局部整体原则

k 数域

$X/_k$ 代数簇， 几何对象

$X(k)$ = 多项式在 k 上的公共解

$k \longrightarrow k_v$ 各种完备化 $\quad \mathbb{Q} \hookrightarrow \mathbb{Q}_p$, $\mathbb{Q} \hookrightarrow \mathbb{R}$

$X(k) \hookrightarrow X(k_v)$

$X(k) \hookrightarrow \prod_{v \in \Omega_k} X(k_v)$ $\quad \Omega_k = \{\underset{k\text{的位}}{\text{place}}\} = \{\text{实. 复嵌入}\} \cup \{\mathfrak{p} \subset O_k\}$

$X(k) \neq \phi \underset{\Leftarrow ?}{\Longrightarrow} \forall v \in \Omega_k \quad X(k_v) \neq \phi$

Def. 若"$\Leftarrow$"成立 则称 满足 Hasse 原则 / 局部整体原则 (HP) P = principle

例 X 由二次型定义。 HP ✓

Rk. 交元域多，二次型越容易。

小目标：对 $X \subset \mathbb{P}^2$ $\quad X: P(x,y,z) = x^2 - ay^2 - bz^2 = 0$
$a, b \in k (=\mathbb{Q})$

给一个"证明"

Def (Hilbert 符号) $K/\mathbb{Q}$ 域扩张 $\quad K = \mathbb{Q}_p, \mathbb{R}, \mathbb{Q}$.

$$(a,b)_K := \begin{cases} +1, & X(K) \neq \phi \\ -1, & X(K) = \phi \end{cases}$$

$(a,b) = (a,b)_{\mathbb{Q}}$.
$(a,b)_\infty = (a,b)_{\mathbb{R}}$
$(a,b)_p = (a,b)_{\mathbb{Q}_p}$

X: Hasse Principle $\Longleftrightarrow$ $\boxed{\text{“} (a,b)_p = 1 \ \forall p \in \Omega_{\mathbb{Q}} \Rightarrow (a,b) = 1 \text{”}}$

问题1 $p \in \Omega$ $\quad n_p \in \{\pm 1\}$. 是否存在 $a, b \in \mathbb{Q}^\times$
$(a,b)_p = n_p \quad \forall p \in \Omega$

必 不

$(a,b)_p = \varepsilon_p \quad \forall p \in \Omega$

答：否

必要条件：局部条件 (C1)
整体条件 (C2)

Th $\forall a,b \in \mathbb{Q}^*$

(C1) $(a,b)_p = 1$ 对几乎所有 p 成立

(C2) 乘积公式 $\prod_{p\in\Omega}(a,b)_p = 1$ (Rk. (C1) $\Rightarrow$ (C2) 中 $\prod$ 是有限积)

Pf

(C1) $P(x,y,z) = x^2 - ay^2 - bz^2$

不妨设 $1, -a, -b \in \mathbb{Z} \subset \mathbb{Z}_p$

对几乎所有 p　$p \nmid a$，$p \nmid b$，$1, -a, -b \in \mathbb{Z}_p^*$

若 $p>2$，$p \neq \infty$，第一次课 $\Rightarrow$ $P(x,y,z) = 0 \mod p$ 有非0解

Hensel 提升为 $\mathbb{Z}_p$.

(C2) 证明思路：

* 首先建立 Hilbert 符号的性质：

$(a,b) = (b,a)$ ✓

$(a,b^2) = 1$　$(1,0,1)$ 解

$(a,-a) = 1$　$(0,1,1)$ 是解

$(a,1-a) = 1$　$(1,1,1)$ 是解

双线性 $(aa',b) = (a,b)(a',b)$

$(a,b) = (a,-ab) = (a,(1-a)b)$

* 利用 Legendre 符号计算 Hilbert 符号

① $(a,b)_\infty = 1 \Leftrightarrow a>0$ 或 $b>0$

② p 奇　$(a,b)_p = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha$　　$\mathbb{Z}_p/p \cong \mathbb{Z}/p\mathbb{Z}$

其中 $a = p^\alpha u$，$b = p^\beta v$　　$u, v \in \mathbb{Z}_p^*$，$\alpha, \beta \in \mathbb{Z}$

$$\varepsilon(p) = \begin{cases} 0 & 若 \frac{p-1}{2} 偶 \\ 1 & 若 \frac{p-1}{2} 奇 \end{cases}$$

③ $p=2$.　$(a,b)_2 = (-1)^{\varepsilon(u)\varepsilon(v) + \alpha\omega(v) + \beta\omega(u)}$

$\varepsilon, \alpha, \beta, u, v$ 同上

③ $p=2$. $(a,b)_2=(-1)$

$\varepsilon,\alpha,\beta,u,v$ 同上

$$\omega(u)=\begin{cases}1, & \frac{u^2-1}{8}\text{ 奇}\\ 0, & \frac{u^2-1}{8}\text{ 偶}\end{cases}$$

※ 计算来和一下算，归结为三情况 $(a,b)=(-1,-1)$

$(a,b)=(-1,\ell)$ ℓ 素数

$(a,b)=(\ell,\ell')$ ℓ,ℓ' 素数. #

<u>问题2</u> 是否只要满足 (c1)(c2)，就可找到 $a,b\in\mathbb{Q}^\times$ 使 $(a,b)_p=n_p$ $(\forall p\in\Omega)$

答：将用"类域论"的观点来回答.

同时证明 X HP ✓.

Def K 域 A 含幺环(可不交换)

若 $K\subset A$ 子环 ($1_K=1_A$) 称 A 是一个 K-代数.

(等价地，K-algebra = 环 + K-向量空间

且两种运算协调)

总设 $\dim_K A<+\infty$

Def 称 A 是 <u>单代数</u> (simple algebra) 若它无非平凡的双边理想

如果还有 $\underset{\text{中心}}{Z(A)}=\{a\in A \mid ab=ba\ \forall b\in A\}=K$

则称 A 为 K 上的<u>中心单代数</u> (central simple algebra)

<u>例</u>. $A=M_n(K)$ $Z(M_n(K))=\{\lambda I_n \mid \lambda\in K\}\cong K$

$\quad\ \ \cup\!\shortmid$

$\quad\ \ K$

Prop A: K-代数，以下等价

(1) A 是中心单代数

(2) $A\otimes_K K^s \underset{K^s\text{-代数}}{\cong} M_n(K^s)$ $K^s=K$ 的可分闭包

(3) $\exists L/K$ 有限可分扩张. $A\otimes_K L \underset{L\text{-代数}}{\cong} M_n(L)$

(3) $\exists L/K$ 有限可分扩张，$\underset{L\text{-代数}}{A\otimes_K L\cong M_n(L)}$

Rk. "中心单代数" $\underset{\uparrow}{\supsetneq}$ "可除代数"
允许有限可分扩张意义下 =.

例. $K=\mathbb{R}$ $\mathbb{H}$ = Hamilton 四元素代数 quaternion algebra（是 $\mathbb{C}$ 的某种推广）

$$\mathbb{H}=\mathbb{R}\cdot 1\oplus\mathbb{R}i\oplus\mathbb{R}\cdot j\oplus\mathbb{R}\cdot k$$ 作为 $\mathbb{R}$-向量空间
基 $(1,i,j,k)$

乘法由以下公式给出：
$$\left.\begin{array}{l} i^2=-1=j^2 \\ ij=-ji=k \end{array}\right\}\Rightarrow k^2=-1$$
$\Rightarrow \mathbb{H}$ 非交换.

Prop $\mathbb{H}$ 是一个可除代数（即 $\mathbb{H}^\times=\mathbb{H}^*$）（$\Rightarrow \mathbb{H}\ncong M_2(\mathbb{R})$，$\dim=4$）

Pf 定义 norm $N:\mathbb{H}\to\mathbb{R}$

$q=x+yi+zj+tk$ $x,y,z,t\in\mathbb{R}$

$\bar{q}=x-yi-zj-tk$

$$N(q)=q\cdot\bar{q}=(x+yi+zj+tk)(x-yi-zj-tk)$$
$$=\cdots$$
$$=x^2+y^2+z^2+t^2\in\mathbb{R}$$

$q=0\Leftrightarrow x=y=z=t=0\Leftrightarrow N(q)=0.$

从而 $q\neq 0$，则 $q^{-1}=\bar{q}/N(q)$ #

Rk. 此例明显依赖于 $K=\mathbb{R}$，若 $\mathbb{R}$ 换 $\mathbb{C}$，最后"$\Leftarrow$"不成立.

事实上 $\underbrace{\mathbb{H}\otimes_{\mathbb{R}}\mathbb{C}\cong M_2(\mathbb{C})}$ $\mathbb{C}$-代数同构

$$1\longmapsto\begin{pmatrix}1&0\\0&1\end{pmatrix}$$
$$i\longmapsto\begin{pmatrix}\sqrt{-1}&0\\0&\sqrt{-1}\end{pmatrix}$$
$$j\longmapsto\begin{pmatrix}0&-1\\1&0\end{pmatrix}$$
$$k\longmapsto\begin{pmatrix}0&-\sqrt{-1}\\-\sqrt{-1}&0\end{pmatrix}$$

$\mathbb{C}$-线性扩张

$\mathbb{H}$ 是中心单代数.
$Z(\mathbb{H})=1\cdot\mathbb{R}$

$$k \longmapsto \begin{pmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{pmatrix}$$

另外. $\mathrm{norm} \otimes_{\mathbb{R}} \mathbb{C} = \det$

Brauer 群

Def $\mathrm{Br}\,K = \{K$上有限维中心单代数$\}/\sim$

$$A \sim B \overset{\text{def}}{\Longleftrightarrow} \exists\, m, n \in \mathbb{N} \ \text{s.t.}\ M_n(A) \underset{K\text{-alg}}{\cong} M_m(B).$$

(例: $A = M_r(K) \sim B = K$
取 $n = 1,\ m = r$)

Prop $\mathrm{Br}\,K$ 是一个交换群

- 乘法: $A \otimes_K B \cong B \otimes_K A$
- 乘法单位元: K. $A \otimes_K K \cong A$.
- 乘法逆: $A \otimes_K A^{op} \cong M_n(K) \sim K$

(A^{op} 是 $(A, \cdot)$ 的反环. $(A^{op}, \circ)$, $a \circ b = b \cdot a$)

推广的四元数代数

$a, b \in K^\times$　　$Q_{a,b} = 1 \cdot K \oplus iK \oplus jK \oplus kK$

$i^2 = a,\quad j^2 = b,\quad ij = -ji = k$

(例 $K = \mathbb{R}$ 时 $Q_{-1,-1} = \mathbb{H}$)　　是中心单代数.

$Q_{a,b} \in \mathrm{Br}\,K$　　$Q_{a,b} \otimes_K Q_{a,b} \sim K$.

即 在 $\mathrm{Br}\,K$ 中 $Q_{a,b}$ 是一个 2-torsion 元

Th (Brauer-Hasse-Noether)(类域论)　K 数域

(*) $0 \to \mathrm{Br}\,K \xrightarrow{\varphi} \bigoplus_{v \in \Omega_K} \mathrm{Br}\,K_v \xrightarrow{\psi} \mathbb{Q}/\mathbb{Z} \to 0$　是正合列.

Rk 以上结论是 Gauss 二次互反律的超大推广

Rk. (1) 类域论是 Gauss 二次互反律的极大推广.

(※) 应用到 Hilbert 符号上得 $\prod_{v\in\Omega}(a,b)_v = 1$)

(2) 类域论有多种观点来阐述:

① Tate's thesis (局部域、整体域上的调和分析)

② 上同调理论 Galois 上同调. $\mathrm{Br}K = H^2(\mathrm{Gal}(\bar{K}/K), \bar{K}^*)$

(3) 进一步推广: Langlands 纲领

关于 $G_m = GL_1 \rightsquigarrow GL_n \rightsquigarrow$ 一般 reductive 代数群的表示论

Galois 表示 $\xleftrightarrow{1:1}$ 自守表示.

代数群 $G \supset$ {自守形式 / 模形式}

回到 Th $K=\mathbb{Q}$.

$$\underbrace{\mathrm{Br}\mathbb{R} = \mathrm{Br}\mathbb{Q}_\infty \simeq \mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}}_{\mathrm{inv}_\infty}$$

$\mathrm{inv}_p : \mathrm{Br}\mathbb{Q}_p \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ $\qquad$ $\underbrace{Q_{a,b} \in \mathrm{Br}\mathbb{Q} \to \mathrm{Br}\mathbb{Q}_p \xrightarrow{\mathrm{inv}_p} \mathbb{Q}/\mathbb{Z}}$

$$Q_{a,b} \longmapsto \begin{cases} 0 \bmod \mathbb{Z} & \text{若 } Q_{a,b} \cong M_2(\mathbb{Q}_p) \ (\Leftrightarrow (a,b)_p = 1) \\ \frac{1}{2} \bmod \mathbb{Z} & \text{若 } Q_{a,b} \text{ 是可除代数 } (\Leftrightarrow (a,b)_p = -1) \end{cases}$$

(※) $\quad 0 \to \mathrm{Br}\mathbb{Q} \xrightarrow{\varphi} \bigoplus_{p\in\Omega} \mathrm{Br}\mathbb{Q}_p \xrightarrow[\psi]{\sum \mathrm{inv}_p} \mathbb{Q}/\mathbb{Z} \to 0$

$$Q_{a,b} \longmapsto (Q_{a,b} \otimes_{\mathbb{Q}} \mathbb{Q}_p)_p \longmapsto \sum_p \mathrm{inv}_p(Q_{a,b}\otimes \mathbb{Q}_p)$$

$$(a,b)_{\mathbb{Q}} \longmapsto ((a,b)_p)_{p\in\Omega} \longmapsto \prod (a,b)_p$$

(C2)
积公式 $\prod (a,b)_p = 1 \Leftrightarrow$ (※) 是复形 $\psi\circ\varphi = 0$

正合性: $\ker(\psi) = \mathrm{im}(\varphi) \Rightarrow$
- $n_p \in \{\pm 1\}$ (C1) 满足的 且 (C2) $\prod n_p = 1$
- 即 $(n_p)_{p\in\Omega} \in \ker\psi \Rightarrow \in \mathrm{im}(\varphi)$
- $\exists a,b \in \mathbb{Q}^*$: $Q_{a,b} \in \mathrm{Br}\mathbb{Q}$
- 且 $(a,b)_p = n_p$ ($\Leftrightarrow Q_{a,b}\otimes\mathbb{Q}_p =$ "n_p")

$\mathbb{Q}$ $(a,b)_p = n_p$ ($\Leftrightarrow$ $Q_{a,b}\otimes\mathbb{Q}_p = $ "n_p")

X在$\mathbb{Q}_p$上有解 $\hookrightarrow$ 回到问题2.
$\Downarrow$

此时中 φ 是平凡: $\underline{(a,b)_p = 1}$ $\forall p\in\Omega$ (即 $Q_{a,b}\otimes\mathbb{Q}_p = 0\in \mathrm{Br}\,\mathbb{Q}_p$)

φ 平 $\Rightarrow$ $\underset{\shortparallel\atop 0}{Q_{a,b}}\in \mathrm{Br}\,\mathbb{Q}$. ($\Leftrightarrow$ $(a,b)_{\mathbb{Q}} = 1$)

即 $X: x^2-ay^2-bz^2=0$ 在$\mathbb{Q}$上有解

HP对X成立.

<u>弱逼近性质</u>

$X(\mathbb{Q}) \hookrightarrow \prod_{p\in\Omega_{\mathbb{Q}}} X(\mathbb{Q}_p)$ 或 $X(K)\hookrightarrow \prod_{v\in\Omega_K} X(K_v)$

$x \longmapsto (x)_p$ $\quad$ <u>弱逼近性质</u> $\overset{def}{\Longleftrightarrow}$ 像是稠密 $\overline{X(\mathbb{Q})} = \prod X(\mathbb{Q}_p)$

WA weak approximation

例.(exer) $X=\mathbb{A}^1$ $\quad S\subset\Omega_{\mathbb{Q}}$ 有限个非阿位.

$\mathbb{Q} = \mathbb{A}^1(\mathbb{Q}) \hookrightarrow \prod_{p\in S}\mathbb{A}^1(\mathbb{Q}_p) = \prod_{v\in S}\mathbb{Q}_p$ 是稠密的

$\mathbb{Z} \subset \prod_{p\in S}\mathbb{Z}_p$ 是稠密的 (以前证过 $\mathbb{Z}\subset\mathbb{Z}_p$ 稠)

(本质: 中国剩余定理)

即 $\mathbb{A}^1$ 满足 WA.

<u>Rk</u>. $\quad$ WA $\Rightarrow$ HP. $\quad$ 例: 二次型 WA ✓

反: $3x^3+4y^3+5z^3=0\,/\mathbb{Q}$ WA ✗

<u>如何解释 WA, HP 的失效. : Brauer-Manin 障碍</u>

K $\qquad$ $\mathrm{Br}\,K$

$X_{/K}$ 代数簇 $\rightsquigarrow$ $\mathrm{Br}\,X = H^2_{et}(X, \mathbb{G}_m)$ 上同调群

$f: X\to Y$ $\rightsquigarrow$ $f^*: \mathrm{Br}\,Y\to\mathrm{Br}\,X$

代数几何语言 $\quad X(K) = \mathrm{Hom}(\underset{K}{\underline{\mathrm{Spec}\,K}}, X)$ $\longrightarrow$ 几何对象之间的同态.

$x\in X(K)$ $\quad x: \mathrm{Spec}\,K\longrightarrow X$

(… K …) 同态.

$x\in X(K)$ $\qquad x: \mathrm{Spec}\,K \to X$

$$x^*: \mathrm{Br}X \to \mathrm{Br}(\mathrm{Spec}\,K) = \mathrm{Br}K$$
$$b \mapsto x^*(b) := b(x)$$

Manin 1970 ICM 配对. X: 射影

$$\mathrm{Br}X \times \prod X(\mathbb{Q}_p) \longrightarrow \mathbb{Q}/\mathbb{Z}$$
$$b,\ (x_p)_{p\in\Omega} \longmapsto \sum_{p\in\Omega} \mathrm{inv}_p(b(x_p)) \in \mathbb{Q}/\mathbb{Z}$$

$$0 \to \mathrm{Br}\,\mathbb{Q} \to \oplus\, \mathrm{Br}\,\mathbb{Q}_p \to \mathbb{Q}/\mathbb{Z} \to 0$$

$$\underset{\neq\emptyset}{X(\mathbb{Q})} \subset \overline{X(\mathbb{Q})} \subset \boxed{\Big[\prod_{p\in\Omega} X(\mathbb{Q}_p)\Big]^{\mathrm{Br}}} \subsetneq \underbrace{\prod_{p\in\Omega} X(\mathbb{Q}_p)}_{\neq\emptyset}$$

$$\Big[\prod_{p\in\Omega} X(\mathbb{Q}_p)\Big]^{\mathrm{Br}} = \{(x_p)_{p\in\Omega} \mid \forall b\in \mathrm{Br}X,\ b\perp (x_p)\}$$

BM-集

Rk 给出 WA, HP 的障碍

例. 亏格 1 的曲线 $C: 3x^3+4y^3+5z^3=0$

$E = \mathrm{Jac}(C)$ Jacobian 是椭圆曲线. $E^\vee \cong E$ 对偶 ell. curv.

$Ш^1(E^\vee) \subset \mathrm{Br}(E^\vee)$

$Ш^1(E) \times Ш^1(E^\vee) \longrightarrow \mathbb{Q}/\mathbb{Z}$ 非退化配对 (若 Ш 有限)

$[C] \neq 0$, $[C] \in Ш^1(E)$ $\qquad$ (⊂) Manin 配对

$[C]$ 不正交于 整个 $Ш^1(E^\vee) \subset \mathrm{Br}(E^\vee) \cong \mathrm{Br}(E)$

Conj (Colliot-Thélène et al.)

$X/_K$: 有理连通代数簇 则 BM 障碍是 WA, HP 的唯一障碍.

即. $\Big[\prod X(K_v)\Big]^{\mathrm{Br}} \neq \emptyset \Rightarrow X(K)\neq\emptyset$

$$\overline{X(K)} = \Big[\prod X(K_v)\Big]^{\mathrm{Br}}$$

$X(k) \neq [\prod X(k_v)]$

$\boxed{\text{有理连通}}$: $k \subset \mathbb{C}$ $X(\mathbb{C})$ 光滑射影复流形

$\forall P, Q \in X(\mathbb{C})$ $\exists\ \mathbb{P}^1_{\mathbb{C}} \xrightarrow{\varphi} X_{/\mathbb{C}}$ 代数簇同态 (即 φ 处处有定义)

使 $\varphi(0)=P$, $\varphi(\infty)=Q$.

($\Longrightarrow$ $\pi_1^{et}(X)=0$)

Rk. ① Conj: 几何决定算术

② Conj $\Longrightarrow$ Galois 反问题 (Conj)

G 有限群, k 数域. ? $\exists\ L/k$ Galois 扩张

$\mathrm{Gal}(L/k)=G$.

③ 非有理连通簇. "Conj" 不成立

1990s. Skorobogatov

2010s Poonen

④ 更精细障碍? $\mathrm{Br}\, X = H^2(X, \mathbb{G}_m)$

推广 $H^1(X, G)$ G (非交换) 代数群.

⑤ 已知结果: Conj ✓: 带特殊结构. ① 带群作用

② 纤维丛结构

Conj (Skorobogatov – Scharaschkin – Stoll)

C: 光滑射影曲线. BM-障碍 HP, WA. 是唯一障碍.

(已知: 对椭圆曲线 $\Longleftarrow$ Ш$(E) < +\infty$)