arXiv:2602.03251v1 [math.NT] 3 Feb 2026

数域二次扩张上的等差数列中的平方数

ENRIQUE GONZ´ALEZ–JIM´ENEZ

摘要。我们研究数域二次扩张上的平方数算术级数。借鉴莫德尔的一种方法，我们将这类等差数列刻画为一条亏格为 5 的曲线上的二次点。具体而言，在基域 K 满足某些条件时，我们确定该曲线上 K-二次点的集合。我们的主要结果依赖于对特定椭圆曲线进行基变换至适当数域后的代数性质。因此，在适当的假设下，我们证明，定义在 K 的二次扩张上的任何由五个或六个平方数组成的非初等等差数列都必定具有特定形式。此外，我们还证明，在这些假设下，不存在长度大于六的此类等差数列。

1. 引言

对等差数列中平方数的研究可以追溯到费马。具体而言，1640 年，费马声称在 $\mathbb{Q}$ 上不存在由四个平方数组成的等差数列。直到 1780 年，欧拉才证明了这一猜想。

这一研究方向接下来的一个自然问题，是探讨数域中平方数等差数列的性质。回顾一下，在数域 K 上的平方数等差数列由满足 $a_i^2 - a_{i-1}^2 = a_{i+1}^2 - a_i^2$（$i \in \{2, \dots, n-1\}$）的元素 a_1，……，$a_n \in K$ 组成。Xarles[16] 在数域中平方数等差数列的研究方面取得了一项重要成果。他证明，对于任意正整数 d，存在一个函数 $S(d)$，其中 $S(d)$ 仅取决于 d，使得在次数为 d 的任何数域中，都不存在长度为 $S(d)$ 的平方数等差数列。值得注意的是，Xarles 证明了对于二次域，$S(2) = 6$。后来，Bremner 和 Siksek [2]，将这一工作推广，证明了对于三次域，$S(3) = 5$。在特定情形 $d = 2$下，作者与 Steuding [6]，研究了在给定二次域中存在四个平方数的等差数列所需的条件。此外，在与 Xarles [8]，的合作研究中，作者提出了若干判据，用于确定哪些二次数域中存在五个平方数的等差数列。

最近，作者与 Tho [7]，共同研究了这一问题在情形 $d = 4$下的情形，即在四次数域上。特别是，若 D 是无平方因子整数，我们在关于 D的某些条件下刻画了 $K = \mathbb{Q}(\sqrt{D})$的二次扩张上的平方数等差数列。这项研究基于莫德尔 [11]的方法。

在该文章所提出的构造基础上，我们将这一刻画推广到数域的二次扩张。我们注意到，Tho [15] 已宣布他已处理情形 $K = \mathbb{Q}(\zeta_8)$，其中我们用 ζ_m 表示一个本原的 m 次单位根

日期：2026年2月4日。2020 数学主题分类。主要分类：11B25、11G05；次要分类：14G05、14H45。关键词和短语。平方数算术级数、二次扩张、椭圆曲线、有理点。作者获 MCIN/AEI 资助的 PID2022-138916NB-I00资助项目支持，资助协议号为 10.13039/501100011033；此外还获 ERDF「建设欧洲之路」项目支持。

主要　本文的结果基于椭圆曲线的代数结构　s

$$E_0 : y^2 = x^3 - x^2 - 9x + 9,$$
$$E_1 : y^2 = x^3 - x^2 + x,$$
$$E_4 : y^2 = x^3 - x^2 - 64x + 220,$$
$$E_6 : y^2 = x^3 - x^2 - 4x + 4,$$

在对特定数域进行基变换后。对于任意椭圆曲线 E 和整数 D，我们将 E^D 记为 E的 D-二次扭曲。

在本文余下部分中，给定一个数域 K，我们将在某些条件成立的假设下建立结果。这些条件如下：

- $\mathrm{cond}_A(K)$：$E_0(K) = E_0(\mathbb{Q})$，$E_4(K) = E_4(\mathbb{Q})$，以及 $E_6(K) = E_6(\mathbb{Q})$。
- $\mathrm{cond}_B(K)$：秩$_{\mathbb{Z}}\, E_1^{\pm 1}(K) = 0$ 且以下两者之一成立：$[K : \mathbb{Q}] < 8$，或 $[K : \mathbb{Q}]$ 为奇数。

我们将范围限制在情形 $[K : \mathbb{Q}] < 8$，因为计算次数大于 7 的数域上椭圆曲线的秩会变得难以处理。

设 n为正整数，K为一个域。设 $a_1, \ldots, a_n \in K$满足条件，使得 $(a_1^2, a_2^2, \ldots, a_n^2)$ 构成长度为 n的等差数列。对于任意 $s \in K^*$，我们称该等差数列与 $(s^2a_1^2, s^2a_2^2, \ldots, s^2a_n^2)$ 等价，也称其与反向数列 $(a_n^2, \ldots, a_2^2, a_1^2)$ 等价。若等差数列 $(a_1^2, a_2^2, \ldots, a_n^2)$ 满足 $a_1, \ldots, a_n \in K$ 且对于任意真子域 F of K，$\{a_1, \ldots, a_n\} \not\subset F$，则称其正确定义在数域 K上。最后，若一个等差数列与常数等差数列等价，或其中有一个元素为 0，则称该等差数列为初等的。

本文的主要结果如下。

定理 1. 设 K 是一个数域，且满足 $K \neq \mathbb{Q}(\zeta_{12})$。假设 $\mathrm{cond}_A(K)$ 或 $\mathrm{cond}_B(K)$成立。设 L 是 K 的二次扩张。则

(i) 若 K 的类数为 1，则任何在 L 上恰当定义的非初等五平方数等差数列在等价意义下都具有形式 $(a_1^2、\ a_2^2、\ a_3^2、\ \alpha\, a_4^2、\ a_5^2)$，其中 $a_1、\ a_2、\ a_3、a_4、\ a_5、\ \alpha \in K$，且 α 为非平方数。

(ii) 若 $K \neq \mathbb{Q}$ 且 $E_0(K) = E_0(\mathbb{Q})$，则不存在任何在 L 上恰当定义的非初等五平方数等差数列。

前述结果涉及不同于 $\mathbb{Q}(\zeta_{12})$ 的数域。下一个结果专门讨论特定情形 $\mathbb{Q}(\zeta_{12})$。注意，在此情形下，条件 $\mathrm{cond}_B(\mathbb{Q}(\zeta_{12}))$ 成立。

定理 2。在 $\mathbb{Q}(\zeta_{12})$ 的二次扩张上恰当地定义的、除等价外唯一的非初等五平方数等差数列是 $(-3, -1, 1, 3, 5)$，它定义在 $\mathbb{Q}(\zeta_{12}, \sqrt{5})$ 上。

最后，在前述结果的假设下，我们确立了长度大于 5 的非初等等差数列的情形。

定理 *3*。设 K 为一个数域，并假设 $\mathrm{cond}_A(K)$ 或 $\mathrm{cond}_B(K)$ 成立。设 L 为 K 的二次扩张。假设 $E_0(K) = E_0(\mathbb{Q})$，或者如果 $E_0(K) \neq E_0(\mathbb{Q})$，则 K 的类数为 *1*。那么，除等价外，唯一的长度大于 *5* 的非初等平方数等差数列为 $(-5, -3, -1, 1, 3, 5)$，其中 $K = \mathbb{Q}(\zeta_{12})$ 且 $L = K(\sqrt{5})$。

本文的结构如下。在第 2 节中，给定一个数域 K，我们将五个平方数的等差数列描述为亏格为 5 的曲线 $\mathcal{C}$上的 K-有理点。特别地，我们证明定理 4，该定理在某些假设下刻画了数域 K 上 $\mathcal{C}$ 的二次点。该定理的证明依赖于命题 5，其证明见第 4 节。在第 3 节中，我们证明命题 7，说明若 E 是定义在 $\mathbb{Q}$ 上的椭圆曲线，且没有复乘、至少有一个有理 2-扭点，并且 2 是唯一的例外素数，那么 E 的挠子群在任何奇数次的数域上都不会增大。这个结果对于平方数等差数列的研究之外也有独立意义，同时将在奇数次数域的情形中发挥关键作用。利用该刻画

定理 4 中给出的刻画，我们在第 6 节中证明定理 1，并在第 7 节中证明其在$K = \mathbb{Q}(\zeta_{12})$这一特定情形下的结论。第 8 节用于证明定理 3。最后，我们在附录中汇集了全文证明所需的某些亏格为 1 的曲线的相关信息。

本文大量使用计算机代数系统 Magma [1]。本文中所述计算结果的验证代码可在 [3] 获取。

2. 数域上亏格为 5 的曲线上的二次点

设 L 是一个数域，且 $a_1, a_2, a_3, a_4, a_5 \in L$ 不全为零。则 a_1^2、a_2^2、a_3^2、a_4^2 和 a_5^2 成等差数列，当且仅当 $a_2^2 - a_1^2 = a_3^2 - a_2^2, a_3^2 - a_2^2 = a_4^2 - a_3^2$ 和 $a_4^2 - a_3^2 = a_5^2 - a_4^2$。在此情形下，$[a_1 : a_2 : a_3 : a_4 : a_5] \in \mathcal{C}(L) \subset \mathbb{P}^4(L)$，其中 $\mathcal{C}$ 是由以下方程组定义的亏格为 5 的曲线

$$\mathcal{C} : \begin{cases} X_0^2 + X_4^2 = 2X_2^2, \\ X_0^2 + X_2^2 = 2X_1^2, \\ X_2^2 + X_4^2 = 2X_3^2. \end{cases}$$

$\mathcal{C}$ 的第一个方程可在 L 上参数化；也就是说，存在 $t \in L$ 使得

$$[X_0 : X_2 : X_4] = \left[\pm(t^2 - 2t - 1) : \pm(t^2 + 1) : \pm(t^2 + 2t - 1)\right]. \tag{1}$$

因此，$\mathcal{C}$ 可以描述为

$$\mathcal{C} : \begin{cases} X_1^2 = G(t), \\ X_3^2 = G(-t), \end{cases} \tag{2}$$

其中 $G(x) = x^4 - 2x^3 + 2x^2 + 2x + 1$。注意，亏格为 1 的曲线 $C_0 : y^2 = G(x)$ 有两个态射 $\varphi_0, \varphi_0' : \mathcal{C} \longrightarrow C_0$，它们由 $\varphi_0(t, X_1, X_3) = (t, X_1)$ 和 $\varphi_0'(t, X_1, X_3) = (-t, X_3)$ 定义。换言之，当且仅当 $(t, X_1), (-t, X_3) \in C_0(L)$ 时，点 $(t, X_1, X_3) \in \mathcal{C}(L)$。

若 $t \in \{0, \pm 1\}$，我们得到点 $[\pm 1 : \pm 1 : \pm 1 : \pm 1 : \pm 1] \in \mathcal{C}$。我们称点$[X_0 : X_1 : X_2 : X_3 : X_4] \in \mathcal{C}$为平凡点，若它对应于 $t \in \{0, \pm 1\}$，或者对于某个$j \in \{0, \ldots, 4\}$有 $X_j = 0$。下表列出了这些点及其对应的 t 值：

表 1：$\mathcal{C}$ 中的平凡点

t	$[X_0 : X_1 : X_2 : X_3 : X_4]$	
$0, \pm 1$	$[\pm 1 : \pm 1 : \pm 1 : \pm 1 : \pm 1]$	
$\left(\frac{1 \pm \sqrt{-1}}{2}\right)(1 \pm \sqrt{3})$	$[0 : \pm 1 : \pm\sqrt{2} : \pm\sqrt{3} : \pm 2]$	$X_0 = 0$
	$[\pm\sqrt{-1} : 0 : \pm 1 : \pm\sqrt{2} : \pm\sqrt{3}]$	$X_1 = 0$
$\left(\frac{-1 \mp \sqrt{-1}}{2}\right)(1 \pm \sqrt{3})$	$[\pm\sqrt{-2} : \pm\sqrt{-1} : 0 : \pm 1 : \pm\sqrt{2}]$	$X_2 = 0$
	$[\pm\sqrt{3} : \pm\sqrt{2} : \pm 1 : 0 : \pm\sqrt{-1}]$	$X_3 = 0$
$-1 \pm \sqrt{2}$	$[\pm 2 : \pm\sqrt{3} : \pm\sqrt{2} : \pm 1 : 0]$	$X_4 = 0$

$\mathcal{C}$ 中的其他显著点如下：

表2： $\mathcal{C}$中的其他点

t	$[X_0 : X_1 : X_2 : X_3 : X_4]$
$\pm 4(1 \pm \sqrt{5})(1 + \sqrt{-3})$	$[\pm\sqrt{3} : \pm 1 : \pm\sqrt{-1} : \pm\sqrt{-3} : \pm\sqrt{-5}]$
$\frac{-1}{4}(1 \pm \sqrt{5})(1 + \sqrt{-3})$	$[\pm\sqrt{-5} : \pm\sqrt{-3} : \pm\sqrt{-1} : \pm 1 : \pm\sqrt{3}]$
$\pm 4(1 \pm \sqrt{5})(1 - \sqrt{-3})$	$[\pm\sqrt{-3} : \pm\sqrt{-1} : \pm 1 : \pm\sqrt{3} : \pm\sqrt{5}]$
$\frac{-1}{4}(1 \pm \sqrt{5})(1 - \sqrt{-3})$	$[\pm\sqrt{5} : \pm\sqrt{3} : \pm 1 : \pm\sqrt{-1} : \pm\sqrt{-3}]$

现在，假设 $t \notin \{0, \pm 1\}$ 并定义 $s = s(t) = t - \frac{1}{t}$。由式（2）可得

$$\frac{G(\pm t)}{t^2} = t^2 + \frac{1}{t^2} \mp 2\left(t - \frac{1}{t}\right) + 2 = s^2 \mp 2s + 4 \in L^2. \tag{3}$$

另一方面，根据 s的定义，我们还有

$$s^2 + 4 = \left(t + \frac{1}{t}\right)^2 \in L^2.$$

由此我们可以推得

$$\begin{cases} (s^2+4)(s^2-2s+4)(s^2+2s+4) = \left(t+\frac{1}{t}\right)^2 \frac{X_1^2}{t^2}\frac{X_3^2}{t^2} \in L^2, \\ s^2(s^2-2s+4)(s^2+2s+4) = \left(t-\frac{1}{t}\right)^2 \frac{X_1^2}{t^2}\frac{X_3^2}{t^2} \in L^2. \end{cases}$$

定义 $r = r(t) = s^2$，则前述方程变为

$$\begin{cases} (r+4)(r^2+4r+16) \in L^2, \\ r(r^2+4r+16) \in L^2. \end{cases}$$

前述构造使我们能够得到六条亏格一曲线 C_i, $i = 1, \ldots, 6$，以及相应的态射 $\varphi_i : \mathcal{C} \longrightarrow C_i$，如表3所示。

表3：曲线与态射

C_i	方程	$\varphi_i(t, \ X_1, \ X_3)$
C_1	$y^2 = (x+4)(x^2+4x+16)$	$\left(r, \left(t^{-1}+t^{-3}\right) X_1X_3\right)$
C_2	$y^2 = x(x^2+4x+16)$	$\left(r, \left(t^{-1}-t^{-3}\right) X_1X_3\right)$
C_3	$y^2 = x(x+4)(x^2+4x+16)$	$\left(r, \left(1-t^{-4}\right) X_1X_3\right)$
C_4	$y^2 = x(x^2+14x+1)$	$(t^4, \ t^2X_1X_3)$
C_5	$y^2 = x^4+4x^2+16$	$(s, \ t^{-2}X_1X_3)$
C_6	$y^2 = x^4+14x^2+1$	$(t^2, \ X_1X_3)$

本文在满足特定条件的情况下，确定了由下式给出的 K-二次点集合： $\mathcal{C}$

$$\Gamma_2(\mathcal{C}, K) = \bigcup \{\mathcal{C}(L) \, : \, K \subset L \subset \overline{\mathbb{Q}} \text{ and } [L : K] = 2\},$$

关于域 K的某些假设。

设 F为类数为 1 的数域。若 $(t, u) \in C_0(F)$，我们定义

$$\mathcal{P}_1(t, u) := \left\{[\pm(t^2 - 2t - 1) : \pm u : \pm(t^2+1) : \pm v\sqrt{m} : \pm(t^2+2t-1)]\right\} \subset \mathbb{P}^4(F),$$

其中 $G(-t) = m\, v^2$；若 $(-t, v) \in C_0(F)$，则定义

$$\mathcal{P}_3(-t, v) := \left\{[\pm(t^2 + 2t - 1) : \pm u\sqrt{n} : \pm(t^2+1) : \pm v : \pm(t^2-2t-1)]\right\} \subset \mathbb{P}^4(F),$$

其中 $G(t) = n\,u^2$。接着定义集合

$$\mathcal{S}_1(F) := \bigcup_{(t,u)\in C_0(F)} \mathcal{P}_1(t,u) \quad \text{and} \quad \mathcal{S}_3(F) := \bigcup_{(-t,v)\in C_0(F)} \mathcal{P}_3(-t,v).$$

为清晰起见，分别记去除表 1 中所列平凡点后的集合 $\Gamma_2^*(\mathcal{C},\ F)$、$\mathcal{S}_1^*(F)$ 和 $\mathcal{S}_3^*(F)$ 为 $\Gamma_2(\mathcal{C},\ F)$、$\mathcal{S}_1(F)$ 和 $\mathcal{S}_3(F)$。我们定义由表2产生的集合 $\mathcal{T}$和$\mathcal{P}_{\mathcal{T}}$。集合

$$\mathcal{T} := \{\pm\frac{1}{4}(1\pm\sqrt{5})(1\pm\sqrt{-3})\}$$

对应于表2的第一列。另一方面，集合

$$\mathcal{P}_{\mathcal{T}} := \left\{ \begin{array}{c} [\pm\sqrt{3}:\pm1:\pm\sqrt{-1}:\pm\sqrt{-3}:\pm\sqrt{-5}],\quad [\pm\sqrt{-5}:\pm\sqrt{-3}:\pm\sqrt{-1}:\pm1:\pm\sqrt{3}], \\ [\pm\sqrt{-3}:\pm\sqrt{-1}:\pm1:\pm\sqrt{3}:\pm\sqrt{5}],\quad [\pm\sqrt{5}:\pm\sqrt{3}:\pm1:\pm\sqrt{-1}:\pm\sqrt{-3}] \end{array} \right\}.$$

由曲线 $\mathcal{C}$ 上定义在 $\mathbb{Q}$ 上的非平凡点组成，这些点出现在表2的第二列，并与 $\mathcal{T}$中的值相关联。

定理 4。设 K 为一个数域，且 $K \neq \mathbb{Q}(\zeta_{12})$。假设 $cond_A(K)$ 或 $cond_B(K)$ 成立。则：

(i) 若 K 的类数为 1，则 $\Gamma_2^*(\mathcal{C}、K) = \mathcal{S}_1^*(K) \cup \mathcal{S}_3^*(K)$。
(ii) 若 $E_0(K) = E_0(\mathbb{Q})$，则 $\Gamma_2^*(\mathcal{C}、K) = \mathcal{S}_1^*(\mathbb{Q}) \cup \mathcal{S}_3^*(\mathbb{Q})$。
在特殊情形 $K = \mathbb{Q}(\zeta_{12})$ 下，我们有 $\Gamma_2^*(\mathcal{C}、\mathbb{Q}(\zeta_{12}) = \mathcal{S}_1^*(\mathbb{Q}) \cup \mathcal{S}_3^*(\mathbb{Q}) \cup \mathcal{P}_{\mathcal{T}}$.

定理 4 的证明依赖于以下结果。

命题 5。设 K 是一个数域，并假设 $cond_A(K)$ 或 $cond_B(K)$ 成立。设 L 是 K 的二次扩张，并令 $(t、X_1、X_3) \in \mathcal{C}(L)$ 为满足 $t \notin \mathcal{T}$ 的非平凡点。则要么 $(t、X_1) \in C_0(K)$，要么 $(-t、X_3) \in C_0(K)$。

3. 挠点不增长的一个结果

在本节中，我们将证明一个关于在某些假设下椭圆曲线的挠点增长的结果。该结果本身具有独立的研究意义。然而，它是针对奇数次数数域推导引言中所述主要结果的关键部分。

设 E 是定义在 $\mathbb{Q}$ 上的椭圆曲线。设 p 是一个素数，并令 $G_E(p)$ 表示模 p 伽罗瓦表示在 E 的 p-挠点上的像（在 $\mathrm{GL}_2(\mathbb{F}_p)$ 中相差共轭）。若 $G_E(p) \neq \mathrm{GL}_2(\mathbb{F}_p)$，则称 p 对于 E 是异常的。在 $p = 2$ 的情形下，众所周知（参见 [12, 13, 17]），$G_E(2)$ 是以下群之一：

$$\mathrm{GL}_2(\mathbb{F}_2),\quad B(2),\quad \mathrm{C}_{ns}(2),\quad \text{or}\quad \mathrm{C}_s(2),$$

其中 $B(2)$（分别为 $\mathrm{C}_{ns}(2)$、$\mathrm{C}_s(2)$）表示 $\mathrm{GL}_2(\mathbb{F}_2)$ 的 Borel 子群（分别为非分裂 Cartan 子群、分裂 Cartan 子群）。注意，$\mathrm{C}_s(2)$ 是平凡群。

引理 6. 设 E 是定义在 $\mathbb{Q}$ 上且没有复乘的椭圆曲线，并设 $P \in E(\mathbb{Q})$ 是一个阶为2的幂的点。

(i) 若 $G_E(2)$ 是 $B(2)$ 或 $\mathrm{C}_s(2)$，则 $[\mathbb{Q}(P):\mathbb{Q}] = 2^n$ 对某个 $n \geq 0$ 成立。
(ii) 若 $G_E(2)$ 是 $\mathrm{GL}_2(\mathbb{F}_2)$ 或 $\mathrm{C}_{ns}(2)$，则 $[\mathbb{Q}(P):\mathbb{Q}] = 3\cdot 2^n$ 对某个 $n \geq 0$ 成立。

证明。假设 $\mathrm{ord}(P) = 2^m$ 对某个 $m \geq 1$成立。如果 $m = 1$（见 [4, 表 1]）：

$$[\mathbb{Q}(P):\mathbb{Q}] = \begin{cases} 1 & \text{if } G_E(2) = \mathrm{C}_s(2), \\ 1 \text{ or } 2 & \text{if } G_E(2) = B(2), \\ 3 & \text{if } G_E(2) = \mathrm{GL}_2(\mathbb{F}_2) \text{ or } \mathrm{C}_{ns}(2). \end{cases} \tag{4}$$

如果 $m > 1$，考虑域塔

$$\mathbb{Q} = \mathbb{Q}(2^m P) \subseteq \mathbb{Q}(2^{m-1}P) \subseteq \cdots \subseteq \mathbb{Q}(2P) \subseteq \mathbb{Q}(P),$$

因此

$$[\mathbb{Q}(P) : \mathbb{Q}] = \prod_{k=0}^{m-1} [\mathbb{Q}(2^k P) : \mathbb{Q}(2^{k+1}P)].$$

根据 [4, T heorem 4.6], 当 $k \neq m-1$ 时，我们有 $[\mathbb{Q}(2^k P) : \mathbb{Q}(2^{k+1}P)] \in \{1, 2, 4\}$，因此

$$[\mathbb{Q}(P) : \mathbb{Q}] = 2^s \cdot [\mathbb{Q}(2^{m-1}P) : \mathbb{Q}]$$

其中某个 s为整数。最后，由于 $2^{m-1}P$ 是一个 2 阶点，结论由 (4) 得出。 □

命题 7. 设 E 是定义在 $\mathbb{Q}$ 上的椭圆曲线，且没有复乘，至少有一个有理 *2* 阶挠点，并且 2 是唯一的例外素数。那么

$$|E(\mathbb{Q})_{\text{tors}}| = 2^n \quad \textit{for some } n \in \{1, 2, 3, 4\}.$$

此外，如果 K 是奇数次数域，那么 $E(K)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$。

证明。 由于 2 是 E 的唯一例外素数，且 E 至少有一个有理 2-扭点，因此

- $G_E(2)$ 要么是 $B(2)$，要么是 $C_s(2)$（见（4）），
- 对于每个奇素数 p，$G_E(p) = \mathrm{GL}_2(\mathbb{F}_p)$。

特别地，如果 $P \in E(\mathbb{Q})$ 是一个阶为奇素数 p 的点，那么根据 [9, 定理 5.1]，$[\mathbb{Q}(P) : \mathbb{Q}] = p^2 - 1$。由于 $p^2 - 1$ 是偶数，因此这样的点不可能定义在任何奇数次的数域上。特别地，$E(\mathbb{Q})$ 不含奇数阶的挠点。根据 Mazur 分类 [10],，我们因此有 $|E(\mathbb{Q})_{\text{tors}}| = 2^n$，其中某个 $n \in \{1, 2, 3, 4\}$。

现在我们继续证明该命题的第二部分。设 K 是一个奇数次数域。如上所示，$E(K)_{\text{tors}}$ 不可能包含阶被某个奇素数整除的点。此外，根据引理 6 (i)，在奇数次数域上不会出现新的 2 的幂次阶挠点。因此，挠子群从 $\mathbb{Q}$ 到 K 不会增长，从而我们得到

$$E(K)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}.$$

证明完毕。 □

注 8。 对于椭圆曲线 E_0，$E_1^{\pm 1}$，E_4 和 $E_6^{\pm 1}$，唯一的例外素数是 2。因此，命题 7 表明，如果 K 是一个奇数次数域，那么对于这些椭圆曲线中的任意一条，挠子群在 K 上都不会增长。特别地，如果 $\mathrm{rank}_{\mathbb{Z}} E_1^{\pm 1}(K) = 0$，则 $\mathrm{cond}_A(K)$ 成立，因为 E_1，E_4 和 E_6 属于同一个 $\mathbb{Q}$-同源类。

4. 命题 5 的证明

设 K 是一个数域，且 L 是 K 的二次扩张。假设 $(t,\ X_1,\ X_3) \in \mathcal{C}(L)$ 是一个未出现在表 1 或表 2 中的点。我们旨在证明，或者 $(t,\ X_1) \in C_0(K)$，或者 $(-t,\ X_3) \in C_0(K)$。

为此，我们将证明分为几个步骤。首先，证明 $r = r(t) \in K$；然后，证明 $s = s(t) \in K$；之后，推出 $t \in K$；最后，得出结论：或者 $(t,\ X_1) \in C_0(K)$，或者 $(-t,\ X_3) \in C_0(K)$。

注9. 证明依赖于对亏格一曲线 C_i 上 K-有理点集合的计算，其中 $i = 0,\ 1,\ \ldots,\ 6$。表 4 列出了相应的 $\mathbb{Q}$-同构椭圆曲线，即 $E_0,\ E_1,\ E_1^{-1},\ E_1,\ E_4,\ E_6^{-1}$ 和 E_6。

注意到，由于 $\mathrm{rank}_{\mathbb{Z}}\, E_1^{\pm 1}(\mathbb{Q}) = 0$，且曲线 E_1，E_4，E_6 是 $\mathbb{Q}$-同源的，因此条件 $\mathrm{cond}_A(K)$ 和 $\mathrm{cond}_B(K)$ 可归结为控制这些曲线及其在 K 上的（-1）-二次扭曲的挠子群。特别地，我们有以下结论：

- 若 $\mathrm{cond}_A(K)$ 成立，则对每个 $i = 1, \ldots\ldots, 6$，均有 $C_i(K) = C_i(\mathbb{Q})$。
- 若 $\mathrm{cond}_B(K)$ 成立，则在 $[K : \mathbb{Q}]$ 为奇数的情形中，注 8 保证 $\mathrm{cond}_A(K)$ 成立，因此论证可归结为前一情形。若 $[K : \mathbb{Q}] < 8$，则条件 $Ш_{\mathbb{Z}}\, E_1^{\pm 1}(K) = 0$ 蕴含：对 $i = 1, \ldots\ldots, 6$，$C_i(K)$ 中尚未落在 $C_i(\mathbb{Q})$ 内的唯一点，对应于相关椭圆曲线的挠子群在 K 上增大的那些点。回顾可知，对于定义在 $\mathbb{Q}$ 上的椭圆曲线 E，仅存在有限多个给定次数的数域，使得 $E(\mathbb{Q})\mathrm{tors} \neq E(K)\mathrm{tors}$。在我们的设定中，所有满足 $[K : \mathbb{Q}] < 8$ 的此类域均在附录中明确列出。特别地，在假设 $Ш_{\mathbb{Z}}\, E_1^{\pm 1}(K) = 0$ 下，所考虑曲线的挠子群可能增大的、$\mathbb{Q}$ 上次数小于 8 的仅有的域，是二次域 $\mathbb{Q}(\sqrt{-3})$、$\mathbb{Q}(\sqrt{-1})$、$\mathbb{Q}(\sqrt{2})$ 与 $\mathbb{Q}(\sqrt{3})$，以及四次数域 $\mathbb{Q}(\zeta_8)$、$\mathbb{Q}(\zeta_{12})$、$\mathbb{Q}(\alpha)$ 与 $\mathbb{Q}(\beta)$，其中 α 的最小多项式为 $x^4 - 3x^2 + 3$，而 β 的最小多项式为 $x^4 - 2x^3 - 2x + 1$。

$\boxed{r \in K}$ 假设 $r \notin K$。由于 $[L : K] = 2$，可得 $L = K(r)$，特别地，r 在 K 上的最小多项式是二次多项式 $Q(x) \in K[x]$。因此，对于 $i = 1, 2$，有 $\varphi_i(t, X_1, X_3) = (r, \alpha_i + \beta_i r) \in C_i(L)$，其中某些 $\alpha_1, \alpha_2, \beta_1, \beta_2 \in K$ 满足条件。因此，存在 $r_1, r_2 \in K$ 使得

$$\begin{aligned}(x+4)\left(x^2+4x+16\right) - (\alpha_1+\beta_1 x)^2 &= Q(x)\,(x-r_1)\,,\\ x\left(x^2+4x+16\right) - (\alpha_2+\beta_2 x)^2 &= Q(x)\,(x-r_2)\,.\end{aligned}$$

因此，$(r_i, \alpha_i + \beta_i r_i) \in C_i(K)$。对于 $P_1 = (x_1, y_1) \in C_1(K)$ 和 $P_2 = (x_2, y_2) \in C_2(K)$，令 $Q_{\beta_1}(x) Q_{\beta_2}(x) \in K[x]$ 满足

$$\begin{aligned}(x+4)\left(x^2+4x+16\right) - (y_1-\beta_1 x_1+\beta_1 x)^2 &= Q_{\beta_1}(x)\,(x-x_1)\,,\\ x\left(x^2+4x+16\right) - (y_2-\beta_2 x_2+\beta_2 x)^2 &= Q_{\beta_2}(x)\,(x-x_2)\,.\end{aligned}$$

我们求解由等式 $Q_{\beta_1}(x) = Q_{\beta_2}(x)$ 导出的二次方程组。若存在解 $\beta_1, \beta_2 \in K$，则得到一个多项式 $Q(x)$。我们舍去 $\deg Q(x) = 1$ 的情形，因为 $[K(r) : K] = 2$。

接下来，我们施加条件 $r = s^2$ 属于 L。若存在这样的元素 s，我们由等式 $t^2 - st - 1 = 0$ 计算 t。最后，我们验证 $t \in L$，并且 $G(t)$ 与 $G(-t)$ 在 L 中均为平方。

现在，借助注 9，在 $\mathrm{cond}_A(K)$ 成立，或者处于 $\mathrm{cond}_B(K)$ 且 $[K : \mathbb{Q}]$ 为奇数的情形下，只需在 $K = \mathbb{Q}$ 上完成前述计算与验证。对于其余 $\mathrm{cond}_B(K)$ 成立且 $[K : \mathbb{Q}] < 8$ 的情形，我们参考表 5，具体是对应于情形 E_1 与 E_1^{-1} 的列。在这些情形中，分析归结为有限个数域的列表，即：

$$\mathbb{Q},\quad \mathbb{Q}(\sqrt{-3}),\quad \mathbb{Q}(\sqrt{-1}),\quad \mathbb{Q}(\sqrt{3}),\quad \mathbb{Q}(\zeta_8),\quad \mathbb{Q}(\zeta_{12}),\quad \mathbb{Q}(\alpha),\quad \text{and}\quad \mathbb{Q}(\beta).$$

对这些域中的每一个，以及对每一对可能的点 $P_1 \in C_1(K)$ 与 $P_2 \in C_2(K)$，均可验证 $r \in K$，除情形 $K = \mathbb{Q}(\zeta_{12})$ 外，此时我们得到 $r \in \left\{\frac{1}{2}(-15 \pm \sqrt{-15})\right\}$。然而，这些异常值对应于 $t \in \mathcal{T}$，而它们在命题 5 的陈述中被明确排除。因此，在所有相关情形中，我们得出 $r \in K$。

$\boxed{s \in K}$ 假设 $r \in K$ 和 $s \notin K$。由于 $[L : K] = 2$，可得 $L = K(s)$，特别是 $r = s^2 \notin K^2$。因此，由 (3) 可知，存在 $\mu, \psi \in K$ 使得 $s^2 \pm 2s + 4 = (\mu \pm \psi s)^2$。由于 $s^2 = r \in K$，我们得到

$$r^2 + 4r + 16 = \left(s^2 - 2s + 4\right)\left(s^2 + 2s + 4\right) = \left(\mu^2 - s^2\psi^2\right)^2 = \left(\mu^2 - r\psi^2\right)^2 \in K^2. \tag{5}$$

由于 $t^2 - st - 1 = 0$，我们有 $t = (s \pm \alpha)/2$，其中 $\alpha \in K$ 满足 $\alpha^2 = s^2 + 4 = r + 4$。我们将证明分为两种情形：

- 情形 $r + 4 \in K^2$。将此与 (5) 结合，我们得到 $(r + 4)\left(r^2 + 4r + 16\right) \in K^2$。因此，$\varphi_1(t, X_1, X_3) = (r, \left(t^{-1} + t^{-3}\right) X_1 X_3)) \in C_1(K)$。
- 情形 $r + 4 \notin K^2$。在此情形下，$L = K(s) = K(\alpha)$，这意味着 $s\alpha \in K$。因此 $r(r + 4) \in K^2$。将此与 (5) 结合，我们得到 $\varphi_3(t, X_1, X_3) = (r, \left(1 - t^{-4}\right) X_1 X_3) \in C_3(K)$。

与前一种情形一样，由于注9，所需的计算可归结为分析表5，具体而言是曲线 C_1 和 C_3，它们对应于椭圆曲线 E_1。在此情形下，域 K 是以下数域之一：

$$\mathbb{Q}, \quad \mathbb{Q}(\sqrt{-3}), \quad \mathbb{Q}(\sqrt{-1}), \quad \mathbb{Q}(\sqrt{3}), \quad \text{and} \quad \mathbb{Q}(\zeta_{12}).$$

对于这些情形中的每一种，以及 $C_1(K)$或 $C_3(K)$中的每一个点，令 r 表示其第一个坐标。由恒等式 $r = \left(t - \frac{1}{t}\right)^2 \notin K^2$，我们解出 t，从而得到 $L = K(s) = K(t)$。最后，我们验证条件 $G(t) \in L^2$ 与 $G(-t) \in L^2$ 永远不会同时成立。因此，我们得出结论 $s \in K$。

$\boxed{t \in K}$ 假设 $r,\ s \in K$ 且 $t \notin K$。由于 $[L :\ K] = 2$，由此可得 $L = K(t)$。我们有如下恒等式：

$$\begin{cases} t^2 = st + 1, \\ t^4 = (s^2 + 2)t^2 - 1, \\ t^8 = (s^4 + 4s^2 + 2)t^4 - 1. \end{cases}$$

由第一个等式我们推出 $t^2 \notin K$，因为 $s \neq 0$，否则 $t = \pm 1$。由第二个等式，我们有 $t^4 \notin K$，否则 $s^2 + 2 = 0$ 与 t 将是一个本原八次单位根，记作$t = \zeta_8$。在此情形下，$L = \mathbb{Q}(\zeta_8)$，但 $G(\zeta_8) \notin L^2$。

因此，若记 $w = t^4$，则有 $L = K(w)$，并且由第三条恒等式可知，w 在 K 上的最小多项式为

$$F(x) = x^2 - (s^4 + 4s^2 + 2)x + 1 \in K[x]. \tag{6}$$

另一方面，我们有 $\varphi_4(t, X_1, X_3) = (t^4, t^2 X_1, X_3) \in C_4(L)$。因此，存在 $\alpha, \beta \in K$使得

$$w(w^2 + 14w + 1) = (\alpha + \beta w)^2.$$

换言之，存在 $\omega_0 \in K$ 使得

$$x(x^2 + 14x + 1) - (\alpha + \beta x)^2 = F(x)(x - \omega_0).$$

因此，$(\omega_0, \alpha + \beta\omega_0) \in C_4(K)$。

对任意点 $P = (x_0, y_0) \in C_4(K)$，我们有

$$x(x^2 + 14x + 1) - (y_0 - \beta x_0 + \beta x)^2 = F_\beta(x)(x - x_0). \tag{7}$$

考虑点 $(0, 0) \in C_4(K)$。于是我们得到 $F_\beta(x) = x^2 + (14 - \beta^2)x + 1$。与 (6) 比较，我们推出 $14 - \beta^2 = -(s^4 + 4s^2 + 2)$，从而 $s^4 + 4s^2 + 16 = \beta^2$。因此，$(s, \beta) \in C_5(K)$。

令 $P = (x_0, y_0) \in C_4(K)$，其中 $P \neq (0,0)$。将 $F_\beta(x)$ 代入 (7) 计算，并与 (6) 比较，得到以下方程组：

$$\begin{cases} \beta^2 x_0 - 2\beta y_0 + x_0^2 + 14x_0 = 0, \\ s^4 + 4s^2 + x_0 + 16 - \beta^2 = 0. \end{cases}$$

特别地，它必须有解 $\beta, s \in K$。在这种情形下，多项式 $x^2 - sx - 1$ 必须在 K 上不可约。最后，我们需要验证 $G(t)$ 和 $G(-t)$ 在 $L = K(t)$ 中都是平方数。

再一次，注9确保在考虑情形 $(0,\ 0) \in C_4$ 时，必须使用有限个数域上的曲线 $C_5(K)$ 上的点进行必要的计算和验证

。根据表5，在对应于这条曲线的列中，即 E_6^{-1}，相关的数域为 K

$$\mathbb{Q}, \quad \mathbb{Q}(\sqrt{-3}), \quad \mathbb{Q}(\sqrt{-1}), \quad \mathbb{Q}(\sqrt{3}), \quad \mathbb{Q}(\zeta_8), \quad \mathbb{Q}(\zeta_{12}), \quad \text{and} \quad \mathbb{Q}(\beta).$$

在所有这些情形下，我们验证了 $t \in K$。

最后，当 $P \neq (0, 0)$ 时，我们参考表5，具体来说是与曲线C_4对应的那一列，即 E_4。相关的数域为

$$\mathbb{Q}, \quad \mathbb{Q}(\sqrt{2}), \quad \text{and} \quad \mathbb{Q}(\sqrt{3}).$$

同样，我们得出结论，在所有这些情形下， $t \in K$。

这就完成了对 $t \in K$ 的证明。

最后一步 假设 r， s， $t \in K$。由于 $[L: K] = 2$，存在 $\alpha \notin K$ 使得 $\alpha^2 \in K$ 且$L = K(\alpha)$。根据 (2)，存在 γ_1， δ_1， γ_3， $\delta_3 \in K$ 使得 $X_1 = \delta_1 + \gamma_1\alpha$ 且 $X_3 = \delta_3 + \gamma_3\alpha$，并且我们有

$$\begin{cases} G(t) = (\delta_1 + \gamma_1\alpha)^2, \\ G(-t) = (\delta_3 + \gamma_3\alpha)^2. \end{cases}$$

由于 $t \in K$ 和 $\alpha \notin K$，我们推得 $\gamma_1\delta_1 = \gamma_3\delta_3 = 0$。因此，共有四种可能的情形:

- $\gamma_1 = \gamma_3 = 0$。在这种情形下， $\varphi_6(t, X_1, X_3) = (t^2, \delta_1\delta_3) \in C_6(K)$。
- $\delta_1 = \delta_3 = 0$。等价地， $\varphi_6(t, X_1, X_3) = \left(t^2, \alpha^2\gamma_1\gamma_3\right) \in C_6(K)$。
- $\gamma_1 = \delta_3 = 0$。我们有 $\varphi_0(t, X_1, X_3) = (t, \delta_1) \in C_0(K)$。特别地， $X_1 = \delta_1$。
- $\delta_1 = \gamma_3 = 0$。我们得到 $\varphi_0'(t, X_1, X_3) = (-t, \delta_3) \in C_0(K)$。特别地， $X_3 = \delta_3$。

为完成命题 5 的证明，还需证明情形 $\gamma_1 = \gamma_3 = 0$和$\delta_1 = \delta_3 = 0$ 不可能成立。再次利用注9，这归结为分析表5中对应于 C_6 的列，即椭圆曲线 E_6。必须进行计算的相关数域为 $\mathbb{Q}$、 $\mathbb{Q}(\zeta_8)$ 和 $\mathbb{Q}(\zeta_{12})$。对于这些域中的每一个，以及每个点 $(x_0, y_0) \in C_6(K)$，我们都必须验证 $x_0 = t^2 \in K^2$ 是否成立。此外，在所有此类情形中，我们舍弃那些在 $\mathcal{C}$上产生平凡点的情形，例如满足 $x_0 \in \{0, \pm 1\}$ 或 $y_0 = 0$的情形。通过这一分析没有得到任何可接受的情形。命题 5 的证明至此完成。

5. 定理 4 的证明

设 K 为一个数域，并假设 $\mathrm{cond}_A(K)$ 或 $\mathrm{cond}_B(K)$ 成立。设 L为 K的一个二次扩张，并令 $(t, X_1, X_3) \in \mathcal{C}(L)$ 为一个非平凡点。我们根据 $t \in \mathcal{T}$是否成立来分别进行证明。

首先，假设 $t \notin \mathcal{T}$。那么由命题 5 可知， $(t, X_1) \in C_0(K)$ 或 $(-t, X_3) \in C_0(K)$。进一步假设 K 的类数为 1。当 $(t, X_1) \in C_0(K)$ 时，存在元素 $u = X_1, v, m \in K$ ，使得 $G(t) = u^2$ ，且 $G(-t) = mv^2$。另一方面，若 $(-t, X_3) \in C_0(K)$，则存在元素 $v = X_3, u, n \in K$ ，使得 $G(t) = nu^2$ ，且$G(-t) = v^2$。

由第 2 节给出的参数化 (1)，可推出 $[X_0 : X_1 : X_2 : X_3 : X_4]$属于 $\mathcal{P}_1(t, u)$，当 $(t, X_1) \in C_0(K)$ 时；而当 $(-t, X_3) \in C_0(K)$ 时， $[X_0 : X_1 : X_2 : X_3 : X_4]$属于 $\mathcal{P}_3(-t, v)$。这证明了定理 4 的 (i) 部分。

此外，如果 $E_0(K) = E_0(\mathbb{Q})$，那么 $C_0(K) = C_0(\mathbb{Q})$，因此 $t, X_1 \in \mathbb{Q}$ 或 $t, X_3 \in \mathbb{Q}$，这就证明了（ii）部分。这就完成了情形 $t \notin \mathcal{T}$下定理 4 的证明。

现在我们假设 $t \in \mathcal{T}$。那么相应的点集为 $\mathcal{P}_{\mathcal{T}}$ （见表2）。特别地，我们有 $\sqrt{-1}, \sqrt{3}, \sqrt{5} \in L$。因此， K 必须包含在 $\mathbb{Q}(\sqrt{-1}, \sqrt{3}, \sqrt{5})$ 中，且$[L: K] \leq 2$。在满足这些性质的所有可能数域 K 中，唯一使得 $\mathrm{cond}_A(K)$ 或 $\mathrm{cond}_B(K)$ 成立的是 $K = \mathbb{Q}(\zeta_{12})$。因此，我们有 $\mathcal{P}_{\mathcal{T}} \subset \mathcal{C}(K(\sqrt{5})) \subset \Gamma_2^*(\mathcal{C}, \mathbb{Q}(\zeta_{12}))$。

此外，由于 $E_0(\mathbb{Q}(\zeta_{12})) = E_0(\mathbb{Q})$，对 (ii) 的证明作类似论证可得

$$\Gamma_2^*(\mathcal{C}, \mathbb{Q}(\zeta_{12})) = \mathcal{S}_1^*(\mathbb{Q}) \cup \mathcal{S}_3^*(\mathbb{Q}) \cup \mathcal{P}_{\mathcal{T}}.$$

这就完成了定理 4 的证明。

6. 定理 1 的证明

设 K 是一个满足 $K \neq \mathbb{Q}(\zeta_{12})$ 的数域，并假设 $\mathrm{cond}_A(K)$ 或 $\mathrm{cond}_B(K)$ 成立。设 L 是 K 的二次扩张。如第 2 节所示，任何五个平方数的等差数列 $(a_1^2,\ a_2^2,\ a_3^2,\ a_4^2,\ a_5^2)$，只要满足 $a_1,\ a_2,\ a_3,\ a_4,\ a_5 \in L$，就对应于 $\mathcal{C}(L)$ 上的一个点，反之亦然。

现在假设 K 的类数为 1。利用定理 4 给出的刻画，我们可以分析可能的五个平方数的等差数列。也就是说，对于每个点 $(t,\ u) \in C_0(K)$，我们可以得到一个由 $\mathcal{P}_1(t,\ u)$ 产生的等差数列，其形式如下：

$$((t^2-2t-1)^2,\, u^2,\, (t^2+1)^2,\, mv^2,\, (t^2+2t-1)^2).$$

注意，若 $m \in K^2$，则上述等差数列已定义在 K 上；因此，它并非恰好定义在 K 的任何二次扩张上。对于每个点 $(-t,\ v) \in C_0(K)$，我们得到一个由 $\mathcal{P}_3(-t,\ v)$ 导出的等差数列，其形式为：

$$((t^2+2t-1)^2,\, nu^2,\, (t^2+1)^2,\, v^2,\, (t^2-2t-1)^2).$$

（情形 $n \in K^2$ 与情形 $m \in K^2$ 类似，并可得出相同结论。）注意，最后这个等差数列与其逆序等价，因此，任何恰好定义在 L 上的非平凡五平方数等差数列，在等价意义下都具有形式 $(a_1^2,\ a_2^2,\ a_3^2,\ \alpha a_4^2,\ a_5^2)$，其中 $a_1,\ a_2,\ a_3,\ a_4,\ a_5,\ \alpha \in K$，且 α 是 K 中的一个非平方数。至此，(i) 部分的证明完成。

现在证明 (ii) 部分。设 $K \neq \mathbb{Q}$ 且 $E_0(K) = E_0(\mathbb{Q})$。与前一种情形一样，所有相关点都满足 $(t,\ u) \in C_0(\mathbb{Q})$ 或 $(-t,\ v) \in C_0(\mathbb{Q})$。因此，任何相应的非平凡五平方数等差数列都定义在某个 $\mathbb{Q}(\sqrt{m})$ 上，其中 $m \in \mathbb{Q}$ 是无平方因子的，但该数列并非恰好定义在 L 上。这就证明了 (ii) 部分。

7. 定理 2 的证明

在定理 4 中，我们证明了 $\Gamma_2^*(\mathcal{C},\ \mathbb{Q}(\zeta_{12})) = \mathcal{S}_1^*(\mathbb{Q}) \cup \mathcal{S}_3^*(\mathbb{Q}) \cup \mathcal{P}_{\mathcal{T}}$。因此，仿照定理 1 (ii) 的证明中的论证，任何由 $\mathcal{S}_1^*(\mathbb{Q}) \cup \mathcal{S}_3^*(\mathbb{Q})$ 中的点所产生的非初等等差数列的五个平方数，都定义在 $\mathbb{Q}$ 的某个二次扩张上，因此不能适当地定义在 $\mathbb{Q}(\zeta_{12})$ 的某个二次扩张上。

剩下要考虑的是 $\mathcal{P}_{\mathcal{T}}$ 中的点。由这些点，我们得到以下定义在 $L = \mathbb{Q}(\zeta_{12},\ \sqrt{5})$ 上的五平方数等差数列：

$$(3,1,-1,-3,-5), \quad (-5,-3,-1,1,3), \quad (-3,-1,1,3,5), \quad (5,3,1,-1,-3).$$

这些数列在 L 上都等价于数列 $(-3,\ -1,\ 1,\ 3,\ 5)$。证明至此完成。

8. Proof of Theorem 3

设 K 是一个满足 $\mathrm{cond}_A(K)$ 或 $\mathrm{cond}_B(K)$ 的数域，并设 L 是 K 的一个二次扩张。定理 3 是定理 1 和定理 2 的推论。

我们首先证明，若 $K \neq \mathbb{Q}(\zeta_{12})$，则任何在 L 上正确定义的非初等五平方数等差数列都无法扩展为六平方数等差数列。

假设在 L 上存在一个定义良好的非初等六平方数等差数列，即 $(a_1^2,\ a_2^2,\ a_3^2,\ a_4^2,\ a_5^2,\ a_6^2)$。那么，$(a_1^2,\ a_2^2,\ a_3^2,\ a_4^2,\ a_5^2)$ 或 $(a_2^2,\ a_3^2,\ a_4^2,\ a_5^2,\ a_6^2)$ 是在 L 上定义良好的非初等五个平方数的等差数列。现在我们来考察 K 的不同可能性：

- 如果 $K=\mathbb{Q}$，那么众所周知，在任意 $\mathbb{Q}$ 的二次扩张上都不存在非恒定的六平方数等差数列（参见 [16]）。
- 若 $K\neq\mathbb{Q}$ 且 $E_0(K)=E_0(\mathbb{Q})$，则定理 1(ii) 表明，无法在 L上正确定义非初等五平方数等差数列，因此不存在长度为六的此类等差数列。
- 否则，我们假设 K 的类数为 1。在此情形下，定理 1(i) 适用，任何在 L上正确定义的非初等五平方数等差数列，都等价于形如 $\left(x_1^2,\ x_2^2,\ x_3^2,\ \alpha x_4^2,\ x_5^2\right)$ 的等差数列，其中 $x_1,\ x_2,\ x_3,\ x_4,\ x_5,\ \alpha\in K$，且 $\alpha\in K$ 为非平方数。

  现在，假设这两个五元组之一（例如 $(a_1^2,\ a_2^2,\ a_3^2,\ a_4^2,\ a_5^2)$ 等价于这样的等差数列。也就是说，存在 $s\in K^\times$，使得 $(sa_1^2,\ sa_2^2,\ sa_3^2,\ sa_4^2,\ sa_5^2)=(x_1^2,\ x_2^2,\ x_3^2,\ \alpha x_4^2,\ x_5^2)$。由恒等式 $sa_1^2=x_1^2$ 和 $sa_4^2=\alpha x_4^2$，我们推得 $\alpha\in K^2$，这与假设 α 不是 K中的平方数相矛盾。因此，不存在长度为六的此类等差数列。

接下来考虑情形 $K=\mathbb{Q}(\zeta_{12})$。如定理 2 所示，在等价意义下，唯一一个能在 $\mathbb{Q}(\zeta_{12})$ 的二次扩张上恰当定义的非初等五平方数等差数列是 $(-3,\ -1,\ 1,\ 3,\ 5)$，它定义在 $L=\mathbb{Q}(\zeta_{12},\ \sqrt{5})$ 上。

任何恰当定义在 L 上的非初等六平方数等差数列都必须扩展这个等差数列。这自然得到两个候选数列：$(-5,\ -3,\ -1,\ 1,\ 3,\ 5)$ 和 $(-3,\ -1,\ 1,\ 3,\ 5,\ 7)$。然而，只有第一个数列定义在 $\mathbb{Q}(\zeta_{12},\ \sqrt{5})$ 上。因此，在等价意义下，这是唯一一个能在 $\mathbb{Q}(\zeta_{12})$ 的二次扩张上恰当定义的非初等六平方数等差数列。

附录

本附录汇集了完成本文计算所需的全部信息。特别是，我们列出了本文中出现的曲线和数域的基本数据。

对于每条曲线 $C_i,\ i=0,\ 1$、.....、6，表 4 的第二行显示了对应的 $\mathbb{Q}$-同构椭圆曲线，第三行则显示其在 LMFDB数据库中的标签 [14]。

表 4：椭圆曲线

C_0	C_1	C_2	C_3	C_4	C_5	C_6
E_0	E_1	E_1^{-1}	E_1	E_4	E_6^{-1}	E_6
192.a2	24.a5	48.a5	24.a5	24.a2	48.a4	24.a4

注意，椭圆曲线 $E_1,\ E_4$ 和 E_6 属于同一个 $\mathbb{Q}$-同源类。因此，对于任意数域 K，都有 $\mathrm{rank}_{\mathbb{Z}}\,E_1(K)=\mathrm{rank}_{\mathbb{Z}}\,E_4(K)=\mathrm{rank}_{\mathbb{Z}}\,E_6(K)$。特别地，它们的任意二次扭曲的秩也都相同。

假设对于给定的数域 K，$\mathrm{rank}_{\mathbb{Z}}\,E_1^{\pm1}(K)=0$，那么计算 $C_i(K)$（其中 $k=i,$ ....., 6）可归结为计算其在 K 上的挠子群。

在我们的具体设定中，给定一条定义在 $\mathbb{Q}$ 上的椭圆曲线 E，只有有限多个固定次数为 d 的数域满足 $E(\mathbb{Q})_{\mathrm{tors}}\neq E(K)_{\mathrm{tors}}$。如果 E 的导子小于 400.000，这些数域会出现在 LMFDB数据库中，[14] 对应于 $d<24$。

表5展示了本文所研究椭圆曲线的挠点增长情况。第一列列出所有挠点会增长的次数为 <8 的数域。对于每个这样的域，后续各列展示该域上的相应挠子群。我们用记号$[n]$ 表示阶为 n的循环群，用 $[n,m]$ 表示阶分别为

[1]挠点增长数据由作者和 Filip Najman 计算得出 [5]。

n 和 m的循环群的乘积。设 $\alpha \in \mathbb{Q}$ 是不可约多项式 $x^4 - 3x^2 + 3$的一个根，设 $\beta \in \mathbb{Q}$ 是不可约多项式 $x^4 - 2x^3 - 2x + 1$的一个根。

例如，椭圆曲线 E_0 的 LMFDB 标签为 192.a2。因此，要获取有关这条椭圆曲线的挠子群增长的相关信息，只需查阅对应的 LMFDB 网页：

$$\text{https://www.lmfdb.org/EllipticCurve/Q/192.a2/}$$

并查看标题为“数域中的挠增长”的部分，其中列出了这条椭圆曲线的挠点会增长的数域。特别是，该网页显示，如果 E_0 的挠点在次数小于 8 的数域 K 上增长，那么 K 必定是以下之一

$$\mathbb{Q}(\sqrt{-2}), \quad \mathbb{Q}(\sqrt{2}, \sqrt{3}), \quad \text{or} \quad \mathbb{Q}(\sqrt{-1}, \sqrt{6}),$$

a并且在所有这些域中，挠子群满足 $E_0(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

表5：次数为 < 8 的数域上的本原挠增长

K	$E_1(K)_{\text{tors}}$	$E_1^{-1}(K)_{\text{tors}}$	$E_4(K)_{\text{tors}}$	$E_6(K)_{\text{tors}}$	$E_6^{-1}(K)_{\text{tors}}$	$E_0(K)_{\text{tors}}$
$\mathbb{Q}$	$[4]$	$[2]$	$[4]$	$[2,4]$	$[2,2]$	$[2,2]$
$\mathbb{Q}(\sqrt{-3})$	$[2,4]$	$[2,2]$	–	–	$[2,4]$	–
$\mathbb{Q}(\sqrt{-2})$	–	–	–	–	–	$[2,4]$
$\mathbb{Q}(\sqrt{-1})$	$[8]$	$[8]$	–	–	$[2,4]$	–
$\mathbb{Q}(\sqrt{2})$	–	–	$[8]$	–	–	–
$\mathbb{Q}(\sqrt{3})$	$[8]$	$[4]$	$[2,4]$	–	$[2,4]$	–
$\mathbb{Q}(\sqrt{6})$	–	–	$[8]$	–	–	–
$\mathbb{Q}(\zeta_8)$	–	–	–	$[2,8]$	$[2,8]$	–
$\mathbb{Q}(\zeta_{12})$	$[2,8]$	$[2,8]$	–	$[4,4]$	$[4,4]$	–
$\mathbb{Q}(\alpha)$	–	$[2,4]$	–	–	–	–
$\mathbb{Q}(\beta)$	–	$[8]$	–	–	$[2,8]$	–
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	–	–	$[2,8]$	$[2,8]$	–	$[2,4]$
$\mathbb{Q}(\sqrt{-1}, \sqrt{6})$	–	–	–	–	–	$[2,4]$

注意，对于这些椭圆曲线和数域 K，$\text{rank}_{\mathbb{Z}} E_1(K) \neq 0$ 仅当 $\sqrt{6} \in K$ 时成立；$\text{rank}_{\mathbb{Z}} E_1^{-1}(K) \neq 0$ 仅当 $K = \mathbb{Q}(i, \sqrt{6})$ 时成立；$\text{rank}_{\mathbb{Z}} E_0(K) \neq 1$ 仅当 $K = \mathbb{Q}(i, \sqrt{6})$ 时成立。最后，对于这些次数为 4 的数域 K，若 $\text{rank}_{\mathbb{Z}} E_1^{\pm 1}(K) = 0$，表6和表7展示了 $C_i(K)$ 在$i = 1, \ldots, 6$ 的情况。

下图展示了与椭圆曲线挠点增长相关的数域格，但不包括那些使任一椭圆曲线的秩增加的数域。

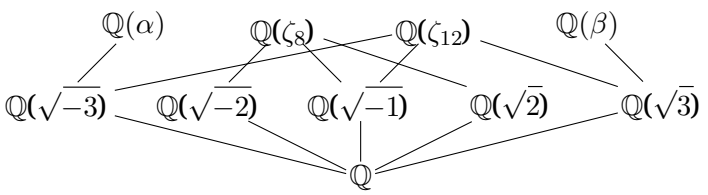


表6：曲线在 $\mathbb{Q}(\zeta_8)$ 和 $\mathbb{Q}(\zeta_{12})$ 上的点

K	$\mathbb{Q}(\zeta_8)$	$\mathbb{Q}(\zeta_{12})$
$C_1(K)$	$(-4,\ 0),\ (0,\ -8),$ $(\pm 4\zeta_8^2-4,\ 8)$	$(-4,\ 0),\ (0,\ -8),$ $(-4\zeta_{12}^2,\ 0),\ (4\zeta_{12}^2-4,\ 0),\ (-8, 16\zeta_{12}^2-8),$ $(\pm 4\zeta_{12}^3-4, 8),$ $(-4\zeta_{12}^3+8\zeta_{12}+4, 16\zeta_{12}^3-32\zeta_{12}-24),$ $(4\zeta_{12}^3-8\zeta_{12}+4, 16\zeta_{12}^3-32\zeta_{12}+24)$
$C_2(K)$	$(0,\ 0),$ $(\pm 4\zeta_8^2, 8\zeta_8^2),\ \ (-4, -8\zeta_8^2)$	$(0,\ 0),$ $(4\zeta_{12}^2-4, 0),\ (-4\zeta^2{}_{12}, 0),$ $(-4\zeta_{12}^3, -8\zeta_{12}^3),\ (-4, -8\zeta_{12}^3),\ (4\zeta_{12}^3, 8\zeta_{12}^3),$ $(4, -8\zeta_{12}^3+16\zeta_{12}),$ $(4\zeta_{12}^3-8\zeta_{12}-8, -24\zeta_{12}^3-32\zeta_{12}^2+16),$ $(-4\zeta_{12}^3+8\zeta_{12}-8, 24\zeta_{12}^3-32\zeta_{12}^2+16)$
$C_3(K)$	$(0,0),\ (-4,0),$ $(\pm 2\zeta_8^2-2, 8\zeta_8^2)$	$(0,0),\ (-4,0),$ $(-4\zeta_{12}^2,\ 0),\ (4\zeta_{12}^2-4,\ 0),\ (-2, 8\zeta_{12}^2-4),$ $(\pm 2\zeta_{12}^3-2, 8\zeta_{12}^3),$ $(-2\zeta_{12}^3+4\zeta_{12}-2, 8\zeta_{12}^3-16\zeta_{12}),$ $(2\zeta_{12}^3-4\zeta_{12}-2, 8\zeta_{12}^3-16\zeta_{12})$
$C_4(K)$	$(0,\ 0),\ (1,\ 4),$ $(-2\zeta_8^3+2\zeta_8-3, -6\zeta_8^3+6\zeta_8-8),$ $(2\zeta_8^3-2\zeta_8-3, -6\zeta_8^3+6\zeta_8+8),$	$(0,\ 0),\ (1,\ 4),$ $(-1, -2\zeta_{12}^3+4\zeta_{12}),$ $(\pm(4\zeta_{12}^3-8\zeta_{12}-7),\ 0)$
$C_5(K)$	$(0, 4),$ $(\pm 2\zeta_8^2,\ 4),$ $(\pm 2\zeta_8^3, 4\zeta_8^3),\ (\pm 2\zeta_8, 4\zeta_8),$	$(0, 4),$ $(\pm 2\zeta_{12}^2, 0),\ (\pm(2\zeta_{12}^2-2), 0),$ $(\pm 2\zeta_{12}^3,\ 4),$ $(\pm 2,\ -4\zeta_{12}^3+8\zeta_{12})$
$C_6(K)$	$(0,\ 1),\ (1, 4),\ \ (-1,\ 4),$ $(\pm(\zeta_8^3-\zeta_8^2+\zeta_8)\ \ 2\zeta_8^3-4\zeta_8^2+2\zeta_8),$ $(\pm(\zeta_8^3+\zeta_8^2+\zeta_8)\ \ -2\zeta_8^3-4\zeta_8^2-2\zeta_8)$	$(0,\ 1),\ (1,\ 4),\ (-1,\ 4)$ $(\pm(2\zeta_{12}^3+2\zeta_{12}^2-1), 0),$ $(\pm(2\zeta_{12}^3-2\zeta_{12}^2+1),\ 0),$ $(\pm\zeta_{12}^3\ \ 4\zeta_{12}^2-2)$

表7： $\mathbb{Q}(\alpha)$ 和 $\mathbb{Q}(\beta)$ 上的曲线上的点

K	$\mathbb{Q}(\alpha)$	$\mathbb{Q}(\beta)$
$C_1(K)$	$(-4,\ 0),\ (0,\ -8),$ $(-4\alpha^2+4, 0),$ $(-8,\ \ 16\alpha^2-24),$ $(4\alpha^2-8,\ 0)$	$(-4, 0), (0, -8),$ $(-4\beta^3+8\beta^2+4\beta+8,$ $\quad -16\beta^3+32\beta^2+16\beta+40),$ $(4\beta^3-8\beta^2-4\beta,$ $\quad -16\beta^3+32\beta^2+16\beta-8)$
$C_2(K)$	$(0,\ 0),$ $(-4\alpha^2+4, 0),\ (4\alpha^2-8, 0),$ $(-4\alpha^3-4\alpha^2+4\alpha+4,\ \ -8\alpha^2-8\alpha),$ $(4\alpha^3-4\alpha^2-4\alpha+4,\ \ -8\alpha^2+8\alpha)$	$(0, 0),$ $(4\beta^2,\ \ -8\beta^3-8\beta+8),$ $(4, 8\beta^3-16\beta^2-8\beta-8),$ $(-8\beta^3+12\beta^2+8\beta+16,$ $\quad -40\beta^3+64\beta^2+24\beta+88)$

下页继续

表7： $\mathbb{Q}(\alpha)$ 和 $\mathbb{Q}(\beta)$ 上曲线的点（续）

K	$\mathbb{Q}(\alpha)$	$\mathbb{Q}(\beta)$
$C_3(K)$	$(0,\ 0),\ (-4,\ 0),$ $(-4\alpha^2+4,\ 0),\ (4\alpha^2-8,\ 0),$ $(-2,\ -8\alpha^2+12)$	$(0,0),\ (-4,0),$ $(2\beta^3-4\beta^2-2\beta-4,\ \ 8\beta^3-16\beta^2-8\beta-8),$ $(-2\beta^3+4\beta^2+2\beta,\ 8\beta^3-16\beta^2-8\beta-8)$
$C_4(K)$	$(1,-4),\ (0,0)$	$(1,-4),\ (0,0),$ $(-4\beta^3+8\beta^2+4\beta-3,0),$ $(-1,-2\beta^3+4\beta^2+2\beta+2),$ $(4\beta^3-8\beta^2-4\beta-11,0)$
$C_5(K)$	$(0,\ 4),$ $(\pm(2\alpha^{2}-4),\ 0),$ $(\pm(2\alpha^{2}-2),\ 0)$	$(0,4),$ $(\pm2,\ \ -4\beta^3+8\beta^2+4\beta+4),$ $(\pm2\beta,\ \ -4\beta^3+4\beta^2+4),$ $(\pm(2\beta^3-4\beta^2-4)\ \ 8\beta^3-12\beta^2-4\beta-20)$
$C_6(K)$	$(0,1),\ (1,4)\ ,\ (-1,4)$	$(0,1),\ (1,4),\ (-1,4)$

致谢。 作者感谢审稿人提出的宝贵意见和建议，这些意见和建议使论文得以改进。

参考文献

[1] W. Bosma、J. Cannon 和 C. Playoust，《MAGMA 代数系统 I：用户语言》，《符号计算杂志》24（1997），第 3-4 期，235-265。[2] A. Bremner 和 S. Siksek，《三次域上等差数列中的平方数》，《国际数论杂志》12（2016），第 5 期，1409-1414。[3] E. Gonz´alez-Jim´enez，《数域二次扩张上等差数列中的平方数》。Magma 源代码。http://matematicas.uam.es/~enrique.gonzalez.jimenez [4] E. Gonz´alez-Jim´enez 和 F. Najman，《椭圆曲线经基变换后的挠点增长》，《数学计算》89（2020），1457-1485。[5] E. Gonz´alez-Jim´enez 和 F. Najman，《确定椭圆曲线挠点增长的算法》，《实验数学》32（2023），70-81。[6] E. Gonz´alez-Jim´enez 和 X. J Steuding，《二次域上四个平方数的等差数列》，《德布勒森数学出版物》77（2010），第 1-2 期，125-138。[7] E. Gonz´alez-Jim´enez 和 N. X. Tho，《某些非本原四次数域上等差数列中的平方数》，《数论杂志》282（2026），13-30。[8] E. Gonz´alez-Jim´enez 和 X. Xarles，《二次域上五个平方数的等差数列》，《伊比利亚美洲数学评论》29（2013），第 4 期，1211-1238。[9] ´A. Lozano-Robledo，《有理数域上椭圆曲线 p-挠点的定义域》，《数学年刊》357（2013），279–305。[10] B. Mazur，《素数次数的有理同源》，《数学发明》44（1978），129–162。[11] L. J. Mordell，《代数数域中的丢番图方程 $x^4+y^4=1$ 》，《算术学报》14（1967/1968），347-355。[12] J.-P. Serre，《椭圆曲线上有限阶点的伽罗瓦性质》，《数学发明》15（1972），259-331。[13] A. V. Sutherland，《计算椭圆曲线相关伽罗瓦表示的像》，《数学论坛 Sigma》4（2016），e4，共 79 页。[14] LMFDB 合作组，《L-函数与模形式数据库》，https://www.lmfdb.org，2025，[在线；访问日期：4 月 15 日 2025]。[15] N. X. Tho，《 $\mathbb{Q}(\zeta_8)$ 的二次扩张上等差数列中的平方数》。预印本。[16] X. Xarles，《数域上等差数列中的平方数》，《数论杂志》132（2012），第 3 期，379-389。[17] D. Zywina，《关于椭圆曲线在 $\mathbb{Q}$ 上所关联的模 ℓ 表示的可能像》。arXiv:1508.07660。

马德里自治大学（Aut´onoma），数学系（Matem´aticas），马德里，西班牙电子邮箱：enrique.gonzalez.jimenez@uam.es