arXiv:2302.01640v1 [math.NT] 3 Feb 2023

椭圆曲线 2-Selmer 群上的 Cassels-Tate 配对

HIMANSHU SHUKLA 和 MICHAEL STOLL

摘要。我们使用 Poonen 和 Stoll 给出的配对的 Albanese-Albanese 定义，显式计算椭圆曲线的 2-Selmer 群上的 Cassels-Tate 配对。这带来了一种新的证明，表明 Cassels 在椭圆曲线的 2-Selmer 群上定义的配对与 Cassels-Tate 配对一致。

1 引言

设 E 是代数数域 K 上的一条椭圆曲线。根据 Mordell-Weil 定理， E 上的 K-有理点集 $E(K)$ 是一个有限生成阿贝尔群，因此 $E(K) \cong E(K)_{\mathrm{tors}} \oplus \mathbb{Z}^{r_{E/K}}$，其中 $E(K)_{\mathrm{tors}}$ 是有限挠群， $r_{E/K} \geq 0$ 是一个整数，称为 E/K 的代数秩或 Mordell-Weil 秩。对于给定的椭圆曲线 E/K，确定 $E(K)$ 的群结构便成为一个自然问题。实际上，确定 E/K 的挠子群 $E(K)_{\mathrm{tors}}$ 并不困难（见 [Sil09，定理 VII.3.4]）。另一方面，迄今尚无已知算法能够确切地确定秩 $r_{E/K}$。

通过展示 $E(K)$ 中的线性无关点，可以得到秩的下界。也可以如下得到 $r_{E/K}$ 的上界。固定一个整数 $n \geq 2$。 K-伽罗瓦模的短正合列

$$0 \longrightarrow E(\bar{K})[n] \longrightarrow E(\bar{K}) \xrightarrow{\cdot n} E(\bar{K}) \longrightarrow 0$$

通过伽罗瓦上同调中的长正合列，诱导出一个短正合列

$$0 \longrightarrow E(K)/nE(K) \longrightarrow \mathrm{H}^1(K, E(\bar{K})[n]) \longrightarrow \mathrm{H}^1(K, E(\bar{K}))[n] \longrightarrow 0\,.$$

我们可以将同样的构造应用于把 K 换成它的任意一个完备化 K_v，其中 v 遍历 K 的赋值。由此得到如下行正合的交换图。

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \dfrac{E(K)}{nE(K)} & \longrightarrow & \mathrm{H}^1(K, E(\bar{K})[n]) & \longrightarrow & \mathrm{H}^1(K, E(\bar{K}))[n] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & \searrow^{\alpha} & \downarrow & & \\
0 & \longrightarrow & \displaystyle\prod_v \frac{E(K_v)}{nE(K_v)} & \longrightarrow & \displaystyle\prod_v \mathrm{H}^1(K_v, E(\overline{K_v})[n]) & \longrightarrow & \displaystyle\prod_v \mathrm{H}^1(K_v, E(\overline{K_v}))[n] & \longrightarrow & 0
\end{array}$$

由此可知， $E(K)/nE(K)$ 单射到 E/K 的 n-塞尔默群 中， $\mathrm{S}^{(n)}(E/K) \coloneqq \ker(\alpha)$。更确切地说，存在一个短正合列

$$0 \longrightarrow E(K)/nE(K) \longrightarrow \mathrm{S}^{(n)}(E/K) \to Ш(E/K)[n] \longrightarrow 0\,, \tag{1.1}$$

本研究期间，HS 获得德国研究联合会（DFG）项目 STO 299/17-1 的资助。

其中

$$Ш(E/K) \coloneqq \ker\bigl(\mathrm{H}^1(K, E(\bar{K})) \to \prod_v \mathrm{H}^1(K_v, E(\overline{K_v}))\bigr)$$

是 ***Shafarevich-Tate*** 群 的 E/K。

这里的相关事实是 $\mathrm{S}^{(n)}(E/K)$ 是 有限的 且（至少原则上如此；参见[Sto12]）可计算。由于

$$\#E(K)_{\mathrm{tors}}[n] \cdot r_{R/K}^n = \#\bigl(E(K)/nE(K)\bigr) \leq \#\mathrm{S}^{(n)}(E/K)\,,$$

这就对每个 n给出了 $r_{E/K}$的一个上界，且当且仅当$Ш(E/K)[n] = 0$时该上界是精确的。关于 Selmer 群的各种解释及其有效计算的详情，也请参见[CFO+08] 和 [SS04]。

一个标准猜想认为 $Ш(E/K)$ 是有限的。这将意味着对于适当的 n，该上界确实是精确的。根据 Kolyvagin、Wiles 等人的研究，当 K =Q 且 E 的 Hasse-Weil L-函数在 $s = 1$处的零点阶数（即其解析秩 ）至多为 1 时，$Ш(E/K)$ 的有限性已得到证明；在这种情况下，代数秩与解析秩相等（这就是弱 Birch–Swinnerton-Dyer 猜想）。但一般而言，这一猜想仍远未解决。

容易看出，自然映射 $E[n^2] \to E[n]$ 诱导出同态s_n: $\mathrm{S}^{(n^2)}(E/K) \to \mathrm{S}^{(n)}(E/K)$, 它嵌入如下的交换图中。

$$\begin{array}{ccc} \dfrac{E(K)}{n^2E(K)} & \longrightarrow & \mathrm{S}^{(n^2)}(E/K) \\ \downarrow & & \downarrow{\scriptstyle s_n} \\ \dfrac{E(K)}{nE(K)} & \longrightarrow & \mathrm{S}^{(n)}(E/K) \end{array}$$

这表明， $E(K)/nE(K)$ 在 $\mathrm{S}^{(n)}(E/K)$ 中的像包含于 s_n 的像中。因此，如果我们能够确定这个像，就可能改进对秩的估计。这可以通过计算 n^2-塞尔默群来实现。或者，我们也可以使用 ***Cassels-Tate*** 配对。这是一个交错配对

$$\langle \cdot, \cdot \rangle_{\mathrm{CT}} \colon Ш(E/K) \times Ш(E/K) \to \mathbf{Q}/\mathbf{Z}\,,$$

将无限可除子群（猜想上它是平凡的；见上文）除去后，该配对是完美的。我们将用缩写 CTP 指代这一配对。通过拉回，我们在 $\mathrm{S}^{(n)}(E/K)$ 上得到一个配对，也称为 CTP。CTP 的性质表明， s_n 的像与 $\mathrm{S}^{(n)}(E/K)$ 上 CTP 的（左或右）核相同。因此，如果我们能够计算 n-塞尔默群上的 CTP，就可以得到关于 $r_{E/K}$ 的一个界，它等价于从 n^2-塞尔默群得到的界。

参见 [PS99] ，了解有关 CTP 的详细信息（CTP 可以更一般地定义在$Ш(A/K) \times Ш(A^\vee/K)$上，其中 A/K 是一个阿贝尔簇，其对偶阿贝尔簇为 $A^\vee$）。尤其是，本文给出了该配对的四种不同定义（并证明它们彼此等价），其中包括***Weil*** 配对定义[PS99，§12。2]、齐性空间定义 [PS99，§3。1] 以及***Albanese-Albanese*** 定义 [PS99，§12。1]。

Cassels [Cas98] 定义了一个配对，作用于 $\mathrm{S}^{(2)}(E/K) \times \mathrm{S}^{(2)}(E/K)$，利用显式模型来表示 2-覆叠，这些覆叠代表 2-Selmer 群中的元素；研究表明，这与 [FSS10] 中的 CTP 相同。Cassels 的这一配对可以看作介于 Weil 配对与齐性空间定义之间。后来，Swinnerton-Dyer [SD13], 、Fisher 和 Newton [FN14] 以及 Fisher 和 van Beek [vBF18] 将 Cassels 的方法推广到计算以下对象上的 CTP

$Ш^{(2)}(E/K) \times Ш^{(2^m)}(E/K)$、$Ш^{(3)}(E/K) \times Ш^{(3)}(E/K)$，以及奇素数次数等ogenies 的 Selmer 群。采用 Donnelly 基于 CTP 齐性空间定义的方法，Fisher [Fis22] 提出了另一种计算 $Ш^{(2)}(E/K) \times Ш^{(2)}(E/K)$ 上 CTP 的方法。Fisher 还提出了一种基于齐性空间定义、适用于 $Ш^{(3)}(E/K) \times Ш^{(3)}(E/K)$ 的方法（未发表）。

本文旨在利用 Albanese-Albanese 定义计算 $Ш^{(2)}(E/K) \times Ш^{(2)}(E/K)$ 上的 CTP。文献 [PS99] 指出，通过 Albanese-Albanese 定义设计算法，计算与曲线雅可比簇相关的 Selmer 群上的 CTP，可能比通过齐性空间或 Weil 配对定义更容易，因为这只涉及处理曲线上的除子；据我们所知，本文是对此的首次尝试。

我们提出了两项技术创新。第一项是将 Albanese-Albanese 定义中使用的两个 Galois 等变配对（分别定义在主因子与零次因子之间）扩展为处处有定义，而不再仅限于支撑集不相交的除子。这样可以避免原始定义中某些假设所带来的复杂性；该定义要求将 $\mathrm{Pic}^0(E)$ 中某些元素提升到 $\mathrm{Div}^0(E)$ 时，其支撑集彼此不相交。第二项创新是将元素 $a \in Ш^{(2)}(E)$ 写成若干 $\mathrm{H}^1(K, E(\bar{K})[2])$ 中的量之和，而这些量不一定属于 $Ш^{(2)}(E)$。借此，我们构造了一些映射（它们可能取决于所作的选择），以模拟 CTP 的构造，并证明 CTP 等于这些函数之和（见第 5.1 节）。通过谨慎地作出选择，我们得到了一个相当简洁的证明，说明 CTP 与 Cassels 在 [Cas98] 中定义的配对等价。

基于本文的方法，第一作者开发了一种算法，用于计算 $Ш^2(J) \times Ш^2(J)$上的 CTP，其中 J 是具有奇数次模型的超椭圆曲线的雅可比簇。相关内容将在后续文章 [Shu23]中介绍。

本文的结构如下。第 2 节和第 3 节介绍所需的记号和预备知识。在第 4 节中，我们在一个特殊情形下计算配对，随后在第 5 节中证明一般情形可由特殊情形推出。同一节中，我们还证明，使用 Albanese-Albanese 定义得到的 CTP 公式与 Cassels 给出的定义一致。

2 记号

对于拓扑群 G 和 G-模 A，令 $\partial, \mathcal{C}^n(G, A)$，$\mathcal{Z}^n(G, A)$，$\mathcal{B}^n(G, A)$ 和 $\mathrm{H}^n(G, A)$ 分别表示余边界映射，以及关于巴分解的连续 n-上链、n-余循环、 n-余边界和 n-上同调类组成的群。对于 G的子群 H，令 res^H_G 和 cor^G_H 分别表示上链层面的限制映射和余限制映射。为简化记号，在上下文明确时，我们将省略 res 和 cor 的下标与上标。注意，要使 cor 有意义， H 必须是 G的有限指数子群。

设 K 和 G_K 分别为完美域 K 的代数闭包和伽罗瓦群 $\mathrm{Gal}(K/K)$；若 K 是整体域，则对 K 的每个赋值 v，令 K_v 表示 K 关于 v的完备化。令 $\mathbb{G}_\mathrm{m} := K^\times$ 为一个伽罗瓦模。我们固定一个嵌入 $K \hookrightarrow \overline{K_v}$；这诱导出绝对伽罗瓦群的嵌入 $G_{K_v} \hookrightarrow G_K$。令 A_v 为由一个 G_K模A 通过 $G_{K_v} \hookrightarrow G_K$得到的 G_{K_v}模。只要上下文明确，我们将省略 A_v 的下标。对于余链 $x \in \mathcal{C}^i(G_K, -)$，我们将其在 $\mathcal{C}^i(G_{K_v}, -)$上的限制记为 x_v。此外，对于有限 G_K模 A，令 $K(A)$表示使 $G_{K(A)}$ 在 A 上平凡作用的 K 的最小有限正规扩张。为简化记号，我们将 $\mathcal{C}^i(G_K, \mathbb{G}_\mathrm{m})$记为 $\mathcal{C}^i(K)$；对于余循环和上同调

类也同样如此。令 $\mathrm{Br}(K) \simeq \mathrm{H}^2(K)$表示布劳尔群；若 K 是数域，则对 K的一个赋值 v，令 $\mathrm{inv}_{K_v}\colon \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$ 表示局部不变量映射；对于 x、$y \in K^\times$，我们将 x 和 y 关于 K的二次希尔伯特符号记为 $(x,y)_K$。若 K是局部域，则有 $(-1)^{2\mathrm{inv}_K([x,y])} = (x,y)_K$，其中 $[(x,y)]$ 表示四元数代数 (x,y) 在 $\mathrm{Br}(K)$ 中的类。

我们假设 $\mathrm{char}(K) \neq 2$。令 E/K 为由方程给出的椭圆曲线

$$Y^2 = f(X) := X^3 + AX + B,$$

其中 $A, B \in K$。令 $e_1, e_2, e_3 \in K$为 f的根。对$1 \leq i \leq 3$, T_0，定义 $T_i := (e_i, 0)$；对$= (0:1:0)$（E上的无穷远点），定义 $\Delta := E[2] \setminus \{T_0\}$。注意，$\Delta$ 是一个 G_K-集合，即带有 G_K 作用的集合。对于任意 G_K-集合 S 和一个G_K-模 M，我们定义映射 $S \to M$ 构成的 G_K-模 M^S。其元素可解释为形如 $\sum_{s\in S} a_s(s)$ 的形式和，其中 $a_s \in M$。群M^S 的结构是逐点定义的，而 G_K-作用自然定义为$\sigma \cdot \sum_{s\in S} a_s(s) := \sum_{s\in S} \sigma a_s(\sigma s)$，其中 $\sigma \in G_K$。由上述内容可知，可以证明

$$\mu_2^\Delta \cong E[2] \oplus \langle (-1)(T_1) + (-1)(T_2) + (-1)(T_3) \rangle;$$

包含映射 $E[2] \hookrightarrow \mu_2^\Delta$由 Weil 配对 $P \mapsto \sum_{T\in\Delta} e_2(P,T)(T)$ 诱导。令 $A := K[X]/\langle f(X) \rangle$ 表示与 Δ 相关联的 étale代数。那么我们有

$$\mathrm{H}^1(G_K, E[2]) \cong \ker\left(N\colon A^\times/(A^\times)^2 \longrightarrow K^\times/(K^\times)^2\right), \tag{2.1}$$

其中 N 表示由范数映射从 A 到 K 诱导的映射。

令 $\bar{A} := A \otimes_K \bar{K}$。$A^\times/(A^\times)^2$ 中的元素可由 $A^\times$ 中的元素表示，而后者可写成 $\beta = l_0 + l_1\theta + l_2\theta^2$ 的形式，其中 l_0、l_1、$l_2 \in K$，且 θ 是 x 在 A 中的像。令 $\beta_i = l_0 + l_1 e_i + l_2 e_i^2 \in K(e_i)^\times$。在识别 $A \hookrightarrow \bar{A} \cong \bar{K}^3$ 下，β 随后映射为 $(\beta_1, \beta_2, \beta_3)$。

若 β通过 (2.1) 表示 $\mathrm{H}^1(G_K, E[2])$ 中的一个元素 a，则 $\beta_1\beta_2\beta_3 \in (K^\times)^2$。固定 β_i的三个平方根 $\sqrt{\beta_i}$，其中 $1 \leq i \leq 3$，并考虑形式和 $\sum_{i=1} \sqrt{\beta_i}(T_i) \in \bar{A}^\times = \mathbb{G}_{\mathrm{m}}^\Delta$。这个元素是 $\beta \in A^\times$ 的一个平方根 $\sqrt{\beta}$，将其视为 $\mathbb{G}_{\mathrm{m}}^\Delta$中的元素。由于 1-余边界 $\sigma \mapsto \sigma\sqrt{\beta}/\sqrt{\beta}$ 的取值在 μ_2^Δ 中，因为β被 G_K固定，它表示一个 1-余循环 $\chi_a \in \mathcal{Z}^1(G_K, \mu_2^\Delta)$。余循环 χ_a与一个取值于 $E[2]$、通过 $(\mathbb{Z}/2\mathbb{Z})^\Delta \to E[2]$3 3 表示 a 的 1-余循环相关联，其映射为 $\sum_{i=1} a_i(T_i) \mapsto \sum_{i=1} a_i T_i$，并使用 $\mu_2 \cong \mathbb{Z}/2\mathbb{Z}$ 作为 G_K-模的同一认定。

注意到 $\mu_2^\Delta \simeq \bigoplus \mu_2^{\Delta_i}$，其中 Δ_i 是 Δ的 G_K-轨道。这诱导出一个轨道同构 $\mathcal{Z}^1(G_K, \mu_2^\Delta) \simeq \bigoplus \mathcal{Z}^1(G_K, \mu_2^{\Delta_i})$，因此 $\chi_a(\sigma)$ 可经由 Δ 的轨道，即 $\chi_a(\sigma) = \sum \chi_{a_i}(\sigma)$ 的轨道分解，其中 χ_{a_i} 在将支撑集 Δ 轨道 3 替换为 G_K-轨道 Δ_i Δ 时对应于 χ_a。我们将三元组 (a_1, a_2, a_3) 与 $\sum_{i=1} a_i(T_i) \in \mu_2^\Delta$ 联系起来，今后将使用这一表示来表示 μ_2^Δ 的元素。记 $\hat{0}$ 为三元组 (1, 1, 1)，记 $\hat{i}$ 为在 i^{th} 位置取 1、其他位置取 -1 的三元组。G_K 对 μ_2^3 中三元组的作用由其对 μ_2^Δ 的作用诱导。若 (x_1, x_2, x_3) 是表示 $(\mu_2^\Delta)^{G_K}$ 中一个元素的三元组，则定义 $\diamond$ 乘积 $\prod x_i$ 为对 Δ 上每个 G_K- 轨道 i 各取一个代表元 i 后所得的乘积（注意，当 i 和 j 属于同一轨道时，$x_i = x_j$）。

3 预备知识

从现在起，我们固定一个数域 K 和一条椭圆曲线 E/K。回顾引言中关于 E/K 及“n-下降序列”（1.1）的 Shafarevich-Tate 群和 Selmer 群的定义。

现在回顾一些稍后将会用到的方程。设 $P=(x,y)$ 在 E/K 上。那么我们有

$$P+T_i=\left(\frac{e_ix+e_je_k-e_i(e_j+e_k)}{x-e_i},\frac{-(e_j-e_i)(e_k-e_i)y}{(x-e_i)^2}\right), \tag{3.1}$$

其中 $\{i,j,k\}=\{1,2,3\}$。利用连接 P 与 T_i 的直线经过 $-P-T_i$ 以及方程 (3.1) 这一事实，我们推得

$$\frac{x(\pm P+T_i)-e_i}{x(\pm P)-e_i}=\frac{(e_j-e_i)(e_k-e_i)}{(x-e_i)^2}=-\frac{y(\pm P+T_i)}{y(\pm P)} \tag{3.2}$$

由 (3.1) 我们还可推出

$$x(\pm P+T_j)-e_i=\frac{(x-e_k)(e_j-e_i)}{x-e_j}, \tag{3.3}$$

结合经过 $P+T_i$ 和 T_k 的直线经过 $-P+T_j$ 这一事实，可得

$$\frac{y(\pm P+T_i)(x(\pm P)-e_k)}{y(\pm P)(x(\pm P+T_i)-e_k)}=\frac{(3B+2Ae_i)(x-e_k)}{e_i(x-e_i)(x-e_j)(e_i-e_k)}=\frac{(x-e_k)^2(e_j-e_i)}{y^2}. \tag{3.4}$$

3.1 群上同调

现在我们回顾一些关于 cor、res 和局部不变量映射 inv 的群上同调结果。设 G 为一个群，$H\leq G$ 为 G的有限指数子群。设 A 为一个 G-模；那么对于 $n\geq 0$，我们有一个称为余限制 的同态，作用于 n-上链:

$$\mathrm{cor}_H^G\colon \mathcal{C}^n(H,A)\to\mathcal{C}^n(G,A). \tag{3.5}$$

我们利用 [NSW08, §I.5.4]中给出的关于标准分解的 cor_H^G 的显式描述，推导关于巴分解的 cor_H^G 的显式描述。取一组 R 代表元，表示 $g\in G$的右陪集 Hg。有一个映射 $r\colon G\to R$，它将 g 映射到 R中 Hg 的代表元。这诱导出一个映射 $m\colon G\to H$，由 $m(\sigma)=\sigma r(\sigma)^{-1}$给出。然后，利用关于巴分解的上链与关于标准分解的齐次上链之间的显式同构，我们得到

$$\begin{aligned}\left(\mathrm{cor}_H^G(\gamma)\right)(\sigma_1,\dots,\sigma_n)\coloneqq\sum_{g\in R}g^{-1}\gamma(m(g\sigma_1),m(g\sigma_1)^{-1}m(g\sigma_1\sigma_2),\dots\\ \dots,m(g\sigma_1\dots\sigma_{n-1})^{-1}m(g\sigma_1\dots\sigma_n)).\end{aligned} \tag{3.6}$$

我们回顾一下下面命题中 cor、res 和 inv 的一些性质。

命题 3.1 ([NSW08，推论 1.5.7、7.1.4，命题 1.5。3])。设 $K\subset L\subset K$ 是域塔，其绝对伽罗瓦群为 G_K，G_L 分别，并且$[L\colon K]<\infty$。对于一个 G_K-模 A，有:

(1) 若 $\gamma\in H^n(G_K,A)$，则 $\mathrm{cor}_{G_L}^{G_K}\circ\mathrm{res}_{G_K}^{G_L}(\gamma)=[L\colon K]\gamma$。*(2)* 若 K 是局部域且 $\gamma\in H^2(K)$，则 $\mathrm{inv}_K\circ\mathrm{cor}_{G_L}^{G_K}(\gamma)=\mathrm{inv}_L(\gamma)$，且 $\mathrm{inv}_L\circ\mathrm{res}_{G_K}^{G_L}(\gamma)=[L\colon K]\,\mathrm{inv}_K(\gamma)$。*(3)* 设 $\gamma\in\mathcal{C}^n(G_K,A)$ 和 $\gamma'\in\mathcal{C}^m(G_L,A')$，其中 A, A' 是 G_K-模。那么有

（只要 $\cup$ 有定义） $$\mathrm{cor}_{G_L}^{G_K}(\mathrm{res}_{G_K}^{G_L}(\gamma)\cup\gamma')=\gamma\cup\mathrm{cor}_{G_L}^{G_K}(\gamma')。$$

现在我们回顾双陪集公式。设 H 是 G 的一个子群，且 B 是一个 G-模 A 的 H-子模。对于 $\sigma \in G$，由 $\tau \mapsto \sigma^{-1}\tau\sigma$ 给出的映射 $H^\sigma := \sigma H \sigma^{-1} \to H$以及由 $b \mapsto \sigma b$ 给出的映射 $B \to \sigma B$ 构成一个相容对，即$\sigma((\sigma^{-1}\tau\sigma)(b)) = \tau(\sigma(b))$, 对所有 $b \in B$和 $\tau \in H^\sigma$均成立。因此，我们有一个定义良好的映射

$$\sigma_* \colon \mathcal{C}^i(H, B) \to \mathcal{C}^i(H^\sigma, \sigma B).$$

可以证明， σ_* 与 inf、cor、res、 $\cup$ 和∂ [可交换（NSW08，命题 1.5.3、1.5.4]）。特别地，若 $H = G$ 且 $B = A$，则利用 σ_*与维数平移可交换这一事实，可以证明 σ_* 是 $\mathrm{H}^i(G, A)$ 上的恒等映射。若 H, U 是 G 的闭子群，且 $[G : H] < \infty$，则有双陪集公式；该公式在上链层面也成立（NSW08，命题 1.5.6]）：

$$\mathrm{res}^U_G \mathrm{cor}^G_H(z) = \sum_{g \in R} \mathrm{cor}^U_{U \cap gHg^{-1}} \mathrm{res}^{U \cap gHg^{-1}}_{gHg^{-1}} g_*(z), \tag{3.7}$$

其中， R是双陪集代表元系 $G = \bigsqcup UgH$，且 $z \in \mathcal{C}^i(H, A)_{g \in R}$

（$\sqcup$ 表示不交并。）

回忆一下，对于 K 的每个赋值 v ，我们固定了一个嵌入$K \hookrightarrow \overline{K_v}$。通过此嵌入，可将 G_{K_v} 视为 G_K 的闭子群（G_K 是豪斯多夫空间，且G_{K_v} 是紧致的）。设 L 是 K的有限扩张，且 $w_1, \ldots, w_m$ 是 L 中位于 v 之上的所有互不相同的赋值，其中 w_1 是由固定嵌入 $K \hookrightarrow \overline{K_v}$诱导的赋值。对每个 w_i ，都有一个相应的 $g_i \in G_K$ ，使得 w_i 由 复合嵌入 $g_i : K \to K \hookrightarrow \overline{K_v}$诱导。若 $L = K(\theta_1)$, 则 g_i 对应于 $L \hookrightarrow K$ 的那些嵌入，它们将 θ_1 映到其某个 G_K-共轭元，但该共轭元不是 G_{K_v}-共轭元。这意味着 $\{g_1, \ldots, g_m\}$ 是 G_K 关于 G_{K_v} 和 G_L的双陪集代表元系m，即 $G_K = \bigsqcup G_{K_v} g_i G_L$。此外，注意到$_{i=1} G_{L_{w_i}} \subset G_{K_v}$ 固定扩张 $g_i L$ ，因此 $G_{L_{w_i}} = G_{K_v} \cap g_i G_L g_i^{-1}$。利用双陪集公式 (3.7)，得到如下观察：

注记 3.2。令 K、 L、 w_i、 g_i 如上所述。则

$$(\mathrm{cor}^{G_K}_{G_L}(z))_v = \mathrm{res}^{G_{K_v}}_{G_K} \circ \mathrm{cor}^{G_K}_{G_L}(z) = \sum_{i=1}^{m} \mathrm{cor}^{G_{K_v}}_{G_{L_{w_i}}} \circ \mathrm{res}^{G_{L_{w_i}}}_{G_{g_i L}} \circ (g_i)_*(z). \tag{3.8}$$

接下来的两个小节回顾 CTP 的两种定义。我们首先考察 Cassels 在 [Cas98] 中给出的定义，然后考察 [PS99]中的 Albanese-Albanese 定义。我们继续假设 K 是一个数域。

3.2 Cassels 配对

令 a、 $a' \in \mathrm{Ш}^{(2)}(E)$ 如第 2 节所述由 $\beta = (\beta_1, \beta_2, \beta_3)$ 和 $\beta' = (\beta'_1, \beta'_2, \beta'_3)$ 表示。对于两两不同的 $1 \le i$、 j、 $k \le 3$，定义变量 (U_1, U_2, U_3, T) 的二次型如下

$$H_i(U_1, U_2, U_3, T) := (\beta_j \Gamma_j^2 - \beta_k \Gamma_k^2)/(e_j - e_k) + T^2, \tag{3.9}$$

其中 $\Gamma_i := U_1 + U_2 e_i + U_3 e_i^2$。注意，$(U_1, U_2, U_3) \mapsto (\Gamma_1, \Gamma_2, \Gamma_3)$ 只是一次线性坐标变换。另请注意，每个 H_i 都定义在 $K(e_i)$ 上。任意两个这样的二次型都定义了坐标为U_1、 U_2、 U_3、 T的 $\mathbb{P}^3$ 中的一条射影曲线 D_a 。对于给定的 $i \in \{1, 2, 3\}$，循环选取 j、 $k \in \{1, 2, 3\}$，可得 $3\sum(e_j - e_k)H_i = 0$。因此，任意两个 H_i都在 K 上定义同一条曲线 D_a。 $D_a{}_{i=1}$在 K 的每个完备化 K_v 上都有点，并且是一个表示 a的 E 的 2-覆盖。详情请参见 [Cas98, §2]。

由于 D_a 在仿射图 $T \neq 0$ 上处处局部都有点，因此对 K的每个赋值 v ，每个 H_i 在 $K_v(e_i)$ 上都有非平凡解；由此，每个 H_i在 $K(e_i)$ 的每个完备化上都有解。这意味着，对每个 i ，都存在一个点 $\mathfrak{q}_i \coloneqq (\mathfrak{u}_1 : \mathfrak{u}_2 : \mathfrak{u}_3 : 1)$ 或 $(\Gamma_j^* : \Gamma_k^* : 1)$，它定义在 $K(e_i)$ 上且满足$H_i = 0$；这是二次型的局部-整体原理的推论。令 $L_i(U_1, U_2, U_3, T)$ 为 $1 \leq i \leq 3$ 上的一个线性形式，使得 $L_i = 0$ 是 H_i 在 $\mathfrak{q}_i$ 处的切线。

若 $\mathfrak{q}_v$ 是定义在 D_a 上、且以 K_v为底域的点，那么 Cassels 配对[Cas98，引理 7.4]定义如下：

$$\langle \alpha, \alpha' \rangle_{\mathrm{Cas}} \coloneqq \prod_v \prod_i{}^{\diamond} (L_i(\mathfrak{q}_v), \beta_i')_{K_v(e_i)}. \tag{3.10}$$

在[Cas98] 中，Cassels 证明了上述定义给出了一个良定义的配对，且与所作的选择无关。

3.3 Cassels-Tate 配对的 Albanese-Albanese 定义

现在我们将使用第2节中的记号，说明椭圆Ш(E)上 Cassels-Tate 配对的 Albanese-Albanese 定义，其中 E/K是椭圆曲线。令Princ(E)表示 $E(K)$上的主因子群。选取 t_P 作为 $P \in E(K)$ 的局部参数，使映射 $P \mapsto t_P$ 为伽罗瓦等变，并考虑如下伽罗瓦等变配对

$$\langle \cdot, \cdot \rangle_1 \colon \big(\mathrm{Princ}(E) \times \mathrm{Div}^0(E)\big) \to \mathbb{G}_{\mathrm{m}} \tag{3.11}$$

$$\langle \cdot, \cdot \rangle_2 \colon \big(\mathrm{Div}^0(E) \times \mathrm{Princ}(E)\big) \to \mathbb{G}_{\mathrm{m}} \tag{3.12}$$

定义如下。

$$\langle \mathrm{div}(f), D \rangle_1 \coloneqq \prod_P (f t_P^{-v_P(f)})(P)^{v_P(D)},$$

and

$$\langle D, \mathrm{div}(f) \rangle_2 \coloneqq \prod_P (-1)^{v_P(f)v_P(D)} (f t_P^{-v_P(f)})(P)^{v_P(D)}.$$

上述配对是良定义的，并扩展了[PS99第 3 节中部分定义的配对2]。下文中，“$\cup_i$”表示关于配对 $\langle \cdot$的上链杯积，$\cdot \rangle_i$ 对于 $i \in \{1, 2\}$，并且在上下文明确时，我们将省略 $\cup_i$中的下标。接下来，我们证明上述定义的两个配对在对角线 $\mathrm{Princ}(E) \times \mathrm{Princ}(E)$上相等。

命题 3.3。设 $\langle \cdot, \cdot \rangle_1$ 和 $\langle \cdot, \cdot \rangle_2$ 如上。则在 $\mathrm{Princ}(E) \times \mathrm{Princ}(E)$上，有 $\langle \cdot, \cdot \rangle_1 = \langle \cdot, \cdot \rangle_2$ 。

证明。对两个非零函数 f 和 g，定义在 P 处的温和符号 如下：

$$[f, g]_P \coloneqq (-1)^{v_P(f)v_P(g)} \frac{f^{v_P(g)}}{g^{v_P(f)}}(P).$$

我们有

$$\begin{aligned} \frac{\langle \mathrm{div}(f), \mathrm{div}(g) \rangle_1}{\langle \mathrm{div}(f), \mathrm{div}(g) \rangle_2} &= \prod_P (-1)^{v_P(f)v_P(g)} \frac{\left(f t_P^{v_P(f)}\right)(P)^{v_P(g)}}{\left(g t_P^{v_P(g)}\right)(P)^{v_P(f)}} \\ &= \prod_P (-1)^{v_P(f)v_P(g)} \left(\frac{f^{v_P(g)}}{g^{v_P(f)}}\right)(P) = \prod_P [f, g]_P = 1. \end{aligned}$$

最后一个等式是强 Weil 互反律的结果 [Wei38]。 □

注记 3.4。 注意，对于任意光滑、射影、绝对不可约的曲线 C/K，都可以用相同的方式定义上述配对，并且它们将满足命题 3.3。

设 $a, a' \in \mathrm{H}^1(G_K, E[n])$ 由取值于$E(\bar{K})[n]$中的 1-上循环 α, α' 表示。将 α, α' 提升为取值于 $\mathrm{Div}^0(E)$ 中的 1-上链 $\mathfrak{a}$ 和 $\mathfrak{a}'$。由于 $\partial\alpha = \partial\alpha' = 0$，上链 $\partial\mathfrak{a}$ 和 $\partial\mathfrak{a}'$ 取值于主因子，这可通过对正合列应用伽罗瓦上同调看出

$$0 \longrightarrow \mathrm{Princ}(E) \longrightarrow \mathrm{Div}^0(E) \longrightarrow \mathrm{Pic}^0(E) \longrightarrow 0.$$

下文中，即使上链/上同调类取值于乘法群，我们也将其群结构记作加法形式。不过，在将上链代入某些参数求值后，我们将使用相应群模的群运算。例如，若 x, $y \in \mathrm{C}^1(K)$，则我们用 $+$ 表示它们作为上链的加法 $z := x + y$；但对于 $\sigma \in G_K$, $z(\sigma)$, $\in \mathbb{G}_{\mathrm{m}}$ 将写作 $x(\sigma)y(\sigma)$，其中使用的是 $\mathbb{G}_{\mathrm{m}}$ 的群运算。

定义 3-余循环 $\eta := \partial\mathfrak{a} \cup_1 \mathfrak{a}' - \mathfrak{a} \cup_2 \partial\mathfrak{a}' \in \mathcal{Z}^3(K)$。容易验证，$\eta$ 中的杯积是有意义的，并且 η 确实是一个余循环。由类域论可知，对于任意数域 K，都有 $\mathrm{H}^3(K) = 0$，因此 $\eta = \partial\varepsilon$ 对于某个 2-上链$\varepsilon \in \mathcal{C}^2(K)$成立。

进一步，假设 $a \in \mathrm{S}^{(n)}(E)$，并令 v 为 K的一个赋值。那么，对于某个 $\beta_v \in E(\overline{K_v})$，有 $\alpha_v = \partial\beta_v$，且我们可以将 β_v 提升为元素 $\mathfrak{b}_v \in \mathrm{Div}^0(E)$。于是 $\mathfrak{a}_v - \partial\mathfrak{b}_v$ 取值于主因子，因此我们可以定义如下 2- 余循环

$$\gamma_v = (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{a}' - \mathfrak{b}_v \cup_2 \partial\mathfrak{a}'_v - \varepsilon_v. \tag{3.13}$$

因此 γ_v 表示某个类 $c_v \in \mathrm{H}^2(K_v) \simeq$ 布劳尔群 (K_v)。我们将 $\mathrm{S}^{(n)}(E) \times \mathrm{H}^1(G_K, E[n])$ 上的 CTP 定义如下：

定义 3.5。 设 $(a, a') \in \mathrm{S}^{(n)}(E) \times \mathrm{H}^1(G_K, E[n])$，且 c_v如上所述。则 a, a' 上的 Cassels-Tate 配对定义如下：

$$\langle a, a' \rangle_{\mathrm{CT}} := \sum_v \mathrm{inv}_{k_v}(c_v). \tag{3.14}$$

注 3.6。 上述定义依赖于 β_v 的选取，即将 β_v 改为 $\beta_v + \kappa_v$（其中 $\kappa_v \in E(K_v)$）会改变配对的值。然而，如果假设 $a' \in \mathrm{S}^{(n)}(E)$，那么 $\langle a, a' \rangle_{\mathrm{CT}}$ 便与所作的选择无关，因此是一个定义良好的配对（见 [PS99]）。

4 计算 $\mathrm{S}^2(E) \times \mathrm{H}^1(G_K, \langle T_1 \rangle)$ 上的 CTP

本节中，我们假设 $e_1 \in K$，即 $[K(E[2]) : K] \leq 2$，并计算 $\mathrm{S}^2(E) \times \mathrm{H}^1(G_K, \langle T_1 \rangle)$ 上的 CTP（按 §3.3 的含义）。注 3.6 表明，由此得到的 CTP 值取决于计算过程中局部部分所作的选择。因此，它是 $\mathrm{S}^{(2)}(E) \times \mathrm{H}^1(G_K, \langle T_1 \rangle)$ 上 CTP 的可能取值之一。此后，我们始终假设 $1 \leq i, j, k \leq 3$，并且如果 i, j, k 中任意几个同时出现在一个表达式中，它们两两不同。计算过程中我们采用 §2 中的记号。

我们首先明确描述由三元组（β_1、β_2、β_3）分别表示的 $a \in \mathrm{S}^{(2)}(E)$ 和 $a' \in \mathrm{H}^1(G_K, \langle T_1 \rangle) \simeq K^\times/(K^\times)^2$, 。表示 a 和 a' 的 1-上循环 α 和 α' 分别如下：

$$\alpha(\sigma) = \begin{cases} T_0 & \chi(\sigma) = \widehat{0}, \\ T_i & \chi(\sigma) = \widehat{i}, \end{cases} \quad \text{and} \quad \alpha'(\sigma) = \begin{cases} T_0 & \chi'(\sigma) = 1, \\ T_1 & \chi'(\sigma) = -1. \end{cases}$$

此处 $\chi = \chi_a$（定义见 §2），但为简化记号，我们省略了下标。此外，$\chi'(\sigma) := \sigma(\sqrt{\beta'})/\sqrt{\beta'}$，其中平方根 $\sqrt{\beta'}$ 是 β'的平方根。

接下来的两个小节专门讨论在a, a' 如上所述时 CTP 的计算。

4.1 整体计算

将 α, α' 提升为取值于 $\mathrm{Div}^0(E)$ 的 1-上链 $\mathfrak{a}$, $\mathfrak{a}'$，如下所示：

$$\mathfrak{a}(\sigma) = \begin{cases} 0 & \chi(\sigma) = \widehat{0}, \\ (T_i) - (T_0) & \chi(\sigma) = \widehat{i}, \end{cases} \quad \text{and} \quad \mathfrak{a}'(\sigma) = \begin{cases} 0 & \chi'(\sigma) = 1, \\ (T_1) - (T_0) & \chi'(\sigma) = -1. \end{cases}$$

我们有：

(4.1)

$$\partial\mathfrak{a}(\sigma,\tau) = \begin{cases} 0 = \mathrm{div}(1) & \chi(\sigma) = \widehat{0} \text{ or } \chi(\tau) = \widehat{0}, \\ 2(T_i) - 2(T_0) = \mathrm{div}(x - e_i) & \chi(\sigma) = \widehat{i},\ \sigma\cdot\chi(\tau) = \widehat{i}, \\ (T_i) + (T_j) - (T_k) - (T_0) = \mathrm{div}(\frac{y}{x-e_k}) & \chi(\sigma) = \widehat{i},\ \sigma\cdot\chi(\tau) = \widehat{j}. \end{cases}$$

类似地，对于 $\mathfrak{a}'$，我们有：

$$\partial\mathfrak{a}'(\sigma,\tau) = \begin{cases} 0 = \mathrm{div}(1) & \chi'(\sigma) = 1 \text{ or } \chi'(\tau) = 1, \\ 2(T_1) - 2(T_0) = \mathrm{div}(x - e_1) & \chi'(\sigma) = \chi'(\tau) = -1. \end{cases} \tag{4.2}$$

令 t_P 表示点 $P \in E(K)$ 处的一个局部参数。我们假设 $t_{T_0} = x/y$, $t_{T_i} = -(x-e_i)/y$，且在所有其他点 $P \notin E[2]$处有 $t_P = x - x(P)$。由$P \mapsto t_p$定义的映射是伽罗瓦等变的。不难看出，$\langle \mathrm{div}(f),\ D\rangle_1 = \langle D,\ \mathrm{div}(f)\rangle_2$，其中 $\mathrm{div}(f)$ 和 D 分别出现在 $\partial\mathfrak{a}, \partial\mathfrak{a}'$ 和 $\mathfrak{a}, \mathfrak{a}'$ 取值中。因此，我们有：

$$\begin{aligned} \langle (x-e_i), (T_i) - (T_0)\rangle_1 &= \frac{y^2/(x-e_i)(T_i)}{(x-e_i)x^2/y^2(T_0)} = (e_i - e_j)(e_i - e_k), \\ \langle (x-e_i), (T_j) - (T_0)\rangle_1 &= \frac{(x-e_i)(T_j)}{(x-e_i)x^2/y^2(T_0)} = e_j - e_i, \\ \langle y/(x-e_k), (T_i) - (T_0)\rangle_1 &= \frac{-y^2/(x-e_k)(x-e_i)(T_i)}{x/(x-e_k)(T_0)} = e_j - e_i, \\ \langle y/(x-e_k), (T_k) - (T_0)\rangle_1 &= \frac{-y(x-e_k)/y(x-e_k)(T_k)}{x/(x-e_k)(T_0)} = -1. \end{aligned}$$

我们令 $s_{ij} := e_i - e_j$为 $i \neq j$，并令 $s_i := s_{ij}s_{ik}$。对于 $\sigma, \tau, \rho \in G_K$，通过配对 $\langle\cdot,\cdot\rangle_1$（分别为 $\langle\cdot,\cdot\rangle_2$），杯积 $(\partial\mathfrak{a} \cup_1 \mathfrak{a}')(\sigma,\tau,\rho)$（分别为 $(\mathfrak{a} \cup_2 \partial\mathfrak{a}')(\sigma,\tau,\rho)$）为 $\langle \partial\mathfrak{a}(\sigma,\tau),\ \sigma\tau(\mathfrak{a}'(\rho))\rangle_1$（分别为 $\langle \mathfrak{a}(\sigma),\ \sigma(\partial\mathfrak{a}'(\tau,\rho))\rangle_2$），其中使用了 [NSW08，命题 1.4.8]。因此，我们有

$$(\partial\mathfrak{a} \cup_1 \mathfrak{a}')(\sigma,\tau,\rho) = \begin{cases} 1 & \chi(\sigma) = \widehat{0} \text{ or } \chi(\tau) = \widehat{0} \text{ or } \chi'_1(\rho) = 1, \\ s_1 & \chi(\sigma) = \widehat{1},\ \sigma\cdot\chi(\tau) = \widehat{1},\ \chi'(\rho) = -1, \\ s_{1j} & \chi(\sigma) = \widehat{j},\ \sigma\cdot\chi(\tau) = \widehat{j},\ \chi'(\rho) = -1, \\ s_{j1} & {\scriptstyle (\chi(\sigma),\sigma\cdot\chi(\tau)) = (\widehat{1},\widehat{j}),\ \text{or} \atop (\chi(\sigma),\sigma\cdot\chi(\tau)) = (\widehat{j},\widehat{1})},\ \chi'(\rho) = -1, \\ -1 & \chi(\sigma) = \widehat{j}, \sigma\cdot\chi(\tau) = \widehat{k},\ \chi'(\rho) = -1, \end{cases} \tag{4.3}$$

and

$$(\mathfrak{a} \cup_2 \partial\mathfrak{a}')(\sigma,\tau,\rho) = \begin{cases} 1 & \chi(\sigma) = \widehat{0} \text{ or } \chi'(\tau) = 1 \text{ or } \chi'(\rho) = 1, \\ s_1 & \chi(\sigma) = \widehat{1}, \chi'(\tau) = \chi'(\rho) = -1, \\ s_{j1} & \chi(\sigma) = \widehat{j}, \chi'(\tau) = \chi'(\rho) = -1. \end{cases} \tag{4.4}$$

我们希望找到一个 2-上链 ε，使得 $\partial\varepsilon = \eta$；正如我们稍后将看到的，这要求我们将某些元素表示为范数。由于 D_a 处处局部可解，根据 §3.2 中的讨论，对于 $1 \le i \le 3$，我们在 $K(E[2])$ 上有一个全局解 $\mathfrak{q}_i := (\Gamma_j^* : \Gamma_k^* : 1)$，满足 $H_i(\Gamma_j : \Gamma_k : 1) = 0$，其中 H_i 如方程（3.9）中所定义。由于 H_i 在 U_1 中以 U_2, U_3 坐标定义于 $K(e_i)$，Γ_j^* 和 Γ_k^* 在 $K(e_i)$ 中具有U_1, U_2, U_3 坐标。因此，若 e_j 和 e_k 互为共轭元，我们便假设 Γ_j^* 和 Γ_k^* 在 $K(e_i)$ 上互为共轭元。定义如下量

$$p_{jk} := \sqrt{\beta_j}\Gamma_j^* + \sqrt{\beta_k}\Gamma_k^*, \quad \text{and} \quad p_i := p_{ij}p_{ik}. \tag{4.5}$$

注 4.1. 设 $\mathfrak{q}_i$ 如上。设 $\sigma \in G_K$ 满足 $\sigma(e_i) = e_k$，则可假设圆锥曲线 $H_k = 0$ 的解为 $\mathfrak{q}_k := \sigma(\mathfrak{q}_i)$。将 $\sigma \in G_{K(e_i)}$写作 $\sigma_s\sigma_p$，其中 $\sigma_s \in G_{K(E[2])}$ 满足 $\chi(\sigma) = \chi(\sigma_s)$，且 $\chi(\sigma_p) = \widehat{0}$，于是有

$$\sigma(p_{ij}) = \sigma_s(p_{\sigma\cdot i,\sigma\cdot j}) \quad \text{and} \quad \sigma(p_i) = \sigma_s\left(\prod_{l\neq i} p_{\sigma\cdot i,\sigma\cdot l}\right) = \sigma_s(p_{\sigma\cdot i}),$$

其中，当 $\sigma(e_j) = e_k$时，指标为 j、k、$\sigma\cdot j = k$。

请注意，上述记号略有歧义。全局点 $\mathfrak{q}_j$（位于 $H_j = 0$ 上）中的 Γ_i^*，可能不等于全局点 $\mathfrak{q}_k$（位于 $H_k = 0$ 上）中的 Γ_i^*，但从上下文中可以看清这一点。

现在我们继续计算满足 $\partial\varepsilon = \eta$ 的 $\varepsilon \in \mathcal{C}^2(K)$。如果 $\varepsilon \in \mathcal{C}^2(K)$ 仅依赖于 $\chi(\tau)$、$\chi'(\tau)$ 和 $\chi'(\rho)$，那么

$$(\partial\varepsilon)(\sigma,\tau,\rho) = \frac{\sigma(\varepsilon(\chi(\tau),\chi'(\tau),\chi'(\rho)))\ \varepsilon(\chi(\sigma),\chi'(\sigma),\chi'(\tau\rho))}{\varepsilon(\chi(\sigma)\chi(\tau),\chi'(\sigma\tau),\chi'(\rho))\ \varepsilon(\chi(\sigma),\chi'(\sigma),\chi'(\tau))},$$

仅取决于 $\chi(\sigma)$ $\chi(\tau)$ $\chi'(\sigma)$ $\chi'(\tau)$ 和 $\chi'(\rho)$。此处及下文中，我们交替使用$\varepsilon(\tau,\rho)$和 $\varepsilon(\chi(\tau)\ \chi'(\tau)\ \chi'(\rho))$。我们有如下命题：

命题 4.2。 设 $\varepsilon \in \mathcal{C}^2(K)$ 如下：

$$\varepsilon(\tau,\rho) = \begin{cases} 1 & \begin{array}{c}\chi(\tau)=\widehat{0},\chi'(\tau)\chi'(\rho)=-1\\ \text{or } \chi(\tau)=\widehat{1},\chi'(\tau)\chi'(\rho)=1,\\ \text{or } \chi'(\rho)=1\end{array} \\ p_1 & \chi(\tau) = \widehat{1},\ \chi'(\tau) = 1,\ \chi'(\rho) = -1, \\ 1/p_1 & \chi(\tau) = \widehat{0},\ \chi'(\tau) = -1,\ \chi'(\rho) = -1, \\ p_{1j} & \chi(\tau) = \widehat{j},\ \chi'(\tau) = 1,\ \chi'(\rho) = -1, \\ 1/p_{1j} & \chi(\tau) = \widehat{k},\ \chi'(\tau) = -1,\ \chi'(\rho) = -1, \end{cases} \tag{4.6}$$

其中 p_{ij}, p_i 如方程 (4.5)中所定义，则 $\partial\varepsilon = \eta$。

证明。如果 $\chi'(\rho) = 1$，那么

$$\partial\varepsilon(\sigma,\tau,\rho) = \frac{\sigma\varepsilon(\chi(\tau),\chi'(\tau),1)\ \varepsilon(\chi(\sigma),\chi'(\sigma),\chi'(\tau))}{\varepsilon(\chi(\sigma\tau),\chi'(\sigma\tau),1)\ \varepsilon(\chi(\sigma),\chi'(\sigma),\chi'(\tau))} = 1 = \eta(\sigma,\tau,\rho).$$

因此，我们假设 $\chi'(\rho) = -1$ 并注意到

$$p_1 = \frac{1}{\varepsilon(\widehat{0}, -1, -1)} = \frac{\varepsilon(\chi(\tau), 1, -1)}{\varepsilon(\chi(\tau), -1, -1)}, \tag{4.7}$$

对所有 $\chi(\tau)$ 的取值。利用这一点，对于 $\chi'(\rho) = -1$ 和 $\chi'(\sigma) = 1$，我们有

$$\partial\varepsilon\big|_{\chi'(\tau)=-1} = \frac{\sigma\varepsilon(\chi(\tau), -1, -1)\ \varepsilon(\chi(\sigma), 1, 1)}{\varepsilon(\chi(\sigma\tau), -1, -1)\ \varepsilon(\chi(\sigma), 1, -1)} = (\partial\mathfrak{a} \cup \mathfrak{a}')(\sigma, \tau)\Gamma(\sigma),$$

其中

$$\Gamma(\sigma) \coloneqq \frac{p_1}{\sigma(p_1)\ \varepsilon(\chi(\sigma), 1, -1)^2}.$$

注 4.1 表明 $\sigma(p_1) = \sigma_s(t_1)$，因此 $\Gamma(\sigma)$ 仅取决于 $\chi(\sigma)$。因此，只需证明对于 $\sigma \in G_{K(E[2])}$，$\Gamma(\sigma) = 1/\mathfrak{a} \cup \partial\mathfrak{a}'(\chi(\sigma)\ -1, -1)$（明确验证见附录（表 1））。

现在我们证明 $\partial\varepsilon\big|_{\chi'(\sigma)=1} = \partial\varepsilon\big|_{\chi'(\sigma)=-1}$。若 $\chi'(\sigma) = -1$ 且 $\chi'(\tau) = 1$，则有

$$\begin{aligned}\partial\varepsilon(\sigma, \tau, \rho) &= \frac{\sigma\varepsilon(\chi(\tau), 1, -1)\ \varepsilon(\chi(\sigma), -1, -1)}{\varepsilon(\chi(\sigma\tau), -1, -1)\ \varepsilon(\chi(\sigma), -1, 1)} = \frac{\sigma\varepsilon(\chi(\tau), 1, -1)\ \varepsilon(\chi(\sigma), 1, -1)}{\varepsilon(\chi(\sigma\tau), 1, -1)\ \varepsilon(\chi(\sigma), -1, 1)} \\ \text{(using (4.7))} \qquad &= \partial\varepsilon\big|_{\chi'(\sigma)=1, \chi'(\tau)=1}(\sigma, \tau, \rho).\end{aligned}$$

若 $\chi'(\tau) = \chi'(\sigma) = -1$，则有

$$\begin{aligned}\partial\varepsilon(\sigma, \tau, \rho) &= \frac{\sigma\varepsilon(\chi(\tau), -1, -1)}{\varepsilon(\chi(\sigma\tau), 1, -1)\ \varepsilon(\chi(\sigma), -1, -1)} = \frac{\sigma\varepsilon(\chi(\tau), -1, -1)}{\varepsilon(\chi(\sigma\tau), -1, -1)\ \varepsilon(\chi(\sigma), 1, -1)} \\ \text{(using (4.7))} \qquad &= \partial\varepsilon\big|_{\chi'(\sigma)=1, \chi'(\tau)=-1}(\sigma, \tau, \rho).\end{aligned}$$

现在剩下要证明的是，如果 $\chi'(\sigma) = 1$，那么

$$\partial\varepsilon\big|_{\chi'(\tau)=1}(\sigma, \tau, \rho) = \eta\big|_{\chi'(\tau)=1}(\sigma, \tau, \rho) = \partial\mathfrak{a} \cup \mathfrak{a}'(\chi(\sigma), \chi(\tau), -1). \tag{4.8}$$

我们注意到

$$\sigma(\varepsilon(\chi(\tau), \chi'(\tau), \chi'(\rho))) = \sigma_s\varepsilon(\sigma \cdot \chi(\tau), \chi'(\tau), \chi'(\rho)), \tag{4.9}$$

注记4.1 推出（4.9），因为 ε 的取值是 p_{1j}和 $\sigma\ (p_{1j}) = \sigma_s\ (p_{1\sigma\cdot j})$ 的乘法组合。这意味着（假设 $\chi'\ (\sigma) = 1$）：

$$\begin{aligned}\partial\varepsilon(\sigma, \tau, \rho)\big|_{\chi'(\tau)=1, \chi'(\rho)=-1} &= \frac{\sigma\varepsilon(\chi(\tau), 1, -1)\varepsilon(\chi(\sigma), 1, -1)}{\varepsilon(\chi(\sigma\tau), 1, -1)} \\ &= \frac{\sigma_s\varepsilon(\sigma \cdot \chi(\tau), 1, -1)\varepsilon(\chi(\sigma), 1, -1)}{\varepsilon(\chi(\sigma)\sigma \cdot \chi(\tau), 1, -1)}.\end{aligned}$$

因此，对于分别满足 $\chi(\sigma) = \widehat{i}$和 $\chi(\tau) = \sigma^{-1} \cdot \widehat{j}$的 $\sigma, \tau \in G_K$，$\partial\varepsilon\big|_{\chi'(\tau)=1, \chi'(\rho)=-1}(\sigma, \tau, \rho)$ 取相同的值，这与 $\partial\mathfrak{a} \cup \mathfrak{a}'$类似。因此，只需在假设 $\sigma, \tau \in G_{K(E[2])}$ 以及 $\chi'(\sigma) = 1 = \chi'(\tau) = 1$ 和 $\chi'(\rho) = -1$ 的条件下验证等式 (4.8) 即可（具体验证见附录（表 2））。□

下一小节将专门讨论利用从 globalpart 获得的 ε 计算 CTP 的局部部分。

4.2 局部计算

我们回顾一下假设： T_1 （因此 β'）定义在 K_v 上。利用 α 的局部平凡性，对于 K 的每个赋值 v ，存在一个 $P_v \coloneqq (x_v, y_v) \in E(\overline{K_v})$，使得对所有 $\sigma \in G_{K_v}$， $\partial P_v(\sigma) = (\sigma - 1)P_v = \alpha_v(\sigma)$。这意味着，对于 $\sigma \in G_{K_v}$，若 $\chi(\sigma) = \widehat{0}$，则 $\sigma(P_v) = P_v$；而当 $\chi(\sigma) = \widehat{i}$ 时， $\sigma(P_v) = P_v + T_i$。因此， P_v 属于 $K_v(\sqrt{\beta_1}, \sqrt{\beta_2})$ 的一个子域。将 P_v 提升为一个零次除子 $\mathfrak{b}_v = (P_v) - (T_0)$，我们得到 (4.10)

$$(\mathfrak{a}_v - \partial\mathfrak{b}_v)(\sigma) = \begin{cases} 0 = \operatorname{div}(1), & \chi(\sigma) = \widehat{0} \\ (T_i) - (P_v + T_i) + (P_v) - (T_0) = \operatorname{div}\left(\frac{y - \frac{y_v(x-e_i)}{x_v - e_i}}{x - x(P_v + T_i)}\right), & \chi(\sigma) = \widehat{i}. \end{cases}$$

对于 $1 \le i \le 3$，令 $x_{v,i}$, $\theta_{v,i}$ 和 $\omega_{v,i}$ 分别表示这些量 $x_v - e_i$, $\frac{y_v}{x_v - e_i}$ 和 $-\theta_{v,i}/p_{jk}$。由此得到：

$$(\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup_1 \mathfrak{a}'_v(\tau, \rho) = \begin{cases} 1 & \chi(\tau)=\widehat{0} \text{ or } \chi'(\rho)=1, \\ z_{v,11} & \chi(\tau)=\widehat{1},\ \chi'(\rho)=-1 \\ z_{v,1j} & \chi(\tau)=\widehat{j},\ \chi'(\rho)=-1, \end{cases} \tag{4.11}$$

其中利用方程 (3.2) 和 (3.4) 可得

$$z_{v,11} = \left(\frac{\left(y - \frac{y_v(x-e_1)}{x_v - e_1}\right)\left(-\frac{y}{x-e_1}\right)}{x - x(P_v + T_1)}\right)(T_1) \times \left(\frac{x - x(P_v + T_1)}{\left(y - \frac{y_v(x-e_1)}{x_v - e_1}\right)(x/y)}\right)(T_0) = x_{v,1}$$

and

$$z_{v,1j} = \left(\frac{\left(y - \frac{y_v(x-e_j)}{x_v - e_j}\right)}{x - x(P_v + T_j)}\right)(T_1) \times \left(\frac{x - x(P_v + T_j)}{\left(y - \frac{y_v(x-e_j)}{x_v - e_j}\right)(x/y)}\right)(T_0) = -\theta_k$$

此外，

$$\mathfrak{b}_v \cup_2 \partial\mathfrak{a}'_v(\tau, \rho) = \begin{cases} 1 & \chi'(\tau) = 1 \text{ or } \chi'(\rho) = 1, \\ x_{v,1} & \chi'(\tau) = \chi'(\rho) = -1, \end{cases} \tag{4.12}$$

并且 $\gamma_v \coloneqq (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup \mathfrak{a}'_v - \mathfrak{b}_v \cup \partial\mathfrak{a}'_v - \varepsilon_v$ 由下式给出：

$$\gamma_v \coloneqq \begin{cases} 1 & \begin{array}{c}\chi(\tau)=\widehat{0},\chi'_1(\tau)\chi'_1(\rho)=-1 \\ \text{or } \chi(\tau)=\widehat{1},\chi'_1(\tau)\chi'_1(\rho)=1, \\ \text{or } \chi'_1(\rho)=1\end{array} \\ x_{v,1}/p_1 & \chi(\tau) = \widehat{1},\ \chi'_1(\tau) = 1,\ \chi'_1(\rho) = -1, \\ p_1/x_{v,1} & \chi(\tau) = \widehat{0},\ \chi'_1(\tau) = -1,\ \chi'_1(\rho) = -1, \\ \omega_{v,k} & \chi(\tau) = \widehat{j},\ \chi'_1(\tau) = 1,\ \chi'_1(\rho) = -1, \\ 1/\omega_{v,k} & \chi(\tau) = \widehat{k},\ \chi'_1(\tau) = -1,\ \chi'_1(\rho) = -1, \end{cases} \tag{4.13}$$

其中 j、$k \neq 1$ 互不相同。

我们讨论 $\omega_{v,\,i}$ 的一些性质，以确定由 γ_v 表示的 c_v 在布劳尔群 $\mathrm{Br}(K_v)$ 中的类。此处我们暂不采用 $e_1 \in K_v$ 这一假设。注意， $\omega_{v,\,i}$ 的定义并不依赖于这一假设。对于满足以下条件的 $\sigma \in G_{K_v}$，

$\chi(\sigma)=\widehat{i}$ and $\sigma\big|_{K_v(\sqrt{\beta_i})}=\mathrm{id}$, and using equation (3.2) we have
($\because \sigma(p_{jk})=-\sigma_s p_{\sigma\cdot j,\sigma\cdot k}=-p_{jk}$.)

$$\sigma(\omega_{v,i})=\sigma\left(\frac{-y_v}{x_{v,i}p_{jk}}\right)=\frac{y(P_v+T_i)}{p_{jk}(x(P_v+T_i)-e_i)}=\frac{-y_v}{x_{v,i}p_{jk}}=\omega_{v,i}.$$

这意味着 $\omega_{v,\ i}\in K_v(\sqrt{\beta_i})$。此外，若 $\sigma\in G_{K_v}$，且 $\chi(\sigma)=\widehat{j}$ 和$\sigma\big|_{K_v(\beta_i)}=$为恒等映射 (即 $\sigma\big|_{K_v(\sqrt{\beta_i})}$ 是 $\mathrm{Gal}(K_v(\sqrt{\beta_i})/K_v(\beta_i))$的非平凡元素），利用方程（3.3），可得

($\because \sigma(p_{jk})p_{jk}=s_{kj}$注 4.1))

$$\sigma(\omega_{v,i})=\sigma\left(\frac{-y_v}{x_{v,i}p_{jk}}\right)=\frac{-y(P_v+T_j)}{\sigma(p_{jk})(x(P_v+T_j)-e_i)}=\frac{-x_{v,i}p_{jk}}{y_v}=\frac{1}{\omega_{v,i}}.$$

假设 β_i 不是 $K_v(\beta_i)$ 中的平方，则 $\mathrm{Norm}_{K_v(\sqrt{\beta_i})/K_v(\beta_i)}(\omega_{v,i})=1$.此外，若 $\sigma\in G_{K_v}$ 满足 $\chi(\sigma)=0$，则有：$\sigma(\omega_{v,i})=\omega_{v,j}$，若 $\sigma(e_i)=e_j$。根据希尔伯特第90定理，存在 $h_{v,i}\in K_v(\sqrt{\beta_i})$，使得 $\omega_{v,i}=h_{v,i}/h_{v,i}$，其中 $x\mapsto\overline{x}$ 表示 $K_v(\sqrt{\beta_i})$ 在 $K_v(\beta_i)$ 上的非平凡自同构。我们选取 $h_{v,i}$ 为 $1+\omega_{v,i}\in K_v(\sqrt{\beta_i})$，并定义：

$$\delta_{v,i}:=h_{v,i}\overline{h_{v,i}}=2+\overline{\omega_{v,i}}+\omega_{v,i}\in K_v(\beta_i)^\times. \tag{4.14}$$

由上可得以下注记：

注4.3。令 $\delta_{v,i}\in K_v(e_i)^\times$ 如上所述。那么 $\sigma(\delta_{v,i})=\delta_{v,j}$ 若 $\sigma(e_i)=e_j$ 对3$\sigma\in G_{K_v}$ 成立。因此，我们得到：$\prod_{i=1}\delta_{v,i}\in K_v^\times$且 $\delta'_{v,i}:=\delta_{v,j}\delta_{v,k}\in K_v(e_i)^\times$。

回到 $e_1\in K_v$ 的情形，我们有：$\delta'_{v,1}\in K_v^\times$。我们将 γ_v 加上余边界 $\partial\xi_v$，其中：

$$\xi_v(\tau)=\begin{cases}1 & \chi'(\tau)=1,\\ \dfrac{1}{h_{v,2}h_{v,3}} & \chi'(\tau)=-1.\end{cases} \tag{4.15}$$

若 $\gamma'_v:=\gamma_v-\partial\xi_v$，则有：

$$\gamma'_v(\tau,\rho)=\begin{cases}1 & \chi'(\tau)=1 \text{ or } \chi'(\rho)=1,\\ \frac{1}{\delta'_{v,1}}\in K_v^\times & \chi'(\tau)=\chi'(\rho)=-1,\end{cases} \tag{4.16}$$

并且 γ'_v 也表示布劳尔群 $\mathrm{Br}(K_v)$ 中的类 $c_v\in$。下面的命题说明，c_v 是四元数代数 $(\delta'_{v,1},\beta')$ 的类，因此 $(-1)^{2\mathrm{inv}_{K_v}(c_v)}=(\delta'_{v,1},\beta')_{K_v}$。

命题*4.4.* 若 $d_1,d_2\in K_v^\times$，则由 $(\sigma,\tau)\mapsto 1$ *if* $\sigma(\sqrt{d_2})=\sqrt{d_2}$ *or* $\tau(\sqrt{d_2})=\sqrt{d_2}$, *and* $(\sigma,\tau)\mapsto d_1$, *if* $\sigma(\sqrt{d_2})=\tau(\sqrt{d_2})=-\sqrt{d_2}$ 给出的 *2*-余循环 z 表示有理数域 K_v 上四元数代数 (d_1,d_2) 在布劳尔群中的类。

证明。 [Ser79，§XIV.2，命题 5] 蕴含余循环

$$x(\sigma,\tau):=\begin{cases}1 & \text{if } \sigma(\sqrt{d_1})=\sqrt{d_1} \text{ or } \tau(\sqrt{d_2})=\sqrt{d_2},\\ -1 & \text{otherwise.}\end{cases}$$

表示四元数代数 (d_1,d_2) 的类。现在可以验证，$z=x-\partial y$ 其中

$$y(\sigma):=\begin{cases}1 & \sigma(\sqrt{d_2})=\sqrt{d_2}\\ 1/\sqrt{d_1} & \sigma(\sqrt{d_2})=-\sqrt{d_2}.\end{cases}$$

□

现在我们用 $x(Q_v)$ 和 $y(Q_v)$ 来表示 $\delta_{v,i}$，其中 $Q_v := 2P_v \in E(K_v)$。

$$\begin{aligned} x(Q_v) - e_i &= \left(\frac{3x_v^2 + c}{2y_v}\right) - (x_v - e_j) - (x_v - e_k) \\ &= \frac{1}{4}\left(\sum_{i=1}^{3} \theta_{v,i}\right)^2 - \theta_{v,i}\theta_{v,k} - \theta_{v,i}\theta_{v,j} = \frac{1}{4}\left(\theta_{v,j} + \theta_{v,k} - \theta_{v,i}\right)^2. \end{aligned}$$

存在 $w_{v,\,i} \in K_v(e_i)^\times$，使得 $x(Q_v) - e_i = \beta_i w_{v,\,i}^2$，因此我们有 $\theta_{v,\,i} = w_{v,\,j}\sqrt{\beta_j} + w_{v,\,k}\sqrt{\beta_k}$ 并且

$$\omega_{v,i} = -\frac{\theta_{v,i}}{p_{jk}} = -\frac{w_{v,j}\sqrt{\beta_j} + w_{v,k}\sqrt{\beta_k}}{\Gamma_j^*\sqrt{\beta_j} + \Gamma_k^*\sqrt{\beta_i}}.$$

这里，若 e_i 是共轭元，则 $w_{v,\,i}$ 也选为关于 K_v 的共轭元。因此，

$$\delta_{v,i} = 2\left(1 - \frac{\beta_j w_{v,j}\Gamma_j^* - \beta_k w_{v,k}\Gamma_k^*}{\beta_j(\Gamma_j^*)^2 - \beta_k(\Gamma_k^*)^2}\right) = 2\left(1 + \frac{\beta_k w_{v,k}\Gamma_k^* - \beta_j w_{v,j}\Gamma_j^*}{s_{kj}}\right). \tag{4.17}$$

$\langle a, a'\rangle_{\mathrm{CT}}$ 的值（取决于上述所作的选择）由以下定理给出。

定理 4.5。鉴于上述讨论以及对上述点 P_v 的选择，*CTP* 在 $(a,\ a') \in \mathrm{Ш}^2(E) \times \mathrm{H}^1(G_K, \langle T_1\rangle)$ 上的值等于：

$$\langle a, a'\rangle_{\mathrm{CT}} = \prod_v (\delta'_{v,i}, \beta')_{K_v}.$$

5 在 $\mathrm{Ш}^2(E) \times \mathrm{Ш}^2(E)$ 上计算 CTP

本节的主要目的是证明上一节所做计算的充分性。

5.1 余限制方法

令 $a' \in \mathrm{Ш}^{(2)}(E)$ 由 1-余循环 α' 表示，该余循环对应于三元组 $(\beta'_1, \beta'_2, \beta'_3)$，如第 2 节所述，并且我们省略 $\chi_{a'}$ 中的下标，称其为 χ'。注意，这个 χ' 与上一节中的并不相同。我们选择 α' 到 $\mathcal{C}^1(G_K, \mathrm{Div}^0(E))$ 的一个提升，如下：

$$\mathfrak{a}'(\sigma) = \begin{cases} 0 & \chi'(\sigma) = \widehat{0}, \\ (T_j) + (T_k) - 2(T_0) & \chi'(\sigma) = \widehat{i}. \end{cases}$$

注意，$\mathfrak{a}'$ 的提升 α' 与 § 4.1 中 α 的提升 的选择不同。下面的引理说明，$\mathfrak{a}'$ 可以写成某些上链的余限制之和。

引理 5.1. 设 $\mathfrak{a}'$ 如上，并设 $\Delta_1, \ldots, \Delta_n$ 是 Δ的不同轨道，其代表元为 $T_1,\ldots,T_n$，对应于 $n \le 3$。则有：

$$\mathfrak{a}' = \sum_{i=1}^{n} \mathrm{cor}(\mathfrak{t}_i),$$

其中 $t_i \in \mathcal{C}^1(G_{K(e_i)}, \mathrm{Div}^0(E))$ 由下式给出：

$$\mathfrak{t}_i(\sigma) := \begin{cases} 0 & \sigma(\sqrt{\beta'_i}) = \sqrt{\beta'_i}, \\ (T_i) - (T_0) & \sigma(\sqrt{\beta'_i}) = -\sqrt{\beta'_i}, \end{cases}$$

并且 $\mathfrak{t}_i$ 的余限制是相对于群 $G_{K(e_i)}$ 和 G_K取的。

证明. 设 $T_i = P_{i,1}, \dots P_{i,k_i}$ 是 T_i 轨道中的点，$\beta_i' = b_{i,1}, \dots, b_{i,k_i}$ 是 β_i' 在 $\{\beta_1', \beta_2', \beta_3'\}$ 中的 G_K-共轭元。设 $\{\mathrm{id} = \tau_{i,1}, \tau_{i,2}, \dots, \tau_{i,k_i}\}$ 是 $G_{K(e_i)}$ 的右陪集代表元，且对 $1 \le j \le k_i$ 有 $\tau_{i,j}(P_{i,j}) = T_i$，并且 $\tau_{i,j} \cdot \left(\sum_{l=1}^{k_i} \sqrt{b_{i,l}}(P_{i,l}) \right) = \sum_{l=1}^{k_i} \sqrt{b_{i,l}}(P_{i,l})$。为说明这样的陪集代表元选择是可能的，我们注意到，任何满足 $\sigma(P) = T_i$（对某个 $P \in \Delta_i$）的 $\sigma \in G_K$ 都具有 $\sigma_s \sigma_p$ 的形式（如注 4.1 所示），因此 σ_p 具有所需性质。设 m, r 是定义中所述的余限制映射。于是 $m(\tau_{i,j}\sigma) \in G_{K(e_i)}$，因此 $r(\tau_{i,j}\sigma)^{-1}(\sqrt{\beta_i'}) = \sqrt{b_{i,\sigma^{-1}\cdot j}}$，其中若 $\sigma^{-1}(P_{i,j}) = P_{i,l}$，则 $(i, \sigma^{-1}\cdot j) = (i,l)$。利用方程（3.6）和 $\mathfrak{t}_i$ 的定义，我们有：

$$\begin{aligned}\sum_{i=1}^{n} \mathrm{cor}_{G_{K(e_i)}}^{G_K}(\mathfrak{t}_i)(\sigma) &= \sum_{i=1}^{n}\sum_{j=1}^{k_i} \tau_{i,j}^{-1}\mathfrak{t}_i(m(\tau_{i,j}\sigma)) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{k_i} g\left(\frac{\sigma(\sqrt{b_{i,\sigma^{-1}\cdot j}})}{\sqrt{b_{i,j}}}\right)((P_{i,j}) - (T_0))\end{aligned}$$

其中 g 是同构 $g: \mu_2 \to \mathbb{Z}/2\mathbb{Z}$。现在根据 χ' 的定义，我们有 $\chi'(\sigma) = \sum_{i=1}^{n}\sum_{j=1}^{k_i} \chi'_{i,j}(\sigma)(P_{i,j})$，其中 $\chi'_{i,j}(\sigma) := {}^{\sigma}(\sqrt{b_{i,\sigma^{-1}\cdot j}})\sqrt{b_{i,j}}$ 表示 $\chi'(\sigma)$ 在 $\overline{P_{i,j}}$ 处的值。因此，$\sum_{i=1}^{n} \mathrm{cor}_{G_{K(e_i)}}^{G_K}(\mathfrak{t}_i) = \mathfrak{a}'$。 □

上述引理结合命题 3.1 的第 (3) 部分，立即得到以下结果

推论 5.2。设 a，$a' \in \mathrm{Ш}^{(2)}(E)$ 以及 α，α'，$\mathfrak{a}$ 和 $\mathfrak{a}'$ 如 *CTP* 的定义中所述。采用引理 *5.1* 中的记号，并且 $\mathfrak{a}'$ 按引理 *5.1*中的方式选取。
于是我们有：$\eta := \partial\mathfrak{a} \cup_1 \mathfrak{a}' - \mathfrak{a} \cup_2 \partial\mathfrak{a}' = \sum_{i=1}^{n} 余迹_{G_{K(e_i)}}^{G_K}\eta_i$，其中

$$\eta_i := \partial \mathrm{res}_{G_K}^{G_{K(e_i)}}(\mathfrak{a}) \cup \mathfrak{t}_i - \mathrm{res}_{G_K}^{G_{K(e_i)}}(\mathfrak{a}) \cup \partial\mathfrak{t}_i \in Z^3(K(e_i)).$$

特别地，若 $\varepsilon_i \in C^2(K(e_i))$ 满足 $\partial\varepsilon_i = \eta_i$，则 $\varepsilon \in C^2(K)$ 可选为 $\partial\varepsilon = \eta$ $\sum_{i=1}^{n} 余迹_{G_{K(e_i)}}^{G_K}(\varepsilon_i)$。

因此，我们将计算适当的 ε（针对 a，$a' \in \mathrm{Ш}^{(2)}(E)$）的问题归结为计算 ε_i 的问题；我们已在命题 4.2 中通过令 K 为 $K(e_i)$ 以及 T_1 为 T_i 而解决了该问题。

$_n$考察计算中的局部部分，我们有：$\gamma_v = \sum_{i=1} \gamma'_{i,v}$ 其中

$$\gamma'_{i,v} := (\mathfrak{a}_v - \partial\mathfrak{b}_v) \cup \left(\mathrm{cor}_{G_{K(e_i)}}^{G_K}(\mathfrak{t}_i')\right)_v - \mathfrak{b}_v \cup \partial\left(\mathrm{cor}_{G_{K(e_i)}}^{G_K}(\mathfrak{t}_i')\right)_v - \left(\mathrm{cor}_{G_{K(e_i)}}^{G_K}(\varepsilon_i)\right)_v.$$

利用双陪集公式（等式（3.8））， 我们有：

$$\left(\mathrm{cor}_{G_{K(e_i)}}^{G_K}(\mathfrak{t}_i)\right)_v = \sum_{w|v} \mathrm{cor}_{G_{K(e_i)_w}}^{G_{K_v}} \mathfrak{t}_{i,w},$$

其中 $\mathfrak{t}_{i,w} := \mathrm{res}_{G_{K(e_{i,w})}}^{G_{K(e_1)_w}}((g_{i,w})_*\mathfrak{t}_i) \in C^1(G_{K(e_i)_w}, \langle (T_{i,w}) - (T_0)\rangle)$，$g_{i,w} \in G_K$ 对应于 w 在 $K(e_i)$ 上方的赋值 v，而 $e_{i,w}$、$T_{i,w}$ 分别是 $g_{i,w}$ 的共轭元 e_i、T_i。具体而言，我们有：

$$\mathfrak{t}_{i,w}(\sigma) := \begin{cases} 0 & \sigma(\sqrt{\beta'_{i,w}}) = \sqrt{\beta'_{i,w}}, \\ (T_{i,w}) - (T_0) & \sigma(\sqrt{\beta'_{i,w}}) = -\sqrt{\beta'_{i,w}}, \end{cases}$$

其中 $\beta'_{i,\ w} := g_{i,\ w}(\beta'_i)$。

同理，对 ε_i 应用双陪集公式，得到：

$$\left(\mathrm{cor}_{G_{K(e_i)}}^{G_K}\varepsilon_i\right)_v = \sum_{w|v}\mathrm{cor}_{G_{K(e_i)w}}^{G_{K_v}}\varepsilon_{i,w}.$$

因此，$\gamma'_{i,v} = \sum_{w|v}\mathrm{cor}_{G_{K(e_i)w}}^{G_{K_v}}\gamma_{i,w}$，其中

$$(5.1)\quad \gamma_{i,w} := \left(\mathrm{res}_{G_K}^{G_{K(e_i)w}}(\mathfrak{a}) - \mathrm{res}_{G_{K_v}}^{G_{K(e_i)w}}(\partial\mathfrak{b}_v)\right)\cup\mathfrak{t}_{i,w} - \mathrm{res}_{G_{K_v}}^{G_{K(e_i)w}}(\mathfrak{b}_v)\cup\partial\mathfrak{t}_{i,w} - \varepsilon_{i,w}.$$

下面的命题表明，$\gamma_{i,w}$ 是一个 2-余循环。

命题 5.3. $\gamma_{i,w}\in\mathcal{Z}^2(K(e_i)w)$.

证明。 利用 $\partial\varepsilon_i = \eta_i$，我们有

$$\begin{aligned}
\partial\gamma_{i,w} &= \mathrm{res}_{G_K}^{G_{(e_i)w}}\partial\mathfrak{a}\cup\mathfrak{t}'_{i,w} - \mathrm{res}_{G_K}^{G_{K(e_i)w}}\mathfrak{a}\cup\partial\mathfrak{t}'_{i,w}\\
&\text{（使用双陪集公式（方程（3.8）于 } \eta_i\text{）}\\
&\quad - \mathrm{res}_{G_{K(e_{i,w})}}^{G_{K(e_i)w}}(g_{i,w})_*\left(\partial\mathrm{res}_{G_K}^{G_{K(e_i)}}\mathfrak{a}\cup\mathfrak{t}'_i - \mathrm{res}_{G_K}^{G_{K(e_i)}}\mathfrak{a}\cup\partial\mathfrak{t}'_i\right)\\
&\text{（}\because (g_{i,\ w})_* \text{与限制映射交换，}\ \cup\text{ 且 }\partial\text{）}\\
&\quad = \mathrm{res}_{G_K}^{G_{K(e_i)w}}(\partial(\mathfrak{a}-(g_{i,w})_*\mathfrak{a}))\cup\mathfrak{t}'_{i,w} - \mathrm{res}_{G_K}^{G_{K(e_i)w}}(\mathfrak{a}-(g_{i,w})_*\mathfrak{a})\cup\partial\mathfrak{t}'_{i,w}.
\end{aligned}$$

因此，如果 $(g_{i,\ w})_*(\mathfrak{a}) = \mathfrak{a}$，那么$\partial\gamma_{i,\ w} = 0$。注意，$\mathfrak{a}(\tau)$ 只取决于 $\chi(\tau)$，因此我们也可以等价地将 $\mathfrak{a}(\tau)$ 写成 $\mathfrak{a}(\chi(\tau))$。我们有 $\sigma\mathfrak{a}(\chi(\tau)) = \mathfrak{a}(\sigma\cdot\chi(\tau))$。3为说明这一点，回忆 $\chi(\tau) = \sum a_i(T_i)$，其中 $a_i\in\mu_2$取决于 τ，因此如果$i=1$ $\chi(\tau) = j$，那么 $\sigma\chi(\tau) = \sigma\cdot j$。

现在对于 $\sigma\in G_K$

$$\begin{aligned}
&\text{（根据定义）}\\
&\quad((g_{i,w})_*(\mathfrak{a}))(\sigma) = g_{i,w}\mathfrak{a}(g_{i,w}^{-1}\sigma g_{i,w})\\
&\quad\qquad = g_{i,w}\mathfrak{a}(\chi(g_{i,w}^{-1}\sigma g_{i,w}))\cdot\mathfrak{a}(g_{i,w}\chi(g_{i,w}^{-1}\sigma g_{i,w}))\\
&\text{（}\chi\text{ 是一个 1-cocycle）}\quad = \mathfrak{a}(\chi(\sigma g_{i,w})\chi(g_{i,w})^{-1}) = \mathfrak{a}(\chi(\sigma)\sigma\chi(g_{i,w})\chi(g_{i,w})^{-1})
\end{aligned}$$

回顾引理 5.1 的证明或备注 4.1 可知，$g_{i,w}$ 可以选取为使得 $\chi(g_{i,w}) = \widehat{0}$ 通过分解 $\sigma = \sigma_s\sigma_p$ 得到 $\sigma\in G_K$。对 $g_{i,w}$ 作此选择，我们有

$$((g_{i,w})_*(\mathfrak{a}))(\sigma) = \mathfrak{a}(\chi(\sigma)\sigma\chi(g_{i,w})\chi(g_{i,w})^{-1}) = \mathfrak{a}(\chi(\sigma)) = \mathfrak{a}(\sigma). \qquad \square$$

上述命题与命题 3.1 第（2）部分共同推出

$$\mathrm{inv}_{K_v}([\gamma_v]) = \sum_{i=1}^n\mathrm{inv}_{K_v}([\gamma'_{i,v}]) = \sum_{i=1}^n\sum_{w|v}\mathrm{inv}_{K_v(e_{i,w})}([\gamma_{i,w}]),$$

其中 $[z]$ 表示余循环 z的上同调类。这表明，CTP 中 K 的赋值 v 处的贡献，等于 Δ的 G_{K_v}-个轨道的贡献之和。回顾 §2 中的定义 $\prod$。由上述计算以及 §4.2，我们得到$\delta'_{i,v}\in K_v(e_i)^\times$，使得 CTP 中 v 处的局部贡献为$\prod_i(\delta'_{i,v},\beta'_i)_{K_v(e_i)}$。因此，我们有以下定理

定理 5.4. 我们有

$$(-1)^{2\langle a,a'\rangle_{\mathrm{CT}}} = \prod_v \prod_i{}^{\diamond} (\delta'_{i,v}, \beta'_i)_{K_v(e_i)},$$

其中，i 遍历 K的每个赋值 v 下， Δ 的 G_{K_v}-轨道。

下面的推论指出，我们只需考虑有限多个赋值对 CTP 的贡献，并说明这些赋值具体是哪些。

推论 5.5. 令 $S_{a,a'}$ 为有限赋值的集合，使得 α_v、 α'_v （分别表示代表 a、 a' 的余循环在 v 处的局部化）中至少一个通过分歧扩张分解。显然，$S_{a,a'} \subset$ {是 E/K} $\cup$ {2}的坏约化素数。于是，采用上述记号，我们有

$$(-1)^{2\langle a,a'\rangle_{\mathrm{CT}}} = \prod_{v\in S} \prod_i{}^{\diamond} (\delta'_{i,v}, \beta'_i)_{K_v(e_i)},$$

其中 i 遍历 Δ的 G_{K_v}-轨道。

证明。 设 v 是 K的一个有限赋值。容易看出，如果 α_v或 α'_v 作为余循环是平凡的，那么 v 处对 CTP 的贡献也是平凡的。因此，我们假设 α_v、 α'_v 通过一个非平凡的非分歧扩张分解。这意味着 $K_v(\sqrt{\beta_i})/K_v(e_i)$是一个非分歧扩张（ β'_i的情形类似）。现在，如果 β_i 或 β'_i 在 $K_v(e_i)$中是平方，那么与 e_i 的轨道对应的局部贡献在局部上是平凡的。否则， $K_v(\sqrt{\beta_i}) = K_v(\sqrt{\beta'_i})$在 $K_v(e_i)$上，因此 $\delta'_{v,i}$是某个元素从 $K_v(\sqrt{\beta'_i})$到 $K_v(e_i)$的范数。

对于无限赋值 v，如果 β_i 是复数或正数，则可将 $\delta_{v,\,i}$ 取为 1。因此，如果 β_i 或 β'_i 是复数或正数，那么来自 e_i 的轨道的贡献为平凡。因此，我们假设 v 是实赋值，那么 β_1、 β_2、 β_3 中至少有一个（不妨设为 β_1）是实数且为负数。如果 β_2、 β_3 是复数，那么 $\delta'_1 = 1$ 及其他轨道对应于复赋值，因此 v 处的贡献为平凡。否则， β_2 和 β_3 是实数，且恰有一个为负数。因此，$\delta'_{v,\,i}$ 是从 $\mathbb{C}$ 到 $\mathbb{R}$ 的范数，故 v 处的贡献为平凡。还可以结合等式 (5.2)（见 §5.2）以及 $\delta_{v,\,i}$ 是 $\mathbb{C}$ 中某个元素的范数这一事实，得出无限赋值处的贡献为平凡。□

5.2 CTP 的精确公式

为了得到 CTP 的精确公式，我们将定理 5.4 中得到的 CTP 公式用希尔伯特符号 $(\delta_{v,i}, \beta'_i)_{K_v(e_i)}$. 表示。注记 3 4.3 意味着存在一个 $d_v \in K_v^\times$， 使得 $\prod d_v\delta_{v,i} \in (K_v^\times)^2$. 。此前，我们$_{i=1}$曾用希尔伯特符号 $(\delta'_{v,i}, \beta'_i)_{K_v(e_i)}$ 表示 CTP。利用定理 5.4，若 c_v 表示 γ_v 在布劳尔群 (K_v) 中的类，则有：

$$\begin{aligned}
(-1)^{2\mathrm{inv}_{K_v}(c_v)} &= \prod_i{}^{\diamond} (\delta'_{v,i}, \beta'_i)_{K_v(e_i)} = \prod_i{}^{\diamond} (d_v^2, \beta'_i)_{K_v(e_i)} (\delta'_{v,i}, \beta'_i)_{K_v(e_i)} \\
&= \prod_i{}^{\diamond} (d_v^2\delta'_{v,i}, \beta'_i)_{K_v(e_i)} = \prod_i{}^{\diamond} (d_v\delta_{v,i}, \beta'_i)_{K_v(e_i)} \\
&= \prod_i{}^{\diamond} (d_v, \beta'_i)_{K_v(e_i)} \prod_i{}^{\diamond} (\delta_{v,i}, \beta'_i)_{K_v(e_i)}.
\end{aligned}$$

◇这里$\delta'_{v,\,i} := \delta_{v,\,j}\delta_{v,\,k}$ 与备注4.3中的情况相同。现在我们证明 $\prod_i (d_v, \beta'_i)_{K_v(e_i)} = 1$。为此，我们利用以下事实：若 L 是 K_v 的有限扩张，且 $z \in K_v^\times$, $z' \in L^\times$,

则$(z, z')_L = (z, \text{范数}_{L/K_v}(z'))_{K_v}$。由此可得：

$$\prod_i^{\diamond}(d_v, \beta_i')_{K_v(e_i)} = \prod_i^{\diamond}(d_v, \mathrm{Norm}_{K_v(e_i)/K_v}(\beta_i)')_{K_v} = (d_v, \beta_1'\beta_2'\beta_3')_{K_v} = 1.$$

因此，我们得到：

$$(-1)^{2\langle a,a'\rangle_{\mathrm{CT}}} = \prod_v \prod_i^{\diamond}(\delta_{v,i}, \beta_i')_{K(e_i)}. \tag{5.2}$$

可以验证，上述方程与 Cassels 配对中方程（3.10）里的表达式相似。以下定理表明，配对 $\langle\cdot,\ \cdot\rangle_{\mathrm{Cas}}$与 $\langle\cdot,\ \cdot\rangle_{\mathrm{CT}}$相同，这里使用了 $\delta_{v,\ i}$ 的表达式（方程（4.17））。

定理 5.6. 对于 $a,\ a' \in \mathrm{S}^{(2)}(E)$，有

$$\langle a, a'\rangle_{\mathrm{Cas}} = \langle a, a'\rangle_{\mathrm{CT}}.$$

证明。设 $\mathfrak{q}_i := (\Gamma_j^*:\ \Gamma_k^*:\ 1)$ 是 $H_i(\Gamma_j,\ \Gamma_k,\ T)$ 上的一个全局点（如方程（4.5）所示），则

$$\begin{aligned} L_i &:= \sum_{l=1}^{3} U_l \frac{\partial H_i}{\partial U_l}(\mathfrak{q}_i) + T\frac{\partial H_i}{\partial T}(\mathfrak{q}_i) \\ &= \frac{\partial H_i}{\partial \Gamma_j}(\mathfrak{q}_i)\left(\sum_{l=1}^{3} U_l \frac{\partial \Gamma_j}{\partial U_l}(\mathfrak{q}_i)\right) + \frac{\partial H_i}{\partial \Gamma_k}(\mathfrak{q}_i)\left(\sum_{l=1}^{3} U_l \frac{\partial \Gamma_k}{\partial U_l}(\mathfrak{q}_i)\right) + T\frac{\partial H_i}{\partial T}(\mathfrak{q}_i) \end{aligned}$$

（$\because (\Gamma_1, \Gamma_2, \Gamma_3)$ 是从 (U_1, U_2, U_3) 出发的线性坐标变换）

$$= \Gamma_j \frac{\partial H_i}{\partial \Gamma_j}(\mathfrak{q}_i) + \Gamma_k \frac{\partial H_i}{\partial \Gamma_k}(\mathfrak{q}_i) + T\frac{\partial H_i}{\partial T}(\mathfrak{q}_i).$$

令 $\mathfrak{q}_v = (w_v, 1 : w_v, 2 : w_v, 3 : 1)$ 为 D_a 上对应于 Q_v（如上一节所述）的点（坐标为 $(\Gamma_1 :\ \Gamma_2 :\ \Gamma_3 :\ T)$）。于是有 $L_i(q_v) = 2(e_k - e_j) + 2(\beta_k\Gamma_k^* w_{v,k} - \beta_j\Gamma_j^* w_{v,j})$。注意，由于 s_{kj} 是一个范数，$(\delta_{v,i}, \beta_i')_{K_v(\beta_i)} = (s_{kj}\delta_{v,i}, \beta_i')_{K_v(\beta_i)}$。进一步利用等式 (4.17) 中 $\delta_{v,i}$ 的表达式，以及 $p_{kj} = \sqrt{\beta_k}\Gamma_k^* + \sqrt{\beta_j}\Gamma_j^*$，可得 $s_{kj}\delta_{v,i} = L_i(\mathfrak{q}_v)$；因此，等式 (3.10) 中定义的配对 $\langle\cdot,\cdot\rangle_{\mathrm{Cas}}$ 与 Cassels-Tate 配对相同。□

6 附录

本节验证命题 4.2 中提出的两个计算性断言，即当 $\chi'(\tau) = 1$且 $\chi'(\rho) = -1$ 时，$1/\Gamma_1(\sigma) = \mathfrak{a} \cup \partial\mathfrak{a}'(\sigma, -1, -1)$，以及 $\partial\varepsilon(\sigma, \tau, \rho) = \partial\mathfrak{a} \cup \mathfrak{a}'(\sigma, \tau, \rho)$。

设 $\sigma, \tau, \rho \in G_K$ 满足 $\chi'(\tau) = \chi'(\rho) = -1$，则有：

$\chi(\sigma)$	$1/\Gamma_1(\sigma)$	$\mathfrak{a} \cup \partial\mathfrak{a}'(\sigma, -1, -1)$
$\widehat{0}$	$\frac{p_1(1)^2}{p_1} = 1$	1
$\widehat{1}$	$\frac{\sigma(p_1)p_1^2}{p_1} = s_1$	s_1
$\widehat{j}$	$\frac{\sigma(p_1)p^2{}_{1j}}{p_1} = s_{j1}$	s_{j1}

表 1。$1/\Gamma_1(\sigma) = \mathfrak{a} \cup \partial\mathfrak{a}'(\sigma, -1, -1)$。

设 σ、τ、$\rho \in G_K$ 满足 $\chi'(\rho) = -1$、$\chi'(\tau) = 1$ 和 $\chi'(\sigma) = 1$，则若 $\chi(\sigma) = \widehat{0}$，那么

$$\partial\varepsilon(\sigma, \tau, \rho) = \frac{\sigma_s\varepsilon(\sigma \cdot \chi(\tau), 1, -1)}{\varepsilon(\sigma \cdot \chi(\tau), 1, -1)} = 1 = \partial\mathfrak{a} \cup \mathfrak{a}'(\sigma, \tau),$$

并且若 $\chi(\tau) = \widehat{0}$，那么

$$\partial\varepsilon(\sigma,\tau,\rho) = \frac{\varepsilon(\chi(\sigma),1,-1)}{\varepsilon(\chi(\sigma),1,-1)} = 1 = \partial\mathfrak{a}\cup\mathfrak{a}'(\sigma,\tau).$$

下表以符号方式验证了所有其他可能的情形：

$\chi(\sigma)$	$\sigma\cdot\chi(\tau)$	$\partial\varepsilon(\chi(\sigma)\ \sigma\cdot\chi(\tau)\ -1)\big\vert_{\chi_1'(\sigma)=\chi_1'(\tau)=1}$
$\widehat{1}$	$\widehat{1}$	$\sigma_s(p_1)p_1 = s_1$
$\widehat{j}$	$\widehat{j}$	$\sigma_s(p_{1j})p_{1j} = s_{1j}$
$\widehat{j}$	$\widehat{k}$	$\frac{\sigma_s(p_{1k})p_{1j}}{p_1} = -1$
$\widehat{1}$	$\widehat{k}$	$\frac{\sigma_s(p_{1k})p_1}{p_{1j}} = s_{k1}$
$\widehat{k}$	$\widehat{1}$	$\frac{\sigma_s(p_1)p_{1k}}{p_{1j}} = s_{k1}$

表 2. $\partial\varepsilon\big\vert_{\chi'(\tau)=1,\chi'(\rho)=-1}(\sigma,\tau,\rho) = \partial\mathfrak{a}\cup\mathfrak{a}'(\sigma,\tau,\rho).$

参考文献

[vBF18] Monique van Beek 和 Tom Fisher，通过三次范数方程计算 3-同源 Selmer 群上的 Cassels-Tate 配对，《算术学报》185 (2018)，第 4 期，367–396。↑2

[82] 1982 ↑ Bro

[62] *1* Kenneth S. Brown，《群的上同调》，Springer-Verlag New York，。Cas J.W.S. Cassels，曲线上属的算术。IV. 主猜想的证明。，《纯粹与应用数学杂志》

1962 1962 211, 95 112 ↑ ( ),

[98] 第 - 期。Cas J. W. S. Cassels，椭圆曲线的二次下降，《纯粹与应用数学杂志》

1998 1998 494, 101 127 ↑2 3 6 7 ( )，第 – 期。 , , , CFO

[+08] J. E Cremona、T. A Fisher、C. O'Neil、D. Simon 和 M. Stoll，椭圆曲线上的显式 n-下降，I. 代数，《纯粹与应用数学杂志》2008 (2008)，第 615 期，121–155，DOI doi:10.1515/CRELLE.2008.012。↑2

[Fis22] Tom Fisher，关于二元四次型与 Cassels-Tate 配对，《数论研究》8 (2022)，第 74 期。↑3

[FN14] Tom Fisher 和 Rachel Newton，计算椭圆曲线的 3-Selmer 群上的 Cassels-Tate 配对，《国际数论杂志》 **10** 2014 07, 1881 1907 ↑2

( )，第 - 期。[FSS10] Tom Fisher、Edward F. Schaefer 和 Michael Stoll，Cassels-Tate 配对的瑜伽，《伦敦数学学会计算与数学杂志》13 (2010)，451-460。↑2

[NSW08]Jürgen Neukirch、Alexander Schmidt 和 Kay Wingberg，《数域的上同调》，第 2 版，《数学科学基础丛书》 [数学科学基本原理]，第 323 卷，Springer-Verlag，柏林，2008。https://www.mathi.uni-heidelberg.de/~schmidt/NSW2e/NSW2.3.pdf。MR2392026↑5，6，9

[PS99] Bjorn Poonen 和 Michael Stoll，极化阿贝尔簇上的 Cassels-Tate 配对，《数学年刊》

150 1999 3, 1109 1149 ↑2 3 6 7 8 ( )，第 – 期。 , , ,

[04] , SS Edward F. Schaefer 和 Michael Stoll，如何对椭圆曲线进行 p- 下降，《美国数学会汇刊》 356 (2004，) 第 3 期，1209–1231。↑2

[Shu23] Himanshu Shukla，计算奇数次超椭圆曲线的 Cassels-Tate 配对，2023。准备中。↑3

[Sil09] Joseph H. Silverman，《椭圆曲线的算术》，Springer-Verlag New York，2009。↑1

[Sto12] Michael Stoll，《椭圆曲线上的下降》，《全景与综合》36 (2012)，151–179。↑2

[SD13] Peter Swinnerton-Dyer，椭圆曲线上对所有 n 的 2^n-下降，《伦敦数学会杂志》87 (2013)，第 3 期，707-723。↑2

[Tat63] John Tate，数域伽罗瓦上同调中的对偶定理，《国际数学家大会论文集》（斯德哥尔摩）

1963, 1963, 288 295 ↑ 页 –。

[38] 9 **17** 1938 Wei André Weil，阿贝尔函数的推广，《纯粹与应用数学杂志》（ ） ( )，47–87。↑7

[Ser79] J.P. Serre，《局部域》，Springer-Verlag New York，1979。↑13

拜罗伊特大学数学研究所，德国电子邮件地址：
Himanshu.Shukla@uni-bayreuth.de

数学研究所，拜罗伊特大学，德国电子邮箱地址：
Michael.Stoll@uni-bayreuth.de