2020年7月13日 15:50

2. Galois 理论 (cf. GTM 167)

Def ① 域扩张 L/K 称作代数扩张 若 $\forall \alpha \in L$ $\exists P \in K[X]$ 使 $P(\alpha)=0$。使之成立的最小次数的首一的 P 称作 α 的极小多项式。

(给定 $\alpha \in L$, $K[X] \xrightarrow{\varphi} L$, $Q \mapsto Q(\alpha)$, $\ker(\varphi)=(P)$)

② 若 $\forall \alpha \in L$, α 的极小多项式均是可分的 (即此多项式在任何域扩张之中无重根) 那么称 L/K 是可分(代数)扩张 (separable).

③ 若 $\forall \alpha \in L$, 极小多项式 P 在 L 上分裂成1次多项式的积, 则称 L/K 是正规扩张 (normal)

④ 若 L/K 同时为可分且正规扩张, 称为 Galois 扩张.

例. 1. 有限扩张 未必代数的, 反之不一定成立.

$[L:K]=n$.

$\forall \alpha \in L$ $\quad 1, \alpha, \alpha^2, \cdots$

$\exists a_i \in K$, 使 $a_0 \cdot 1 + a_1\alpha^1 + \cdots + a_n\alpha^n = 0$

$K=\mathbb{Q}$. $L=\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt{5}, \sqrt[3]{5}, \cdots)$

2. * $\mathrm{char}\, K=0$ 则 K 的任何代数扩张均是可分的.

* 任何有限域 $\mathbb{F}_{p^r}$ 的代数扩张也是可分的

不可分扩张: $K=\mathbb{F}_p(t)=\mathrm{Frac}(\mathbb{F}_p[t])$

$L=\mathbb{F}_p(t)(\sqrt[p]{t})/K$ 不可分.

$\alpha=\sqrt[p]{t}$. 极小多项式 $P=X^p-t \in K[X]$

$=(X-\alpha)^p$

3. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 是正规扩张 (L/K)

$\alpha=\sqrt{2}$ 极小多项式 $P=X^2-2=(X-\sqrt{2})(X+\sqrt{2})$

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是正规扩张 在 $\mathbb{C}$ 中

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是正规扩张

L/K

$\alpha = \sqrt[3]{2}$. 极小多项式 $p = x^3 - 2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ 在 L 上

但中三个根 $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$

其中 $\omega = e^{\frac{2\pi i}{3}} = -\frac{\sqrt{3}}{2} + \frac{1}{2}i$

$\sqrt[3]{2}\cdot\omega \notin L = \mathbb{Q}(\sqrt[3]{2})$

4. $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \mathbb{Q}(\alpha)/\mathbb{Q}$ 为代数扩张$\}$ 是 $\mathbb{Q}$ 的(无限) Galois 扩张.

L/K Galois 的扩张

定义 Galois 的群: $Gal(L/K) = Aut_K L = \{\sigma : L \to L$ 环同构且 $\sigma|_K = id_K\}$

$Gal(L/K) \times L \longrightarrow L$ ($G \times S \to S$ 群作用)

$\sigma, \alpha \longmapsto \sigma(\alpha)$

任一子群 $H < Gal(L/K)$ 记 $L^H = \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$

Th (有限 Galois 理论的基本定理) L/K 有限 Galois 扩张. 则以下是一个双射. 保序

$\{L/K$ 的中间域 $M\}$ $\underset{\longleftarrow}{\overset{1:1}{\longrightarrow}}$ $\{G = Gal(L/K)$ 的子群$\}$

$M = L^H$ $\longleftarrow$ H

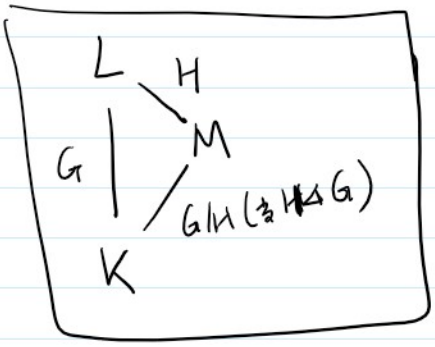
M $\longmapsto$ $H = Gal(L/M)$

而且在此对应下

$|H| = [L:M]$

$[G:H] = [M:K]$

H 为正规子群 $\Leftrightarrow$ M/K 是 Galois 的, 此时有 $Gal(M/K) = G/H$.



例① $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 是 Galois 扩张 $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} = \langle\sigma\rangle = \{\sigma, id\}$

例 ① $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 是Galois扩张 $\quad Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} = \langle\sigma\rangle = \{\sigma, id\}$

$$\sigma: \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$$
$$a+\sqrt{2}\cdot b \longmapsto a-\sqrt{2}b$$

$\mathbb{Q}(\sqrt{2}) = \{a+\sqrt{2}b \mid a, b\in\mathbb{Q}\}$

② $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ 也是Galois扩张. 4次.

$$G = Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} = \langle\sigma,\tau\rangle = \{id, \sigma, \tau, \sigma\tau=\tau\sigma\}$$

$\sigma: \mathbb{Q}(\sqrt{2},\sqrt{3}) \longrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3})$ 即 $\sigma(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})$

$\sqrt{2} \longmapsto -\sqrt{2}$ $\qquad = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}.$

$\sqrt{3} \longmapsto \sqrt{3}$

$\tau: \mathbb{Q}(\sqrt{2},\sqrt{3}) \longrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3})$

$\sqrt{2} \longmapsto \sqrt{2}$

$\sqrt{3} \longmapsto -\sqrt{3}$

G 只有3个非平凡子群 $\qquad$ 分别对应中间域

$\langle\sigma\rangle = \{id, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$ $\quad \mathbb{Q}(\sqrt{3})$

$\langle\tau\rangle = \{id, \tau\} \cong \mathbb{Z}/2\mathbb{Z}$ $\quad \mathbb{Q}(\sqrt{2})$

$\langle\sigma\tau\rangle = \{id, \sigma\tau\} \cong \mathbb{Z}/2\mathbb{Z}$ $\quad \mathbb{Q}(\sqrt{6})$

③ L/K Galois扩张. E/K 椭圆曲线 $\quad G = Gal(L/K)$

$E(L)$ = 坐标在 L 中的方程的解

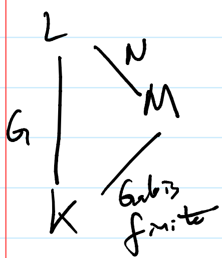
G 作用在 $E(L)$ 上. $\qquad E(L)^G = E(K)$

无穷Galois理论

L/K Galois扩张, · 需定义 $Gal(L/K)$ 上的一个拓扑 使之成为拓扑群.

当 L/K 有限Galois扩张时, $Gal(L/K)$ 上赋予离散拓扑.

Krull 拓扑. $\qquad G = Gal(L/K)$



$I = \{M$ 为 L/K 的中间域, 且 M/K 有限Galois扩张$\}$

$\mathcal{N} = \{N$ 为 G 的子群 且 $\exists M\in I$ 使 $N = Gal(L/M)\}$

子集 $X\subset G$ 是 G 的开集 若 X = 并式

X 是若干个(可以无穷多个) σN 的并 (其中 $\sigma\in G$, $N\in\mathcal{N}$)

$K \overset{\text{over}}{\subset}_{\text{finite}}$ 子集 $X \subset G$ 是 G 的群论 X 生成式

X 是有限个（可以无穷个）$\sigma N \sigma^{-1}$ 的并 ($\forall \sigma \in G,\ N \in \mathcal{N}$)

换言之，$\mathcal{N}$ 是 G 在 1 处的一组邻域基.

$\{\sigma N \mid \sigma \in G,\ N \in \mathcal{N}\}$ 是 G 的一组开集基

Th. 上述定义的 Krull 拓扑使 $G = Gal(L/K)$ 成为一个拓扑群，是 Hausdorff 的、紧、完全不连通（即连通分支都是单点集，这比离散拓扑弱）

而且此时 $G \cong \varprojlim_{N} G/N$ 其中 N 取遍 G 的开正规子群（从而 G/N 是有限的）

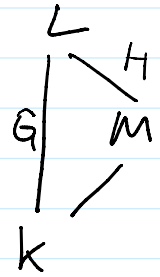
即 G 是有限群的逆极限. 称作 <u>profinite group</u>

Th. (Galois 理论基本定理) L/K Galois 扩张. $G = Gal(L/K)$ 则以下是一个右方 22 射（"$\subseteq$" $\to$ "$\supseteq$"）

$$\{L/K \text{ 的中间域 } M\} \overset{1:1}{\rightleftharpoons} \{G \text{ 的闭子群}\}$$

$$M = L^H \longleftarrow H$$

$$M \longmapsto H = Gal(L/M)$$



而且在此对应下 $[M:K]$ 有限 $\Leftrightarrow [G:H]$ 有限 $\Leftrightarrow$ H 为开群

此时 $[M:K] = [G:H]$.

$H \triangleleft G \Leftrightarrow M/K$ 是 Galois 扩张，此时 $Gal(M/K) \cong G/H$

（作为拓扑群同构）

<u>Cor</u> L/K 同上.

$$G = Gal(L/K) \cong \varprojlim_{K \subseteq M \subseteq L,\ M/K \text{ 有限 Galois 扩张}} Gal(M/K)$$

特别地. $Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \cong \varprojlim_{K/\mathbb{Q} \text{ 有限 Galois 扩张}} Gal(K/\mathbb{Q})$

$$\overline{\mathbb{Q}} = \bigcup_{\substack{K/\mathbb{Q} \\ \text{有限 Galois}}} K = \varinjlim_{K/\mathbb{Q}} K$$

$$H^r(Gal(\overline{\mathbb{Q}}/\mathbb{Q}), M) = \varinjlim_{K/\mathbb{Q}} H^r(Gal(K/\mathbb{Q}), M^{Gal(\overline{\mathbb{Q}}/K)})$$

$$H^r(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), M) = \varinjlim_{K/\mathbb{Q}\text{ 有限Galois}} H^r(\mathrm{Gal}(K/\mathbb{Q}), M^{\cdots})$$

Open Question (Galois 反问题)

给定有限群 G，是否存在 $L/\mathbb{Q}$ 为有限Galois扩张且 $\mathrm{Gal}(L/\mathbb{Q}) = G$？

…… 的有限群 —— —— Galois扩张 —— ——？

(也可以把 $\mathbb{Q}$ 换成别的域)

① 当 G 是Abel群时，反问题 ✓ (利用分圆域)

② 当 $G = S_n$ ✓ (先在 $\mathbb{Q}(X_1, \cdots, X_n)$ 上处理，再用Hilbert不可约定理↝到处)

③ 当 G 是可解群 时，反问题 ✓. (Shafarevich 1954)

↳ 这包括了所有奇阶有限群! (Feit–Thompson 1962-63)

一般情形？ G 有限 $\Rightarrow$ $\exists n \in \mathbb{N}$ $G \hookrightarrow SL_n$

作为代数群的齐次空间 $X = SL_n/G$

Colliot-Thélène : K-代数簇 X 上的有理点的某种弱逼近性质 $\Rightarrow$ G 是 K 上的Galois群

$$X(K) \hookrightarrow \prod_{v \in \Omega_K S} X(K_v)$$

可利用代数n的/含求n的的工具

↳ 最新进展：Y. Harpaz 与 O. Wittenberg 之著.

回到 Galois 上同调

例. ① $M = \bar{K}^*$ $G = \mathrm{Gal}(\bar{K}/K)$ $(\bar{K}^*)^{\mathrm{Gal}(\bar{K}/L)} = L^*$

$$H^1(G, \bar{K}^*) = \varinjlim_{L/K\text{ 有限Galois}} H^1(\mathrm{Gal}(L/K), L^*) = \varinjlim 0 = 0.$$

↑ Hilbert 90

② 对域 L，令 $\mu_n(L) = \{\zeta \in L^* \mid \zeta^n = 1\}$ $G = \mathrm{Gal}(\bar{K}/K)$

L/K

② 对域 L，令 $\mu_n(L)=\{\zeta\in L^*\mid \zeta^n=1\}$　$G=Gal(\bar{K}/K)$

L/K

G-模正合列：　$GL_1(\bar{K})$　$GL_1(\bar{K})$　GL_1

$$1\to \mu_n(\bar{K})\to \bar{K}^*\xrightarrow{n}\bar{K}^*\to 1$$

$\alpha\mapsto\alpha^n$

（G_m 的 Kummer 序列）

↝ 长正合列：

Hilbert 90

$$1\to\mu_n(K)\to K^*\xrightarrow{n}K^*\to H^1(G,\mu_n(\bar{K}))\to H^1(G,\bar{K}^*)=0$$

从而　$K^*/K^{*n}\xrightarrow{\simeq} H^1(G,\mu_n(\bar{K}))$

③ 若 $G=Gal(\bar{K}/K)$ 平凡作用于 M

$H^1(G,M)=Hom_c(G,M)$

G 带 Krull 拓扑，M 离散拓扑。

$\varphi\in Hom_c(G,M)$ 即　$\varphi: G\to M$ 在 G 的某个开子群 N 上是平凡的

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & M \\ \pi\downarrow & \nearrow_{\bar{\varphi}=\alpha} & \\ G/N & & \end{array}$$

N 对应于有限 Galois 扩张 L/K

$G/N\cong Gal(L/K)$

φ 相当于一个对　(α, L)

其中 L/K 有限 Galois 扩张

$\alpha: Gal(L/K)\hookrightarrow M$ 为单的平凡表示

④ $G=Gal(\bar{K}/K)$　K 数域，　E/K 椭圆曲线

$M=E(\bar{K})$ 连续 G-模

简记 $H^r(Gal(\bar{K}/K),E(\bar{K}))$ 为　$H^r(K,E)$

$\forall v\in\Omega$　　$K\hookrightarrow K_v$ 诱导出

$$\begin{array}{ccc} \bar{K} & \hookrightarrow & \bar{K}_v \\ \uparrow & & \uparrow \\ K & \hookrightarrow & K_v \end{array}$$

$G_v=Gal(\bar{K}_v/K_v)$ 作用于 $\bar{K}_v\supseteq\bar{K}$　　$\bar{K}/K$ 正规扩张

$G_v\supseteq\bar{K}$

于是诱导出一个单同态　$G_v=Gal(\bar{K}_v/K_v)\hookrightarrow Gal(\bar{K}/K)=G$

从而同态　$Gal(\bar{K}/K)\xrightarrow{f}E(\bar{K})$　开始

$$\begin{array}{ccc} \uparrow & & \uparrow \\ & & \end{array}$$

从对应为

$$\begin{array}{ccc} Gal(\overline{K}/K) & \xrightarrow{\pi} & E(\overline{K}) \\ \uparrow & & \updownarrow \\ Gal(\overline{K_v}/K_v) & \dashrightarrow & E(\overline{K_v}) \end{array}$$

开始

f也是对应为

$$H^1(K, E) \longrightarrow H^1(K_v, E) \quad (G_v \subset G)$$

Def (Tate-Shafarevich群)

$$Ш(E/K) = Ш^1(K, E) := \ker\left(H^1(K, E) \to \prod_{v \in S_K} H^1(K_v, E) \right)$$

Cor K 数域，则 $Ш^1(K, E)$ 是有限群.

(衡量整体局部-整体原则失效的程度)

↳ 描述数域的类群

椭圆曲线的 Kummer 序列

$$0 \to E[n](K) \to E(\overline{K}) \xrightarrow{[n]} E(\overline{K}) \to 0$$

$E[n] = E[n](\overline{K})$

$$\left(E(\mathbb{C}) \cong \mathbb{C}/\Lambda \cong \mathbb{R}^2/\mathbb{Z}^2 \cong S^1 \times S^1 \right)$$

$[n]$ 是满的

↝ 长正合列

$$0 \to E[n](K) \to E(K) \xrightarrow{[n]} E(K) \to H^1(K, E[n]) \to H^1(K, E) \xrightarrow{[n]} H^1(K, E) \to \cdots$$

$$\to 0 \to E(K)/nE(K) \to H^1(K, E[n]) \to H^1(K, E)[n] \to 0$$

有限的时候

↳ 一般不是有限的.