目标：证明弱MW定理：引入Galois上同调工具

III. Galois上同调

几何、拓扑 —— 几何对象，中心问题之一，上同调作不变量

例如：Riemann面的亏格

"几何" 指在$\mathbb{C}$上（代数闭域）的对象的性质。
↳ 算术上很简单

Grothendieck 代数几何 两个极端 ⟨ 几何 / 算术

域K（一般 $\bar{K}\neq K$）—— $\mathrm{Spec}(K)$ 几何上平凡。
算术上很复杂

Galois群 $\mathrm{Gal}(\bar{K}/K)$

$K=\mathbb{R}$ $\mathrm{Gal}(\mathbb{C}/\mathbb{R})\cong \mathbb{Z}/2\mathbb{Z}=\langle\sigma\rangle$ → 复共轭

$K=\mathbb{F}_p$ $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)\cong\hat{\mathbb{Z}}=\langle \mathrm{Frob}\rangle$

$K=\mathbb{Q}$ 太复杂 $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ 难。

现代代数几何学：（统一的语言）

$\mathrm{Gal}(\bar{K}/K)$ 与 Riemann面的 π_1
←类比→

域扩张 ⟷ 覆盖空间. $\mathbb{R}\to S^1=\mathbb{R}/\mathbb{Z}$
$\pi_1\cong\mathbb{Z}$ $m\mathbb{Z}$
$S^1\to S^1$ $S^1\subset\mathbb{C}^1\setminus\{0\}$
$z\mapsto z^m$

Galois群的上同调 ⟷ Riemann面上的向量丛的上同调

Galois上同调（更一般：étale上同调）

1. 群上同调

1. 群的上同调

G 有限群　　(以后将取为 Galois 群)

Def. 一个 G-模 M 是一个 Abel 群且带有 G 的作用.

$G\times M\to M$

(1) $\sigma(m+m')=\sigma m+\sigma m'$　　$\forall \sigma\in G,\ \forall m,m'\in M.$

(2) $(\sigma\tau)(m)=\sigma(\tau m)$　　$\forall \sigma,\tau\in G,\ \forall m\in M$

(3) $1\cdot m=m$　　$\forall m\in M$

($1\in G$).

(这也相当于给定一个群同态　$G\to Aut(M)$)

exer 尝试定义 G-模之间的同态.

例. L/K 为有限 Galois 扩张. $G=Gal(L/K)$

$M=L,\ L^*,\ E(L)$ 均是 G-模.

Def　　$H^0(G,M):=M^G=\{m\in M \mid \sigma m=m\ \ \forall\sigma\in G\}\subset M$

上例中　$H^0(G,L)=L^G=K$,　$H^0(G,L^*)=K^*$

$H^0(G,E(L))=E(K)$

$Gal(L/K)=Aut_K(L)=\{\sigma: L\to L \mid \sigma$ 是环同构, 且 $\sigma_{|K}=id_K\}$

$G\times L\to L$

$\sigma, x\mapsto \sigma(x)=\sigma x$

E: K-椭圆曲线　$G=Gal(L/K)$

$G\times E(L)\longrightarrow E(L)$

$\sigma,\ (x:y:z)\quad (\sigma(x):\sigma(y):\sigma(z))$

E:　$a,b\in K$.

$(x:y:z)$ 满足 $y^2=x^3+ax+b$

$\sigma\in G$　　$\sigma(a)=a$　$\sigma(b)=b$

$(\sigma(x):\sigma(y):\sigma(z))$ 仍满足方程

称定义 $H^1(G,M)$

为 $f: G\to M$ 为交叉同态 (crossed homomorphism)

(但未必是一个群同态!)

若 $f(\sigma\tau)=f(\sigma)+\sigma f(\tau)$　　$\forall\sigma,\tau\in G$

由此易知有 $f(1)=f(1)+f(1)\in M\Rightarrow f(1)=0\in M$

$\forall m\in M$. 令 $f(\sigma):=\sigma m-m \quad \forall\sigma\in G$

$f: G\to M$

easy 验证 f是一个交叉同态，称为 主交叉同态

$Z^1(G,M)=\{$交叉同态 $f:G\to M\}$ 在映射加法之下，$Z^1(G,M)$是一个 Abel群.

$B^1(G,M)=\{$主交叉同态$\}\lhd Z^1(G,M)$ 正规子群

定义 $H^1(G,M)=\dfrac{Z^1(G,M)}{B^1(G,M)}$ Abel群.

若考虑 $f:\underbrace{G\times G\times\cdots\times G}_{r个}\to M$ 满足一些特定条件. $H^r(G,M)=\dfrac{Z^r(G,M)}{B^r(G,M)}$

若 G 平凡作用在 M上. $\forall\sigma\ \forall m\quad \sigma m=m$.

$H^0(G,M)=M^G=M$

$H^1(G,M)=\dfrac{Z^1(G,M)}{B^1(G,M)}$ 此时交叉同态正是群同态 $G\to M$ 交换群

主交叉同态只有"0"

$G\to M$, $G\to G^{ab}=G/[G,G]\to M$

$=\mathrm{Hom}(G,M)$

$=\mathrm{Hom}(G^{ab},M)$

Prop (Hilbert 90定理) $H^1(G,L^*)=0$ $\quad G=\mathrm{Gal}(L/K)$

即 任何交叉同态 $G\to L^*$ 均是主交叉同态 $\sigma\mapsto\dfrac{\sigma\gamma}{\gamma}$.

Pf. $f:G\to L^*$ 交叉同态

乘法记号下 即 $f(\sigma\tau)=f(\sigma)\cdot\sigma(f(\tau))\quad\forall\sigma,\tau\in G$.

我们要找 $\gamma\in L^*$ 使 $f(\sigma)=\dfrac{\sigma\gamma}{\gamma}\ (\forall\sigma\in G)$

> **Lem** (Dedekind 独立性 引理) H 群. $\sigma_i: H\to L^*$ 两两互异的群同态
> 看作从 H 到 L 的函数 $\sigma_i\in F(H,L)$ (L-向量空间)
> 那么 $(\sigma_1,\cdots,\sigma_n)$ 是线性无关的.

$\forall\ \tau\in G=\mathrm{Gal}(L/K)$ ...

$\forall\ \tau\in G=Gal(L/K)$　　$0\neq f(\tau)\in L$

$\tau: L\to L$　　$\tau: H=L^{*}\to L^{*}$ 群同态

$0\mapsto 0$

Lem $\Rightarrow$　$\sum_{\tau\in G} f(\tau)\cdot\tau\neq 0$　　(作为从 L^{*} 到 L 的函数)

即 $\exists\alpha\in L^{*}$ 使 $\beta=\sum_{\tau\in G} f(\tau)\cdot\tau(\alpha)\neq 0$

此时 $\forall\sigma\in G$　　$\sigma\beta=\sum_{\tau\in G}\sigma(f(\tau))\cdot\sigma\tau(\alpha)=\sum_{\tau\in G} f(\sigma)^{-1}\cdot f(\sigma\tau)\cdot\sigma\tau(\alpha)$

f: 2-cocycle

$$=f(\sigma)^{-1}\cdot\sum_{\tau\in G} f(\sigma\tau)\sigma\tau(\alpha)=f(\sigma)^{-1}\cdot\beta$$

$\Rightarrow f(\sigma)=\frac{\beta}{\sigma\beta}=\frac{\sigma(\beta^{-1})}{\beta^{-1}}=\frac{\sigma\gamma}{\gamma}$　取 $\gamma=\beta^{-1}$ 即可.　　#

Pf of Lem of Dedekind: 对 n 作归纳. $n=1$: $\forall x\in H$　$a_1\sigma_1(x)=0\in L$

$\sigma_1(x)\in L^{*}$ 于是 $a_1=0$.

$n>1$: 假设有 (*)　$a_1\sigma_1(x)+\cdots+a_n\sigma_n(x)=0$　$\forall x\in H$　$(a_i\in L)$

且 a_i 不全为 0.

不妨设 a_i 全不为 0　(否则 σ 个数 $<n$, 由归纳假设证毕),

还可设其中某个为 1,　$a_n=1$

$\sigma_n\neq\sigma_1$ 即 $\exists y\in H$　$\sigma_n(y)\neq\sigma_1(y)$

(*) 对 $\forall x\in H$ 从而对 yx 也成立

$$a_1\sigma_1(y)\sigma_1(x)+\cdots+a_{n-1}\sigma_{n-1}(y)\sigma_{n-1}(x)+\sigma_n(y)\sigma_n(x)=0\quad(y\text{ 固定},\ \forall x\in H)$$

除以 $\sigma_n(y)$

$$(**)\quad a_1\frac{\sigma_1(y)}{\sigma_n(y)}\sigma_1(x)+\cdots+a_{n-1}\frac{\sigma_{n-1}(y)}{\sigma_n(y)}\sigma_{n-1}(x)+\sigma_n(x)=0$$

$(**)-(*)$:

$$a_1\left(\frac{\sigma_1(y)}{\sigma_n(y)}-1\right)\sigma_1(x)+\cdots+a_{n-1}\left(\frac{\sigma_{n-1}(y)}{\sigma_n(y)}-1\right)\sigma_{n-1}(x)=0\quad(\forall x\in H)$$

项数 $<n$, 用归纳假设, 所有系数为 0, 即

项数减少，用归纳假设，所有系数为0，即

$$a_1\left(\frac{\sigma_1(y)}{\sigma_n(y)}-1\right)=0 \Rightarrow \sigma_1(y)=\sigma_n(y)\ \text{矛盾} \qquad \#$$

Prop 对任何 G-模的正合列

$$0\to M\xrightarrow{\alpha}N\xrightarrow{\beta}P\to 0$$

$\operatorname{Ker}\beta=\operatorname{Im}\alpha$
M处正合 ⟺ α单射
P —— ⟺ β满射.

那么有以下长正合列：

$$0\to H^0(G,M)\to H^0(G,N)\to H^0(G,P)\xrightarrow{\delta}H^1(G,M)\to H^1(G,N)\to H^1(G,P)\to\cdots$$

Rk. 1. 长正合列可一直下去

2. 没有δ的地方的映射都是显然的

$$\frac{Z^1(G,M)}{B^1(G,M)}=H^1(G,M)\to H^1(G,N)=\frac{Z^1(G,N)}{B^1(G,N)}$$

$\alpha: M\to N$

$$H^0(G,M)\to H^0(G,N)$$
$$\| \qquad\qquad \|$$
$$M^G \qquad\qquad N^G$$
$$m\ \longmapsto\ \alpha(m)$$

3. H^r 是 $H^0: M\mapsto M^G$ 的导出函子

Pf. 给出δ的定义，剩下的按"正合列"的定义来验证

$$\delta: H^0(G,P)=P^G\longrightarrow H^1(G,M)=\frac{Z^1(G,M)}{B^1(G,M)} \text{ 如下定义：}$$
$$p\ \longmapsto\ \delta(p):=\varphi.$$

(#) $0\to M\xrightarrow{\alpha}N\xrightarrow{\beta}P\to 0$ ⇒ $\exists\, n\in N$ 映为 p.

$\forall\,\sigma\in G$ 考虑 $\sigma n-n\in N$ 映到 P 中 $\sigma p-p=0$ ($p\in P^G$)

从而 $\sigma n-n\in M$

定义 $\varphi: G\to M$
$\sigma\mapsto \sigma n-n$

它是个交叉同态（⚠，实际上 $M\hookrightarrow N$ 之后是主交叉同态，从G到N，未复合前不是主交叉同态 从G到M的）

于是 $\varphi\in Z^1(G,M)$

把它在 $H^1=\frac{Z^1(G,M)}{B^1(G,M)}$ 中的类定义为 $\delta(p)$.

若取另一个 n' 为 p 的原象，n 与 n' 均映成 p. 即，$n'-n$ 映为0.

(#)正合 ⇒ $n'-n\in M$. ($m=$)

这样定义出来的 φ' 与 φ 相差 $(\sigma n'-n')-(\sigma n-n)=\sigma m-m$ $(m\in M)$

即 $\varphi'-\varphi\in B^1(G,M)$ 为一个主交叉同态

即 $\psi-\varphi\in B^1(G,M)$ 为一个主观同态

从而 φ' 与 φ 在 $H^1=\frac{Z^1}{B^1}$ 中是一样的

即 $\varphi=\delta(p)$ 的定义不依赖于 p 的原像 n 的选取，良定义！ #

Rk. 从正合列 $0\to M\to N\to P\to 0$ 出发 作用 $H^0(G,-)$

一般只得左正合列，$H^1(G,M)$ 正是衡量 $H^0(G,-)$ 与正合函子的差距。

这是一般上同调理论的套路。Grothendieck 同调代数《Tohoku》

$H^r(G,-)$ 是 $M\mapsto M^G=H^0(G,M)$ 的右导出函子。

比观点可统一定义 代数簇 Zariski 拓扑的上同调

étale 拓扑 上同调（Gal 的上同调是一个特殊情形）。

"函子性"

$H<G$ 子群 对 $f:G\to M$ 交叉同态 考虑 $f|_H:H\to M$ 也是交叉同态 可得

$$\mathrm{Res}:H^1(G,M)\to H^1(H,M)$$ Abel 群同态

同调代数自动得到： $M^G\subset M^H\subset M$

即 $H^0(G,-)$ "$\longrightarrow$" $H^0(H,-)$

自动诱导出 $\mathrm{Res}:H^r(G,M)\to H^r(H,M)\quad\forall r\in\mathbb{N}$

"对偶地" 若 $H<G$, $s=[G:H]<+\infty$. 考虑一组完全的左陪集代表元 $\{\sigma_1,\dots,\sigma_s\}$

即 $G=\coprod_{i=1}^{s}\sigma_i H$

可定义
$$M^H\to M^G$$
$$m\mapsto\sum_{i=1}^{s}\sigma_i m$$

$$\forall\sigma\in G\qquad \sigma\sum_{i=1}^{s}\sigma_i m=\sum_{i=1}^{s}(\sigma\sigma_i)m\overset{\text{重排}}{=}\sum_{i=1}^{s}\sigma_i m\in M^G$$

$\{\sigma_1,\dots,\sigma_s\}$ 是一组完全左陪集代表元

$\{\sigma\sigma_1,\dots,\sigma\sigma_s\}$ - - - - - - -

自动诱出 $\mathrm{Cores}:H^r(H,M)\to H^r(G,M)$

Corestriction

限制映射　　Cores: $H^1(H,M) \to H^1(G,M)$

Corestriction

lem　$Cores \circ Res = s$ 为乘以 s 的映射.　　$s = [G:H]$

Pf: 只需在 H^0 验证, H^r 上的会由此导出

$$M^G \longrightarrow M^H \longrightarrow M^G$$

$$m \mapsto m \longmapsto \sum_{i=1}^{s} \sigma_i m = \sum_{i=1}^{s} m = sm.$$

#

Cor. 若 $|G| = s$ 则 $H^1(G,M) \xrightarrow{\cdot s} H^1(G,M)$ 为 0 同态.

Pf. 取 $H = \{1\} \lhd G$.　　$Cores \circ Res = \cdot s$

而 $H^1(\underset{\{1\}}{H}, M) = 0$

#

除了 Res 与 Cores. 还有一个 Inflation 映射. 如下定义:

$H \lhd G$ 正规子群　　M: G-模

M^H 成为 G/H-模

$f: G/H \longrightarrow M^H$ 为交叉同态 $\rightsquigarrow$ $G \to M$ 交叉同态

$$\begin{array}{ccc} G & \dashrightarrow & M \\ \downarrow & & \cup \\ G/H & \xrightarrow{f} & M^H \end{array}$$

从而导出: $Inf: H^1(G/H, M^G) \to H^1(G,M)$

$$0 \to H^1(G/H, M^H) \xrightarrow{Inf} H^1(G,M) \xrightarrow{Res} H^1(H,M)$$ 正合列.

(它是 Hochschild-Serre 谱序列的低阶项

$$H^p(G/H, H^q(H,M)) \Rightarrow H^{p+q}(G,M)$$

III 有限群 + 拓扑工具

例如 $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ 拓扑群.

即 G 是群又是拓扑空间, 且这两种结构是相容的. 即

$G \times G \to G$　　及　$G \to G$　连续映射

$G\times G \to G$ 及 $G \to G$ 连续映射
$a, b \mapsto ab$ 　 $a \mapsto a^{-1}$

例 $(\mathbb{R},+)$. $(\mathbb{R}^*,\cdot)$ 　 Galois群均是拓扑群. 紧的有限(profinite)

群上同调 → 推广到无限群中.

Def. M: G-模, 称为离散G-模 是指当它取离散拓扑时 $G\times M \to M$ 是连续映射. ($\Leftrightarrow$ $M=\bigcup_H M^H$ 其中H取遍G的开子群)

即 M中每一个元素均被G的某个开子群固定.

例. $G=\mathrm{Gal}(\bar{K}/K)$ 紧群. $H \underset{\text{开}}{\trianglelefteq} G$ 闭开. 　 G/H 有限群. $(G=\bigsqcup_{\sigma\in S}\sigma H)$

无穷维Galois理论中. 对应至 $\bar{K}/K$ 中间域 L 使 $[L:K]$ 有限

$M=\bar{K}$, $\bar{K}^*$, $E(\bar{K})$
$M^H=L$, L^*, $E(L)$ 　均是离散G-模

此时 $\bar{K}=\bigcup_{L/K \text{有限}} L$ 　 $\bar{K}^*=\bigcup_{L/K \text{有限}} L^*$ 　 $E(\bar{K})=\bigcup_{L/K \text{有限}} E(L)$

M: 离散G-模 　 $H^0(G,M)=M^G$

定义 H^1时 只考虑 $f: G\to M$ 连续的交叉同态 $Z^1(G,M)$

$$\frac{Z^1(G,M)}{B^1(G,M)}=H^1(G,M) \overset{\text{Th}}{=} \varinjlim_{\substack{H \\ H\trianglelefteq G \\ \text{开}}} H^1(G/H, M^H)$$
(G/H: 有限群)

$$0\to H^1(G/H,M^H)\xrightarrow{\mathrm{Inf}} H^1(G,M)\xrightarrow{\mathrm{Res}} H^1(H,M)$$

lim 可以理解为 $H^1(G,M)$ 是"很多" $H^1(G/H,M^H)$ 的"并"

Rk 可理解为 $H^1(G,M)$ 是"所有" $H^1(G/H, M^H)$ 的"并"

若有 $H' \underset{open}{\triangleleft} G$ 　 $H' \subset H$

$$H^1\left(\frac{G/H'}{H/H'}, (M^{H'})^{H/H'}\right) \overset{\gamma}{=} H^1(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^1(G,M)$$

$$H^1\left(\frac{G/H'}{H/H'}, (M^{H'})^{H/H'}\right) \xrightarrow{\mathrm{Inf}} H^1(G/H', M^{H'}) \xrightarrow{\mathrm{Inf}} H^1(G,M)$$

$\gamma \in H^1(G/H, M^H)$ 在 $H^1(G,M)$ 中的像为0

$\Longleftrightarrow$ 存在某 $H' \underset{open}{\triangleleft} G$, $H' \subset H$, 使

γ 在 $H^1(G/H', M^{H'})$ 这个有限群上同调中已经为0.

Rk. 之前已证明 有限群 的上同调可被 群的阶所零化

此时 profinite gp. 的上同调 $H^1(G,M)$ 作为群 也是扭群

Rk. 在 G 有限时 $G \curvearrowright M$ 平凡作用. 　 $H^1(G,M) = \mathrm{Hom}(G,M) = \mathrm{Hom}(G/[G,G], M)$

无限群时. $G \curvearrowright M$ 平凡作用, 　 $H^1(G,M) = \mathrm{Hom}_{cts}(G,M) = \mathrm{Hom}_{cts}(G/\overline{[G,G]}, M)$

即从 G 到 M 的连续的群同态的集合