid (x^p-1) = (x-1)(x^{p-1}+x^{p-2}+\cdots+x+1)$

$x-1\big|_{x=a} \neq 0$, then $m_{a,F} \mid (x^{p-1}+x^{p-2}+\cdots+x+1)$ 不可约法: $p(x)$ irr $\Leftrightarrow$ $p(x+\text{const}) = q(x)$ irr

(引用): HW10.3: 以下中 $a_n x^n + a_{n-1}x^{n-1} + \cdots a_0 \in \mathbb{Z}[x]$, 让 $\exists$ 一个 $p \in \mathbb{Z}$ 满足 $p \nmid a_n$, $p \mid a_i$, $p \nmid a_0$

then $f(x)$ irr in $\mathbb{Z}[x]$, $F[x]$

让 $x^{p-1}+x^{p-2}+\cdots x+1$ irr in $\mathbb{Q}[x]$, 即为 a 在 $\mathbb{Q}$ 上的最小多项式

Corol D: L/F is field extension, a is algebraic over F, L; then in $L[x]$, $m_{a,L}(x) \mid m_{a,F}(x)$

$m_{a,F}(x) \in L[x]$, $m_{a,F}(a)=0$

$\therefore m_{a,L}(x) \mid m_{a,F}(x)$ 打域话最小多项式小,

下例: $\forall a \in \mathbb{C}$, $a \notin \mathbb{R}$, let $F=\mathbb{R}$, $L=\mathbb{C}$

in $F[x]$, $m_{a,F} = x^2+1$; in $L[x]$, $m_{a,L} = x-1$

in $L[x]$: $x-1 \mid x^2+1$, 即 $m_{a,L} \mid m_{a,F}$, 而在 $\mathbb{R}[x]$ 中 $x-1 \mid x^2+1$ 是违背常理的

Psu Prop 12: a algebraic over F $\Leftrightarrow$ the simple extension $F(a)/F$ finite degree

proof: claim: $\deg(F(a)) = \deg(\text{minimal polynomial for } a \text{ over } F)$

$F(a) = \{a_0 + a_1 a + \cdots a_{n-1} a^{n-1} : a_i \in F\}$, basis: $1, a, a^2 \cdots a^{n-1}$

即: $\forall B_0, B_1 \cdots B_{n-1}$, $B_0 + B_1 a + \cdots + B_{n-1} a^{n-1} = 0 \Leftrightarrow B_0 = \cdots B_{n-1} = 0$

$\{b_0 + b_1 a + \cdots + b_{n-1} a^{n-1} + b_n a^n = 0$ $b_n \neq 0$, $b_0 \cdots b_{n-1}$ 也不全为 0

$\therefore p(x) = b_0 + b_1 x + \cdots b_n x^n$; 取上面的 $b_0, b_1 \cdots b_n$

then $p(x)$ irreducible in $F[x]$, or. 存在 $\deg(p') > \deg(p)$, $p'(a)=0$, 即 $\exists B_i \neq 0$, 矛盾}

$\therefore \deg(m_{a,F}) \geq \deg(p) = n$, 符合"最小", irr, $p\big|_{x=a}=0$" $\Rightarrow \deg(m_{a,F})=n$ p 即最小多项式.

由此可打造出上方性质

下例：HW10T. α transcendental over K, then $\exists$ infinitely embeddings $K(\alpha) \to K(\alpha)$

φ: $K(\alpha) \to K(\alpha)$ 考虑 $K(\alpha)$ 中的生成元 2.1

$1 \mapsto 1$ (K部分)

$\alpha \mapsto \alpha^n$, $n=1,2,\cdots$

α transcendental. 即 $\forall\, b_0, b_1 \cdots b_n$ not all zero: $b_0 + b_1 x + b_2 x^2 + \cdots b_n x^n \big|_{x=\alpha} \neq 0$

即: $b_0 + b_1\alpha + \cdots b_n\alpha^n \neq 0 \Rightarrow b_0 = b_1 = \cdots b_n = 0$; $\forall n \in \mathbb{N}^+$

证明: $1, \alpha, \alpha^2, \alpha^3, \cdots \alpha^n, \cdots$ 之间全部 independent, $\therefore \forall \alpha^n$ different with n different

$\varphi_1 \neq \varphi_2 \neq \varphi_3 \cdots$ $\therefore$ infinite φ

Thm: $F \subseteq K \subseteq L$ fields. then: $[L:F] = [L:K]\cdot[K:F]$; $[K:F] \mid [L:F]$

设 $\alpha_1 \alpha_2 \cdots \alpha_m$ basis of L over K; $\beta_1 \beta_2 \cdots \beta_n$ basis of K over F

then $\forall z \in L$, $z = a_1\alpha_1 + a_2\alpha_2 + \cdots a_m\alpha_m$; $a_i \in K$ $\alpha_i \in L$

for $a_i \in K$, $a_i = b_{i1}\beta_1 + b_{i2}\beta_2 + \cdots + b_{in}\beta_n$; $b_{ij} \in F$, $\beta_i \in K$

代回: $z = \sum_{\substack{i \in [1,m] \\ j \in [1,n]}} b_{ij}\alpha_i\beta_j$; $b_{ij} \in F$, $\alpha_i\beta_j \in L$

$\Rightarrow \{\alpha_i\beta_j\}_{i=1,j=1}$ spans the space L over F. 接下来证 independent

if $\sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}\alpha_i\beta_j = 0$, $= \sum_{i=1}^{m}\left(\sum_{j=1}^{n} b_{ij}\beta_j\right)\alpha_i$

$b_{ij}, \beta_i \in K$; $1, \alpha_1 \alpha_2 \cdots$ is basis in L $\therefore \sum_{j=1}^{n} b_{ij}\beta_j = 0\ \forall i$

$\therefore b_{ij} = 0\ \forall j$ since $\beta_1 \beta_2 \cdots$ is basis in K

即 $\{\alpha_i\beta_j\}_{i=1,j=1}$ 是 L over F 的 basis, $[L:F] = m \times n = [L:K]\times[K:F]$

Rmk: 写法 "degree of L" 是不严谨的. 应写成 "degree 时 L over ..."

L 是 k 的 field extension, $L = L/k$

then $L = \{k_0 + k_1 v_1 + k_2 v_2 + \cdots k_n v_n : k_i \in k, v_i \in L\}$, n 为 "L over F" 的维度

如果换一个 primitive field, L 作为 extension. degree 是会变的

理解: $L \supseteq K$, by "$k_0 \times 1$" as basis; 且 k 与 L 的其它元素 (若底基, 以此...) 要封闭

Example 6. *Find $\mathbb{F}_{p^2} > \mathbb{F}_p$, we need to find $x^2 - r$ and $x^2 - r$ irre. with $r \in \mathbb{F}_p$, then $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[x]/(x^2 - r)$.*

Definition 2. *F is called a algebraic closed field if any polynomial $f(x) \in F[x]$ is reducible unless $\deg f = 1$.*

Definition 3. *Let E/F be a field extension. Then E can be view as a vector space over F. If $\dim_F E = n$ is finite, then E is called a finite extension of F of degree n.*

复习：recall 域扩张部分

- 域扩张的基本概念
  - K/F, $F(\alpha)$, $F[x]/(p(x))$
- 域的代数扩张与超越扩张
  - algebraic: $\exists f \in F[x]$, $f \neq 0$, $f(\alpha)=0$, 则 α alg over F (α不一定在F上的), obv存在 monic f
    α在F中, 则 α必定 algebraic
  - 代数扩张: K/F, K上所有元素均为 algebraic over F
  - $F \subseteq E$, EF field, $\alpha \in E \setminus F$,
    (1) α trans, $F(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} : f,g \in F[x], g \neq 0\}$ (2): α alge, $F(\alpha) \cong F[x]/(m(x))$, m is minimal poly $m_{\alpha F}$
    (2) $\varphi: F[x] \to F(\alpha)$
    $f(x) \mapsto f(\alpha)$
    $F(\alpha) = \{f(\alpha) : \forall f \in F[x]\}$ 显, surjective, $\Rightarrow F[x]/\ker\varphi \cong F(\alpha)$, $\ker\varphi = (m_{\alpha F})$
    (1): 考虑另一同态 $\phi: F(x) \to F(\alpha)$, $F(x)$是F上的一切分式域, here ϕ is field homo $\Rightarrow$ 0或inj
    $\frac{f(x)}{g(x)} \mapsto \frac{f(\alpha)}{g(\alpha)}$

Q [关键]: $F(\alpha) = \{f(\alpha) : f \in F[x]\}$ 许 α alge, $F(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} : f,g \in F[x], g(x) \neq 0\}$ ($\subseteq$ ✓) if α not
超越α我能的也是?: "α和F"可以取到以所
α trans, $F(\alpha) \subseteq \{\frac{f(\alpha)}{g(\alpha)}\}$ obv
✓ { WTS: $\{\frac{f(\alpha)}{g(\alpha)}\} \subseteq F(\alpha)$, $f(\alpha) \in F(\alpha)$, $g(\alpha) \in F(\alpha)$ $\therefore g^{-1}(\alpha) \in F(\alpha)$ $\therefore \frac{f(\alpha)}{g(\alpha)} \in F(\alpha)$ $\forall f,g \neq 0$

超越元α: 是否有 $F(\alpha) = \{f(\alpha) : f \in F[x]\} = \{\frac{f(\alpha)}{g(\alpha)} : f \in F[x], g \neq 0\}$
(and 代数元α)
不行, 因为没有 $\alpha^{-1} = \sum_{n=0}^{N} a_n \alpha^n$ 即 $\alpha, \alpha^2, \cdots \alpha^n$ 不为基 for $\forall N$
因为没有 $0 = \sum_{n=0}^{N} a_n \alpha^{n+1}$, α trans

- 代数单扩张
  - $p(x)$ 在 $F[x]$ 中 irr; $\exists K = F[x]/(p(x))$, F的扩域 在其中 p 有 root
    $\varphi: F[x] \to F[x]/(p(x))$ $p(\varphi(x)) = \varphi(p(x))$
  - K/F中有 $p(x)$ root α, then $F(\alpha) \cong F[x]/(p(x))$
  - $\deg(p) = n$, $F[x]/(p) = \{a_0 + a_1 x + \cdots a_m x^m : a_i \in F\}$;
  - 极小多项式: $m_{\alpha F}$ 或 $\operatorname{Irr}(\alpha, F)$, $\Rightarrow$ { unique monic poly irr 取 monic min 即所
    $f(\alpha) = 0 \Leftrightarrow m_{\alpha F} \mid f$

$\deg(F(\alpha)) = \deg(m_{\alpha F})$ since α alge:
$\exists k = \deg(m_{\alpha F})$. $1, \alpha, \alpha^2, \cdots \alpha^{k-1}$ independent; $1, \alpha, \alpha^2, \cdots \alpha^{k-1}\alpha^k$ dependent

- 有限域扩张(维度)
  - $F(\alpha)/F$ finite degree $\Leftrightarrow$ α algebraic ($\Leftarrow$)以及$[F(\alpha):F]=\deg(\mathrm{Irr}(\alpha,F))$
  - $[K:F]=[K:L][L:F]$, 域 $K\supseteq L\supseteq F$
  - $p\in F[x]$. p irr, $\deg(p)=n$; $K=F[x]/(p(x))$

    $\theta=x \bmod (p(x))$, then $1,\theta,\theta^2,\cdots\theta^{n-1}$ 为 basis for K as vector space over F

    $\Rightarrow$ $\varphi: F[x]\to F[x]/p(x)$, φ ring homo

    $\therefore \varphi(p(x))=p(\varphi(x))=p(\theta)=0\in F$

    $0\in F[x]/(p)$

    $K=F[x]/(p(x))=\{a_0+a_1\theta+\cdots a_{n-1}\theta^{n-1}: a_i\in F\}=F(\theta)$, θ is alge over F

(?) $F(\theta)$和 $F[x]/(p)$我觉得都不是数域, 多项式和数都有

{ $p(x)=a_0+a_1x+\cdots a_nx^n$. $a_i\in F$. $x+(p(x))=x \bmod(p)=x$? 我觉得想表达的是θ是p的root

- α alge over Q, $\deg \mathrm{Irr}(\alpha,Q)=n$, α为 n次代数元 $\quad\theta$ 即$\theta=x \bmod(p)$?
- 总之>>P108: K/F finite degree $\Leftrightarrow$ K/F为有限生成的代数域扩张

  $F(\alpha_1,\alpha_2,\alpha_3\cdots\alpha_n)$

  $\Rightarrow$易

  $\Leftarrow$(引理)

  { Dummit P575 $F(\alpha,\beta)=(F(\alpha))(\beta)=(F(\beta))(\alpha)$;

  { $F_i=F(\alpha_1,\alpha_2,\cdots\alpha_i)$, then $[K:F]=[K:F_{n-1}][F_{n-1}:F_{n-2}]\cdots[F_2:F_1][F_1:F]$

  α_i alge over F, $\therefore \alpha_i$ alge over F_{i+1}, then $[F_i:F_{i+1}]$ finite

  $\deg(m_{\alpha_i,F})=n_i$. $\deg(m_{\alpha_i,F_{i+1}})\le n_i$ since $m_{\alpha_i,F_{i+1}}\mid m_{\alpha_i,F}$; $[F_i:F_{i+1}]\le n_i$

  $\therefore [K:F]\le\prod_{i=1}^{n}\deg(\alpha_i)$
- algebraic closed field F: $\forall f\in F[x]$, f re, unless $\deg f=1$ / 次数大于0均有0点 Q: why$\Leftrightarrow$ P54 up def ✓
- 代数闭包 closure: K/F, $\alpha\in K$, α alge over F; F和α子形成K的子域, 即F在K中的代数闭包

  F和α子形成 algebraic closure 要证形成 field $\Leftrightarrow$四则运算封闭即可

  F和α子形成E; $\alpha,\beta\in E$ $[F(\alpha,\beta):F]<+\infty$

  $\alpha+\beta\in F(\alpha,\beta)$ $\therefore F(\alpha+\beta)\subseteq F(\alpha,\beta)$, $[F(\alpha+\beta):F]<+\infty\Leftrightarrow\alpha+\beta$也为代数元

  $\therefore$同样有 $\alpha-\beta$, $\alpha\beta$, $\alpha\div\beta(\beta\neq0)\in E$.

  $\Rightarrow$ {algebraic number} closed under $+-\times\div$,