Lq: 分裂域; Galois群

《定义》多项式分裂域; 正规扩张, 有限扩

P536: F is field, $f(x)\in F[x]$, 则 $\exists K/F$ as extension of F; 在K中f has a root $\Leftrightarrow$ K中, $\exists f(a)=0$, $\Leftrightarrow$ f(x) has linear factor $x-a$ in $K[x]$ ← 最简多项式 deg=1

def: K/F is field extension; K is splitting field for $f(x)\in F[x]$ over F, if:

在K[x]中, f(x) factors completely into linear factors $a(x-a_1)(x-a_2)\cdots(x-a_n)$, $a_i\in K$,

而在任意 proper subfield $F\subseteq H\subsetneq K$; 在H[x]中 f(x)无法分解成如上形式, 必有2次及以上因子不可分

$\Leftrightarrow$《定义》def 2.2. K/F is extension; K含有 $f(x)\in F[x]$ 的所有零点, $H\subseteq K$ is splitting field if:

H是K/F中, 含有f(x)所有root的最小子域 $\Leftrightarrow$ F上由f(x)所有root生成的K的子域

Thm: $\forall$ field F, $f(x)\in F[x]$, $\exists$ extension K/F which is splitting field of f(x) over F; 分裂域必存在

数归: if deg(f)=1, E=F 用下面的同构提升, 可以证 unique

deg(f)≥2, F is field, F[x] is ED thus UFD; ∴f有唯一的 irreducible 分解. $f=f_1(x)\cdot f_2(x)\cdots f_n(x)$, $f_i(x)\in F[x]$

if $\deg(f_i)=1\ \forall i$. E=F

if $\exists \deg(f_i)\geq 2$, f_i irr in F[x]; 由域扩张: f_i irr in F[x]; $\exists F(a)$. $f_i(a)=0$

即在F(a)(或其它F(β))等中, $\deg(f_i):=\deg(f_i)-1$;

if irr, 这个过程可以一直持续, ∴最后 f_i 分成一次因子; $\forall f_i$ holds

例: $f(x)=x^3-2$. f(x)=0 has root $\sqrt[3]{2}$ $\sqrt[3]{2}w$. $\sqrt[3]{2}w^2$, $w=\frac{-1+\sqrt{3}i}{2}$

$\sqrt[3]{2}$, $\sqrt[3]{2}w$. $\sqrt[3]{2}w^2$ algebraic over Q[x]; 含$\sqrt[3]{2}$. $\sqrt[3]{2}w$. $\sqrt[3]{2}w^2$ 的Q的扩张, 加上基即可 $\sqrt[3]{2}$.w.

$K=Q(\sqrt[3]{2}, \frac{-1+\sqrt{3}i}{2})$ is splitting field of f over Q,

而实际上 $K=Q(\sqrt[3]{2}+\lambda w)\ \forall\lambda$ ⇐ $K=Q(\theta_1,\theta_2)$. $\mathrm{span}(\theta_1,\theta_2)=\mathrm{span}(\sqrt[3]{2}, \frac{-1+\sqrt{3}i}{2})$ 即可

‖ 这个后面会证 ⇓

here, 如 $K=Q(\sqrt[3]{2},\sqrt{3})$, 求 $[Q(\sqrt[3]{2},\sqrt{3}):Q]$:

① $[Q(\sqrt[3]{2}):Q]=\deg(m_{\sqrt[3]{2},Q})=\deg(x^3-2)=2$; $[Q(\sqrt{3}):Q]=\deg(x^2-3)=3$

$[Q(\sqrt[3]{2}):Q]\mid$ 原式, $[Q(\sqrt{3}):Q]\mid$ 原式, $\gcd(2,3)=1$ ∴ $6\mid$ 原式.

又: 原式 $=[Q(\sqrt[3]{2}):Q(\sqrt{3})]\times[Q(\sqrt{3}):Q]\leq 2\times 3$ ⇒ 原式=6

② $Q(\sqrt[3]{2},\sqrt{3})=\{a_1+a_2\sqrt[3]{2}+a_3(\sqrt[3]{2})^2+a_4\sqrt{3}+a_5\sqrt[3]{2}\sqrt{3}+a_6(\sqrt[3]{2})^2\sqrt{3}: a_i\in Q\}$ 为基下的数

prop 2b: $f\in F[x]$. deg(f)=n; the splitting field of f(x) over F is at most degree n!

在Galois th中会证,

f的4根是 $a_1,a_2\cdots a_n$, $F(a_1a_2\cdots a_n)$ 的基 $a_1a_1^2\cdots a_1^{n'}$; $a_2a_2^2,\cdots a_2^{n'}$; $\cdots$ $a_1^{n''}a_2^{n'}$, $a_1^{n'}a_2$ 共n!个, 含F的

F没法用$\sqrt{3},\sqrt[3]{2}$线性表示, 所以单拎出来.

例: Splitting field of x^n-1 over $\mathbb{Q}$

$x^n=1$: $x^n=\cos(2k\pi)+\sin(2k\pi)i$. $k\in\mathbb{Z}$.

$\therefore x=\cos(\frac{2k}{n}\pi)+\sin(\frac{2k}{n}\pi)i$. $k=0,1,2,\cdots n-1$ 一个循环周期

$K/\mathbb{Q}$ is splitting field of x^n-1 over $\mathbb{Q}$, $K=\mathbb{Q}(a_1,a_2,\cdots a_n)$

K is closed under multiplication, (有1的域必为乘法群), 且K is cyclic group

· 引理 prop18 P314: a finite sub group of the multiplicative group of a field is cyclic

有限Abel基本定理: finite Abel $G=G_1\times G_2\times\cdots G_n$ $|G_i|=p_i^{r_i}$

$=\langle a_{11}\rangle\cdots\langle a_{1n}\rangle\langle a_{21}\rangle\cdots\langle a_{2n_2}\rangle\cdots\langle a_{n1}\rangle\cdots\langle a_{nn_n}\rangle\cdots①$

field的char = p或0, 有限field大小只能 p^n, $char(F)=p$; $\cdots②$

$\langle a_{i1}\rangle$, a_{i1}是G_i中order最高的元素

$char(F)=\arg\min_k(k\cdot 1=0)=p$, $\therefore x^p=x^{p-1}=1$ $\forall x$ 阶必定小于等于p

p Prime $\therefore$ 只能 $=p$ 即 $\forall x\in\mathbb{F}_{p^d}$. $|\langle x\rangle|=p$ in $\mathbb{F}^\times$

$\Rightarrow$ $\mathbb{F}^\times$乘法群中, a_{i1}对应任何一个x, since $\forall x$ order $=p$

$\mathbb{F}^\times=\mathbb{F}_{p^n}=\mathbb{F}_p\times\mathbb{F}_p\times\cdots\mathbb{F}_p$, $\mathbb{F}_p$ cyclic $\therefore\mathbb{F}^\times$也是

· def: generator of this "cyclic group" of $\forall n^{th}$ roots" of unity 称为 primitive n-th root of unity

记ξ是一个 primitive $\cdots$, 则 $\langle\xi\rangle=\langle\xi^j\rangle$ iff $\gcd(n,j)=1$

即生成元个数为 Euler φ-function of n, $\varphi(n)=\cdots$

· def: 由上知, splitting field of x^n-1 over $\mathbb{Q}$, 记为 $\mathbb{Q}(\xi)$, called "cyclotomic field of pri..."

考虑n Prime的情况, $x^p-1=(x-1)(x^{p-1}+x^{p-2}+\cdots+x+1)$

$g(x)=x^{p-1}+x^{p-2}+\cdots+x+1$, $h(x)=g(x+1)=x^{p-1}+px^{p-2}+\cdots+\frac{p(p-1)}{2}x+p$

· 引理 由HW10T2, Eisenstein UFD中 $\exists$ irr $q\nmid a_1$, $q\mid$其它a_i, $q^2\nmid a_0\Rightarrow$ irr

$\therefore g(x)$ irr by $=h(x)$ irr "

$\therefore\deg(m_{\xi,\mathbb{Q}})=\deg(x^{p-1}+\cdots+x+1)=[\mathbb{Q}(\xi):\mathbb{Q}]$; 即 ξ在Q上的扩域, 相对于Q, 阶为p-1

结论: 之后还有证 $[\mathbb{Q}(\xi_n):\mathbb{Q}]=\varphi(n)$ $\forall n$, ξ_n为$x^n-1=0$的原根

例: splitting field of $x^p-2=0$ over $\mathbb{Q}$,

$x^p-q=0$ p次多项式的根少多项式 p-1次

$x^p-1=(x-1)\cdot(x^{p-1}+x^{p-2}+\cdots+1)$
= irr

$x^p=2$, $x=\xi\sqrt[p]{2}$, 其中ξ为 $x^p-1=0$ 的根

$\xi^p=1$ $\therefore\xi^{2p}=1$, $x=\xi^2\cdot\sqrt[p]{2}$也满足 $x^p=2$

$\therefore\mathbb{Q}$上$x^p-2=0$的分裂域 $=\mathbb{Q}(\xi_p\sqrt[p]{2},\xi_p^2\sqrt[p]{2},\cdots\xi_p^{p-1}\sqrt[p]{2})=\mathbb{Q}(\xi_p\sqrt[p]{2})$

这里要求ξ_p为原根, 这样 $\xi_p,\xi_p^2\cdots\xi_p^{p-1}$ 才含所有 $x^p=1$ 的根

$[\mathbb{Q}(\sqrt[p]{2},\xi_p):\mathbb{Q}]=[\mathbb{Q}(\sqrt[p]{2}):\mathbb{Q}][\mathbb{Q}(\xi_p):\mathbb{Q}]=p(p-1)$ since p与p-1互质

Thm: Let $\varphi: F \to F'$ is field isomorphism; $f \in F[x]$, $f' \in F'[x]$, $f' = \varphi(f)$ 由splitting引出的automorphism 扩张

同构可以是升: E 为 splitting field of f over F, E' 为 splitting field of f' over F', then:

$\Rightarrow$ field iso φ 同构 extends to field iso $\delta: E \to E'$; 即:

$$\begin{array}{ccc} \varphi: F & \xrightarrow{\text{iso}} & F' \\ \cap | & & | \ \varphi(f) \\ \delta: E & \longrightarrow & E' \end{array}$$

proof: 考虑 $p(x) \in F[x]$, p irr; then $\varphi(p) = p'(x) \in F'[x]$ irr

- E 中含有 p 的 root α_1, E' 中含有 p' 的 root β_1

  则可以将 φ extends to $\varphi_1: F(\alpha_1) \to F'(\beta_1)$, $\varphi_1|_F = \varphi$

  $F \mapsto F'$

  $\alpha_1 \mapsto \beta_1$

  ☆应用: HW12, T3 & L9最后一个定理 $[L(\alpha):K(\alpha)] = [L:K(\beta)]$

  $\varphi_1(p(\alpha_1)) = \varphi_1(p)\varphi_1(\alpha_1)$, by: φ_1 homo, $\therefore p'(\beta_1) = \varphi_1(p(\alpha_1)) = 0$, well-defined

  注意, $\varphi_1(p(x)) = p(\varphi(x))$ 在 $\psi: F[x] \to F[x]/(p)$ 成立; then: $p(\varphi(x)) = 0 \in F[x]/(p)$

  $f(x) \mapsto f(x) + (p)$

  但这里并不是 $\varphi_1(p(\alpha_1)) = p(\varphi(\alpha_1))$

- 上过程考虑 α_1, β_1, 将 $\varphi \to \varphi_1$,

  f 和 f' root 以同样方式相同的, 考虑 α_2, β_2; $\alpha_3 \beta_3$; ...

  E 为 splitting field of $f \div (x-\alpha_1)$ over $F(\alpha_1)$, ... of $f \div (x-\alpha_1) \div (x-\alpha_2)$ over $F(\alpha_1)(\alpha_2)$ ...

  (对 $\alpha_i \in F$ 说明一下)

☆ review: 考虑 $\varphi: F[x] \to F[x]/(p(x))$

$f = a_0 + a_1 x + a_2 x^2 + \cdots a_n x^n$,

$\varphi(a_n x^n) = \varphi(a_n) \cdot \varphi(x^n) = a_n \varphi(x^n)$ 这一步是与 φ 的特殊定义有关的

$\therefore \varphi(f) = a_0 + a_1 \varphi(x) + \cdots + a_n \varphi(x^n) = f(\varphi(x))$

$\therefore p(\varphi(x)) = \varphi(p(x)) = 0 \in F[x]/(p)$; 即 $p(x)$ 在 $F[x]/(p)$ 这个扩域上的解是 $\varphi(x) = x + (p(x))$

Q: 这怎么理解呀? root 应该是一个数的吧? 从数域 F 扩到了 $F[x]/(p(x))$ 不是数域了? 并非 splitting 呢?

这部分开始Galois理论

def: $F < K \le E$, K is the splitting of $f(x)$ over F

σ is F-automorphism of E if: $\sigma: E \to E$, $\sigma(a) = a\ \forall a \in F$ (fix F)

记{∀ F-automorphism of E}为 E/F 的 Galois group, 记为 Gal(E:F), or Gal(E/F)

P559 Prop2: $\sigma \in Gal(E/F)$, σ permutes the roots of irr polynomials (如果不irr, 有root $\beta \in F$, $\sigma(\beta) = \beta$ 不管这种)

f在F[x]上irr. $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

$\alpha \in E$, α algebraic over F, $f(\alpha) = 0$.

$\sigma(f(\alpha)) = (\sigma(\alpha))^n + a_{n-1}(\sigma(\alpha))^{n-1} + \cdots + a_1 \cdot \sigma(\alpha) + a_0 = 0$ 即 $\sigma(\alpha) \in E$ 也是f的root

σ fix F, σ iso. $\therefore \sigma(\alpha) \in E$, $\sigma(\alpha) \notin F$.

f(x)的roots为 $\alpha_1 \alpha_2 \cdots \alpha_t$, $\xrightarrow{\sigma}$ $\sigma(\alpha_1), \sigma(\alpha_2), \cdots \sigma(\alpha_t)$, 就是一个permute, $\sigma(\alpha_i)$ 与 α_j 对应 some ij

prop: ∀ F-automorphism of E 可以 induced to 一个对应的 F-automorphism of K (前提是 $F \le K \le E$, K是splitting)

f和σ(f)解集相同, has the same splitting

def: K is splitting field of f over F, 记 Gal(K/F), or Gal(f) 为多项式的Galios group
‖
即{∀ F-automorphism of K}

例1: $F = \mathbb{R}$, $E = \mathbb{C}$, E is the splitting field of some $f \in F[x]$ over F, 求 Gal(f) = Gal(E/F) ⇒ 求σ的形式

consider $\sigma: E \to E$

σ fixs F $\therefore \sigma(1) = 1$

$\sigma(i)^2 = \sigma(-1) = -1$ $\therefore \sigma(i) = \pm i$, 代入这2种均满足Aut

$\therefore$ Gal(E/F) = {fix F 的E内自同构} = $\langle\sigma\rangle \cong \mathbb{Z}_2$

例2: $E = \mathbb{Q}[x]/(x^2-2)$, $F = \mathbb{Q}$, 求Gal(E/F)

consider $\sigma: E \to E$, σ fix $\mathbb{Q}$

$E \cong F(\sqrt{2}) \cong F(-\sqrt{2})$, 考虑 $Gal(E/F) \cong Gal(F(\sqrt{2})/F)$

$\varphi: F(\sqrt{2}) \to F(\sqrt{2})$

$\varphi(1) = 1$; $\varphi(\sqrt{2})^2 = 2$ $\therefore \varphi(\sqrt{2}) = \pm\sqrt{2}$ 代入均可

$\therefore Gal(E/F) \cong \langle\varphi\rangle \cong \mathbb{Z}_2$

例3: $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, the splitting of f(x) over $\mathbb{Q}$ is $E = \mathbb{Q}(\alpha, w)$, 求 $Gal(x^3-2)$

$\alpha = \sqrt[3]{2}$, $w = \frac{-1+\sqrt{3}i}{2}$, $w^2 = \frac{-1-\sqrt{3}i}{2} = \bar{w}$

$\sigma: E \to E$, σ fix $\mathbb{Q}$

$\begin{cases} \sigma(1) = 1, \\ \sigma(\sqrt[3]{2})^3 = 2, \quad \sigma(\sqrt[3]{2}) = \alpha, \text{或 } \alpha w, \alpha w^2 \\ \sigma(i)^2 = -1 \quad \therefore \sigma(i) = \pm i \end{cases}$

Q: 求出来的都可以吗, since linear independent

如果 $\sigma(\sqrt[3]{2}) = \alpha w$, $\sigma(i) = -i$; then $\sigma(w) = w^2$

乘法是不用验证的, 1, $\sqrt[3]{2}$, w 满足即可

⇒ 如何验证 σ 加法、乘法均 homomorphism 且无冲突

$\sigma(w^2) = \sigma(w) \cdot \sigma(w) = \sigma(-\frac{1}{2}) + \sigma(\frac{\sqrt{3}}{2}i)$

L21 证了 ≅ Sp 的情况

= S_6 不是直积!

$\varphi: E \to E$, $\varphi(1) = 1$, 剩下的 $\sigma(\sqrt[3]{2}) = \alpha, \alpha w, \alpha w^2$; $\tau(i) = i, -i$ $\varphi \cong \{\sigma, \tau, id\}$ Gal ≅ $\langle\sigma\rangle \times \langle\tau\rangle \times$ ~~id~~

下例4: $\sqrt{2}, \sqrt{2}w, \sqrt{2}w^2$ 是 $f(x)=x^3-2$ 的 root,

{ $\mathbb{Q}(\sqrt{2})$ is not splitting field of f over $\mathbb{Q}$
$F=\mathbb{Q}(w)$, $F(\sqrt{2})$ is splitting field of f over $F=\mathbb{Q}(w)$ $\Rightarrow$ 基域的选择

$f \in \mathbb{Q}(w)[x]$, f 的全体根 $\sqrt{2}, \sqrt{2}w, \sqrt{2}w^2$

$\therefore$ splitting of $f(x)$ over $\mathbb{Q}(w)$ is $\mathbb{Q}(w)(\sqrt{2}, w) = \mathbb{Q}(w)(\sqrt{2})$, since $\mathbb{Q}(w)(w)=\mathbb{Q}(w)$

注意: Consider $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$: $\sigma: \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$, $\sigma(1)=1$

$\sigma(\sqrt{2})^2 = 2$,

但此时(与例3又对比) $\sigma(\sqrt{2}) = \pm\sqrt{2}$, since $w \notin \mathbb{Q}(\sqrt{2})$

下例5: • $E=\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 的基有 $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. 但 generators 只有 $\sqrt{2}, \sqrt{3}, 1$,

Automorphism 只考虑 generators, 而不是 basis

• $F=\mathbb{R}$, (或 $\mathbb{Q}$), $f(x)=(x^2-2)(x^2-3)$, Obv: E is splitting of $f(x)$ over F

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$, $[(\sqrt{2}+\sqrt{3})^2-5]^2 = 24$ $\Rightarrow g(x)=(x^2-5)^2-24 = x^4-10x^2+1$

E 同样是 g-splitting over F

L18中证明过 $F(\alpha, \beta) = F(\alpha+c\beta)$, c 取值 infinite

$(\sqrt{2}+c\sqrt{3})^2 = (2+3c^2)+2c\sqrt{6}$ $[(\sqrt{2}+c\sqrt{3})^2-(2+3c^2)]^2-24c^2=0$ $\Rightarrow g^*(x)=x^4-(4+6c^2)x^2+(3c-2)^2$

g^* 的 root 不在 F 中, E is splitting of g^* over F

此处 F split to E 的函数 g^*, 有 infinite 取值, 预成 $\alpha\beta$ 也应该是 (since linear inelependent)

• $Gal(f) = Gal(h)$

$\varphi: E \to E$, $\varphi(1)=1$

$\sigma(\sqrt{2}) = \pm\sqrt{2}$, $\tau(\sqrt{3}) = \pm\sqrt{3}$

$\varphi = \sigma \times \tau$ $\therefore Gal(f) = \langle\sigma\rangle \times \langle\tau\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ 为什么可以写成 $\langle\sigma\rangle \times \langle\tau\rangle$: $\sqrt{2}$ 与 $\sqrt{3}$ 线性无关互不影响

Th: L is splitting field of some $g(x)$ over K, then $\forall f(x) \in K[x]$, f irreducible, 若 f 在 L 中有根

$\Rightarrow f$ 所有根均在 L 中

注: UFD. f 可分成 irr 因式的积, 因式唯一

$\therefore$ 设 here f reducible, 也不影响, $f=f_1 f_2 \cdots f_n$, f_i irr; f 在 L 中有 root $\Rightarrow f_i$ 在 L 中有 root

我们一般考虑 irr, 只是考虑最小的多项式结构.

proof: g irr on K, g 的 root: $\alpha_1, \alpha_2 \cdots \alpha_n$, then $L = K(\alpha_1, \alpha_2, \cdots \alpha_n)$

f irr on K, 设 α, β 是 root of f, $\alpha \in L$, 希望证 $\beta \in L$

(irr $\Leftrightarrow$ 次数最低), f is minimal polynomial of α, β over F

$\therefore [K(\alpha):K] = [K(\beta):K]$

$[L(\alpha):K(\alpha)] = [L(\beta):K(\beta)]$

$\therefore L = L(\beta)$

另: $[L(\alpha):K] = [L(\beta):K]$ (把基域看成一样的才能比)

lem: L is splitting field extension of K, f irr in $K[x]$, 有根 α,β; $[L(\alpha):K(\alpha)]=[L(\beta):K(\beta)]$

设 $g(x)\in K[x]$, g has roots $\alpha_1,\alpha_2,\cdots\alpha_m$, 不妨设 $\alpha_i\notin K$, $L=K(\alpha_1,\alpha_2,\cdots\alpha_m)$;

f irr in $K[x]$, $f(\alpha)=f(\beta)=0$

$\therefore K(\alpha)\cong K[x]/(f)\cong K(\beta)$, (实际上 f 即为 K 中 α,β 的最小多项式, 因为 irr $\Rightarrow$ deg 没法降了)

考虑 lift-automorphism: $K(\alpha)\xrightarrow{\sigma}K(\beta)$ $\sigma|_K=id$, $\sigma(\alpha)=\beta$ 这个一定 well-defined

$K(\alpha)(\alpha_i)\xrightarrow{\varphi}K(\beta)(\alpha_j)$ $\varphi|_{K(\alpha)}=\sigma$.

α_i 是 g 的 root, $g(x)=a_0+a_1x+\cdots+a_nx^n$

$\sigma(g(x))=g(x)$ since $\sigma|_K=id$; $\therefore\varphi$ is extension of σ, then $\varphi(\alpha_i)=\alpha_j$ Some j

(HW1 订正, 用了类似的, 给出 φ, φ permutes root of g since $\varphi|_{\cdots}=\sigma$ 而 σ fix g)

设 $\alpha_i\in K(\alpha)$, $\varphi|_{K(\alpha)}=\sigma: K(\alpha)\to K(\beta)$;

then $\varphi(\alpha_i)=\alpha_j\in K(\beta)$, 其实这里没到用, 有助于理解 lifting 的同构性

同样的有 $K(\alpha)(\alpha_i)\xrightarrow{\varphi}K(\beta)(\alpha_j)$

$K(\alpha)(\alpha_i)(\alpha_k)\xrightarrow{\phi}K(\beta)(\alpha_j)(\alpha_s)$ $\phi|_{K(\alpha)(\alpha_i)}=\varphi$

Note: if α_{j+1} can be expressed by α_i,α from isomorphism, exist α_{j+1} expressed by α_j,β

以下省略, 当 $K(\alpha)$ 扩到 $K(\alpha)(\alpha_1,\alpha_2\cdots\alpha_m)=L(\alpha)$ 时, 右侧也为 $K(\beta)(\alpha_1\alpha_2,\cdots\alpha_m)=L(\beta)$

since: 此时从 $K(\alpha)(\alpha_1\alpha_2\cdots\alpha_m)$ 出发的 τ, $\tau|_K=id$; 故 τ permutes $\{\alpha_1\alpha_2\cdots\alpha_m\}$ of $g(x)$

存在一个 φ, $\varphi|_{K(\alpha)}=\sigma$ $\therefore\varphi(g)=g$; $\therefore\varphi$ 将 g 的一个 root 映到另一个 root (同一个), 存在性 $\Rightarrow$ well-defined in $K[x]$

Frobenius map (看一下 L20 后的例 2, 便用 ϕ,ϕ^n 生成)

- in $\mathbb{F}_p$. $\phi: x\to x^p$ is isomorphism, $\phi\in Aut(\mathbb{F}_p)$, p 是素数

  $\phi(x+y)=x^p+(px^{p-1}y+\frac{p(p-1)}{2}x^{p-2}y^2+\cdots pxy^{p-1})+y^p=x^p+y^p=\phi(x)+\phi(y)$; homo 易证

  ϕ is field homomorphism, $\phi\neq0$ $\therefore\phi$ inj

  $\mathbb{F}_p$ 的乘法群为 $\mathbb{F}_p^\times=\{1,2,\cdots p-1\}\cong\mathbb{Z}_{p-1}$, $\forall x\in\mathbb{F}_p$ $x\neq0$, $x^{p-1}=1$, $\therefore x^p=x$, $\therefore$ surj

  综上所述说明 $\phi:\mathbb{F}_p\to\mathbb{F}_p$, $x\mapsto x^p$ 是恒等映射; $\phi^n:\mathbb{F}_p\to\mathbb{F}_p$, $x\mapsto x^{p^n}$ 也是恒等映射 $\forall n$.

  - Ferma Th: p 素数, $\gcd(a,p)=1$, then $a^{p-1}\equiv1\pmod p$, $a^p\equiv a\pmod p$ 此处也可用于证 surj

- in $\mathbb{F}_{p^n}$, $\varphi: x\to x^{p^n}$ is isomorphism, $\varphi\in Aut(\mathbb{F}_{p^n})$

  homomorphic 和 inj 在选取 $x\mapsto x^{p^m}$ $\forall m$ 也成立

  $\mathbb{F}_{p^n}$ 的乘法群阶为 p^n-1, $\therefore x^{p^n-1}=1$ $\forall x\in\mathbb{F}_{p^n}\setminus\{0\}$

  - finite Abel group G, $\exists g\in G$, $o(g)=\mathrm{lcm}$(所有元素的阶), 没什么用, review 一下即可

  $\mathbb{F}_{p^n}^\times\cong\mathbb{Z}_{p^n-1}$, $\therefore$ 一定存在 some $g\in\mathbb{F}_{p^n}^\times$, $o(g)=p^n-1$; 且 $\mathbb{F}_{p^n}^\times$ 中, 与 p^n 互素的元素均为生成元, order $=p^n-1$

  $\therefore$ 若 $\varphi_m: x\mapsto x^{p^m}$, $m<n$; $\mathbb{F}_{p^n}$ 中的很多元素无法恒等映射