



关于孙智伟一个猜想的证明

献给陆洪文教授 85 寿辰

宋恒*, 徐飞

首都师范大学数学科学学院, 北京 100048

E-mail: songheng@cnu.edu.cn, xufei@math.ac.cn

收稿日期: 2023-12-10; 接受日期: 2024-05-16; 网络出版日期: 2024-06-07; * 通信作者

国家自然科学基金 (批准号: 12231009) 资助项目

摘要 本文证明了, 若 a, b, c 和 d 为全实数域 k 中的元素且其中至少有一个是全正数, 则 k 中每个非负元 r 均可表为 $x^2 + y^2 + z^2 + w^2$ 使得 x, y, z 和 w 为 k 中非负元并且 $ax + by + cz + dw$ 为 k 中的平方元. 若将 $ax + by + cz + dw$ 为 k 中的平方元换为 $ax + by + cz + dw$ 为 k 中的立方元, 结论也成立. 这是孙智伟的一个猜想.

关键词 弱逼近 dyadic 局部域 有理点

MSC (2020) 主题分类 11E20, 14G05, 14G12

1 引言

代数方程的有理解和整数解是数论的基本问题之一. 研究这类问题大致分为解析方法和代数方法. 解析方法包括圆法和 Diophantus 逼近等. 代数方法主要有代数几何方法, 如下降理论和纤维化方法. 事实上, 关于有理二次型的 Hasse-Minkowski 定理 (参见文献 [10, 66:4]) 可以通过 Chebotarev 密度定理和纤维化方法来证明. Colliot-Thélène 和 Sansuc^[1] 将 Chebotarev 密度定理替换成 Schinzel 猜想, 利用纤维化方法证明了更一般的有理代数簇的弱逼近, 如经典的 Châtelet 曲面等. 随后文献 [3–5, 12] 对此方法做了改进和推广. 另外, Harari^[8] 将纤维化方法应用于研究带有 Brauer-Manin 障碍的弱逼近. Harpaz 和 Wittenberg^[9] 进一步发展了 Harari 的理论, 用纤维化方法重新证明了用下降理论或解析方法等其他方法得到的 Brauer-Manin 障碍下的弱逼近.

孙智伟^[11] 研究了有理数域上带有约束条件的四平方和问题, 并提出了如下猜想 (参见文献 [11, 猜想 6.3(i)]).

猜想 1.1 若 a, b, c 和 d 为全实域 k 中的元素且其中至少有一个是全正数, 则对于 k 中每个非负元 r , 均存在 k 中非负元 x, y, z 和 w 使得 $r = x^2 + y^2 + z^2 + w^2$ 并且 $ax + by + cz + dw$ 为 k 中的平方元. 将 k 中的平方元换为 k 中的立方元也成立.

英文引用格式: Song H, Xu F. Proof of one of Sun Zhi-Wei's conjectures (in Chinese). Sci Sin Math, 2024, 54: 1345–1356, doi: 10.1360/SSM-2023-0335

当 $k = \mathbb{Q}$ 时, 孙智伟^[11] 已证明这个猜想 (参见文献 [11, 定理 1.1]). 本文将利用纤维化方法建立的结果彻底证明这个猜想. 为陈述本文的主要结果, 先介绍下面几个概念.

定义 1.1 设 X 是定义在数域 k 上的代数簇, Ω_k 为 k 的所有素除子集合, k_v 是 k 在素除子 $v \in \Omega_k$ 处的完备化.

(1) 如果

$$\prod_{v \in \Omega_k} X(k_v) \neq \emptyset \Rightarrow X(k) \neq \emptyset,$$

则称 X 满足 Hasse 原则;

(2) 如果 $\prod_{v \in \Omega_k} X(k_v) \neq \emptyset$ 并且对角映射

$$X(k) \rightarrow \prod_{v \in \Omega_k} X(k_v)$$

的像稠密, 这里箭头右边的乘积取乘积拓扑, 则称 X 满足弱逼近.

本文主要结果如下:

定理 1.1 设 a, b, c 和 d 是数域 k 中满足 $a^2 + b^2 + c^2 + d^2$ 不为 0 的元素. 若 r 为 k 中取定的不为 0 的元素, 则 X_r 是由如下方程组定义的在 A_k^5 中的代数簇:

$$\begin{cases} x^2 + y^2 + z^2 + w^2 = r, \\ ax + by + cz + dw = p(u), \end{cases}$$

其中 $p(u)$ 是 k 上给定的一元多项式. 如果 $p(u)^2 - r(a^2 + b^2 + c^2 + d^2)$ 是 k 上没有重根的非零多项式, 则 X_r 满足 Hasse 原则. 更进一步地, 当 $\prod_{v \in \Omega_k} X_r(k_v) \neq \emptyset$ 时, X_r 满足弱逼近.

利用定理 1.1, 可以证明孙智伟猜想.

定理 1.2 设 a, b, c 和 d 是全实数域 k 中元素. 对于 k 中任何全正数 r , 由如下方程组定义 k 上代数簇 X_r :

$$\begin{cases} x^2 + y^2 + z^2 + w^2 = r, \\ ax + by + cz + dw = p(u), \end{cases}$$

其中 $p(u) = u^2$ 或 $p(u) = u^3$. 如果 a, b, c 和 d 中有一个是全正数, 则

$$\prod_{v \in \infty_k} X_r^+(k_v) \times \prod_{v \in \Omega_k \setminus \infty_k} X_r(k_v)$$

是乘积拓扑空间 $\prod_{v \in \Omega_k} X_r(k_v)$ 的非空开集, 其中

$$X_r^+(k_v) = \{(x_v, y_v, z_v, w_v, u_v) \in X_r(k_v) : x_v > 0, y_v > 0, z_v > 0, w_v > 0\}.$$

特别地, 由弱逼近性质可知上述开集中存在 $X_r(k)$ 中的点, 故孙智伟猜想成立.

定理 1.2 指出: 如果 r 全正, 那么猜想中的 x, y, z 和 w 也可取为全正.

2 主要结果的证明

本节给出定理 1.1 和 1.2 的证明. 由于证明中需要一些二次型的算术理论, 我们采用文献 [10] 的记号和术语. 例如, k 是一个数域, k 上的所有素除子集合为 Ω_k . 对于任意 $v \in \Omega_k$, k_v 表示 k 关于 v

的完备化, $\mathfrak{o}_v$ 表示 k_v 的整数环, $\mathfrak{o}_v^\times$ 表示 $\mathfrak{o}_v$ 中的可逆元构成的乘法群. 对于 k_v 中的两个非零元 a 和 b , $(a, b)_v$ 代表由 a 和 b 定义的 Hilbert 符号 (参见文献 [10, §63 B]). 对于 k_v 上的一个非退化二次型

$$f(x_1, \dots, x_n) = \sum_{i=1}^n \alpha_i x_i^2,$$

其中, α_i ($1 \leq i \leq n$) 为 k_v 中的非零元, f 的 Hasse 符号定义为

$$S_v(f) = \prod_{1 \leq i \leq j \leq n} (\alpha_i, \alpha_j)_v$$

(参见文献 [10, §63 B]). 如果在 k_v 上有 $f = g \perp h$, 则

$$S_v(f) = S_v(g) \cdot (\det(g), \det(h))_v \cdot S_v(h)$$

(参见文献 [10, §63 B]).

定理 1.1 的证明 因为 $a^2 + b^2 + c^2 + d^2$ 不为 0, 所以存在 a 、 b 、 c 和 d 中的 3 个元素使得其平方和非零. 否则, 有

$$a^2 + b^2 + c^2 + d^2 = \frac{1}{3}((b^2 + c^2 + d^2) + (a^2 + c^2 + d^2) + (a^2 + b^2 + d^2) + (a^2 + b^2 + c^2)) = 0,$$

这与 $a^2 + b^2 + c^2 + d^2$ 不为 0 矛盾. 不失一般性, 可以假设 $a^2 + b^2 + d^2$ 不为 0. 同样地, 可以假设 $a^2 + d^2$ 和 d^2 均不为 0. 那么定理 1.1 的方程等价于

$$x^2 + y^2 + z^2 + \frac{1}{d^2}(p(u) - ax - by - cz)^2 = r,$$

整理可得

$$\begin{aligned} & (a^2 + d^2)x^2 + (b^2 + d^2)y^2 + (c^2 + d^2)z^2 + 2abxy + 2bcyz + 2acxz - 2p(u)(ax + by + cz) \\ & = d^2r - p(u)^2. \end{aligned}$$

再根据 $a^2 + d^2$ 、 $a^2 + b^2 + d^2$ 和 $a^2 + b^2 + c^2 + d^2$ 均不为 0, 方程的前一部分可以写成

$$\begin{aligned} & (a^2 + d^2) \left[x^2 + \frac{2a}{a^2 + d^2} x(by + cz - p(u)) + \frac{a^2}{(a^2 + d^2)^2} (by + cz - p(u))^2 \right] \\ & - \frac{a^2}{a^2 + d^2} (by + cz - p(u))^2 + (b^2 + d^2)y^2 + (c^2 + d^2)z^2 + 2bcyz - 2p(u)(by + cz) \\ & = (a^2 + d^2) \left[x + \frac{a}{a^2 + d^2} (by + cz - p(u)) \right]^2 \\ & + \frac{d^2(a^2 + b^2 + d^2)}{a^2 + d^2} \left[y^2 + \frac{2b}{a^2 + b^2 + d^2} y(cz - p(u)) + \frac{b^2}{(a^2 + b^2 + d^2)^2} (cz - p(u))^2 \right] \\ & - \frac{b^2 d^2}{(a^2 + d^2)(a^2 + b^2 + d^2)} (cz - p(u))^2 - \frac{a^2}{a^2 + d^2} (cz - p(u))^2 + (c^2 + d^2)z^2 - 2cp(u)z \\ & = (a^2 + d^2) \left[x + \frac{a}{a^2 + d^2} (by + cz - p(u)) \right]^2 + \frac{d^2(a^2 + b^2 + d^2)}{a^2 + d^2} \left[y + \frac{b}{a^2 + b^2 + d^2} (cz - p(u)) \right]^2 \\ & + \left(1 - \frac{b^2 d^2}{(a^2 + d^2)(a^2 + b^2 + d^2)} - \frac{a^2}{a^2 + d^2} \right) (cz - p(u))^2 - p(u)^2 + d^2 z^2 \end{aligned}$$

$$\begin{aligned}
 &= (a^2 + d^2) \left[x + \frac{a}{a^2 + d^2} (by + cz - p(u)) \right]^2 + \frac{d^2(a^2 + b^2 + d^2)}{a^2 + d^2} \left[y + \frac{b}{a^2 + b^2 + d^2} (cz - p(u)) \right]^2 \\
 &\quad + \frac{d^2}{a^2 + b^2 + d^2} (cz - p(u))^2 - p(u)^2 + d^2 z^2 \\
 &= (a^2 + d^2) \left[x + \frac{a}{a^2 + d^2} (by + cz - p(u)) \right]^2 + \frac{d^2(a^2 + b^2 + d^2)}{a^2 + d^2} \left[y + \frac{b}{a^2 + b^2 + d^2} (cz - p(u)) \right]^2 \\
 &\quad + \frac{d^2(a^2 + b^2 + c^2 + d^2)}{a^2 + b^2 + d^2} \left[z - \frac{c}{a^2 + b^2 + c^2 + d^2} p(u) \right]^2 - \frac{c^2 d^2 + (a^2 + b^2)(a^2 + b^2 + c^2 + d^2)}{(a^2 + b^2 + d^2)(a^2 + b^2 + c^2 + d^2)} p(u)^2.
 \end{aligned}$$

作变量替换

$$\begin{cases} x' = x + \frac{ab}{a^2 + d^2} y + \frac{ac}{a^2 + d^2} z - \frac{a}{a^2 + d^2} p(u), \\ y' = y + \frac{bc}{a^2 + b^2 + d^2} z - \frac{b}{a^2 + b^2 + d^2} p(u), \\ z' = z - \frac{c}{a^2 + b^2 + c^2 + d^2} p(u), \\ u' = u, \end{cases}$$

定理 1.1 的方程变为

$$\frac{a^2 + d^2}{d^2} x'^2 + \frac{a^2 + b^2 + d^2}{a^2 + d^2} y'^2 + \frac{a^2 + b^2 + c^2 + d^2}{a^2 + b^2 + d^2} z'^2 = -\frac{1}{a^2 + b^2 + c^2 + d^2} p(u')^2 + r.$$

由上式定义的代数簇 Y_r 与 X_r 作为 k 上的代数簇同构. 由假设作为 u' 的多项式 $-\frac{1}{a^2 + b^2 + c^2 + d^2} p(u')^2 + r$ 没有重根, 根据文献 [7, 引理 3.3], Y_r 光滑. 再根据文献 [7, 命题 6.3] 或 [6, 定理 3.10], Y_r 满足 Hasse 原则和弱逼近. 因此, X_r 也满足 Hasse 原则和弱逼近. $\square$

为证明定理 1.2, 需要下面的一些引理.

引理 2.1 设 v 是数域 k 上的一个有限素除子. 如果 a, b, c 和 d 是 k_v 中的元素且满足

$$d(a^2 + d^2)(a^2 + b^2 + d^2)(a^2 + b^2 + c^2 + d^2) \neq 0,$$

则三元二次型

$$\frac{a^2 + d^2}{d^2} x^2 + \frac{a^2 + b^2 + d^2}{a^2 + d^2} y^2 + \frac{a^2 + b^2 + c^2 + d^2}{a^2 + b^2 + d^2} z^2$$

在 k_v 上的 Hasse 符号 (参见文献 [10, §63 B]) 为 1.

特别地, 如果 $\text{ord}_v(2) = 0$, 则上述三元二次型在 k_v 上迷向, 因此定理 1.1 中的 $X_r(k_v) \neq \emptyset$ 对所有 $r \in k$ 成立.

证明 记该三元二次型的 Hasse 符号为 ε_v , 根据文献 [10, 58:3.注和 57:10], 有

$$\begin{aligned}
 (-1, -1)_{v\varepsilon_v} &= \left(-\frac{a^2 + d^2}{d^2} \cdot \frac{a^2 + b^2 + d^2}{a^2 + d^2}, -\frac{a^2 + d^2}{d^2} \cdot \frac{a^2 + b^2 + c^2 + d^2}{a^2 + b^2 + d^2} \right)_v \\
 &= (-(a^2 + b^2 + d^2), -(a^2 + d^2)(a^2 + b^2 + d^2)(a^2 + b^2 + c^2 + d^2))_v \\
 &= (-(a^2 + b^2 + d^2), -(a^2 + d^2)(a^2 + b^2 + c^2 + d^2))_v \\
 &= (-(a^2 + b^2 + d^2), -(a^2 + d^2))_v \cdot (-(a^2 + b^2 + d^2), a^2 + b^2 + c^2 + d^2)_v.
 \end{aligned}$$

因为三元二次型

$$-(a^2 + b^2 + d^2)u^2 + (a^2 + b^2 + c^2 + d^2)v^2 = w^2$$

有非平凡解 $(1, 1, c)$, 根据文献 [10, 57:9], 有

$$(-(a^2 + b^2 + d^2), a^2 + b^2 + c^2 + d^2)_v = 1.$$

所以根据文献 [10, 57:10], 有

$$(-1, -1)_v \varepsilon_v = (-(a^2 + b^2 + d^2), -(a^2 + d^2))_v = (-1, -(a^2 + d^2))_v (a^2 + b^2 + d^2, -(a^2 + d^2))_v.$$

由于三元二次型

$$(a^2 + b^2 + d^2)u^2 - (a^2 + d^2)v^2 = w^2$$

有非平凡解 $(1, 1, b)$, 同样根据文献 [10, 57:9], 有

$$(a^2 + b^2 + d^2, -(a^2 + d^2))_v = 1.$$

再由文献 [10, 57:10], 得到 $\varepsilon_v = (-1, a^2 + d^2)_v$. 由于三元二次型

$$-u^2 + (a^2 + d^2)v^2 = w^2$$

有非平凡解 $(a, 1, d)$, 根据文献 [10, 57:9], 有 $(-1, a^2 + d^2)_v = 1$.

当 $\text{ord}_v(2) = 0$ 时, 根据文献 [10, 63:11a], 有 $(-1, -1)_v = 1 = \varepsilon_v$. 由文献 [10, 58:6] 可知此三元二次型迷向. 故定理 1.1 的证明中 $Y_r(k_v) \neq \emptyset$. 所以 $X_r(k_v) \neq \emptyset$ 对所有 $r \in k$ 成立. $\square$

根据引理 2.1, 对于 k 的有限除子 v , 只有当 v 是 dyadic 素除子时才有可能使得 $X_r(k_v) = \emptyset$. 事实上, 可以对这种情形进行一个完整的刻画.

引理 2.2 设 v 是 k 的 dyadic 素除子, $r_0 \in k$. 则定理 1.1 中的代数簇满足 $X_{r_0}(k_v) = \emptyset$ 当且仅当 $(-1, -1)_v = -1$, 并且对于任意 $u \in k_v$ 均有

$$p(u)^2 - (a^2 + b^2 + c^2 + d^2)r_0$$

是 k_v 中的平方元.

证明 必要性 根据定理 1.1 的证明, $X_{r_0}(k_v) = \emptyset$ 等价于 $Y_{r_0}(k_v) = \emptyset$, 故三元二次型

$$\frac{a^2 + d^2}{d^2}x'^2 + \frac{a^2 + b^2 + d^2}{a^2 + d^2}y'^2 + \frac{a^2 + b^2 + c^2 + d^2}{a^2 + b^2 + d^2}z'^2$$

在 k_v 上非迷向. 利用文献 [10, 58:6], 此二次型的 Hasse 符号为 $\varepsilon_v = -(-1, -1)_v$. 另外, 根据引理 2.1, 有 $\varepsilon_v = 1$. 故 $(-1, -1)_v = -1$. 若存在 $u'_0 \in k_v$ 使得 $p(u'_0)^2 - (a^2 + b^2 + c^2 + d^2)r_0$ 不是 k_v 中的平方元, 根据文献 [10, 63:18.注], 四元二次型

$$\frac{a^2 + d^2}{d^2}x'^2 + \frac{a^2 + b^2 + d^2}{a^2 + d^2}y'^2 + \frac{a^2 + b^2 + c^2 + d^2}{a^2 + b^2 + d^2}z'^2 + \left(\frac{p(u'_0)^2}{a^2 + b^2 + c^2 + d^2} - r_0 \right) w'^2$$

在 k_v 上非退化而且迷向. 由此可知 $Y_{r_0}(k_v) \neq \emptyset$, 即 $X_{r_0}(k_v) \neq \emptyset$, 矛盾.

充分性 因为 $(-1, -1)_v = -1$, 利用引理 2.1 和文献 [10, 58:6], 三元二次型

$$\frac{a^2 + d^2}{d^2}x'^2 + \frac{a^2 + b^2 + d^2}{a^2 + d^2}y'^2 + \frac{a^2 + b^2 + c^2 + d^2}{a^2 + b^2 + d^2}z'^2$$

在 k_v 上非迷向. 若 $X_{r_0}(k_v) \neq \emptyset$, 则根据定理 1.1 的证明, 有 $Y_{r_0}(k_v) \neq \emptyset$. 因为 Y_{r_0} 是光滑代数簇, 根据隐函数定理 (参见文献 [2, 定理 10.5.1]), $Y_{r_0}(k_v)$ 在 Y_{r_0} 中 Zariski 稠密. 因为多项式方程

$$p(u')^2 - (a^2 + b^2 + c^2 + d^2)r_0 = 0$$

在 k_v 上仅有有限多个解并且每个解 α_0 只能给出 $Y_{r_0}(k_v)$ 中一个点 $(0, 0, 0, \alpha_0)$, 所以存在 $(x'_0, y'_0, z'_0, u'_0) \in Y_{r_0}(k_v)$ 使得

$$p(u'_0)^2 - (a^2 + b^2 + c^2 + d^2)r_0 \neq 0.$$

故非退化四元二次型

$$\frac{a^2 + d^2}{d^2}x'^2 + \frac{a^2 + b^2 + d^2}{a^2 + d^2}y'^2 + \frac{a^2 + b^2 + c^2 + d^2}{a^2 + b^2 + d^2}z'^2 + \left(\frac{p(u'_0)^2}{a^2 + b^2 + c^2 + d^2} - r_0 \right)w'^2$$

在 k_v 上迷向, 并且该二次型的判别式

$$\frac{p(u'_0)^2 - (a^2 + b^2 + c^2 + d^2)r_0}{d^2}$$

是 k_v 的平方元. 根据文献 [10, 63:18.注], 该四元二次型同构于两个双曲平面的正交和 $\mathbb{H} \perp \mathbb{H}$. 利用文献 [10, 58:3.注], 此四元二次型的 Hasse 符号为 $(-1, -1)_v = -1$. 另外, 同样利用文献 [10, 58:3.注], 该四元二次型的 Hasse 符号也可以通过前面的三元二次型的 Hasse 符号 ε_v 与最后一项的 Hasse 符号来计算. 故此四元二次型的 Hasse 符号等于

$$\varepsilon_v \cdot (a^2 + b^2 + c^2 + d^2, a^2 + b^2 + c^2 + d^2)_v \cdot (a^2 + b^2 + c^2 + d^2, a^2 + b^2 + c^2 + d^2)_v = 1,$$

这里用到了 $p(u'_0)^2 - (a^2 + b^2 + c^2 + d^2)r_0$ 是 k_v 的平方元以及引理 2.1 中 $\varepsilon_v = 1$. 由此产生了矛盾. $\square$

引理 2.3 若 $[k_v : \mathbb{Q}_2]$ 是偶数, 则 $(-1, -1)_v = 1$.

证明 只需要考虑 -1 不是 k_v 中平方元的情形. 由于 Hilbert 符号是二次扩张 $k_v(\sqrt{-1})/k_v$ 的 Artin 映射与 $\text{Gal}(k_v(\sqrt{-1})/k_v)$ 的非平凡特征的复合, 根据文献 [13, 第 12 章, 定理 2], 有

$$(-1, -1)_v = (-1, N_{k_v/\mathbb{Q}_2}(-1))_2 = (-1, (-1)^{[k_v:\mathbb{Q}_2]})_2 = (-1, 1)_2 = 1,$$

其中, $N_{k_v/\mathbb{Q}_2}$ 是 norm 映射, $(\cdot, \cdot)_2$ 是 $\mathbb{Q}_2$ 上的 Hilbert 符号. $\square$

引理 2.4 设 v 是 k 的实际子. 假设定理 1.1 中的代数簇 X_r 满足在 k_v 中 $r > 0$ 且 a, b, c 和 d 中至少有一个大于 0. 如果 $p(u) = u^n$, 其中 $n \in \mathbb{N}$, 则

$$\{(x_v, y_v, z_v, w_v, u_v) \in X_r(k_v) : x_v > 0, y_v > 0, z_v > 0, w_v > 0\}$$

是 $X_r(k_v)$ 中的非空开集.

证明 因为

$$\{(x_v, y_v, z_v, w_v, u_v) \in \mathbb{R}^5 : x_v > 0, y_v > 0, z_v > 0, w_v > 0\}$$

是 $\mathbb{R}^5$ 中的非空开集, 只需要证明集合

$$\{(x_v, y_v, z_v, w_v, u_v) \in X_r(k_v) : x_v > 0, y_v > 0, z_v > 0, w_v > 0\}$$

非空. 不妨假设 d 在 k_v 中大于 0. 取方程 $x^2 + y^2 + z^2 + w^2 = r$ 在 k_v 中的一组解 (x_0, y_0, z_0, w_0) 满足 $x_0 > 0, y_0 > 0, z_0 > 0, w_0 > 0$ 并且

$$\max\{x_0, |ax_0|, y_0, |by_0|, z_0, |cz_0|\} < \min\left\{\frac{1}{4}\sqrt{r}, \frac{1}{4}d\sqrt{r}\right\}.$$

故 $w_0 > \frac{\sqrt{13}}{4}\sqrt{r}$. 由此可知

$$ax_0 + by_0 + cz_0 + dw_0 > -\frac{3}{4}d\sqrt{r} + \frac{\sqrt{13}}{4}d\sqrt{r} > 0.$$

所以方程 $u^n = ax_0 + by_0 + cz_0 + dw_0$ 在 k_v 中有解. $\square$

定理 1.2 的证明 在定理 1.1 中, 定义 X_r 的系数 a, b, c 和 d 是对称的. 若 a, b, c 和 d 是全实域 k 中至少有一个全正数, 则定理 1.2 中的 X_r 满足定理 1.1 的条件. 利用引理 2.1 和 2.4, 本文只需要证明: 当 $p(u) = u^2$ 或 $p(u) = u^3$ 时, 对于 k 中 dyadic 素除子 v , 有 $X_r(k_v) \neq \emptyset$.

对于 k 中的 dyadic 素除子 v , 根据引理 2.2 和 2.3, 本文只需要考虑 $[k_v : \mathbb{Q}_2] = ef$ 是奇数的情形, 其中 $e = \text{ord}_v(2)$ 以及 f 为相应的剩余类域扩张次数. 根据文献 [10, §63 A], 可以定义 k_v 中元素 ξ 的二次亏量 (quadratic defect)

$$\delta(\xi) = \bigcap_{\alpha} (\alpha \mathfrak{o}_v),$$

其中 $\xi = \eta^2 + \alpha$, 这里 $\alpha, \eta \in k_v$, 故 ξ 是 k_v 中的平方元当且仅当 $\delta(\xi) = 0$. 取定 $\Delta = 1 + 4\rho$ 其中 $\rho \in \mathfrak{o}_v^\times$ 使得 $\delta(\Delta) = 4\mathfrak{o}_v$ (参见文献 [10, 63:3]).

(1) $p(u) = u^2$ 的情形. 如果 $-(a^2 + b^2 + c^2 + d^2)r$ 不是 k_v 中的平方元, 取 $u = 0$, 根据引理 2.2, 则 $X_r(k_v) \neq \emptyset$. 只需要考虑 $-(a^2 + b^2 + c^2 + d^2)r$ 是 k_v 中平方元的情形. 记

$$-(a^2 + b^2 + c^2 + d^2)r = r_1^2 \quad \text{以及} \quad r_1 = \alpha\pi_v^l, \quad \text{其中 } \alpha \in \mathfrak{o}_v^\times, \quad l \in \mathbb{Z}.$$

以下证明: 存在 $u \in k_v$ 使得 $u^4 + r_1^2$ 不是 k_v 中的平方元. 再利用引理 2.2, 仍有 $X_r(k_v) \neq \emptyset$.

当 $l \equiv 0 \pmod{2}$ 时, 取 $u = \pi_v^{\frac{l}{2}}$, 则

$$u^4 + r_1^2 = \pi_v^{2l} + \alpha^2\pi_v^{2l} = \pi_v^{2l}[(1 + \alpha)^2 - 2\alpha].$$

如果 $\text{ord}_v(1 + \alpha)^2 < e$, 则

$$(1 + \alpha)^2 - 2\alpha = (1 + \alpha)^2(1 - 2\alpha(1 + \alpha)^{-2}).$$

根据文献 [10, 63:5], 有

$$\delta(1 - 2\alpha(1 + \alpha)^{-2}) = (\pi_v)^s, \quad \text{其中 } s = e - 2\text{ord}_v(1 + \alpha).$$

所以 $1 - 2\alpha(1 + \alpha)^{-2}$ 不是 k_v 中的平方元.

如果 $\text{ord}_v(1 + \alpha)^2 > e$, 则

$$\text{ord}_v((1 + \alpha)^2 - 2\alpha) = e$$

是奇数. 故 $(1 + \alpha)^2 - 2\alpha$ 不是 k_v 中的平方元.

当 $l \equiv 1 \pmod{2}$ 时, 根据剩余类域是特征为 2 的完全域, 可知存在 $\xi \in \mathfrak{o}_v^\times$ 使得

$$\xi^2 \equiv -2\pi_v^{-e}\alpha\rho \pmod{\pi_v}.$$

取 $u = \xi\pi_v^{\frac{e+l}{2}}$, 有

$$u^4 + r_1^2 = \xi^4\pi_v^{2(e+l)} + \alpha^2\pi_v^{2l} = \alpha^2\pi_v^{2l}[(1 + \alpha^{-1}\xi^2\pi_v^e)^2 - 2\alpha^{-1}\xi^2\pi_v^e].$$

因为

$$(1 + \alpha^{-1}\xi^2\pi_v^e)^2 - 2\alpha^{-1}\xi^2\pi_v^e \equiv (1 + \alpha^{-1}\xi^2\pi_v^e)^2 + 4\rho \equiv (1 + \alpha^{-1}\xi^2\pi_v^e)^2(1 + 4\rho) \pmod{4\pi_v},$$

利用文献 [10, 63:1], 可知存在 $\eta \in \mathfrak{o}_v^\times$ 使得

$$(1 + \alpha^{-1}\xi^2\pi_v^e)^2 - 2\alpha^{-1}\xi^2\pi_v^e = (1 + \alpha^{-1}\xi^2\pi_v^e)^2\eta^2\Delta,$$

故上述元素不是 k_v 中的平方元.

(2) $p(u) = u^3$ 的情形. 类似地, 只需要考虑 $-(a^2 + b^2 + c^2 + d^2)r$ 是 k_v 中平方元的情形. 记

$$-(a^2 + b^2 + c^2 + d^2)r = r_1^2 \quad \text{以及} \quad r_1 = \alpha\pi_v^l, \quad \text{其中, } \alpha \in \mathfrak{o}_v^\times, \quad l \in \mathbb{Z}.$$

以下证明: 存在 $u \in k_v$ 使得 $u^6 + r_1^2$ 不是 k_v 中的平方元. 利用引理 2.2, 同样有 $X_r(k_v) \neq \emptyset$.

当 $l \equiv 0 \pmod{3}$ 时, 取 $u = \pi_v^{\frac{l}{3}}$, 则

$$u^6 + r_1^2 = \pi_v^{2l} + \alpha^2\pi_v^{2l} = \pi_v^{2l}[(1 + \alpha)^2 - 2\alpha].$$

利用上面同样的讨论, 通过比较 $\text{ord}_v(1 + \alpha)^2$ 与 e , 可知此元素不是 k_v 中的平方元.

当 $l \equiv 1 \pmod{3}$ 并且 $e > 1$ 时, 取 $u = \pi_v^{\frac{l+2}{3}}$, 则

$$u^6 + r_1^2 = \pi_v^{2l+4} + \alpha^2\pi_v^{2l} = \pi_v^{2l}[(\alpha + \pi_v^2)^2 - 2\alpha\pi_v^2].$$

因为 $e \geq 3$, 所以根据文献 [10, 63:5], 有

$$\delta((\alpha + \pi_v^2)^2 - 2\alpha\pi_v^2) = (\pi_v)^{e+2}.$$

故 $u^6 + r_1^2$ 不是 k_v 中的平方元.

当 $l \equiv 1 \pmod{3}$ 并且 $e = 1$ 时, 利用剩余类域是特征为 2 的完全域, 可知存在 $\rho_1 \in \mathfrak{o}_v^\times$ 满足 $\rho \equiv \rho_1^2 \pmod{\pi_v}$. 因为 f 是奇数, 所以 $2^f - 1$ 与 3 互素. 故 $x \mapsto x^3$ 是 k_v 剩余类域乘法群的自同构. 因此存在 $u_1 \in \mathfrak{o}_v^\times$ 使得

$$u_1^3 \equiv 2^{-1}\pi_v\alpha\rho_1^{-1} \pmod{\pi_v}.$$

取 $u = u_1 \pi_v^{\frac{l-1}{3}}$, 则

$$u^6 + r_1^2 = \pi_v^{2l-2} u_1^6 (1 + u_1^{-6} \alpha^2 \pi_v^2).$$

根据文献 [10, 63:1], 有

$$1 + u_1^{-6} \alpha^2 \pi_v^2 = 1 + 4(u_1^{-3} 2^{-1} \pi_v \alpha)^2 \equiv 1 + 4\rho_1^2 \equiv 1 + 4\rho = \Delta \pmod{4\pi_v}$$

不是 k_v 中的平方元.

当 $l \equiv 2 \pmod{3}$ 并且 $e > 1$ 时, 取 $u = \pi_v^{\frac{l-2}{3}}$, 则

$$u^6 + r_1^2 = \pi_v^{2l-4} (1 + \alpha^2 \pi_v^4) = \pi_v^{2l-4} [(1 + \alpha \pi_v^2)^2 - 2\alpha \pi_v^2].$$

因为 $e \geq 3$, 根据文献 [10, 63:5], 有

$$\delta((1 + \alpha \pi_v^2)^2 - 2\alpha \pi_v^2) = (\pi_v)^{e+2}.$$

故 $u^6 + r_1^2$ 不是 k_v 中的平方元.

当 $l \equiv 2 \pmod{3}$ 并且 $e = 1$ 时, 利用剩余类域是特征为 2 的完全域以及 $2^f - 1$ 与 3 互素, 存在 $\rho_1, u_1 \in \mathfrak{o}_v^\times$ 使得

$$\rho \equiv \rho_1^2 \pmod{\pi_v} \quad \text{并且} \quad u_1^3 \equiv 2\pi_v^{-1} \alpha \rho_1 \pmod{\pi_v}.$$

取 $u = u_1 \pi_v^{\frac{l+1}{3}}$, 则

$$u^6 + r_1^2 = \alpha^2 \pi_v^{2l} (1 + \alpha^{-2} u_1^6 \pi_v^2).$$

根据文献 [10, 63:1], 有

$$1 + \alpha^{-2} u_1^6 \pi_v^2 = 1 + 4(2^{-1} \pi_v \alpha^{-1} u_1^3)^2 \equiv 1 + 4\rho_1^2 \equiv 1 + 4\rho = \Delta \pmod{4\pi_v}$$

不是 k_v 中的平方元. □

注 2.1 在定理 1.2 的证明中, 我们事实上证明了, 当 $[k_v : \mathbb{Q}_2]$ 为奇数时, 对于 k_v 中的任意给定非零元 r_1 , 都存在 k_v 中元素 u 使得 $r_1^2 + u^6$ 不是 k_v 中的平方元. 需要指出的是, $[k_v : \mathbb{Q}_2]$ 为奇数的假设条件不能去掉. 例如 $k_v = \mathbb{Q}_2(\sqrt{5})$, 利用文献 [10, 63:1], 对于任意 $u \in k_v$ 总有 $4 + u^6$ 是 k_v 的平方元.

3 例子

自然延伸的问题是, 若 a, b, c 和 d 为全实域 k 中的元素且其中有一个是全正数, 是否 k 中每一个全正的元素 r 都存在 k 的全正元 x, y, z 和 w 使得 $r = x^2 + y^2 + z^2 + w^2$ 同时 $ax + by + cz + dw$ 为 k 中四次或更高次元, 或其他一些多项式的形式? 根据定理 1.1 和引理 2.1, 这个问题取决于在 k 中的 dyadic 素除子和实除子局部可解性.

例 3.1 设 $k = \mathbb{Q}(\sqrt{D})$ 为实二次域, 其中 D 是无平方因子的正整数并且满足 $D \not\equiv 1 \pmod{8}$. 取定 k 中的元素 a, b, c 和 d 并且其中有一个是全正元. 如果 n 是任意给定的正整数, 则对于 k 中任何全正元 r 都存在 k 中的全正元 x, y, z 和 w 使得 $r = x^2 + y^2 + z^2 + w^2$ 并且 $ax + by + cz + dw$ 是 k 中的元素的 n 次方.

证明 根据引理 2.4, 对应的代数簇 X_r 满足

$$\{(x_v, y_v, z_v, w_v, u_v) \in X_r(k_v) : x_v > 0, y_v > 0, z_v > 0, w_v > 0\}$$

是 $X_r(k_v)$ 中的非空开集, 这里 v 是 k 的实除子.

利用引理 2.1, 有 $X_r(k_v) \neq \emptyset$, 这里 v 是有限 non-dyadic 除子. 因为 $D \not\equiv 1 \pmod{8}$, 所以 $k/\mathbb{Q}$ 中存在唯一的素除子 v 位于 2 之上. 故

$$[k_v : \mathbb{Q}_2] = [k : \mathbb{Q}] = 2.$$

利用引理 2.2 和 2.3, 对于 dyadic 素除子 v , 也有 $X(k_v) \neq \emptyset$. 结果由定理 1.1 给出. $\square$

另外, 类似的结果在有理数域 $\mathbb{Q}$ 上不成立.

例 3.2 若 a, b, c 和 d 为 $\mathbb{Q}$ 中不全为 0 的元素, 则对于任意给定的正整数 $n \geq 4$, 非零有理数 r 使得方程组

$$\begin{cases} x^2 + y^2 + z^2 + w^2 = r, \\ ax + by + cz + dw = u^n \end{cases}$$

在 $\mathbb{Q}_2$ 中无解当且仅当

$$r \in \left\{ -\frac{4^{kn+l}(t+8s)}{(a^2+b^2+c^2+d^2)t} : k, l, s, t \in \mathbb{Z}; 2 \leq l \leq (n-2); (t, 2) = 1 \right\}.$$

证明 设 X_r 是由上述方程定义的代数簇. 利用引理 2.2 和文献 [10, 73:2], 有 $X_r(\mathbb{Q}_2) = \emptyset$ 当且仅当对所有 $u \in \mathbb{Q}_2$ 均有 $u^{2n} - (a^2 + b^2 + c^2 + d^2)r$ 是 $\mathbb{Q}_2$ 中的平方元.

若

$$r \in \left\{ -\frac{4^{kn+l}(t+8s)}{(a^2+b^2+c^2+d^2)t} : k, l, s, t \in \mathbb{Z}; 2 \leq l \leq (n-2); (t, 2) = 1 \right\},$$

根据文献 [10, 63:1], 当 $u = 0$ 时,

$$-(a^2 + b^2 + c^2 + d^2)r = 4^{kn+l} \left(1 + \frac{8s}{t} \right)$$

是 $\mathbb{Q}_2$ 中的平方元. 当 $u \neq 0$ 时,

$$\left| \frac{1}{2} \text{ord}_2(-(a^2 + b^2 + c^2 + d^2)r) - n \cdot \text{ord}_2(u) \right| = |kn + l - n \cdot \text{ord}_2(u)| \geq 2.$$

利用文献 [10, 63:1], $u^{2n} - (a^2 + b^2 + c^2 + d^2)r$ 是 $\mathbb{Q}_2$ 中的平方元.

若

$$r \notin \left\{ -\frac{4^{kn+l}(t+8s)}{(a^2+b^2+c^2+d^2)t} : k, l, s, t \in \mathbb{Z}; 2 \leq l \leq (n-2); (t, 2) = 1 \right\},$$

我们将证明存在 $u \in \mathbb{Q}_2$ 使得 $u^{2n} - (a^2 + b^2 + c^2 + d^2)r$ 不是 $\mathbb{Q}_2$ 中的平方元.

当 $-(a^2 + b^2 + c^2 + d^2)r$ 不是 $\mathbb{Q}_2$ 的平方元时, 则取 $u = 0$ 即可. 只需要考虑

$$-(a^2 + b^2 + c^2 + d^2)r$$

是 $\mathbb{Q}_2$ 中平方元的情形. 因此可以记

$$-(a^2 + b^2 + c^2 + d^2)r = 4^\delta \left(1 + \frac{8s}{t}\right),$$

其中 $\delta, s, t \in \mathbb{Z}$ 并且 $(t, 2) = 1$. 利用带余除法, 有 $\delta = qn + l$, 其中 $q, l \in \mathbb{Z}$ 并且 $0 \leq l \leq n - 1$. 根据 r 的选取, $l = 0, 1$ 或 $n - 1$.

如果 $l = 0$, 取 $u = 2^q$, 则

$$u^{2n} - (a^2 + b^2 + c^2 + d^2)r = 2^{2qn} + 4^{qn} \left(1 + \frac{8s}{t}\right) = 2^{2qn} \left(2 + \frac{8s}{t}\right)$$

不是 $\mathbb{Q}_2$ 的平方元.

如果 $l = 1$, 取 $u = 2^q$, 则

$$u^{2n} - (a^2 + b^2 + c^2 + d^2)r = 2^{2qn} + 4^{qn} \left(4 + \frac{32s}{t}\right) = 2^{2qn} \left(5 + \frac{32s}{t}\right)$$

不是 $\mathbb{Q}_2$ 的平方元.

如果 $l = n - 1$, 取 $u = 2^{q+1}$, 则

$$u^{2n} - (a^2 + b^2 + c^2 + d^2)r = 4^{(q+1)n} + 4^{(q+1)n} \left(4^{-1} + \frac{2s}{t}\right) = 4^{(q+1)n-1} \left(5 + \frac{8s}{t}\right)$$

不是 $\mathbb{Q}_2$ 的平方元. □

致谢 感谢南京大学孙智伟教授让我们注意到文献 [11] 以及他的猜想, 感谢审稿人详尽的修改意见.

参考文献

- 1 Colliot-Thélène J L, Sansuc J J. Sur le principe de Hasse et l'approximation faible, et sur une hypothèse de Schinzel. *Acta Arith*, 1982, 41: 33–53
- 2 Colliot-Thélène J L, Skorobogatov A N. *The Brauer-Grothendieck Groups*. Switzerland: Springer, 2021
- 3 Colliot-Thélène J L, Skorobogatov A N, Swinnerton-Dyer S P. Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points. *Invent Math*, 1998, 134: 579–650
- 4 Colliot-Thélène J L, Skorobogatov A N, Swinnerton-Dyer S P. Rational points and zero-cycles on fibred varieties: Schinzel's hypothesis and Salberger's device. *J Reine Angew Math*, 1998, 495: 1–28
- 5 Colliot-Thélène J L, Swinnerton-Dyer S P. Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties. *J Reine Angew Math*, 1994, 453: 49–112
- 6 Colliot-Thélène J L, Sansuc J J, Swinnerton-Dyer P. Intersections of two quadrics and Châtelet surfaces I. *J Reine Angew Math*, 1987, 373: 37–107
- 7 Colliot-Thélène J L, Xu F. Strong approximation for the total space of certain quadric fibrations. *Acta Arith*, 2013, 157: 169–199
- 8 Harari D. Méthode des fibrations et obstruction de Manin. *Duke Math J*, 1994, 75: 221–260
- 9 Harpaz Y, Wittenberg O. On the fibration method for zero-cycles and rational points. *Ann of Math (2)*, 2016, 186: 229–295
- 10 O'Meara O T. *Introduction to Quadratic Forms*. New York: Springer-Verlag, 1971
- 11 Sun Z W. Sum of four rational squares with certain restrictions. *arXiv:2010.05775v7*, 2022
- 12 Swinnerton-Dyer S P. Rational points on pencils of conics and on pencils of quadrics. *J Lond Math Soc (2)*, 1994, 50: 231–242
- 13 Weil A. *Basic Number Theory*. Berlin: Springer-Verlag, 1967

Proof of one of Sun Zhi-Wei's conjectures

Heng Song & Fei Xu

Abstract We prove one of Sun Zhi-Wei's conjectures. Let k be a totally real field and set $k_{\geq 0} = \{t \in k : t \geq 0\}$. Let $a, b, c, d \in k$, where one of all is totally positive and $n \in \{2, 3\}$. Then each $r \in k_{\geq 0}$ can be written as $x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in k_{\geq 0}$ such that $ax + by + cz + dw \in \{t^n : t \in k\}$.

Keywords weak approximation, dyadic local field, rational point

MSC(2020) 11E95, 14G05, 14G12

doi: 10.1360/SSM-2023-0335