arXiv:2301.02107v2 [math.NT] 1 Feb 2024

用10个量词在 $\mathbb{Z}$ $\mathbb{Q}$ 中给出全称定义

NICOLAS DAANS

Abstract. 我们证明，对于整体域 K，每个 S-整数环都可以在 K 中用含10个量词的全称一阶定义来定义。我们还证明， K 中任意有限个赋值环的交都可以在 K 中用含3个量词的存在定义来定义。

1. Introduction

长期以来，一个尚未解决的问题是：整数环 $\mathbb{Z}$ 是否能在环的语言下的有理数域 $\mathbb{Q}$ 中用存在一阶定义来定义。用更代数的术语来说，问题是是否存在一个自然数 m 和一个多项式 $F \in \mathbb{Q}[X, Y_1, \dots, Y_m]$，使得

$$\mathbb{Z} = \{x \in \mathbb{Q} \mid \exists y_1, \dots, y_m \in \mathbb{Q} : F(x, y_1, \dots, y_m) = 0\}.$$

尽管这个问题的答案仍然未知，Koenigsmann还是证明了补集 $\mathbb{Q} \setminus \mathbb{Z}$ 在 $\mathbb{Q}$ [Koe16]中是存在可定义的。换句话说，他证明了存在一个自然数 m和一个多项式 $F \in \mathbb{Q}[X, Y_1, \dots, Y_m]$，使得

$$\mathbb{Z} = \{x \in \mathbb{Q} \mid \forall y_1, \dots, y_m \in \mathbb{Q} : F(x, y_1, \dots, y_m) \neq 0\}. \tag{1}$$

也就是说， $\mathbb{Z}$ 在 $\mathbb{Q}$中具有全称一阶定义，数值m 称为量词的数量。在本文中，我们证明可以找到一个多项式 F，使得（1）对于 $m = 10$已经成立，即 $\mathbb{Z}$ 在 $\mathbb{Q}$ 中具有仅含10个量词的全称一阶定义。

事实上，我们证明了更强的结论。Park [Par13], Eisentr¨ager、Morrison [EM18] 和作者 [Daa21] 的工作表明，Koenigsmann 的方法可以更广泛地应用，从而证明：在任意整体域 K中，任意S-整数环都有一个全称一阶定义。整体域指的是数域（即 $\mathbb{Q}$的有限域扩张），或整体函数域（即有限域上的单变元函数域）。对于整体域 K 及其赋值的有限（可能为空）集合 S， K的 S-整数环定义为 K 的所有赋值环的交集，但不包括由以下赋值确定的赋值环

日期：2024年 2nd 星期五。本文是以下文章的已接受版本，该文章已以最终形式发表于 https://doi.org/10.1112/jlms.12864：Nicolas Daans。《用10个量词对 $\mathbb{Z}$ 进行全称定义》。载于：《伦敦数学学会杂志》109.2（2024），e12864。

S中的赋值。注意，$\mathbb{Z}$ 是 $\mathbb{Q}$的 $\emptyset$-整数环。我们的主要结果可概述如下。

定理（见定理 5.6）。设 K 是一个整体域，S 是 K上的有限赋值集。存在一个多项式 $F \in K[X, Y_1, \dots, Y_{10}]$，使得对于 S-整数环 $\mathcal{O}_S$，我们有

$$\mathcal{O}_S = \{x \in K \mid \forall y_1, \dots y_{10} \in K : F(x, y_1, \dots, y_{10}) \neq 0\}.$$

在 [Koe16；Par13；EM18] 中，量词的数量并未计算；根据 Koenigsmann 文章的预印本，他的方法可导出一个含 418 个量词的全称定义 [Koe10，定理 1]。在 [Daa21] 中，证明了整体域中的 S-整数环具有一个含 37 个量词的全称定义；对于 $\mathbb{Z}$ 在 $\mathbb{Q}$中的情形，Sun 和 Zhang 在 [ZS22]中将其进一步改进为 32 个量词。

研究存在性定义域的子集所需的量词数量有多方面的动机。例如，众所周知，如果 $\mathbb{Z}$ 能在 $\mathbb{Q}$中存在可定义，那么就可以推出不存在能够判定多项式方程在 $\mathbb{Q}$中是否有零点的算法。这一观察可以定量化（见 [DDF21，命题 8.21，评注 8.22]）：如果 $\mathbb{Z}$ 能在 $\mathbb{Q}$中用 N 个量词存在可定义，其中 N是某个自然数，那么就可以推出 $\mathbb{Q}$的每个递归可枚举子集都能用 $12N$ 个量词存在可定义。特别地，由希尔伯特第十问题的否定解可知，不存在能够判定含有 $12N$个变元的多项式方程在 $\mathbb{Q}$上是否有零点的算法。

我们可以使用类似的论证，根据 $\mathbb{Z}$ 在 $\mathbb{Q}$ 中由 10 个量词给出的全称可定义性，推导出以下不可判定性结果：

推论（见推论 6.2）。存在一个 $F \in \mathbb{Z}[X, Y_1, \dots, Y_9, Z_1, \dots, Z_{10}]$，具有以下性质：不存在算法能够判定，对于给定的 $x \in \mathbb{Q}$，是否

$$\forall y_1, \dots, y_9 \in \mathbb{Q}\ \exists z_1, \dots, z_{10} \in \mathbb{Q} : F(x, y_1, \dots, y_9, z_1, \dots, z_{10}) = 0.$$

非正式地说，上述推论表明，$\mathbb{Q}$ 的 $\forall_9\exists_{10}$ 理论是不可判定的。Koenigsmann 已证明，$\mathbb{Q}$ 的 $\forall\exists$ 理论是不可判定的（即不考虑全称量词或存在量词的数量）。$\mathbb{Q}$ 的 $\forall_9\exists_{32}$ 理论的不可判定性见于 [ZS22，定理 1.3]。

在证明主定理的过程中，我们还得到了其他一些界限更优的经典存在性可定义性结果。例如：

命题（见命题 4.2）。设 K 为整体域，R 为 K的赋值环的有限交。则存在一个多项式 $F \in K[X, Y_1, Y_2, Y_3]$ 使得

$$R = \{x \in K \mid \exists y_1, y_2, y_3 \in K : F(x, y_1, y_2, y_3) = 0\}.$$

整体域的赋值环（因而整体域的赋值环的有限交）是存在可定义的，这一事实几十年来一直为人所知；在某些情形下，甚至早已证明可以用 3 个量词实现这一点；参见备注4.3中的讨论。我们为上述命题提供了一个概念上简洁的论证，一次性涵盖所有情形，并且进一步以一致的方式实现这一点；参见备注4.4。

本文结构如下。接下来的两节介绍预备知识。具体而言，第2节陈述关于域（尤其是整体域）上的存在可定义子集的一些一般性结果（大多是众所周知的），并特别关注量词的数量。四元数代数（以及二次型）在整体域上的研究，在确立整体域子环的存在可定义性方面发挥了重要的历史作用。因此，第3节概述有关整体域和四元数代数的一些代数成分——更多细节见 [Daa21，第3节和 4]。

第4节陈述并证明本文所述的整体域中赋值环的存在可定义性结果。我们还将发展一些技巧，以少于朴素做法所需的量词数量，对赋值环的某些子集以及赋值环的笛卡尔积进行存在性定义。第5节给出主定理的证明。最后，在较短的第6节中，我们讨论这一结果对研究 $\mathbb{Q}$的递归可枚举子集所产生的影响。

致谢。作者感谢 Yong Hu 指出本稿先前版本第4节开头的一处错误，感谢 Silvain Rideau-Kikuchi 指出定理 5.6 证明先前版本中的一些歧义，并感谢匿名审稿人提出的多项建议，这些建议有助于改善本文的表达。

本工作源自作者的博士论文 [Daa22], ，该论文得到 FWO博士奖学金基础研究资助 51581 和 83494 的支持。

2. Existentially definable subsets of fields and number of quantifiers

将域的子集定义为存在可定义，有多种不同方式；根据具体语境，在这些等价定义之间切换会很方便。这些等价关系广为人知，但证明时往往并未考虑尽量减少量词数量这一目标。因此，本节为这些结论提供简短证明或参考文献，并给出量化界限。最后，我们以关于整体域的存在可定义子集所需量词数量的一些一般性结果作为本节的结尾。

我们用 $\mathbb{N}$ 表示自然数集，用 $\mathbb{N}^+$ 表示非零自然数构成的真子集。

我们将采用一阶语言的基本框架，许多逻辑或模型论入门教材都介绍了这一框架，例如参见 [EFT94，第 II–III 章]。我们用 $\mathcal{L}_{\mathrm{ring}}$ 表示环的语言。它由两个常元符号 0 和 1，以及三个二元运算符号 $+$、$-$ 和 $\cdot$ 组成。类似地，$\mathcal{L}_{\mathsf{field}}$ 表示域的签名，它由两个常元符号 0 和 1、三个二元运算符号 $+$、$-$ 和 $\cdot$，以及一个一元运算符号 $.^{-1}$ 组成。给定一个域K，我们以自然的方式将 K 解释为一个 $\mathcal{L}_{\mathrm{ring}}$-结构或一个 $\mathcal{L}_{\mathsf{field}}$-结构；我们约定 $0^{-1}=0$。当 $C\subseteq K$ 时，我们用 $\mathcal{L}_{\mathrm{ring}}(C)$ 表示这样一种签名：在 $\mathcal{L}_{\mathrm{ring}}$ 中为 C 的每个元素添加一个常元符号。于是，我们可以以自然的方式将 K 解释为一个 $\mathcal{L}_{\mathrm{ring}}(C)$-结构。

对于一个签名 $\mathcal{L}$、一个 $\mathcal{L}$-公式 φ、一个变元 X 和一个 $\mathcal{L}$-项 t，我们用$\varphi(X\mid t)$表示将X 在 φ 中所有自由出现的实例替换为 t后得到的公式。引入签名为 $\mathcal{L}$的一阶公式 φ 时，我们可能写作 $\varphi(X_1,\dots,X_n)$，以表示它的自由变元属于 $X_1,\dots,X_n$。给定一个 $\mathcal{L}$-结构 K和一个元组 $(a_1,\dots,a_n)\in K^n$，我们便可以简写为$\varphi(a_1,\dots,a_n)$，而不写作 $\varphi(X_1\mid a_1,\dots,X_n\mid a_n)$。与通常一样，对于一个语句 φ，我们写 $K\models\varphi$ 表示 φ 在 K中成立。

我们主要考虑存在 $\mathcal{L}$-公式。沿用 [DDF21], 中针对 $m\in\mathbb{N}$的记法，我们用 $\exists_m$-$\mathcal{L}$- 公式表示 “ 含有 m 个量词的存在 $\mathcal{L}$- 公式 ”，也就是说，它在逻辑上等价于某个形如 $\exists X_1,\dots X_m\psi$ 的公式，其中 $\mathcal{L}$-公式 ψ不含量词。类似地，我们用 $\forall_m$-$\mathcal{L}$-公式表示“含有 m 个量词的全称$\mathcal{L}$-公式”，也就是说，它在逻辑上等价于某个形如 $\forall X_1,\dots,X_m\psi$ 的公式，其中 $\mathcal{L}$-公式 ψ不含量词。给定m_1，$m_2\in\mathbb{N}$，一个 $\exists_{m_1}\forall_{m_2}$-$\mathcal{L}$-公式等价于某个形如$\exists X_1,\dots,X_{m_1}\psi$的公式，其中 ψ 是一个 $\forall_{m_2}$-$\mathcal{L}$-公式；类似地，可以定义 $\forall_{m_1}\exists_{m_2}$-$\mathcal{L}$-公式。

2.1. 定义。设 K 是一个域，m、$n\in\mathbb{N}$。如果集合 $D\subseteq K^n$ 可用 m 个量词在 K^n 中通过一个 $\exists_m$-$\mathcal{L}_{\mathrm{ring}}$（$K$）公式定义，则称其为存在可定义的。

在所有有意义的情形下，这与引言中所提示的定义一致：

2.2. 命题。设 K 是一个域，m、$n\in\mathbb{N}^+$，并且假设 $D\subseteq K^n$ 可用 m 个量词存在可定义。那么存在 $r\in\mathbb{N}$ 以及多项式f_1、.....、$f_r\in K[X_1,\dots,X_n,Y_1,\dots,Y_m]$，使得

$$D=\{x\in K^n\mid \exists y\in K^m : f_1(x,y)=\ldots=f_r(x,y)=0\}. \tag{2}$$

此外，若 K 不是代数闭的，则不失一般性，我们可以假设 $r=1$ 在（2）中。

证明。根据 [DDF21，推论 4.12] ，我们知道 D 可以用一个含有 m 个量词的正存在 $\mathcal{L}_{\mathrm{ring}}(K)$ 公式定义，即一个在逻辑上等价于 $\exists Y_1,\dots,Y_m\psi$ 的公式，其中某个 $\mathcal{L}_{\mathrm{ring}}(K)$ 公式 ψ 由原子 $\mathcal{L}_{\mathrm{ring}}(K)$ 公式仅通过合取和析取构成（不含否定）。根据

[DDF21，评注 3.4] 这意味着，对于某些 r 和 $f_1, \ldots, f_r$， D 可以按 (2) 中的方式描述；当 K 不是代数闭时，可以取 $r = 1$。□

我们进一步注意到，如果我们使用域 $\mathcal{L}_{\mathsf{field}}$ 的签名，而不是环的语言 $\mathcal{L}_{\mathrm{ring}}$，那么并不会获得任何额外益处：

2.3. 命题。设 $\varphi(x_1, \ldots, x_n)$ 是一个无量词的 $\mathcal{L}_{\mathsf{field}}$公式。存在一个无量词的 $\mathcal{L}_{\mathrm{ring}}$公式 $\psi(x_1, \ldots, x_n)$，使得对于每个以自然方式解释为 $\mathcal{L}_{\mathsf{field}}$结构的域 K，以及所有 $(a_1, \ldots, a_n) \in K^n$，我们都有

$$K \models \varphi(a_1, \ldots, a_n) \;\Leftrightarrow\; K \models \psi(a_1, \ldots, a_n).$$

非正式地说，该命题表明，可以从一个无量词的 $\mathcal{L}_{\mathsf{field}}$公式中“消去分母”，从而得到一个无量词的 $\mathcal{L}_{\mathrm{ring}}$公式。为完整起见，我们给出形式证明。

命题 2.3 的证明。考虑 $n \in \mathbb{N}$ 以及两个 $\mathcal{L}_{\mathrm{ring}}$项 $t(x_1, \ldots, x_n)$ 和$s(x_1, \ldots, x_n)$。我们可以找到多项式 f、$g \in \mathbb{Z}[X_1, \ldots, X_n]$，使得对于所有域 K和 $a \in K^n$，$t^K(a) = f(a)$，且 $s^K(a) = g(a)$。令 $d \in \mathbb{N}$和 $f_0, \ldots, f_d \in \mathbb{Z}[X_2, \ldots, X_n]$ 满足 $f = \sum_{i=0}^{d} X_1^i f_i(X_2, \ldots, X_n)$，并考虑

$$h = \sum_{i=0}^{d} X_1^{d-i} f_i(X_2, \ldots, X_n).$$

现在我们看到，公式 $t(x_1 \mid x_1^{-1}) \doteq s$ 对所有域都等价于

$$\begin{aligned}&(h(x_1, \ldots, x_n) \doteq x_1^d g(x_1, \ldots, x_n) \wedge \neg(x_1 \doteq 0))\\ &\vee (x_1 \doteq 0 \wedge f(0, x_2, \ldots, x_n) \doteq g(0, x_2, \ldots, x_n)).\end{aligned}$$

对无量词的 $\mathcal{L}_{\mathsf{field}}$-公式 φ递归地应用这一过程，可以消去所有出现的 $^{-1}$，并得到一个等价的无量词 $\mathcal{L}_{\mathrm{ring}}$-公式。□

2.4. 推论。设 K 是一个域，$m, n \in \mathbb{N}$。若子集 $D \subseteq K^n$ 可由一个 $\exists_m$-$\mathcal{L}_{\mathsf{field}}(K)$-公式定义，则它也可由一个 $\exists_m$-$\mathcal{L}_{\mathrm{ring}}(K)$-公式定义。

证明。这直接由命题 2.3 得出。□

我们进一步注意到，若 $D_1, D_2 \subseteq K^n$ 分别可由含有 m_1个和 m_2 个量词的公式存在可定义，则 $D_1 \cup D_2$ 可由含有 $\max\{m_1, m_2\}$ 个量词的公式存在可定义。另一方面，在相同情况下，$D_1 \cap D_2$可由含有 $m_1 + m_2$ 个量词的公式朴素定义。以下结果表明，至少对于整体域，在后一种情况下我们也能稍作改进。

2.5. 定理。设 K 是一个在完美子域上有限生成的域。对于任意的 m_1、m_2、$n \in \mathbb{N}$，若 m_1、$m_2 \geq 1$ 以及 D_1、$D_2 \subseteq K^n$ 满足：D_1 是 $\exists_{m_1}$-$\mathcal{L}_{\mathrm{ring}}(K)$-可定义的，且 D_2 是 $\exists_{m_2}$-$\mathcal{L}_{\mathrm{ring}}(K)$-可定义的，则 $D_1 \cap D_2$ 是$\exists_{m_1+m_2-1}$-$\mathcal{L}_{\mathrm{ring}}(K)$-可定义的。

证明。参见 [DDF21，第 1.4] 定理。 □

最后，我们提到，目前我们没有太多合适的技术可以证明，给定整体域的一个子集对于给定的自然数 m不是 $\exists_m$-$\mathcal{L}_{\text{ring}}(K)$-可定义的；参见 [DDF21 第 8] 节中的讨论。特别是，我们没有任何一个整体域 K 的 $\exists$-$\mathcal{L}_{\text{ring}}(K)$-可定义子集，并能证明它不是 $\exists_2$-$\mathcal{L}_{\text{ring}}(K)$-可定义的。

另一方面，对于整体域 K 的子集为 $\exists_1$-$\mathcal{L}_{\text{ring}}(K)$-可定义的情形，已有一些必要条件。若 K 是特征为 p 的非完美域（例如特征为 p 的整体域），且 $k \in \mathbb{N}$，则 p^k 次幂的集合 $K^{(p^k)}$ 是 $\exists_1$-$\mathcal{L}_{\text{ring}}$- 可定义的无限真子环 K。若 K 是整体域，则可以证明，这些正是 K 的唯一 $\exists_1$-$\mathcal{L}_{\text{ring}}(K)$-可定义的无限真子环：

2.6. 定理。设 K 是整体域， $R \subseteq K$ 是 K 的一个无限真子环。那么 $K \setminus R$ 在 K 中不是 $\exists_1$-$\mathcal{L}_{\text{ring}}(K)$-可定义的。若 $\text{char}(K) = p > 0$，且 R 在 K 中是 $\exists_1$-$\mathcal{L}_{\text{ring}}(K)$-可定义的，则 $R = K^{(p^k)}$ 对某个 $k \in \mathbb{N}$ 成立。

证明。令 $p = \text{char}(K)$。首先假设，如果 $p > 0$，那么 $R \not\subseteq K^{(p)}$；稍后我们将说明如何将问题归约到这一情形。

根据 [DDF21, 推论 8.5]（鉴于 [DDF21, 推论 4.21]），为了证明R 和 $K \setminus R$ 在 K中不是 $\exists_1$-$\mathcal{L}_{\text{ring}}(K)$-可定义的，只需证明 R 和$K \setminus R$ 不是 K 的薄子集（见 [DDF21, 定义 8.1]）。我们将使用以下事实：如果 L/K 是有限可分域扩张，且 $D \subseteq L$ 是 L的薄子集，那么$D \cap K$ 是 K [的薄子集 FJ08, 推论 12.2.3]。

如果 $p = 0$，令 $K_0 = \mathbb{Q}$。否则，固定一个超越元 $T \in R$，使得 $K/\mathbb{F}_p(T)$ 是有限可分域扩张，并令 $K_0 = \mathbb{F}_p(T)$。令$R_0 = R \cap K_0$。由于 R_0 包含 $\mathbb{Z}$ 或 $\mathbb{F}_p[T]$中的一个，根据 K_0 [DDF21, 评注 8.14], ，它在 K_0 [中不是薄的，从而 R 在 K中不是薄的。这就完成了以下证明：当 $R \not\subseteq K^{(p)}$时， R 在 K 中不是 $\exists_1$-$\mathcal{L}_{\text{ring}}(K)$-可定义的。

为了证明 $K \setminus R$ 在 K 中不是 $\exists_1$-$\mathcal{L}_{\text{ring}}(K)$-可定义的，我们分两种情况讨论。对于第一种情况，假设 $R_0 = K_0$。那么 R 是一个域，因此存在 $x \in K$ 使得 $xR \subseteq K \setminus R$。由于 R 在 K 中不是薄的， xR 也不是薄的，因此 $K \setminus R$ 也不是薄的。在第二种情况下， $R_0 \neq K_0$。那么 $(K_0 \setminus R_0)^{-1}$ 包含 K_0 上某个离散赋值的极大理想，因此不是薄的 K_0，从而 $K_0 \setminus R_0$ 在 K_0 中不是薄的，进而 $K \setminus R$ 在 K 中也不是薄的。我们得出结论：当 $R \not\subseteq K^{(p)}$ 时，$K \setminus R$ 在 K 中不是 $\exists_1$-$\mathcal{L}_{\text{ring}}(K)$-可定义的。

现在考虑 $R \subseteq K^{(p)}$ 的情形。在这种情形下， R 在 K 中是薄的，因此 $K \setminus R$ 在 K 中不是薄的，从而 $K \setminus R$ 不是 $\exists_1$-$\mathcal{L}_{\text{ring}}(K)$-可定义的。我们进一步作如下观察：如果 R 在 K 中是 $\exists_1$-$\mathcal{L}_{\text{ring}}(K)$-可定义的，那么它在 $K^{(p)}$ 中也会是 $\exists_1$-$\mathcal{L}_{\text{ring}}($ $K^{(p)}$)-可定义的。事实上，根据命题 2.2，存在 $f \in K[X, Y]$ 使得

$$R = \{x \in K \mid \exists y \in K : f(x, y) = 0\} = \{x \in K^{(p)} \mid \exists y \in K^{(p)} : f(x, y^{1/p})^p = 0\}.$$

由于 $f(X, Y^{1/p})^p \in K^{(p)}[X, Y]$，我们得到所需的 $\exists_1$-$\mathcal{L}_{\mathrm{ring}}(K^{(p)})$-可定义性，即 R 在 $K^{(p)}$ 中的可定义性。此外，除非 $R = K^{(p)}$，否则 $R \cap K^{(p)}$ 是整体域 $K^{(p)}$ 的一个无限真子环。反复应用这一观察，并利用对于某个 $k \in \mathbb{N}$ 有 $R \not\subseteq K^{(p^k)}$，我们可以将问题归结为此前已处理的情形 $R \not\subseteq K^{(p)}$，并得出结论：事实上，R 在 K 中不是 $\exists_1$-$\mathcal{L}_{\mathrm{ring}}(K)$- 可定义的。□

3. Quaternion algebras over global and local fields

我们回顾一些关于整体域及其上的四元数代数的基本事实；其中大多数也见于 [Daa21 的第3节和 4]。

对于域 K上的赋值 v，我们用 $\mathcal{O}_v$ 表示 v的赋值环，用 $\mathfrak{m}_v$表示 $\mathcal{O}_v$的唯一极大理想，并用 K_v 表示 $\mathcal{O}_v$的完备化的分式域。我们也称有序对（K，v）为赋值域。给定 $a \in \mathcal{O}_v$，我们用$\overline{a}^v$ 表示 a 模 $\mathfrak{m}_v$的剩余类。类似地，对于多项式 $f \in \mathcal{O}_v[X_1, \ldots, X_n]$，我们用 $\overline{f}^v$ 表示 $Kv[X_1, \ldots, X_n]$中的相应剩余多项式。对于域 K，我们用 $\mathcal{V}_K$ 表示 K上 $\mathbb{Z}$赋值的集合，即 K 上赋值群为 $\mathbb{Z}$的赋值的集合。

现在假设 K 是一个整体域。在这种情况下，K 上的 $\mathbb{Z}$赋值对应于通常所说的有限素点。注意，对于 $x \in K^\times$，仅有有限多个 $v \in \mathcal{V}_K$ 满足 $v(x) \neq 0$（另见例如 [OMe00，定理 33:1]）。对于 $v \in \mathcal{V}_K$，域 K_v 是一个具有有限剩余域的完备 $\mathbb{Z}$赋值域。我们称具有有限剩余域的完备 $\mathbb{Z}$赋值域为局部域。若域 K 上的赋值 v 满足 $v(2) > 0$（等价地，$\mathrm{char}(Kv) = 2$），则称其为二进赋值的；否则称为非二进。

我们先介绍赋值论中的两个标准结果，以便后续使用。对于一元多项式 f，我们用 f'表示它的形式导数。

3.1. 定理（亨泽尔引理）。设 K 是一个赋有完备 $\mathbb{Z}$赋值 v的域。设 $f \in \mathcal{O}_v[X]$ 是一个多项式，且 $a_0 \in \mathcal{O}_v$ 满足$v(f(a_0)) > 2v(f'(a_0))$。那么存在某个 $a \in \mathcal{O}_v$，使得 $f(a) = 0$且 $v(a_0 - a) > v(f'(a_0))$。

证明。参见例如 [EP05，定理 1.3.1]。□

更一般地，若域 K 上的赋值 v 满足定理 3.1 的结论，我们就称其为亨泽尔赋值。关于赋值域的结构理论，参见 [EP05，第 4] 章。本文中出现的亨泽尔赋值仅为局部域上的完备 $\mathbb{Z}$-赋值，但我们也会陈述一些关于一般亨泽尔赋值的辅助结果。

3.2. 定理（弱逼近定理）。设 K 是一个域，$n \in \mathbb{N}$，并设 v_1、……、v_n 是 K 上两两不同的 $\mathbb{Z}$-赋值。对于任意 a_1、……、$a_n \in K$ 和 $\gamma \in \mathbb{Z}$，存在一个 $x \in K$，使得对所有 $i \in \{1, \ldots, n\}$，$v_i(x - a_i) > \gamma$。

证明。参见例如 [EP05，定理 2.4.1]；对于两两不同的 $\mathbb{Z}$-赋值，那里提到的独立性假设自动成立。□

如果一个域具有域序，则称其为实域，否则称为非实域。对于整体域 K，K 上的域序集合与 K 到 $\mathbb{R}$的域嵌入集合之间存在一一对应关系。特别地，一个整体域是实域，当且仅当它可以嵌入到 $\mathbb{R}$中。

K 上的四元数代数是一个 4 维中心单代数，且为 K-代数。若四元数代数含有零因子，则称其为分裂的；否则称为非分裂的。给定域扩张 L/K 以及 K 上的四元数代数 Q，则$Q\otimes_K L$ 是 L上的四元数代数。若 $Q\otimes_K L$ 是分裂的（分别为非分裂的），则称 Q 在 L 上是分裂的（分别在 L上是非分裂的）。

给定 a、$b\in K$，满足 $b(1+4a)\neq 0$，我们定义 4 维 K-代数$[a,b)_K = K\oplus Ku\oplus Kv\oplus Kuv$，其中 $u^2-u=a$、$v^2=b$和 $uv+vu=v$。这是一个K-四元数代数；事实上，每个 K-四元数代数都具有这种形式，其中 a 和 b [，见 Alb39，第 IX 节.10]。对于 K-四元数代数 Q，我们将约化迹和约化范数映射分别记为 Trd 和 Nrd，$Q\to K$；定义及基本性质见 Sch85，第 8 节.5]

若四元数代数 Q 在整体域 K 上，对 K 到 $\mathbb{R}$的每个嵌入，Q 都分裂，则称其为非实的。根据定义，如果 K 不能嵌入 $\mathbb{R}$（即 K 是非实的），则 K 上的所有四元数代数都是非实的。

设 Q 是域 K上的四元数代数。定义

$$\Delta Q = \{v\in\mathcal{V}_K \mid Q \text{ is non-split over } K_v\}.$$

3.3. 命题。设 K 是局部域。对于每个二次域扩张 L/K以及 K上的任意四元数代数 Q，Q 在 L上分裂。

证明。参见 [Pie82，第 17.10] 节。□

3.4. 命题。设 K 是赋值为 v的局部域，且该赋值为 $\mathbb{Z}$-赋值。设 a、$b\in K$ 满足 $(1+4a)b\neq 0$，并且 $[a,b)_K$ 在 K上不分裂。则 $v(a)\leq 0$，此外，以下条件至少有一个成立：

(a) $v(b)$ 是奇数；(b) $v(2)=0$，且 $v(1+4a)$ 是奇数；(c) $v(2)>0$，且 $v(a)<0$。

证明。这是对 [Daa21, 命题 4.1] 的重新表述。□

3.5. 定理（阿尔伯特-布劳尔-哈塞-诺特定理与希尔伯特互反律）。设 K 为整体域，并设 Q 为非实 K四元数代数。那么 $|\Delta Q|$为偶数；此外，$\Delta Q=\emptyset$ 当且仅当 Q 分裂。反之，给定一个子集 $S\subseteq\mathcal{V}_K$，使得 $|S|$ 为偶数，则存在一个在 K-同构意义下唯一的非实 K四元数代数 Q，使得 $\Delta Q=S$。

证明。参见 [NSW08，定理 8.1.17]。□

3.6. 命题。设 K 是一个域。设 $a, b \in K$ 满足 $(1+4a)b \neq 0$，并令 $Q = [a,b)_K$。此外，设 $c, d \in K$。以下各项等价。

(i) Q 在 $X^2 - cX + d$的分裂域上分裂。(ii) 存在 $\alpha \in Q \setminus K$ 使得 $\mathrm{Trd}(\alpha) = c$ 且 $\mathrm{Nrd}(\alpha) = d$。(iii) 存在 x、y、$z \in K$，满足 $2x - c$、y 且 z 不全为零。

$$x^2 + x(c-2x) - a(c-2x)^2 - b(y^2 + yz - az^2) = d.$$

证明。(ii) 与 (iii) 之间的等价性可直接由 [Daa21 的第 3] 节中给出的约化范数和迹的公式得到。

现在我们讨论 (i) 与 (ii) 之间的等价性。若 Q 本身已经是分裂的，那么 $Q \cong \mathbb{M}_2(K)$ 中的 Trd 与矩阵迹一致，而 Nrd 与矩阵行列式一致（再参见 [Sch85，第 8.5] 节）。由于在 $\mathbb{M}_2(K)$ 中存在迹和行列式为任意指定值的非对角矩阵，因此 (i) 和 (ii) 均成立。

从现在起假设 Q 是非分裂的。对于 $\alpha \in Q \setminus K$，根据约化迹和范数的定义，我们有 $\alpha^2 - \mathrm{Trd}(\alpha)\alpha + \mathrm{Nrd}(\alpha) = 0$。因此，若 (ii) 成立，则 $K(\alpha)$ 是 $X^2 - cX + d$ 的分裂域。由于 Q 在其子域 $K(\alpha)$ 上分裂（例如参见 [Sch85, 定理 5.4]），故得到 (i)。

反过来，假设 (i) 成立。由于 Q 是非分裂的，$X^2 - cX + d$ 的分裂域是 K 的真二次扩张。根据 [Alb39, 定理 IV.27]，$X^2 - cX + d$ 的分裂域可在 K 上嵌入 Q。记 $\alpha \in Q$ 为满足 $\alpha^2 - c\alpha + d = 0$ 的一个元素，则得到 $\alpha \notin K$，$\mathrm{Trd}(\alpha) = c$ 且 $\mathrm{Nrd}(\alpha) = d$，如所需。□

4. Defining valuation rings, individually and uniformly

本节将证明，整体域 K 的子环 R 若是 K 的赋值环的有限交，则在 K 中是 $\exists_3$-$\mathcal{L}_{\mathrm{ring}}(K)$- 可定义的（命题 4.2）。这意味着，事实上对于每个自然数 n，R^n 在 K^n 中都是 $\exists_3$-$\mathcal{L}_{\mathrm{ring}}(K)$-可定义的，正如我们将在命题 4.8 中看到的。最后，在本节末尾，我们回顾一个关于赋值环有限交的一致存在可定义性的结果（主要归功于 Poonen 和 Koenigsmann），见命题 4.10。

对于域 K 和 $a \in K$，用 $K_{(a)}$ 表示 $X^2 - X - a$ 在 K 上的分裂域。换言之，若 $X^2 - X - a$ 在 K 中有根，则 $K_{(a)} = K$；否则为 $K_{(a)} \cong K[X]/(X^2 - X - a)$。

4.1. 引理。设 K 是一个整体域。设 S 是 K 上的一个有限 $\mathbb{Z}$-赋值集，Q 是 K 上的一个非实四元数代数，且 $S \subseteq \Delta Q$。设 π、$a \in K^\times$，使得对所有 $v \in \Delta Q$，都有 $v(\pi) = 1$、$v(a) \geq v(1+4a) = 0$，并且当且仅当 $v \in S$ 时，$X^2 - X - a$ 在 K_v 上有根。那么

$$\bigcap_{v \in S} \mathcal{O}_v = \{0\} \cup \{x \in K \mid Q \text{ is split over } K_{(a-(\pi x^2)^{-1})}\}. \tag{3}$$

证明。考虑 $x \in K^\times$，并令 $L = K_{(a-(\pi x^2)^{-1})}$。由于 Q 是非实的（因而在 L 上仍为非实），由定理 3.5 可知，对于 L 上的所有 $\mathbb{Z}$-赋值 w， Q 在 L 上分裂，当且仅当它在 L_w 上分裂。由于对于 L 上的任意 $\mathbb{Z}$-赋值 w，存在某个 K 上的 $\mathbb{Z}$-赋值 v，使得 $L_w \cong LK_v = (K_v)_{(a-(\pi x^2)^{-1})}$，我们得出：对所有 $v \in \Delta Q$， Q 在 L 上分裂，当且仅当它在 $(K_v)_{(a-(\pi x^2)^{-1})}$ 上分裂。为了证明 (3)，因此必须证明，对于所有 $v \in \Delta Q$， $x \in \bigcap_{v\in S} \mathcal{O}_v$ 当且仅当 Q 在 $(K_v)_{(a-(\pi x^2)^{-1})}$ 上分裂。最后，根据命题 3.3，对于任意 $v \in \Delta Q$， Q 在 $(K_v)_{(a-(\pi x^2)^{-1})}$ 上分裂，当且仅当 $(K_v)_{(a-(\pi x^2)^{-1})}/K_v$ 是一个二次域扩张，也就是说，当且仅当 $X^2 - X - (a - (\pi x^2)^{-1})$ 在 K_v 上不可约。综上，我们还需证明以下内容：

$$x \in \bigcap_{v\in S} \mathcal{O}_v \quad \Leftrightarrow \quad \forall v \in \Delta Q : X^2 - X - (a - (\pi x^2)^{-1}) \text{ is irreducible over } K_v.$$

考虑一个赋值 $v \in \Delta Q$。首先假设 $x \in \mathcal{O}_v$。设 $\alpha \in K_v$是 $X^2 - X - (a - (\pi x^2)^{-1})$ 的一个根。由于此时必有 $v(\alpha) < 0$，我们计算得 $2v(\alpha) = v(\alpha^2 - \alpha - a) = v((\pi x^2)^{-1}) = -1 - 2v(x)$，这与 v 是一个 $\mathbb{Z}$- 赋值这一事实矛盾。因此，我们得到 $X^2 - X - (a - (\pi x^2)^{-1})$ 在 K_v 上不可约。

另一方面，对于 $v \in \Delta Q$ 和 $x \in K \setminus \mathcal{O}_v$，有 $X^2 - X - (a - (\pi x^2)^{-1}) \equiv X^2 - X - a$ 模 $\mathfrak{m}_v$，因此根据亨泽尔引理（定理 3.1）， $X^2 - X - (a - (\pi x^2)^{-1})$ 在 K_v 上有根，当且仅当 $X^2 - X - a$ 在 K_v 上有根；根据假设，这恰好发生在 $v \in S$ 时。

如预期，我们得出，对于 $x \in K^\times$ 和 $v \in \Delta Q$， $X^2 - X - (a - (\pi x^2)^{-1})$ 在 K_v 上不可约，当且仅当 $v \notin S$ 或 $x \in \mathcal{O}_v$。□

4.2. 命题。设 K 为整体域。设 S 为 K上的一个有限集，其中包含 $\mathbb{Z}$-赋值。那么 $\bigcap_{v\in S} \mathcal{O}_v$ 在 K中有一个 $\exists_3$-$\mathcal{L}_{\text{ring}}(K)$-定义。

证明。存在一个 K 上的非实四元数代数 Q，使得 $S \subseteq \Delta Q$，此外， ΔQ 是有限的。这可由定理 3.5 的第二部分推出；也可以用更初等的方法看出，参见例如 [Daa22，引理 6.3。6]

由弱逼近（定理 3.2），我们可以找到 $\pi, a \in K^\times$，使引理 4.1 的条件得到满足，从而 (3) 成立。因此，只需证明 (3) 右侧的集合在 K中有一个 $\exists_3$-$\mathcal{L}_{\text{ring}}(K)$-定义。这可直接由命题 3.6 得出。□

4.3. 评注。引理 4.1 和命题 4.2 中的证明技巧可追溯至 Julia Robinson。事实上，她证明了，对于 $K = \mathbb{Q}$, $\bigcap_{v\in S} \mathcal{O}_v$ 可用 $\exists_3$-$\mathcal{L}_{\text{ring}}$ 存在可定义，其中 $S = \{v_2, v_p\}$ 满足 p 是一个模 4 同余于 $p \equiv 3$ 的素数。类似地，她证明了 $\bigcap_{v\in S} \mathcal{O}_v$ 可用 $\exists_3$-$\mathcal{L}_{\text{ring}}$ 存在可定义，其中 $S = \{v_p, v_q\}$ 满足 p 和 q是模 4 同余于 $p \equiv 1$ 的素数，并且 q 不是模 p [的平方（Rob49，引理 3 和 4]）。 [中也有类似论证：ZS22，引理 3。1] 对于$S = \{v_2\}$。

无论如何，众所周知，在整体域中，任何赋值环（因而任何有限个赋值环的交）都是存在可定义的，参见例如：[KR92，命题 3，适用于数域；[Shl94，引理 3，适用于奇特征的整体域；或 [Eis98，定理 5，其中给出了适用于所有特征的证明。我们的论证的优点在于，在所有情形下都能得到一个只需要 3 个存在量词的公式。

4.4. 评注。考察命题 4.2 的证明可知，定义公式具有如下意义上的一致性：存在一个 $\exists_3$-$\mathcal{L}_{\mathrm{ring}}$ 公式 $\varphi(X, C_1, \ldots, C_m)$，使得对于每个整体域 K 以及 K 上的每个有限集 S 个 $\mathbb{Z}$-赋值，都存在参数 $c_1, \ldots, c_m \in K$，使得

$$\bigcap_{v \in S} \mathcal{O}_v = \{x \in K \mid K \models \varphi(x, c_1, \ldots, c_m)\}.$$

命题 4.10 将给出一个更稳健、但量词更多的公式。

在命题 4.2 的设定下，且对于 $S \neq \emptyset$，由定理 2.6 可知，$\bigcap_{v \in S} \mathcal{O}_v$ 在 K 中不可由 $\exists_1$-$\mathcal{L}_{\mathrm{ring}}(K)$ 定义。

4.5. 问题。设 K 是一个整体域。设 K 上 $\mathbb{Z}$-赋值的一个非空有限集为 S。$\bigcap_{v \in S} \mathcal{O}_v$ 在 K 中是否有一个 $\exists_2$-$\mathcal{L}_{\mathrm{ring}}(K)$ 定义?

当 R 是域 K 的子环，且 R 在 K 中存在可定义时，显然 $R^\times$ 也在 K 中存在可定义，并且对所有 $n \in \mathbb{N}$，R^n 都在 K^n 中存在可定义。然而，例如，若 R 在 K 中可用 $\exists_m$-$\mathcal{L}_{\mathrm{ring}}(K)$ 定义，那么用朴素方法在 K^n 中对 R^n 进行存在性定义需要 nm 个量词；若可应用定理 2.5，则需要 $n(m-1)$ 个量词。我们将研究在哪些情形下，所需量词数量的上界可以更小，尤其是当 R 是赋值环的有限交时。

4.6. 命题。设 R 是整闭整环，且 $K =$ = Frac(R)。对于 $x \in K$，有

$$x \in R^\times \text{ if and only if } x \neq 0 \text{ and } x + x^{-1} \in R.$$

特别地，若对 $m \in \mathbb{N}$，R 可用 $\exists_m$-$\mathcal{L}_{\mathrm{ring}}(K)$ 定义，则 $R^\times$ 也可用 $\exists_m$-$\mathcal{L}_{\mathrm{ring}}(K)$ 定义。

证明。从左向右的蕴含是显然的。反过来，假设$x + x^{-1} \in R$，那么 $x \in R[x^{-1}]$。这意味着 x 在 R上是整的，因此根据假设 $x \in R$。于是还有 $x^{-1} = (x + x^{-1}) - x \in R$，从而 $x \in R^\times$。

可定义性陈述立即得出。 □

4.7. 引理。设 K是一个域，$n \in \mathbb{N}$, v是 K上的赋值。设 $f(X_1, \ldots, X_n) \in \mathcal{O}_v[X_1, \ldots, X_n]$ 是一个没有非平凡零点的齐次多项式。对于任意元素 $a_1, \ldots, a_n \in K$，有

$$v(f(a_1, \ldots, a_n)) = \deg(f) \min\{v(a_i) \mid i \in \{1, \ldots, n\}\}$$

证明。若 $a_1 = \ldots = a_n = 0$，则无须证明，因此我们可以假设情况并非如此。将 $(a_1, \ldots, a_n)$ 乘以 $K^\times$中的一个元素不会影响命题的成立，因此不失一般性，可假设 $\min_{i=1}^n v(a_i) = 0$；我们需要证明 $v(f(a_1, \ldots, a_n)) = 0$。否则便有 $\overline{f}^v(\overline{a_1}^v, \ldots, \overline{a_n}^v) = f(a_1, \ldots, a_n)^v = 0$属于 Kv，这与 $\overline{f}^v$ 没有非平凡零点的假设矛盾。□

4.8. 命题。设 K 是一个域，S 是 K 上的有限赋值集。设 $R = \bigcap_{v\in S} \mathcal{O}_v$。假设对于所有 $v \in S$，Kv 都不是代数闭的。对于每个 $n \in \mathbb{N}^+$，存在一个多项式 $G \in K[X_1, \ldots, X_n]$，使得对于所有 $x \in K^n$，$G(x) \in R$ 当且仅当 $x \in R^n$。特别地，若对于某个 $m \in \mathbb{N}$，R 是 $\exists_m$-$\mathcal{L}_{\text{ring}}(K)$- 可定义的，那么 R^n 也是 $\exists_m$-$\mathcal{L}_{\text{ring}}(K)$- 可定义的。

证明。必要时用适当的子集替换 S 后，我们可以假设任意两个不同的 v、$w \in S$ 都满足 $\mathcal{O}_v \not\subseteq \mathcal{O}_w$。

根据关于剩余域的假设以及弱逼近的一个版本[EP05，定理 3.2.7.(3)]，，对于每个 $v \in S$，我们可以找到一个首一多项式 $f_v \in R[X]$，使其剩余类 $\overline{f_v}^v$ 的次数至少为 2，且在 Kv 上不可约。令$d = \prod_{v\in S} \deg(f_v)$，并对每个 $v \in S$ 令 $d_v = d/\deg(f_v)$。记 $f_v^* \in R[X, Y]$ 为 f_v 的齐次化，并注意到 $\overline{f_v^*}^v$ 在 Kv 上没有非平凡零点。最后，再次引用 [EP05，定理 3.2.7.(3)]，，为每个 $v \in S$ 固定一个元素 $\alpha_v \in R$，使得对所有 $w \in S \setminus \{v\}$，$v(\alpha_v) = 0$ 且 $w(\alpha_v) > 0$。现在我们定义

$$F(X, Y) = \sum_{v\in S} \alpha_v f_v^*(X, Y)^{d_v} \in R[X, Y],$$

它是 d 次齐次的。考虑 $v \in S$。我们断言，对于所有 $x, y \in K$，都有

$$v(F(x, y)) = d \min\{v(x), v(y)\}$$

为此，注意到由引理 4.7 可得

$$v(\alpha_v f_v^*(x, y)^{d_v}) = 0 + (\deg(f_v)d_v) \min\{v(x), v(y)\} = d \min\{v(x), v(y)\},$$

而对于 $w \in S \setminus \{v\}$，我们有

$$v(\alpha_w f_w^*(x, y)^{d_w}) \geq v(\alpha_w) + (\deg(f_w)d_w) \min\{v(x), v(y)\} > d \min\{v(x), v(y)\},$$

由此即可得到所需结论。由于这对所有 $v \in S$ 都成立，因此我们得到，对于所有 x，$y \in K$，都有

$$F(x, y) \in R \Leftrightarrow x \in R \text{ and } y \in R.$$

现在，我们可以对 $i \geq 1$ 归纳地定义多项式 $G_i(X_1, \ldots, X_i)$，方法是令$G_1(X_1) = X_1$，并令 $G_i(X_1, \ldots, X_i) = F(G_{i-1}(X_1, \ldots, X_{i-1}) X_i)$。我们看到，对于$x_1, \ldots, x_n \in K$，有

$$G_n(x_1, \ldots, x_n) \in R \Leftrightarrow x_1, \ldots, x_n \in R,$$

因此，G符合要求。可定义性陈述立即得出。□

我们以简短讨论一个一致的存在性可定义性结果作为本节结尾。该结果本质上归功于 Poonen 和 Koenigsmann [Poo09; Koe16], , 并将在主定理的证明中发挥核心作用。我们回顾 [Daa21, Section 5] 中的以下定义。对于一个域 K 以及其上的四元数代数 Q over$K$，我们定义 K的以下子集:

$$S(Q) = \{\mathrm{Trd}(\alpha) \mid \alpha \in Q \setminus K, \mathrm{Nrd}(x) = 1\}.$$

4.9. 定理。设 Q 是整体域 K上的非实四元数代数。那么

$$\bigcap_{v \in \Delta Q} \mathcal{O}_v = \{x + y \mid x, y \in S(Q)\}.$$

证明。参见 [Dit18, 命题 2.9]。在 $K = \mathbb{Q}$的情形中，这一论证可追溯至 [Koe16, 命题 6], , 其中运用了 [Poo09]中已提出的思想。□

4.10. 命题。设 K 是整体域。存在一个 $\exists_6$-$\mathcal{L}_{\mathrm{ring}}(K)$-公式$\varphi(X, A, B)$，使得对于所有满足$(1 + 4a)b \neq 0$ 且 $[a, b)_K$为非实的 $a, b \in K$，均有

$$\bigcap_{v \in \Delta [a,b)_K} \mathcal{O}_v = \{x \in K \mid K \models \varphi(x, a, b)\}.$$

证明。根据命题 3.6，我们有

$$\{(x, a, b) \in K^3 \mid (1 + 4a)b \neq 0 \text{ and } x \in S([a, b)_K)\}$$

是 $\exists_3$-$\mathcal{L}_{\mathrm{ring}}$-可定义的。此外，根据定理 4.9，对于满足$(1 + 4a)b \neq 0$ 且 $[a, b)_K$ 为非实的 $a, b \in K$, 我们有

$$x \in \bigcap_{v \in \Delta [a,b)_K} \mathcal{O}_v \;\Leftrightarrow\; \exists y \in K : y \in S([a, b)_K) \text{ and } x - y \in S([a, b)_K).$$

通过应用定理 2.5,

$$D_1 = \{(x, y, a, b) \in K^4 \mid (1 + 4a)b \neq 0 \text{ and } y \in S([a, b)_K)\} \quad \text{and}$$
$$D_2 = \{(x, y, a, b) \in K^4 \mid (1 + 4a)b \neq 0 \text{ and } x - y \in S([a, b)_K)\}$$

并利用 D_1 和 D_2 都可用 $\exists_3$-$\mathcal{L}_{\mathrm{ring}}(K)$定义，我们得到所需结果。□

5. Universally defining rings of S-integers

现在，我们将着手证明整体域中 S-整数环的普适可定义性，所用量词为 10个量词（定理 5.6）。

5.1. 引理。设 V 是域 K 上的一个非空赋值集， $n \in \mathbb{N}$。集合 $\bigcup_{v \in V} \mathfrak{m}_v$ 在 K 中有一个 $\exists_n$-$\mathcal{L}_{\mathrm{ring}}(K)$-定义，当且仅当 $\bigcap_{v \in V} \mathcal{O}_v$ 在 K 中有一个 $\forall_n$-$\mathcal{L}_{\mathrm{ring}}(K)$-定义。

证明。由推论 2.4，只需证明 $\bigcup_{v\in V}\mathfrak{m}_v$ 在 K 中有一个 $\exists_n$-$\mathcal{L}_{\mathsf{field}}(K)$-定义，当且仅当 $\bigcap_{v\in V}\mathcal{O}_v$ 在 K 中有一个 $\forall_n$-$\mathcal{L}_{\mathsf{field}}(K)$-定义。这又可由以下观察得出

$$\bigcap_{v\in V}\mathcal{O}_v = \left(K\setminus\left(\bigcup_{v\in V}\mathfrak{m}_v\right)^{-1}\right)\cup\{0\}.$$

□

按照 [Daa21，第 6] 节，对于整体域 K、非空有限集 $S\subseteq\mathcal{V}_K$ 和 $u\in\bigcap_{v\in S}\mathcal{O}_v^\times$，定义集合

$$\Phi_u^S = \left\{(a,b)\in K^2 \;\middle|\; b\in\bigcap_{v\in S}\mathcal{O}_v^\times, a\equiv u \bmod \prod_{v\in S}\mathfrak{m}_v\right\}.$$

5.2. 引理。设 K 为整体域，$S\subseteq\mathcal{V}_K$ 为非空有限集且 $u\in\bigcap_{v\in S}\mathcal{O}_v^\times$。集合 Φ_u^S 在 K^2 中具有一个 $\exists_3$-$\mathcal{L}_{\mathrm{ring}}(K)$- 定义。

证明。根据弱逼近，我们可以找到 $\pi\in K^\times$，使得对于所有 $v\in S$，都有 $v(\pi)=1$。我们看到，对于 a、$b\in K$，有

$$\begin{aligned}(a,b)\in\Phi_u^S &\Leftrightarrow b\in\bigcap_{v\in S}\mathcal{O}_v^\times \text{ and } \frac{a-u}{\pi}\in\bigcap_{v\in S}\mathcal{O}_v\\ &\Leftrightarrow \frac{b^2+1}{b}, \frac{a-u}{\pi}\in\bigcap_{v\in S}\mathcal{O}_v.\end{aligned}$$

其中第二个等价关系由命题 4.6 得出。根据命题 4.2，$\bigcap_{v\in S}\mathcal{O}_v$ 是 $\exists_3$-$\mathcal{L}_{\mathrm{ring}}(K)$-可定义的，因此所需结论由命题 4.8（以及推论 2.4）得出。□

5.3. 引理。设 (K,v) 是一个赋值域，并考虑有理函数

$$g(X,Y)=\frac{16X^4}{1+4X^2}-\left(\frac{(Y-1)^2}{Y}\right)^2\in K(X,Y).$$

设 $a,b\in K$ with $(1+4a^2)b\neq 0$。我们有如下结论：

(1) 若 $1+4a^2, b\in\mathcal{O}_v^\times$，则 $g(a,b)\in\mathcal{O}_v$。(2) 若 $v(1+4a^2)=0$ 且 $v(b)\neq 0$，则 $v(g(a,b))=-2|v(b)|$。(3) 若 v 是亨泽尔且非二进的，X^2-X-a^2 不可约，并且 $g(a,b)\in\mathcal{O}_v$，则 $1+4a^2, b\in\mathcal{O}_v^\times$。

证明。我们可以计算得，对于 $a\in K$，有

$$v\left(\frac{16a^4}{1+4a^2}\right)\begin{cases}=-v(1+4a^2)<0 & \text{if } v(1+4a^2)>0,\\ =2v(a)+2v(2)<0 & \text{if } v(1+4a^2)<0,\\ \geq 0 & \text{if } v(1+4a^2)=0,\end{cases}$$

类似地，对于 $b \in K$

$$v\left(\frac{(b-1)^2}{b}\right)\begin{cases} = -|v(b)| < 0 & \text{if } v(b) \neq 0, \\ \geq 0 & \text{if } v(b) = 0. \end{cases}$$

（1）和（2）现在可以立即得出。

对于（3），假设 v 是亨泽尔非二进赋值的，$X^2 - X - a^2$ 不可约，并且 $1+4a^2 \notin \mathcal{O}_v^\times$ 或 $b \notin \mathcal{O}_v^\times$ 成立；我们需要证明 $g(a,b) \notin \mathcal{O}_v$。若 $b \in \mathcal{O}_v^\times$，则由上文中的计算可立即得到结论。为导出矛盾，假设 $b \notin \mathcal{O}_v^\times$ 且 $v(g(a,b)) \geq 0$。于是

$$v\left(\left(\frac{4a^2b}{(b-1)^2}\right)^2 \frac{1}{1+4a^2} - 1\right) = v\left(\left(\frac{b}{(b-1)^2}\right)^2 g(a,b)\right) \geq |v(b)| > 0.$$

利用 (K,v) 是亨泽尔非二进赋值的这一点，可知 $1+4a^2$ 是 K 中的一个平方，这与 $X^2 - X - a^2$ 不可约的假设矛盾。□

5.4. 引理。设 (K,v) 是一个赋值域，并考虑有理函数

$$g(X,Y) = X^5\left(\left(\frac{(Y-1)^2}{Y}\right)^2 - \left(\frac{(Y-1)^2}{Y}\right) - X^2\right) \in K(X,Y).$$

设 $a, b \in K^\times$。我们有如下结论：

(1) 若 $a, b \in \mathcal{O}_v^\times$，则 $g(a,b) \in \mathcal{O}_v$。(2) 若 $v(a) = 0$ 且 $v(b) \neq 0$，则 $v(g(a, b)) = -2|v(b)|$。(3) 若 $\mathrm{char}(K) = 2$，v 是亨泽尔的，$X^2 - X - a^2$ 不可约，且 $g(a,b) \in \mathcal{O}_v$，则 $a, b \in \mathcal{O}_v^\times$。

证明。对于 $b \in K$，我们有

$$v\left(\frac{(b-1)^2}{b}\right)\begin{cases} = -|v(b)| < 0 & \text{if } v(b) \neq 0, \\ \geq 0 & \text{if } v(b) = 0. \end{cases}$$

由此，(1) 和 (2) 立即成立。

对于 (3)，假设 $\mathrm{char}(K) = 2$，v 是亨泽尔的，$X^2 - X - a^2$ 不可约，且 $a \notin \mathcal{O}_v^\times$ 或 $b \notin \mathcal{O}_v^\times$；我们需要证明 $g(a,b) \notin \mathcal{O}_v$。注意，无论如何都有 $v(a) \leq 0$；否则，由于 v 的亨泽尔性，$X^2 - X - a^2$ 将是可约的。更准确地说，对于任意 $y \in K$，由于 v 是亨泽尔的，我们有 $v(y^2 - y - a^2) \leq -4v(a)$。若 $v(a) < 0$，则可得 $v(g(a,b)) < v(a) < 0$。另一方面，若 $v(a) = 0$ 且 $v(b) \neq 0$，则由 (2) 可得 $v(g(a,b)) = -2|v(b)| < 0$。这就证明了 (3)。□

对于域 K 和 $c \in K^\times$，定义集合

$$\mathsf{Odd}(c) = \{v \in \mathcal{V}_K \mid v(c) \text{ is odd}\}.$$

5.5. 引理。设 K 是一个整体域。设 $\pi \in K^\times$ 满足 $S =$Odd(π) 的基数为奇数。设 $u \in K^\times$ 满足对于所有 $v \in S$，都有 $v(u) = 0$ 且$X^2 - X - u^2$ 在 Kv上不可约。若 char(K) $= 2$，令 $g(X,Y) \in K(X,Y)$ 如引理 5.4 中所述。若 char(K) $\neq 2$，则假设 S 包含所有二进赋值，并令 $g(X,Y) \in K(X,Y)$ 如引理 5.3 中所述。

对于 $x \in K$，我们有

$$x \in \bigcup_{v \in \mathcal{V}_K \setminus S} \mathfrak{m}_v \quad \Leftrightarrow \quad \exists (a,b) \in \Phi_u^S : \frac{a^2x^2g(a,b)}{1-x-a^2x^2} \in \bigcap_{v \in \Delta[a^2, b\pi)_K} \mathcal{O}_v.$$

证明。我们首先考虑从左到右的蕴含。考虑某个 $x \in \mathfrak{m}_w$，其中 $w \in \mathcal{V}_K \setminus S$。如 Daa21 的证明中引理 6.6], 所示，我们可以找到 $(a,b) \in \Phi_u^S$，使得 $\Delta[a^2, b\pi)_K = S \cup \{w\}$ 且 $w(1+4a^2) = 0$。根据命题 3.4，必有 $w(b\pi)$ 为奇数；又因为 $w(\pi)$ 为偶数，这就意味着 $w(b)$ 为奇数。如有必要，可用 K 中的一个平方对 b 重新缩放（这不会影响 $[a^2, b\pi$ 的 K-同构类）$_K$，因此不失一般性，我们可以假设 $w(b) = 1$。

由引理 5.3 或引理 5.4 可得 $w(g(a,b)) = -2$，而对于 $v \in S$，$v(g(a,b)) \geq 0$。此外，由于对所有 $v \in S \cup \{w\}$，$X^2 - X - a^2$ 在 Kv 上不可约，因此形式 $X^2 - XY - a^2Y^2$ 在 Kv 上没有非平凡零点；由引理 4.7 计算可得，对于 $v \in S \cup \{w\} =\Delta[a^2, b\pi)_K$，有

$$\begin{aligned} v\left(\frac{a^2x^2g(a,b)}{1-x-a^2x^2}\right) &= 2v(a) + 2v(x) + v(g(a,b)) - \min\{0, 2v(a) + 2v(x)\} \\ &= \max\{v(g(a,b)), 2v(x) + v(g(a,b))\} \geq 0 \end{aligned}$$

其中，末尾的不等式由以下事实得出：$v(g(a,b)) \geq 0$ for$v \in S$，以及 $w(g(a,b)) = -2$ and $w(x) \geq 1$。因此，我们得到 $\frac{a^2x^2g}{(a,b)\,\overline{1-x-a^2x^2}} \in \bigcap_{v \in \Delta[a^2, b\pi)_K} \mathcal{O}_v$，正如所需。

对于另一个蕴含，任取（a,b） $\in \Phi_u^S$。如[Daa21，引理 6.6] 的证明中所示，我们看到 $S \subseteq \Delta[a^2, b\pi)_K$，且 $[a^2, b\pi)_K$ 是非实的，因此根据定理 3.5，存在 $w \in \Delta[a^2, b\pi)_K \setminus S$。根据命题 3.4，并利用当 char($K$) $\neq 2$时 w 为非二进赋值的这一事实，以下至少有一种情况成立：

(i) $w(b\pi)$ 是奇数。由于 $w(\pi)$ 是偶数，这意味着 $w(b)$ 是奇数；(ii) char(K) $\neq 2$ 且 $w(1+4a^2)$ 是奇数；(iii) char(K) $= 2$ 且 $w(a) < 0$。

此外，我们知道 $X^2 - X - a^2$ 在 K_w 上不可约，因为 $[a^2, b\pi)_K$ 在 K_w 上不可分裂。由引理 5.3 或引理 5.4 可得 $w(g(a,b)) < 0$。

我们计算得，对于满足 $\frac{a}{a^2x^2g(\overline{1-x-a^2x^2}} \in \bigcap_{v\in\Delta[a^2,b,\ b)\ )_K} \mathcal{O}_v$ 的 $x \in K$，有

$$\begin{aligned} 0 \le w\left(\frac{a^2x^2g(a,b)}{1-x-a^2x^2}\right) &\le 2w(a)+2w(x)+w(g(a,b))-\min\{0,2w(a)+2w(x)\} \\ &= \max\{2w(a)+2w(x)+w(g(a,b)), w(g(a,b))\} \end{aligned}$$

由于 $w(g(a,b)) < 0$，我们推断出 $2w(x) \ge -2wa(-w(g(a,b)) > 0)$，从而$x \in \mathfrak{m}_w$。这说明了另一个蕴含方向。□

5.6. 定理。设 K 为整体域，$S \subseteq \mathcal{V}_K$ 为非空有限集。集合$\bigcap_{v\in\mathcal{V}\setminus S}\mathcal{O}_v$ 在 K中具有一个 $\forall_{10}$-$\mathcal{L}_{\text{ring}}(K)$-定义。

证明。根据引理 5.1，我们只需证明$\bigcup_{v\in\mathcal{V}\setminus S}\mathfrak{m}_v$ 在 K中具有一个 $\exists_{10}$-$\mathcal{L}_{\text{ring}}(K)$-定义。此外，只需对某个包含集合 S的赋值有限集S' 证明这一点即可。事实上，我们有

$$\bigcup_{v\in\mathcal{V}\setminus S}\mathfrak{m}_v = \bigcup_{v\in S'\setminus S}\mathfrak{m}_v \cup \bigcup_{v\in\mathcal{V}\setminus S'}\mathfrak{m}_v$$

并且，对每个 $v \in S' \setminus S$ 分别而言，根据命题 4.2，$\mathfrak{m}_v$ 是 $\exists_3$-$\mathcal{L}_{\text{ring}}(K)$-可定义的：固定 v的一个一致化元 π 后，有 $\mathfrak{m}_v = \{x \in K \mid x\pi^{-1} \in \mathcal{O}_v\}$。由于 $S' \setminus S$ 是有限的，因此$\bigcup_{v\in\mathcal{V}\setminus S}\mathfrak{m}_v$ 的 $\exists_{10}$-$\mathcal{L}_{\text{ring}}(K)$-可定义性由$\bigcup_{v\in\mathcal{V}\setminus S'}\mathfrak{m}_v$的$\exists_{10}$-$\mathcal{L}_{\text{ring}}(K)$-可定义性推出。因此，在证明的其余部分中，不妨将 S 替换为一个更大的有限集。

若 $\text{char}(K) = 0$，我们将 S 扩大，使其包含所有二进赋值。根据 [Daa21, 引理 6.7]，我们还可以进一步扩大 S，使得对某个 $\pi \in K^\times$，有 $S = \text{Odd}(\pi)$，且 $|S|$ 为奇数。固定 $u \in \bigcap_{v\in S}\mathcal{O}_v^\times$，使得对于所有 $v \in S$，$X^2 - X - u^2$ 在 Kv 上不可约；根据弱逼近和 [Daa21，引理 6.5]，这样的元素 u 存在。由引理 5.5，存在一个有理函数 $g(X,Y) \in K(X,Y)$，使得对任意 $x \in K$，都有

$$x \in \bigcup_{v\in\mathcal{V}_K\setminus S}\mathfrak{m}_v \ \Leftrightarrow\ \exists a,b \in K : (a,b) \in \Phi_u^S \text{ and } \frac{a^2x^2g(a,b)}{1-x-a^2x^2} \in \bigcap_{v\in\Delta[a^2,b\pi)_K}\mathcal{O}_v.$$

由于根据引理 5.2，Φ_u^S 是 $\exists_3$-$\mathcal{L}_{\text{ring}}(K)$-可定义的，且集合$\bigcap_{v\in\Delta[a^2,b\pi)_K}\mathcal{O}_v$ 是一致地 $\exists_6$-$\mathcal{L}_{\text{ring}}(K)$-可定义的（由命题 4.10），根据定理 2.5（并结合命题 2.3），我们得到 $\bigcap_{v\in\mathcal{V}_K\setminus S}\mathfrak{m}_v$ 是用 $2+3+6-1=10$ 个量词存在可定义的。□

5.7.问题。最小的自然数是多少 m，使得 $\mathbb{Z}$ 在 $\mathbb{Q}$ 中是 $\forall_m$-$\mathcal{L}_{\text{ring}}$-可定义的?

由定理 5.6 和定理 2.6 可知，问题 5.7 的答案至少为 2，至多为 10。

6. Recursively enumerable subsets of $\mathbb{Q}$

最后，我们证明关于 $\mathbb{Q}$ 的 $\forall_9\exists_{10}$-$\mathcal{L}_{\mathrm{ring}}$-理论的预告不可判定性结果（推论 6.2）。我们将以一种清晰展现以下关系的方式给出论证：对 $\mathbb{Q}$ 中 $\mathbb{Z}$ 的普适可定义性作出进一步的定量改进，会如何影响这一不可判定性结果。该论证本质上是对 [ZS22，定理 1.3] 的证明的重新表述。

准确地说：当我们称环 R 的 $\forall_m\exists_n$-$\mathcal{L}_{\mathrm{ring}}$理论不可判定时，意思是不存在这样的算法：它以任意的 $\forall_m\exists_n$-$\mathcal{L}_{\mathrm{ring}}$语句 φ 为输入，并在有限步之后，若 $R \models \varphi$则输出 YES，若 $R \not\models \varphi$则输出 NO。

6.1. 命题。设 $m \in \mathbb{N}$ 满足 $m \geq 4$。假设 $\mathbb{Z}$ 在 $\mathbb{Q}$中是 $\forall_m$-$\mathcal{L}_{\mathrm{ring}}$可定义的。那么， $\mathbb{Q}$ 的每个递归可枚举子集都在 $\mathbb{Q}$中是 $\exists_{10}\forall_m$-$\mathcal{L}_{\mathrm{ring}}$可定义的。此外， $\mathbb{Z}$ 的每个递归可枚举子集都在 $\mathbb{Q}$中是 $\exists_9\forall_m$-$\mathcal{L}_{\mathrm{ring}}$可定义的。

特别地， $\mathbb{Q}$ 的 $\forall_9\exists_m$-$\mathcal{L}_{\mathrm{ring}}$理论是不可判定的。

证明。取一个多项式 $f \in \mathbb{Z}[X, Y]$，使得 f定义了一个单射 $\mathbb{Z}\times\mathbb{Z} \to \mathbb{N}$（例如参见 [DDF21，引理 8.19]）。对于子集 $A \subseteq \mathbb{Q}$，定义

$$\tilde{A} = \{f(a, b) \mid a, b \in \mathbb{Z}, b \neq 0, \frac{a}{b} \in A\}$$

并注意，对于任意 $a \in \mathbb{Q}$，我们有

$$a \in A \quad \Leftrightarrow \quad \exists y_0 \in \mathbb{Q}(y_0 \in \mathbb{Z}, ay_0 \in \mathbb{Z} \text{ and } f(ay_0, y_0) \in \tilde{A}).$$

˜现在假设 A 是递归可枚举的。那么 A 也是递归可枚举的。根据 [Sun21，定理 1.1(i)]，存在一个多项式 $g_{\tilde{A}} \in \mathbb{Z}[X, Y_1, \ldots, Y_9]$，使得

$$\tilde{A} = \{x \in \mathbb{N} \mid \exists y_1, \ldots, y_8 \in \mathbb{Z}, y_9 \in \mathbb{N} : g_{\tilde{A}}(x, y_1, \ldots, y_9) = 0\}.$$

我们得到，对于任意 $a \in \mathbb{Q}$，有 $a \in A$ 当且仅当

(4)
$$\exists y_0, \ldots, y_9 \in \mathbb{Q}\,(ay_0, y_0, \ldots, y_9 \in \mathbb{Z}, y_9 \geq 0, \text{ and } g_{\tilde{A}}(f(ay_0, y_0), y_1, \ldots, y_9) = 0)$$

由于 $\mathbb{Z}$ 在 $\mathbb{Q}$ 中是 $\forall_m$-$\mathcal{L}_{\mathrm{ring}}$-可定义的，且根据欧拉四平方定理，非负元素集在 $\mathbb{Q}$ 中是 $\forall_4$-$\mathcal{L}_{\mathrm{ring}}$-可定义的，因此我们得到 A 在 $\mathbb{Q}$中所需的 $\exists_{10}\forall_m$-$\mathcal{L}_{\mathrm{ring}}$-可定义性。若 $A \subseteq \mathbb{Z}$，则可以去掉 (4) 中对 y_0 的量化，并等价地写为

(5)
$$\exists y_1, \ldots, y_9 \in \mathbb{Q}\,(y_1, \ldots, y_9 \in \mathbb{Z}, y_9 \leq 0, \text{ and } g_{\tilde{A}}(f(a, 1), y_1, \ldots, y_9) = 0)$$

从而得到 A 在 $\mathbb{Q}$中是 $\exists_9\forall_m$-$\mathcal{L}_{\mathrm{ring}}$-可定义的。

对于最后一个结论，固定一个递归可枚举子集 A of $\mathbb{N}$ such that$\mathbb{N} \setminus A$ is not recursively enumerable（换言之， A is not recursive）。根据上述结果， A is $\exists_9\forall_m$-$\mathcal{L}_{\mathrm{ring}}$-definable in $\mathbb{Q}$。然而，由于 A is not recursive，不存在一种算法，能够判定给定的 $\mathbb{Q}$lies in A。这

表明， $\exists_9\forall_m$-$\mathcal{L}_{\text{ring}}$-理论——或者等价地， $\forall_9\exists_m$-$\mathcal{L}_{\text{ring}}$-理论——of $\mathbb{Q}$is 不可判定。□

6.2. 推论。 $\mathbb{Q}$ 中的每个递归可枚举子集都是 $\exists_{10}\forall_{10}$-$\mathcal{L}_{\text{ring}}$-可定义的。此外， $\mathbb{Z}$ 中的每个递归可枚举子集都是 $\exists_9\forall_{10}$-$\mathcal{L}_{\text{ring}}$-可定义的 $\mathbb{Q}$。

特别是， $\mathbb{Q}$ 的 $\forall_9\exists_{10}$-$\mathcal{L}_{\text{ring}}$理论是不可判定的。

证明。这由命题 6.1 和定理 5.6 得出。 □

References

[Alb39] A. Adrian Albert.《代数结构》。美国数学学会，1939年。[Daa21] Nicolas Daans.《整体域中有限生成子环的普遍定义》。载于：Documenta Mathematica 26（2021年），第 1851–1869 页。[Daa22] Nicolas Daans.《存在一阶定义与二次型》。博士论文。安特卫普大学，2022年。[DDF21] Nicolas Daans、Philip Dittmann 和 Arno Fehm.《丢番图集的存在秩与本质维数》。可见 arXiv:2102.06941。2021年。[Dit18] Philip Dittmann.《数域上多项式的不可约性是丢番图的》。载于：Compositio Mathematica 154（2018年），第 761–772 页。[EFT94] H.-D. Ebbinghaus、J. Flum 和 W. Thomas.《数理逻辑》。第二版。Springer，1994年。[Eis98] Kirsten Eisentr¨äger.《希尔伯特第十问题与算术几何》。博士论文。加利福尼亚大学，1998年。[EM18] Kirsten Eisentr¨äger 和 Travis Morrison.《整体域中可普遍定义与可存在定义的子集》。载于：Mathematical Research Letters 25.4（2018年），第 1173–1204 页。[EP05] Antonio J. Engler 和 Alexander Prestel.《赋值域》。Springer，2005年。[FJ08] Michael D. Fried 和 Moshe Jarden.《域算术》。第二版。Springer，2008年。[Koe10] Jochen Koenigsmann.《在 $\mathbb{Q}$中定义 $\mathbb{Z}$ 》。预印本。可见 arXiv:1011.3424v

1.

2010年10月。[Koe16] Jochen Koenigsmann. “在 $\mathbb{Q}$中定义 $\mathbb{Z}$”。载于：数学年刊。183（2016年），第73–93页。[KR92] Ki Hang Kim 和 Fred Roush。“有理数上的丢番图不可判定性的一种方法”。载于：1990年亚洲数学大会论文集。世界科学出版社，1992年，第242–248页。[NSW08] J¨urgenNeukirch、Alexander Schmidt 和 Kay Wingberg。《数域的上同调》。第二版。Springer，2008年。[OMe00] Timothy O’Meara。《二次型导论》。Springer，2000年。

[Par13] Jennifer Park。“在数域中定义整数环的一个全称一阶公式”。载于：Mathematical Research Letters 20，第5期（2013年），第961–980页。[Pie82] Richard S. Pierce。《结合代数》。Springer，1982年。[Poo09] Bjorn Poonen。“用全称存在公式刻画有理数中的整数”。载于：American Journal of Mathematics 131（2009年），第675–682页。[Rob49] Julia Robinson。“算术中的可定义性与判定问题”。载于：Journal of Symbolic Logic 14（1949年2月），第98–114页。[Sch85] Winfried Scharlau。《二次型与厄米型》。Springer，1985年。[Shl94] Alexandra Shlapentokh。“整体域全纯环的丢番图类”。载于：Journal of Algebra 1（1994年），第139–175页。[Sun21] Zhi-Wei Sun。“关于希尔伯特第十问题的进一步结果”。载于：中国科学：数学 64.2（2021年），第281–306页。[ZS22] Geng-Rui Zhang 和 Zhi-Wei Sun。“$\mathbb{Q}\setminus\mathbb{Z}$在 $\mathbb{Q}$ 上是丢番图的，含32个未知数”。载于：波兰科学院数学通报 70.2（2022年），第93–106页。

Universiteit Antwerpen, Departement Wiskunde, Middelheimlaan 1, 2020 Antwer-pen, Belgium.

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 186 75 Praha 8, Czech Republic.电子邮箱地址：nicolas.daans@matfyz.cuni.cz