arXiv:2303.02521v3 [math.NT] 3 Jun 2024

利用单位群定义 $\mathbb{Z}$

BARRY MAZUR、KARL RUBIN 和 ALEXANDRA SHLAPENTOKH

谨以此文致敬 *Henryk Iwaniec* 七十五岁寿辰

摘要。我们研究有理数域的代数扩张的整数环上的一阶可定义性与可判定性问题，并特别关注定义的统一性。定义的统一性源于我们对 $\mathbb{Z}$所给出的一阶定义十分简洁。具体而言，我们证明，对于一大类代数扩张 $K/\mathbb{Q}$,

$$\{x \in \mathscr{O}_K : \forall \varepsilon \in \mathscr{O}_K^\times \ \exists \delta \in \mathscr{O}_K^\times \text{ such that } \delta - 1 \equiv (\varepsilon - 1)x \pmod{(\varepsilon - 1)^2}\} = \mathbb{Z}$$

其中， $\mathscr{O}_K$ 表示 K的整数环。我们的结果的推论之一是，可作图数域的不可判定性；这是 Tarski 于 1948年提出的问题。

目录

1. 引言 1 2. 从子幺半群到子环的一阶转换 6 3. 在特殊情形下计算 R_K 9 4. 主定理的证明 14 5. $\mathbb{Z}$ 17不存在一致的存在量词定义或纯全称定义 参考文献 18

1. 引言

我们研究代数扩张 $\mathbb{Q}$的环和整数域中的一阶可定义性与可判定性问题，并关注建立可定义性的方式是否具有一致性。

设 K 是 $\mathbb{Q}$ 的代数扩张（可能是无限扩张），并设 $\mathscr{O}_K$ 是 K 的整数环。

2020数学主题分类。主要分类 11U05。关键词和短语。希尔伯特第十问题、丢番图定义、一阶定义。作者谨此感谢 Caleb Springer 仔细审阅本文，并感谢匿名审稿人提出的宝贵意见，以及指出我们结果对 Tarski 某个问题的影响。本文研究部分由 DMS资助项目 2152098（AS）、2152149（BM）、2152262（KR）资助。AS 在2022年夏季还获得了 ECU创意活动与研究资助的部分支持。

问题 1.1. 在环的语言中，是否存在 $\mathbb{Z}$ 在 $\mathscr{O}_K$ 上的一阶定义?

问题 1.2。 $\mathscr{O}_K$ 在环的语言中的一阶理论是否不可判定?

问题 1.3。 K 在环的语言中的一阶理论是否不可判定?

众所周知，若 $\mathscr{O}_K$ 可在 K 上定义，且 $\mathscr{O}_K$的一阶理论不可判定，则 K 的一阶理论也不可判定。本文着重研究 $\mathbb{Q}$ 的无限代数扩张的整数环的一阶理论，随后利用关于这些域的整数环相对于这些域的可定义性的若干已有结果，得到有关域的不可判定性结果。

特别地，我们回答了 A. Tarski 关于可作图数域的一阶理论（不）可判定性的一个问题（见 [Tar48], Notes #10，以及下文的推论1.11），并回答了 C. Martinez-Ranero、J. Utreras 和 C. Videla 提出的关于 $K^{(d)}$不可判定性的一个问题； $K^{(d)}$是数域 K 所有次数不超过某个固定整数 d 的扩张的合成域（见[MRUV20]）。

1.1. **环的语言**。 环的一阶语言 $(0, 1, +, \times)$ 本质上就是多项式方程的语言。对于固定的环 R，可以证明，该语言中的一个语句等价于具有如下形式的语句:

$$E_1 x_1 \dots E_r x_r \bigwedge_{i=1}^{\ell} P_i(x_1, \dots, x_r) = 0, \tag{1.4}$$

其中，每个 E_i 都是遍历 R 的全称量词或存在量词，而每个 P_i 都是系数属于 $\mathbb{Z}$ 的多项式。

可数环 R 的一阶理论，是所有形如 (1.4) 且在 R 上为真的语句所组成的集合。

利用这种语言，我们可以定义环的子集:

$$A = \{a \in R | E_1 x_1 \dots E_r x_r \bigwedge_{i=1}^{\ell} P_i(a, x_1, \dots, x_r) = 0\}, \tag{1.5}$$

其中，如上所述，每个 E_i 都是遍历 R 的全称量词或存在量词，而 P_i 是 $\mathbb{Z}$ 上的多项式。也就是说，元素 $a \in R$ 属于 A，当且仅当语句 $E_1 x_1 \dots E_r x_r \bigwedge_{i=1}^{\ell} P_i(a, x_1, \dots, x_r) = 0$ 在 R 上为真。如果 (1.5) 对集合 A 成立，我们就称集合 A 在 （一阶）可定义于 R。

如果语句 1.4 仅含存在量词，那么它属于所谓的环的存在语言，我们称满足 1.5 的集合 A 在 R上是存在可定义的。判定一个语句在环的语言中对于环 R 是否为真的问题，本质上就是该环的希尔伯特第十问题。

有时，我们会扩充环的语言，加入可数多个常量符号，使多项式的系数可以属于 R。

给定两个环 $R_1 \subset R_2$，其中 R_1 具有不可判定一阶理论，并且 R_1 在 R_2 上有如（1.5）所示的一阶定义，我们可以得出结论： R_2 的一阶理论是不可判定的。因为，如果 R_2 是可判定的，那么将给出 R_2 一阶可判定性的算法与 R_1在 R_2 上的一阶定义结合起来，就能得到判定 R_1的算法，这就产生了矛盾。

应用这一推理并取 $R_1 = \mathbb{Z}$，可知如果上述问题 1.1 的答案是“是”，那么问题 1.2 的答案也同样是“是”。

1.2. **一致定义**。

定义 1.6（代数整数环上的一致定义）。设 K 是一个代数数域， $\mathscr{L}$ 是 K 在代数闭包 K 中的一族扩张，且 A 是 $\mathscr{O}_{\bar{K}}$ 的一个子集。若存在一个多项式 $P(t, \bar{x}) \in \mathscr{O}_K[t, \bar{x}]$，它属于 $1 + r$ 个变量（t 和 $\bar{x} = (x_1, x_2, \ldots x_r)$，其中某个 $r \in \mathbb{Z}_{\geq 1}$），以及一个一阶公式，使得 A 在 $\mathscr{L}$ 中所有域的整数环上具有一致的一阶定义

$$Q(t) := E_1 x_1 \ldots E_r x_r P(t, \bar{x}),$$

其中 E_i 是全称量词或存在量词，且 t 是唯一的自由变量，并且对每个 $L \in \mathscr{L}$， $Q(t)$ 都是 $A \cap \mathscr{O}_L$ 在 $\mathscr{O}_L$ 上的一阶定义。

注记 1.7. 由于 $\mathbb{Z}$ 是存在量词不可判定的，如果 $\mathbb{Z}$ 在 $\mathscr{L}$ 中所有域的整数环上都有一致的一阶定义，那么我们就有一个单一公式，可以以一种“一致的”方式证明这些整数环是一阶不可判定的。

1.3. **简史**。关于环的一阶理论不可判定的首个结果出自 J.B. Rosser [Ros36]，其工作建立在 A. Church[Chu36] 和 K. G¨odel [G¨od31]的结果之上。所讨论的环是 $\mathbb{Z}$。J. Robinson [Rob49]为每个数域的整数环构造了 $\mathbb{Z}$ 的定义，从而证明这些环的一阶理论不可判定。她的定义形式简单 $\forall\exists \ldots \exists$，但明确依赖于扩张的次数。后来，在 [Rob62] 中，她构造了一个适用于所有数域整数环的 $\mathbb{Z}$ 一致定义，但该一致公式复杂得多。（关于一致性的含义，见定义 1.6。）本文中，我们将在所有数域的整数环以及 $\mathbb{Q}$ 的若干类无限代数扩张上，构造一个无参数的 $\mathbb{Z}$ 定义。该定义具有形式 $\forall\forall\exists \ldots \exists$。

当然，也存在关于某些数域的整数环以及某些无限代数扩张的整数环上 $\mathbb{Z}$ 的存在定义（例如，参见[Den75]，[DL78]，[Den80]，[Phe88]，[SS89]，[Shl89]，[Vid89]，[CPZ05]，[Shl07]，[Shl08]，[Shl09]，[GFP20]，[MRS22]），并且一些众所周知的猜想意味着$\mathbb{Z}$ 在每个数域的整数环上都有存在定义（参见[MR10]，[MP18]，[Pas23]）。然而，这些定义并非对所有数域一致，根据推论 5.4，它们也不可能做到一致。

尽管我们现在对数域整数环的一阶理论已有相当深入的了解，但谈到

有理数域的无限代数扩张时，情况却大不相同。例如，有些无限扩张的整数环具有可判定一阶理论（[Rum86] 和 [vdD88]），而另一些无限扩张的整数环则具有不可判定一阶理论。

J. Robinson 是首位给出 $\mathbb{Q}$ 的无限代数扩张实例的人，在这些实例中，整数环的一阶理论是不可判定的。她提出了一种方法，可为全实整数的整数环构造 $\mathbb{Z}$ 的一阶定义；她还提出了一种方法，可构造 $\mathbb{Z}$ 的一阶模型，从而证明某些非全实整数环的整数环具有不可判定性。例如，请参见 [Vid00b], [VV15], [VV16], [GR19], [CVV20], [MRUV20], [Spr20], [CF21], [Spr23]，其中给出了运用 J. Robinson 方法所得的结果，该方法应用于全实整数环以及全实域的二次扩张的整数环。

关于某些 $\mathbb{Q}$ 的无限代数扩张的整数环可在其分式域上一阶可定义，最早的重要结果由 C. Videla 得出（参见 [Vid00a], [Vid00b]）。第三位作者在 [Shl18] 中推广了这些结果。

1.4.**全实代数数与全实代数整数**。整数环及其分式域在其一阶理论的可判定性／不可判定性方面，表现并不总是相同。M. Fried、D. Haran 和 H. V¨olklein 在 [FHV94] 中的一项杰出成果表明，全体全实代数数域的一阶理论是可判定的。这个域构成了“可判定”与“不可判定”之间某种意义上的边界，因为 J. Robinson 在 [Rob62] 中证明，$\mathbb{Z}$ 可在全体全实整数环上作一阶定义，因此全体全实整数环的一阶理论是不可判定的。

1.5. **非大代数数域**。我们用于定义 $\mathbb{Z}$ 的公式并不取决于所讨论的环是否为实环，而取决于所讨论的域是“大”还是非大（见 [MR20]）。

定义 1。 **8.** 设 K 是一个代数数域。我们称 K 为大 i f

$$[K:\mathbb{Q}] = \prod_{p \text{ prime}} p^{\infty}.$$

等价地，若对每个正整数 n，K 都包含一个数域 F，使得 $[F:\mathbb{Q}]$ 可被 n 整除，则称 K 为大。

我们的主要定理将在 §4 中证明，内容如下。

定理 4.8。设 $\mathscr{A}$ 为所有非大代数数域的集合。存在一个形如“$\forall\forall\exists\ldots\exists$”的一阶公式，可在 $\mathscr{A}$ 中所有域的整数环上，一致地定义 $\mathbb{Z}$。特别是，可以一致地证明这些环的一阶理论是一阶不可判定的。

定义 1.9. 设 $\{F_i\}, i \in \mathbb{Z}_{>0}$ 是一列域，使得 $F_i \subset F_{i+1}$ 和 F_{i+1}/F_i 是伽罗瓦扩张。那么我们称序列 $\{F_i\}$ 为一个伽罗瓦扩张塔。

推论 y 1.10. 下列域具有不可判定的一阶理论 y.

(1) 数域的伽罗瓦扩张塔的非大并集。*(2)* 数域的非大伽罗瓦扩张。*(3)* 次数小于或等于 $d \in \mathbb{Z}_{>1}$的扩张塔的并集。*(4)* 数域所有次数小于或等于 $d \in \mathbb{Z}_{>1}$ 的扩张的合成域。*(5)* 数域在取 n次根，或取正元素的 $2n$次根运算下的闭包。

证明。若 M 是数域 K 的伽罗瓦扩张塔（或伽罗瓦扩张），且不是大扩张，则存在某个素数 p，使得域 M 在 [Shl18], 的意义下是一致的 p-有界域，因此 $\mathscr{O}_M$ 在 M上有一阶定义。（证明见 [Shl18]；请注意，该论文用“q-有界”一词代替“p-有界”。）由定理 4.8可知，$\mathbb{Z}$ 在 $\mathscr{O}_M$上是一阶可定义的。因此，$\mathbb{Z}$ 在 M 上是一阶可定义的，故 M 的一阶理论不可判定。

对于该推论的最后三条断言，所涉及的域显然是非大的，并且对任意 $p > d$ 都是一致 p有界的（在合成域或次数小于等于 d 的扩张塔的情形下），而在对 n次根或 $2n$次根封闭的情形下，对任意$p > 2n$ 也是如此。其余论证与该推论前两条断言的论证相同。

□

该推论的最后一项得出以下推论，回答了 Tarski 提出的一个问题。

推论1.11. 可作图数域的一阶理论是不可判定的。

证明.可作图数域是代数数域中最小的子域，它对在域的正元素上开平方这一运算封闭。

□

我们的方法还为证明 $\mathbb{Q}$ 的最大阿贝尔扩张的整数环不可判定提供了一种可能的途径（见推论2.14）。

1.6. **使用单位**。我们使用单位背后的主要思想之一，是一个简单的代数恒等式 $\frac{x^n-1}{x-1} \equiv n$ 模（$x-1$），在 $\mathbb{Z}[x]$ 中适用于 $x \neq 1$。如果 x 是整数环中的单位，那么 x^n 也是，因此我们得出了定义 2.1。

首次利用这一代数恒等式，通过佩尔方程的形式实现（存在性）可定义性的单位方法，归功于 J. Robinson 和 M. Davis（见 [Dav73]）。毕竟，有理数域 $\mathbb{Z}$ 上的佩尔方程只是二次扩张中单位的范数方程。后来，J. Denef 和 L. Lipshitz 将这一思想推广到代数扩张（见 [Den 75], [Den80],[DL78]）。受他们启发，T. Pheidas（[Phe88]）、C. Videla（[Vid89]）以及第三位作者（[Shl89]）将这一特定的单位方法用于另一系列数域。第三位

作者使用单位、 S-单位以及更一般的单位范数方程，在数域的大子环和有理数域 $\mathbb{Q}$ 的无限代数扩张中定义整数环 $\mathbb{Z}$（例如见 [Shl94], [Shl02], [Shl04]）。

C. Martinez-Ranero、J. Utreras 和 C. Videla 在 [MRUV20] 以及 C. Springer 在[Spr20] 和 [Spr23] 中也利用了所研究域的单位，但他们的方法与我们截然不同。

2. 从子幺半群到子环的一阶转化

对于任意代数扩张 K of $\mathbb{Q}$，令 $\mathscr{O}_K$ 表示 K 的整数环，并令$U_K := \mathscr{O}_K^\times$ 表示 $\mathscr{O}_K$的单位群。

定义 2.1. 设 K 为一个代数数域，$M \subset \mathscr{O}_K$ 为一个乘法幺半群。定义

$$\begin{aligned} R_{K,M} :=& \{x \in \mathscr{O}_K : \forall \varepsilon \in M\ \exists \delta \in M\ \exists w \in \mathscr{O}_K \text{ such that } \delta - 1 = (\varepsilon-1)x + (\varepsilon-1)^2 w\} \\ =& \{x \in \mathscr{O}_K : \forall \varepsilon \in M\ \exists \delta \in M \text{ such that } \delta - 1 \equiv (\varepsilon-1)x \pmod{(\varepsilon-1)^2}\}. \end{aligned}$$

当 $M = U_K$ 时，我们将 $R_{K,\ U_K}$ 简记为 R_K。

引理 2.2. *S* 假设 ε，x_1，x_2，……，x_n，δ_1，……，$\delta_n \in \mathscr{O}_K$对某个 $n \geq 1$成立，并且对每个 i

$$\delta_i - 1 \equiv (\varepsilon-1)x_i \pmod{(\varepsilon-1)^2}.$$

Then

$$\prod_i \delta_i - 1 \equiv (\varepsilon-1)\sum_i x_i \pmod{(\varepsilon-1)^2}.$$

证明。 由归纳法，只需证明该引理对 $n = 2$成立。由于 $\delta_i - 1 \equiv 0 (\mathrm{mod}\ (\varepsilon-1))$，当 $n = 2$ 时，该引理由同余关系得出

$$\begin{aligned} \delta_1\delta_2 - 1 &= (\delta_1 - 1) + (\delta_2 - 1) + (\delta_1 - 1)(\delta_2 - 1) \\ &\equiv (\delta_1 - 1) + (\delta_2 - 1) \equiv (\varepsilon-1)x_1 + (\varepsilon-1)x_2 \pmod{(\varepsilon-1)^2}. \end{aligned}$$

□

命题 2.3。 设 M是 $\mathscr{O}_K$中的一个幺半群，并设 $\mathbb{Q}(M)$是由 M在 $\mathbb{Q}$ 上生成的域。那么：

(1) $R_{K,\ M}$ 对加法和乘法封闭（即是一个“半环”）。*(2)* 若 M 是 U_K 的子群，则 $R_{K,\ M}$ 是 $\mathscr{O}_K$的子环。*(3)* 若 M 包含一个无限阶单位，则 $R_{K,\ M} \subset \mathscr{O}_{\mathbb{Q}(M)}$。

证明。 $R_{K,\ M}$ 对加法封闭这一点可直接由引理 2.2 得出。

设 $x, y \in R_{K,M}$和 $\varepsilon \in M$。由于 $x \in R_{K,M}$，存在一个 $\delta \in M$使得

$$\delta - 1 \equiv (\varepsilon-1)x \pmod{(\varepsilon-1)^2}.$$

由于 $y \in R_{K,M}$，存在一个 $\delta' \in M$ 使得

$$\delta' - 1 \equiv (\delta-1)y \equiv ((\varepsilon-1)x)y \pmod{(\varepsilon-1)^2}.$$

由此可得 $xy \in R_{K,M}$，这就完成了 (1) 的证明。

现在假设 M 是 U_K 的子群。一旦证明 $-1 \in R_{K,M}$，便可由 (1) 得出 $R_{K,M}$ 是一个环。假设 $\varepsilon \in M \subset U_K$。由于 M 是一个群，$\varepsilon^{-1} \in M$，并且

$$\varepsilon^{-1} - 1 = -(\varepsilon - 1) + \varepsilon^{-1}(\varepsilon - 1)^2 \equiv -(\varepsilon - 1) \pmod{(\varepsilon - 1)^2}.$$

由此得到 $-1 \in R_{K,\ M}$，从而完成了(2)的证明。

最后，假设 M 含有一个 ε 无限阶的单位。如果 $\mathfrak{a}$ 是 $\mathscr{O}_{\mathbb{Q}(\varepsilon)}$的非零理想，那么 ε 的约化在$(\mathscr{O}_{\mathbb{Q}(\varepsilon)}/\mathfrak{a})^\times$中具有有限阶，即对于某个 $n \geq 1$，有 $\varepsilon^n - 1 \in \mathfrak{a}$。因此

$$\bigcap_{n \geq 1} (\varepsilon^n - 1)\mathscr{O}_K \subset \bigcap_{\text{nonzero ideals } \mathfrak{a} \text{ of } \mathscr{O}_{\mathbb{Q}(\varepsilon)}} \mathfrak{a}\mathscr{O}_K = 0. \tag{2.4}$$

假设$x \in R_{K,\ M}$，且 $n \in \mathbb{Z}_{>0}$。由于 $\varepsilon^n \in M$，存在一个 $\delta \in M$使得

$$\delta - 1 \equiv x(\varepsilon^n - 1) \pmod{(\varepsilon^n - 1)^2}.$$

如果 y 是 $\mathbb{Q}(M)$上 x 的任意一个共轭元，那么将 x替换为 y后，同一个同余关系仍然成立；由于 $\varepsilon^n \neq 1$，我们得到

$$x - y \in (\varepsilon^n - 1)\mathscr{O}_K.$$

因此 $x - y \in \cap_{n>0}(\varepsilon^n - 1)\mathscr{O}_K$，由(2.4)可知其为零。所以 $y = x$，从而得到 $x \in \mathscr{O}_{\mathbb{Q}(M)}$。□

注 2.5. 假设 M 是 U_K的子群。原则上，环 $R_{K,M}$ 不一定是其分式域中的整个整数环 $R_{K,\ M}$。但是，$R_{K,M}$ 可以用 $R_{K,M}$作存在性定义：

命题 2.6. 若 M 是 U_K的子群，则

$$\tilde{R}_{K,M} = \{x \in \mathscr{O}_K \mid \exists y, z \in R_{K,M}, y \neq 0, xy = z\}.$$

证明。注意，根据 Denef 的一个结果（[Den80，引理 9]；另见 [MRS22，引理 4.6]），集合 $\{y \in \mathscr{O}_K : y \neq 0\}$ 具有一个存在性定义。

令 R 表示命题中等式的右端。则 $R \subset R_{K,M}$。

对于包含在 $R_{K,M}$的分式域中的任意数域 F，存在一个元素 $\alpha \in R_{K,M}$ 使得 $\mathbb{Q}(\alpha) = F$。对于每个 $\beta \in \mathscr{O}_F$，都存在 $m \in \mathbb{Z}$ 使得 $m\beta \in \mathbb{Z}[\alpha] \subset R_{K,M}$；在定义 R 时取 $x = \beta$、$y = m$和 $z = m\beta$，我们便可得出 $\beta \in R$。因此，R 包含 F的每个代数整数。由于这对分式域包含于 $R_{K,M}$中的每个数域 F 都成立，因此可知 R 在其分式域中是˜整闭的，即 $R = R_{K,M}$。□

推论 2.7。如果 M 是 U_K的子群，并且 M 在$\mathscr{O}_K$中有一阶定义，那么环 $R_{K,\ M}$ 和 $R_{K,\ M}$ 在 $\mathscr{O}_K$ 中也有一阶定义。

引理 2.8. 设 L/K是一个有限扩张。假设 $\varepsilon \in U_K$、$x \in \mathscr{O}_K$ 和 $\delta \in U_L$满足

$$(\varepsilon - 1)x \equiv \delta - 1 \pmod{(\varepsilon - 1)^2\mathscr{O}_L}.$$

Then

$$(\varepsilon - 1)[L : K]x \equiv N_{L/K}(\delta) - 1 \pmod{(\varepsilon - 1)^2\mathscr{O}_K}.$$

~证明. 设 Σ 是从 L/K 到 L/K的伽罗瓦闭包 L 中的嵌入集合。由于 x 和 ε 属于 K, 对每个 $\sigma \in \Sigma$, 我们都有

$$(\varepsilon-1)x \equiv \sigma(\delta)-1 \pmod{(\varepsilon-1)^2\mathscr{O}_{\tilde{L}}}.$$

我们有 $\prod_{\sigma\in\Sigma}\sigma(\delta) = N_{L/K}(\delta)$ 和 $|\Sigma| = [L: K]$。因此，将引理 2.2 应用于$n = [L : K]$, 给定的 ε，所有 x_i 均等于给定的 x，以及 δ_i 等于 $\sigma(\delta)$ 的 $\sigma \in \Sigma$ ，可得

$$N_{L/K}(\delta)-1 \equiv (\varepsilon-1)[L:K]x \pmod{(\varepsilon-1)^2\mathscr{O}_{\tilde{L}}}.$$

这个同余式的两边都属于 $\mathscr{O}_K$，因此该同余式模 $(\varepsilon-1)^2\mathscr{O}_K$ 成立。□

回顾一下，我们将 R_{K,U_K} 简记为 R_K。

引理 2.9。设 W 是 U_K 的子群，设 $n \in \mathbb{Z}_{>0}$，并设 $\mathfrak{a}$ 是 $\mathscr{O}_K$ 的理想。令

$$M := \{u^n : u \in W, u \equiv 1 \pmod{\mathfrak{a}}\}.$$

则 $nR_{K,W} \subset R_{K,M}$。

证明。设 $x \in R_{K,W}$。我们将证明 $nx \in R_{K,M}$。设 $\varepsilon \in W$。由于 $x \in R_{K,W}$，存在 $\delta \in W$ 使得

$$(\varepsilon-1)x \equiv \delta-1 \pmod{(\varepsilon-1)^2}$$

并且可得 $\delta \equiv 1$ （模 $\mathfrak{a}$）以及 $\delta^n \in M$。因此，将引理 2.2 应用于此处的 n 和 ε，可得所有 $x_i := x$，以及所有 $\delta_i := \delta$,

$$(\varepsilon-1)nx \equiv \delta^n-1 \pmod{(\varepsilon-1)^2}.$$

因此 $nx \in R_{K,M}$。 □

定义 2.10。我们称代数数域 K 为 *CM* 域，如果 K 是全实域的全虚二次扩张。我们也包括情形$[K: \mathbb{Q}] = \infty$。

命题 2.11。设 K 是一个非虚二次域的 *CM* 域，并设 F 是 K 的最大实子域。那么 $R_K \subset \mathscr{O}_F$。

证明。固定 $d \in \mathbb{Z}_{>2}$，并令 $M:= \{u^2: u \in U_K, u \equiv 1$（模 $d\mathscr{O}_K$）$\}$。我们首先断言$M \subset U_F$。令 $\alpha \mapsto \bar{\alpha}$ 表示 K 上的复共轭。若 $\varepsilon \in M$，我们可以写成$\varepsilon = u^2$，其中 $u \in U_K, u \equiv 1$ （模 d）。因此

$$\varepsilon = u^2 = (u\bar{u})(u/\bar{u}).$$

由于 $u/\bar{u} \in U_K$ 及其所有阿基米德绝对值均为 1， $u/\bar{u}$ 是一个单位根。由于 $u \equiv 1$ （模 d），我们必须有 $u/\bar{u} = 1$。因此 $\varepsilon = u\bar{u} \in U_F$。

由于 K 不是虚二次域， M 包含无限阶单位。因此，根据第一次包含关系所用的引理 2.9以及第二次包含关系所用的命题 2.3(3)，我们有

$$2R_K \subset R_{K,M} \subset \mathscr{O}_{\mathbb{Q}(M)} \subset \mathscr{O}_F.$$

由此可得 $R_K \subset \mathscr{O}_F$。 □

注记 2.12. 我们可以将命题 2.11 应用于 $\mathbb{Q}^{\mathrm{ab}}$（即 $\mathbb{Q}$ 的最大阿贝尔扩张），从而得出存在一个全实环（即 $R_{\mathbb{Q}^{\mathrm{ab}}}$），它在 $\mathscr{O}_{\mathbb{Q}^{\mathrm{ab}}}$ 上是一阶可定义的。遗憾的是，目前我们无法确定环 $R_{\mathbb{Q}^{\mathrm{ab}}}$。

备注 2.13。令 $\mathbb{Q}^{\mathrm{ab},+}$ 为 $\mathbb{Q}^{\mathrm{ab}}$ 的极大全实子域。不难看出，J. Robinson 在 [Rob62] 中证明全实数域的整数环不可判定的方法，同样适用于 $\mathbb{Q}^{\mathrm{ab},+}$ 的整数环。因此，$\mathscr{O}_{\mathbb{Q}^{\mathrm{ab},+}}$ 的一阶理论是不可判定的。此外，她猜想任意全实域的整数环都是不可判定的。J. Koenigsmann [Koe14] 猜想 $\mathscr{O}_{\mathbb{Q}^{\mathrm{ab},+}}$ 在 $\mathscr{O}_{\mathbb{Q}^{\mathrm{ab}}}$ 上有一阶定义；由上述结果可知，$\mathscr{O}_{\mathbb{Q}^{\mathrm{ab}}}$ 也具有不可判定一阶理论。作为命题 2.11 的推论，我们可以补充以下条件；满足其中任意一项，便可推出 $\mathscr{O}_{\mathbb{Q}^{\mathrm{ab}}}$ 的一阶理论不可判定。

推论2.14。若满足以下条件中的至少一项，则环 $\mathscr{O}_{\mathbb{Q}^{ab}}$ 是一阶不可判定的：

(1) 环 $R_{\mathbb{Q}^{ab}}$ 是不可判定的，或 *(2)* $\mathbb{Q}$ 的每个实阿贝尔扩张的整数环都是不可判定的，或 *(3)* 存在 $\mathbb{Q}^{\mathrm{ab}}$ 的一个非大子域，其整数环在 $\mathscr{O}_{\mathbb{Q}^{\mathrm{ab}}}$上是一阶可定义的。

3. 在特殊情形下计算 R_K

命题 **命题 3.1.** 设 K 是一个虚二次域。那么 $R_K = \mathbb{Z} + 2\mathscr{O}_K$.

证明。对于 ε， $\delta \in U_K$ 设

$$S_{\varepsilon,\delta} := \{x \in \mathscr{O}_K : \delta - 1 \equiv (\varepsilon - 1)x \pmod{(\varepsilon-1)^2}\}.$$

于是根据定义，

$$R_K := \bigcap_{\varepsilon \in U_K} \Big(\bigcup_{\delta \in U_K} S_{\varepsilon,\delta} \Big). \tag{3.2}$$

容易验证，$S_{1,1} = \mathscr{O}_K$，$S_{-1,1} = 2\mathscr{O}_K$，以及 $S_{-1,-1} = 1 + 2\mathscr{O}_K$。当$U_K = \{-1, 1\}$时，命题便由 (3.2) 得出。

现在假设 $K = \mathbb{Q}(i)$。在这种情况下

$$S_{i,1} = S_{i,-1} = (1+i)\mathscr{O}_K, \quad S_{i,i} = S_{i,-i} = 1 + (1+i)\mathscr{O}_K,$$
$$S_{-i,1} = S_{-i,-1} = (1+i)\mathscr{O}_K, \quad S_{-i,i} = S_{-i,-i} = 1 + (1+i)\mathscr{O}_K,$$
$$S_{-1,i} = S_{-1,-i} = \emptyset.$$

同样，由 (3.2) 可得 $R_{\mathbb{Q}(i)} = \mathbb{Z} + 2\mathbb{Z}[i]$。当 $K = \mathbb{Q}(\sqrt{-3})$ 时的证明类似。□

以下定理将用于研究秩 1 的单位群情形。其证明见于 [EG15]。

定理 3.3 （ [EG15]的推论 6.1.2）。 设 K 是一个数域。那么方程 $x_1 + x_2 + x_3 = 1$ 仅有有限多个解，且所有 $x_i \in U_K - \{1\}$。

引理 3.4。 设 K 是一个数域， $\varepsilon \in U_K$ 是一个无限阶单位，且a， $b \in \mathbb{Z}$。令 $g :=$ 最大公约数(a, b)。

(1) 若 $b \mid a$ ，则$(\varepsilon^b - 1) \mid (\varepsilon^a - 1)$，且$(\varepsilon^a - 1)/(\varepsilon^b - 1) \equiv a/b$ (模$(\varepsilon^b - 1)$)。*(2)* 由 $\varepsilon^a - 1$ 和 $\varepsilon^b - 1$ 生成的 $\mathscr{O}_K$ 的理想是$(\varepsilon^g - 1)\mathscr{O}_K$。*(3)* 若$(\varepsilon^b - 1) \mid (\varepsilon^a - 1)$，则$(\varepsilon^b - 1)/(\varepsilon^g - 1) \in U_K$。

证明。 断言(1)由多项式恒等式 $X^n - 1 = (X - 1)\sum_{i=0}^{n-1} X^i$得出，其中代入 $X := \varepsilon^b$, $n := a/b$。

令 $\mathfrak{d}$ 为由 $\varepsilon^a - 1$ 和 $\varepsilon^b - 1$ 生成的 $\mathscr{O}_K$ 的理想。由 (1) 可知，$\mathfrak{d} \subset (\varepsilon^g - 1)\mathscr{O}_K$。固定 x、$y \in \mathbb{Z}$，使得 $ax - by = g$。再次利用 (1)，我们看到 $\mathfrak{d}$ 包含

$$(\varepsilon^{ax} - 1) - (\varepsilon^{by} - 1) = \varepsilon^{ax} - \varepsilon^{by} = \varepsilon^{by}(\varepsilon^{ax-by} - 1) = \varepsilon^{by}(\varepsilon^g - 1).$$

由于 ε 是一个单位，我们有 $\varepsilon^g - 1 \in \mathfrak{d}$，由此完成了 (2) 的证明。

由 (1) 和 (2) 可知，$(\varepsilon^b - 1)/(\varepsilon^g - 1)$ 和 $(\varepsilon^a - 1)/(\varepsilon^g - 1)$ 是 K 中互素的整数。此外，若 $(\varepsilon^b - 1)/(\varepsilon^g - 1)$ 整除 $(\varepsilon^a - 1)/(\varepsilon^g - 1)$，则 $(\varepsilon^b - 1)/(\varepsilon^g - 1)$ 必为一个单位。这证明了 (3)。□

命题 3.5。 设 K 是一个数域，且 $u \in U_K$ 是一个无限阶单位。存在一个 $N \in \mathbb{Z}_{>0}$，使得对于每个 a， $b \in \mathbb{Z}_{>0}$，以及每个 $n > N$，单位 $\varepsilon := u^n$ 满足

$$(\varepsilon^b - 1) \mid (\varepsilon^a - 1) \iff b \mid a.$$

证明。 “$\Longleftarrow$”这一蕴含对每个 n 都成立，这是由引理 3.4(1)得出的。

考虑集合

$$S := \{d \in \mathbb{Z}_{\neq 0} : \exists x_2, x_3 \in U_K - \{1\} \text{ such that } u^d + x_2 + x_3 = 1\}.$$

根据定理 3.3， S 是有限的，我们令 $N := \sup(S)$。固定 $n > N$，并令 $\varepsilon = u^n$。

假设 $(\varepsilon^b - 1) \mid (\varepsilon^a - 1)$。由引理 3.4(3)可得 $\delta := (\varepsilon^b - 1)/(\varepsilon^g - 1) \in U_K$，其中 $g := \gcd(a, b)$。因此，我们得到单位方程的一个解

$$\varepsilon^b - \delta\varepsilon^g + \delta = 1.$$

我们有 $\varepsilon^b = u^{nb}$ ，且 $nb \geq n > N$，因此根据 S 的定义，必有$-\delta\varepsilon^g = 1$ 或 $\delta = 1$。

假设 $-\delta\varepsilon^g = 1$。由于 u 具有无限阶， $\varepsilon^{b+g} \neq 1$。与此同时，根据 δ 的定义可得

$$\varepsilon^g - 1 = -\delta\varepsilon^g(\varepsilon^g - 1) = \varepsilon^g(1 - \varepsilon^b) = \varepsilon^g - \varepsilon^{b+g}$$

并且 $\varepsilon^{b+g} = 1$。这一矛盾说明 $-\delta\varepsilon^g \neq 1$。因此 $\delta = 1$，即$\varepsilon^b - 1 = \varepsilon^g - 1$。再次利用 u 具有无限阶这一点，我们得出 $g = b$，所以$b \mid a$。□

命题 3.6。 设 K 是一个数域，且 W 是 U_K 的一个子群，使得 秩 $W = 1$。那么 $R_{K,W} = \mathbb{Z}$。

证明。令 $M := \{u^n : u \in W\}$，其中 n 取足够大，使得 M 是无挠的，并且 n 大于命题 3.5 中的 N。应用引理 2.9，并取此M（以及 $\mathfrak{a} = \mathscr{O}_K$），可得 $nR_{K,\,W} \subset R_{K,\,M}$，因此要证明该命题，只需证明 $R_{K,\,M} = \mathbb{Z}$。

固定 M的一个生成元 ε，并假设 $x \in R_{K,\,M}$。取 $m \in \mathbb{Z}_{>0}$，并取$b \in \mathbb{Z}_{>0}$ 使得 $\varepsilon^b \equiv 1$ (模 m)。根据 $R_{K,\,M}$的定义，存在某个 $a \in \mathbb{Z}$ 使得

$$\varepsilon^a - 1 \equiv (\varepsilon^b - 1)x \pmod{(\varepsilon^b - 1)^2}.$$

特别地，$(\varepsilon^b - 1) \mid (\varepsilon^a - 1)$，因此由命题 3.5 得出 $b \mid a$。于是

$$x \equiv (\varepsilon^a - 1)/(\varepsilon^b - 1) \equiv a/b \pmod{(\varepsilon^b - 1)}$$

由引理 3.4(1) 得，因此 $x - a/b \in m\mathscr{O}_K$。特别地，$x$ 在自由 $\mathbb{Z}$-模 $\mathscr{O}_K/\mathbb{Z}$中可被 m 整除。由于 m是任意的，我们得出 $x = 0$属于 $\mathscr{O}_K/\mathbb{Z}$，即$x \in \mathbb{Z}$。□

引理 3.7。设 p 是一个有理素数，K 是一个数域。假设 $j \in \mathbb{Z}_{>0}$，且 $\varepsilon \in U_K - \{1\}$ 满足 $\varepsilon \equiv 1$ (模 p^{j+1})。那么存在 $x \in \mathscr{O}_K$，使得对于每个与 p互素的整数 n，同余式

$$\delta - 1 \equiv (\varepsilon - 1)p^j nx \pmod{p^{j+1}(\varepsilon - 1)\mathscr{O}_K}$$

没有 解 $\delta \in U_K$。

证明。令 $\mathfrak{a} = \prod_{\mathfrak{p}|p} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\varepsilon-1)}$，其中 $\mathfrak{p}$ 遍历 K 上方的素数。注意，根据我们对 ε的选择，p^{j+1} 整除 $\mathfrak{a}$。定义群

$$W_{\mathfrak{a}} := \{u \in U_K : u \equiv 1 \pmod{p^j\mathfrak{a}}\}, \quad V_{\mathfrak{a}} := p^j\mathfrak{a}/p^{j+1}\mathfrak{a}.$$

于是 $W_{\mathfrak{a}} \subset U_K$ 是秩严格小于 $[K$ 的自由阿贝尔群：$\mathbb{Q}]$（不存在模 $p\mathfrak{a}$同余于 1 的非平凡单位根），而 $V_{\mathfrak{a}}$ 是维数为 $[K$ 的 $\mathbb{F}_p$-向量空间：$\mathbb{Q}]$。存在一个自然的同态

$$\lambda_{\mathfrak{a}} : W_{\mathfrak{a}} \longrightarrow V_{\mathfrak{a}}$$

定义为

$$\lambda_{\mathfrak{a}}(u) = u - 1 \pmod{p^{j+1}\mathfrak{a}},$$

a由此可知，$\lambda_{\mathfrak{a}}$ 的余核维数至少为一。

映射

$$\mathscr{O}_K/p\mathscr{O}_K \longrightarrow p^j\mathfrak{a}/p^{j+1}\mathfrak{a} = V_{\mathfrak{a}} \quad \textbf{defined by} \quad x \mapsto (\varepsilon - 1)p^j x$$

是一个同构，因此我们可以选择 $x \in \mathscr{O}_K$，使得对于每个与 p 互素的整数 n，乘积 $(\varepsilon - 1)p^j nx$ 不属于 $\lambda_{\mathfrak{a}}$ 的像。但不属于 $\lambda_{\mathfrak{a}}$ 的像，恰好意味着不存在 $\delta \in U_K$ 使得

$$\delta - 1 \equiv (\varepsilon - 1)p^j nx \pmod{p^{j+1}(\varepsilon - 1)\mathscr{O}_K}.$$

□

定义 3.8。设 p 为一个素数。设 $K/\mathbb{Q}$ 为一个次数可能无限的代数扩张。那么，如果 $\mathrm{ord}_p[K:\mathbb{Q}] < \infty$，我们就称 K 是 p-有限的；等价地，存在某个数域 $L \subset K$，使得 K 中 L 的任何有限扩张，其次数都不被 p 整除。

注记 3.9。 $\mathbb{Q}$ 的代数扩张不是大扩张（参见定义 1.8），当且仅当存在一个素数 p，使其为 p-有限的。

引理 3.10。设 K 是一个数域，且 U_K 是无限的。令 L 为 K 的一个不是大扩张的代数扩张。那么对于每个 $m \in \mathbb{Z}_{>0}$，都有$m\mathscr{O}_K \not\subset R_L$。

证明。由于 L 不是大扩张，我们可以选择一个有理素数 p，使得 L 是 p-有限的。固定 $m \geq 1$, 并定义

$$j := 1 + \mathrm{ord}_p(m) + \sup\{\mathrm{ord}_p[K' : K] : K' \text{ is a finite extension of } K \text{ in } L\}$$

根据假设，这是有限的。由于 U_K 是无限的，我们可以固定 $\varepsilon \in U_K - \{1\}$，使得 $\varepsilon \equiv 1$（模 p^{j+1}）。令 $x \in \mathscr{O}_K$ 为在引理 3.7 中根据 p、 K、 ε的这一选择以及此 j所取的元素。

假设 $mx \in R_L$。那么存在 $\delta \in U_L$ 使得

$$\delta - 1 \equiv (\varepsilon - 1)mx \pmod{(\varepsilon - 1)^2\mathscr{O}_L}.$$

由引理 2.8,

$$N_{K(\delta)/K}\delta - 1 \equiv (\varepsilon - 1)[K(\delta) : K]mx \pmod{(\varepsilon - 1)^2\mathscr{O}_K}.$$

记 $[K(\delta) : K]m = np^s$，其中 n 与 p互素。那么 $s < j$，并由引理 2.

$$(N_{K(\delta)/K}\delta)^{p^{j-s}} - 1 \equiv (\varepsilon - 1)[K(\delta) : K]p^{j-s}mx \equiv (\varepsilon - 1)p^j nx \pmod{(\varepsilon - 1)^2\mathscr{O}_K}.$$

这与我们对 x 的选择（引理 3.7）矛盾，因此必有 $mx \notin R_L$。 □

定理3.11。设 K 是 $\mathbb{Q}$ 的代数扩张，且不是大扩张。则 $R_K = \mathbb{Z}$ 或 R_K 是包含于 K 中的某个虚二次域 F 的整环。

证明。设 $x \in R_K$，并假设 $\mathbb{Q}(x)$ 既不是 $\mathbb{Q}$，也不是虚二次域。特别地， $U_{\mathbb{Q}(x)}$ 是无限的。由于 R_K 是一个环，我们有 $\mathbb{Z}[x] \subset R_K$，因此存在 $m \in \mathbb{Z}_{>0}$ 使得 $m\mathscr{O}_{\mathbb{Q}(x)} \subset R_K$。于是与引理 3.10 矛盾。

因此，对于任意 $x \in R_K$， $\mathbb{Q}(x) = \mathbb{Q}$ 或 $\mathbb{Q}(x)$ 是一个虚二次域。若 x_1、 $x_2 \in R_K$ 生成两个不同的虚二次域 $\mathbb{Q}(x_1)$ $\mathbb{Q}(x_2)$，则 R_K 包含一个元素 x，使得 $\mathbb{Q}(x) = \mathbb{Q}(x_1, x_2)$, 再次导致矛盾。因此， $R_K = \mathbb{Z}$ 或 K 是一个虚二次域。□

推论 3.12. 假设 K 不是大。如果 K 不包含虚二次域，或者 K 是一个 *CM* 域，那么 $R_K = \mathbb{Z}$。

证明。 K 不含虚二次子域的域的情形直接由定理3.11推出。CM 域的情形由定理3.11和命题 3.6推出。□

推论 3.13。 设 K 是 $\mathbb{Q}$的 *4* 次扩张。那么 $R_K = \mathbb{Z}$.

证明。 如果 K 不包含虚二次域，则该推论由推论 3.12得出。如果 K 包含虚二次域，则 K没有实嵌入，因此秩为 $U_K = 1$ ，该推论由命题 3.6得出。□

设非大域 K 包含多个虚二次域。这些域中至多有一个可以是 R_K 的分式域。这种不对称性，加上推论 3.12 和 3.13，引出了以下猜想。

猜想 3.14。 设 K 是一个非大且非虚二次的域。那么$R_K = \mathbb{Z}$。

我们将通过描述一类（必然是大域的）域 K 来结束本节，使得 $R_K = \mathscr{O}_K$。

引理 3.15。 设 K 是一个数域， $I \subset \mathscr{O}_K$ 是一个非零理想，且 $\beta \in \mathscr{O}_K$与 I互素。那么存在一个有限扩张 L/K 和一个单位 $\delta \in U_L$ ，使得 $\delta \equiv \beta$ （模 $I\mathscr{O}_L$）。此外，域 L 可以取为由一个形如 $X^d + aX^{d-1} + b$ 的多项式的根生成，其中 $d \in \mathbb{Z}_{>0}$且 a， $b \in \mathscr{O}_K$。

证明。 不失一般性（必要时将 I 替换为其倍数），我们可以假设 I 是主理想。取 I的一个生成元 μ 。

令 d为 U_K}在$\mathscr{O}_K/I^\times$/{的像中的阶。那么我们可以取一个单位 $u \in U_K$，使得$(-\beta)^d \equiv u$ (模 I)。

考虑多项式

$$f(X) := X^d + aX^{d-1} + b \in \mathscr{O}_K[X]$$

其中 a、 $b \in \mathscr{O}_K$稍后选定。令 f的一个根为 ρ，令ρ($L = K$)，并定义另一个首一多项式

$$g(X) := \mu^d f((X - \beta)/\mu) \in \mathscr{O}_K[X].$$

那么$= \mu\rho + \beta \in \mathscr{O}_L$: δ 是 g的一个根，并且 $\delta \equiv \beta$ (模 $I\mathscr{O}_L$)。

我们断言，存在元素 a、 $b \in \mathscr{O}_K$ ，使得 $g(0) = u$ 是一个单位。在这种情况下， δ 将是一个单位，因此 δ 将具备所有所需性质，从而完成引理 3.15 的证明。

为证明该断言，我们有

$$g(0) = \mu^d f(-\beta/\mu) = (-\beta)^d + a\mu(-\beta)^{d-1} + \mu^d b \\ = u + ((-\beta)^d - u) + a\mu(-\beta)^{d-1} + b\mu^d. \tag{3.16}$$

由于 β 与 μ 互素，我们有

$$\{a\mu(-\beta)^{d-1} + b\mu^d : a, b \in \mathscr{O}_K\} = \mu\mathscr{O}_K.$$

特别地，由于 $(-\beta)^d \equiv u$ (模 μ)，我们可以找到 $a, b \in \mathscr{O}_K$ 使得

$$a\mu(-\beta)^{d-1} + b\mu^d = u - (-\beta)^d.$$

由 (3.16) 得 $g(0) = u$。至此，该断言及引理的证明完成。□

命题3.17。 设 F 是一个代数数域，使得对每个 $d \in \mathbb{Z}_{>0}$ 和每个 a， $b \in \mathscr{O}_F$，多项式 $X^d + aX^{d-1} + b$ 在 F 中都有一个根。那么 $R_F = \mathscr{O}_F$。

*Pro*同上。 设 $x \in \mathscr{O}_F$ 和 $\varepsilon \in U_F$、$\varepsilon \neq 1$。将引理 3.15 应用于 wit h

$$K := \mathbb{Q}(x, \varepsilon), \quad \beta := 1 + x(\varepsilon - 1), \quad I := (\varepsilon - 1)^2$$

我们得到一个单位 $\delta \in U_F$，满足

$$\delta - 1 \equiv x(\varepsilon - 1) \pmod{(\varepsilon - 1)^2}$$

（注意，由于我们对 F 的假设， $\delta \in U_F$ 如此）。由此可得 $x \in R_F$。 □

备注 3.18。 域 $\overline{\mathbb{Q}}$ 满足命题3.17的假设；我们不知道还有其他域满足该假设。

在代数数的大域 K 中，哪些具有这样的性质： R_K 的分式域是 K?

对于一个大域 K，记 R_K 的分式域为 $K_{\{1\}}$。根据命题 2.3(2)，我们有 $K_{\{1\}} \subset K$；并且可以迭代这一运算，记环 $R_{K_{\{i\}}}$ 的分式域为 $K_{\{i+1\}}$。这一塔

$$\mathbb{Q} \subset \cdots K_{\{i\}} \subset K_{\{i-1\}} \cdots \subset K_{\{1\}} \subset K$$

给出了 $K_{\{i\}}$ 在 $\mathscr{O}_K$ 中的整数环的一个一阶定义（涉及 $i+1$ 个全称量词）。

是否存在这样的大域 K，使得这个域的递降序列不会稳定？也就是说，对于所有 i， $K_{\{i+1\}}$ 都是 $K_{\{i\}}$ 的真子域?

4. 主要定理的证明

在证明主要结果定理 4.8 之前，我们需要一个引理来处理这样的情形：我们的公式可能定义了一个虚二次域中的整环。下文中我们省略——也就是说，默认理解——用于说明环中的一个元素是单位，或某个同余在环上成立所需的方程和/或变量。

Let

$$D(w) := 3^{12} w^4 (w-1)^4 (w-2)^4 \in \mathbb{Z}[w]$$

为 [MRS22 第 11] 节中记作 $D(2, w)$ 的量。

引理 4.1 (参见 [Den75] 的第§3节)。 固定一个模 $d \equiv 3\,4$ 非平方的正整数。对于F 一个虚二次域，令 $\mathscr{S}_F = \mathscr{S}_{F,\ d}(w,\ s_1,\ s_2,\ t_1,\ t_2,\ u_1,\ u_2,\ v_1,\ v_2)$ 表示方程与同余系统 (4.2) 至 (4.5):

$$\delta_i := s_i + t_i\sqrt{d} \in U_{F(\sqrt{d})}, \quad s_i, t_i \in \mathscr{O}_F, \quad i = 1, 2, \tag{4.2}$$

$$\varepsilon_i := \delta_i^2 = u_i + v_i\sqrt{d}, \quad u_i, v_i \in \mathscr{O}_F, \quad i = 1, 2, \tag{4.3}$$

$$\varepsilon_1 \equiv 1 \pmod{dD(w)\mathscr{O}_F}, \tag{4.4}$$

$$\varepsilon_2 - 1 \equiv w(\varepsilon_1 - 1) \pmod{(\varepsilon_1 - 1)^2}. \tag{4.5}$$

那么，$\mathscr{S}_{F,\ d}$ 构成了 $\mathbb{Z}$ 在任意虚二次域 F 的整数环$\mathscr{O}_F$上的一致存在定义。

证明。 假设 $(w, s_1, s_2, t_1, t_2, u_1, u_2, v_1, v_2) \in \mathscr{O}_F^9$是 $\mathscr{S}$的一个零点。那么，根据 (4.2)、(4.3)，ε_1和 ε_2是单位的平方；根据 (4.4)、(4.5)，它们模 d同余于 1。因此，仿照命题 2.11 的证明中的论证，我们得出 $\varepsilon_1, \varepsilon_2 \in \mathbb{Z}[\sqrt{d}] = \mathscr{O}_{\mathbb{Q}(\sqrt{d})}$。现在，将推论 11.12 应用于扩张$F(\sqrt{d})/\mathbb{Q}(\sqrt{d})$和理想 $I = (\varepsilon - 1)$，可得 $w \in \mathscr{O}_F \cap \mathbb{Z}[\sqrt{d}] = \mathbb{Z}$。

反过来，假设 $w \in \mathbb{Z}$。令 $s_1, t_1 \in \mathbb{Z}$ 满足 $\delta_1 \in U_{\mathbb{Q}(\sqrt{d})} \subset U_{F(\sqrt{d})}$ 且

$$s_1 \equiv 1, \quad t_1 \equiv 0 \pmod{dD(w)}.$$

设 u_1、$v_1 \in \mathbb{Z}$ 满足 $\varepsilon_1 = \delta_1^2$。则对于 $i = 1$，(4.2)–(4.4) 成立。

设 s_2、$t_2 \in \mathbb{Z}$ 满足 $\delta_2 = \delta_1^w$。设 u_2、$v_2 \in \mathbb{Z}$ 满足 $\varepsilon_2 = \delta_2^2$。则对于 $i = 2$，(4.2)–(4.4) 成立。□

注 4.6。 如果我们将 $\mathscr{O}_F$ 替换为 $\mathbb{Z}$，那么对于任意整数 w，在引理 4.1 的证明中仍可满足所有方程 $\mathscr{S}_F$。

注 4.7。 Denef 在 [Den75]，中的证明虽然没有正式断言虚二次域之间的一致性，但可以很容易地转换为一致的证明。

定理 4.8。 设 $\mathscr{A}$ 为所有非大代数数域的集合。存在一个形式为“$\forall\forall\exists\ldots\exists$”的一阶公式，在 $\mathscr{A}$ 中所有域的整数环上一致地定义 $\mathbb{Z}$。因此，这些环的一阶理论是不可判定的。

在开始证明之前，令 K 为任意一个代数数域，并考虑以下形式为“$\forall\forall\exists\ldots\exists$”的一阶公式，以及它所定义的集合 $Z_K \subset \mathscr{O}_K$：

定义 4.9。 将 $Z_K \subset \mathscr{O}_K$ 定义为满足以下条件的所有 $w \in \mathscr{O}_K$ 的集合

$$\forall\varepsilon \in U_K \setminus \{1\}, \exists\mu, \mu_1, \mu_2, \nu_1, \nu_2, \gamma_1, \gamma_2, \tau_1, \tau_2 \in U_K, s_1, s_2, t_1, t_2, u_1, u_2, v_1, v_2 \in \mathscr{O}_K$$

使得

$$w(\varepsilon-1)\equiv\mu-1 \pmod{(\varepsilon-1)^2}, \tag{4.10}$$

$$u_i(\varepsilon-1)\equiv\mu_i-1 \pmod{(\varepsilon-1)^2}, \quad i=1,2, \tag{4.11}$$

$$v_i(\varepsilon-1)\equiv\nu_i-1 \pmod{(\varepsilon-1)^2}, \quad i=1,2, \tag{4.12}$$

$$s_i(\varepsilon-1)\equiv\sigma_i-1 \pmod{(\varepsilon-1)^2}, \quad i=1,2, \tag{4.13}$$

$$t_i(\varepsilon-1)\equiv\tau_i-1 \pmod{(\varepsilon-1)^2}, \quad i=1,2, \tag{4.14}$$

$$\mathscr{S}_F(w,s_1,s_2,t_1,t_2,u_1,u_2,v_1,v_2), \tag{4.15}$$

其中 $\mathscr{S}$ 与引理 4.1 的证明中相同。

注 4.16。 遗憾的是，我们无法对单位群中的元素进行量化。因此，在定义 4.9 中，我们将不使用“$\forall\varepsilon\in U_K\setminus\{1\}$”，而是对所有 ε、$\beta\in\mathscr{O}_K$ 进行量化：若 $\varepsilon\beta$ 不等于 1 或若 $\varepsilon=1$，则不要求任何条件；若 $\varepsilon\beta=1$，则要求满足 (4.10)–(4.15)。更正式地说，我们有如下关于 $\mathbb{Z}$ 的定义：

$$\forall\varepsilon\forall\beta\in\mathscr{O}_K:(\varepsilon\beta=1\wedge[(\varepsilon=1)\vee((\varepsilon\neq1)\wedge\ldots))])\vee(\varepsilon\beta\neq1),$$

我们在“...”处插入方程 (4.10)–(4.15)。实质上，若 ε 不是单位，我们就需要第二个全称量词。若能对非单位作出一致的存在性定义，便可免去第二个全称量词，但我们不知道如何构造这样的定义，甚至不知道它是否存在。

定理 4.8 的证明。 设 K 为非大域，且 Z_K 如定义 4.9 所述。我们将证明 $Z_K=\mathbb{Z}$。

假设 $w\in Z_K$。那么根据定理3.11，我们有以下两种情况之一：

$$w,u_1,u_2,v_1,v_2,s_1,s_2,t_1,t_2\in\mathbb{Z} \quad \text{or} \quad w,u_1,u_2,v_1,v_2,s_1,s_2,t_1,t_2\in\mathscr{O}_F$$

对于某个虚二次域 F。无论哪种情况，方程 (4.15) 都蕴含 $w\in\mathbb{Z}$。

反过来，若 $w\in\mathbb{Z}$，则引理 4.1 的证明表明，方程组 (4.15) 可以满足，且所有变量都取值于 $\mathbb{Z}$。因此，方程组 (4.10)–(4.15) 可以在 $\mathscr{O}_K$上得到满足，所以 $w\in Z_K$。□

注 4.17。 令 $\mathscr{A}$ 表示所有满足以下条件的代数扩张 K 的集合：$\mathbb{Q}$ 的定义 4.9 中的集合 Z_K 等于 $\mathbb{Z}$。定理 4.8 蕴含 $\mathscr{A}$ 包含所有非大域，尤其包括所有数域。这引出了以下问题。

问题 4.18。 $\mathscr{A}$ 中是否包含大域?

问题 4.19。 $\mathscr{A}$ 中是否包含所有阿贝尔域?

注 4.20. 我们上面使用的构造可以推广到数域的情形，从而得到一个形式为 $\forall\exists\ldots\exists$ 的 $\mathbb{Z}$ 定义。遗憾的是，与 J. Robinson 所构造的这种形式的定义一样，这个定义仅在有界次数的数域类中是一致的。

5. 不存在 $\mathbb{Z}$ 的一致存在定义或纯全称定义

回顾“一致的”的定义（定义 1.6），并考虑以下定义。

定义 5.1. 设 R 是一个环。设 $A \subset R$，并假设存在一个多项式$p(t, x_1, \ldots, x_k) \in R[t, x_1, \ldots, x_k]$，使得

$$A = \{t \in R | \exists x_1, \ldots, x_k \in R^k : p(t, x_1, \ldots, x_k) = 0\}.$$

则称 $p(t, \bar{x})$ 是 A 在 R 上的一个丢番图定义。

命题 5.2. 设 K 是一个数域，L 是 K 的一个代数扩张，且 A 是 $\mathscr{O}_L$ 的一个子集。若存在一个丢番图定义，在所有 L 中 K 的有限扩张 L' 所对应的代数整数环 $\mathscr{O}_{L'}$ 上，对 $A \cap \mathscr{O}'_L$ 在 $\mathscr{O}_{L'}$ 上的一致，则存在一个 A 在 $\mathscr{O}_L$ 上的丢番图定义。

证明. 设 $p(t, \bar{x}) \in \mathscr{O}_K[t, \bar{x}]$ 是一个丢番图定义，适用于 L 中 K 的所有有限扩张 L'，以定义 $\mathscr{O}_{L'} \cap A$。设 $t \in A \subset \mathscr{O}_L$。令 $L' = K(t)$。那么存在一个 m 元组$\bar{x} \in \mathscr{O}_{L'}^m \subset \mathscr{O}_L^m$，使得 $p(t, \bar{x}) = 0$。

现在假设存在 $t \in \mathscr{O}_L \setminus A$，使得对于某个 $\bar{y} \in \mathscr{O}_L$，我们有$p(t, \bar{y}) = 0$。令 $L' = K(t, \bar{y})$。那么 $p(t, \bar{x})$ 不是 $\mathscr{O}_{L'}$上 $A \cap \mathscr{O}_{L'}$的丢番图定义，这与我们关于 $p(t, \bar{x})$ 的假设矛盾。因此，对于任意 $t \in \mathscr{O}_L$，存在 $\bar{x} \in \mathscr{O}_L$，使得 $p(t, \bar{x}) = 0$ 当且仅当 $t \in A$。□

推论 5.3. 令 K 为一个数域，$\mathscr{L}$ 为 K 的所有有限扩张的集合。那么，在 $\mathscr{L}$ 的元素的整数环中，不存在对$\mathscr{O}_K$ 的一致纯存在定义或纯全称定义。

证明。 我们将命题 5.2 应用于 $A := A_1 = \mathscr{O}_K$ 和 $A := A_2 = \mathscr{O}_{\bar{K}} \setminus \mathscr{O}_K$，其中$F = K$ 是 K 的代数闭包。如果 A_1 在 $\mathscr{L}$ 中的域上有一致的丢番图定义，那么 $\mathscr{O}_K$ 在 $\mathscr{O}_{\bar{K}}$ 上有丢番图定义。如果 A_2 在 $\mathscr{L}$ 中的域的整数环上有一致的丢番图定义，那么 $\mathscr{O}_{\bar{K}} \setminus \mathscr{O}_K$ 在 $\mathscr{O}_{\bar{K}}$ 上有丢番图定义，或者等价地，$\mathscr{O}_K$ 在 $\mathscr{O}_{\bar{K}}$ 上有纯全称定义。无论哪种情况，$\mathscr{O}_K$ 在$\mathscr{O}_{\bar{K}}$ 上都有一阶定义。但根据 J. Robinson 的结果（[Rob49]），我们知道任何数域的一阶理论都是不可判定的；而根据 van den Dries 的结果（[vdD88]），我们知道 $\mathscr{O}_{\bar{\mathbb{Q}}}$ 的一阶理论是可判定的。因此，A_1和 A_2 都不可能在 $\mathscr{L}$ 的元素上有一致存在定义。因此，在 $\mathscr{L}$ 的元素的整数环中，不存在对 $\mathscr{O}_K$ 的一致纯全称定义。□

将上述讨论应用于 $K = \mathbb{Q}$，我们得到：

推论 *5.4. </style}*在所有数域的整数环中，不存在对 $\mathbb{Z}$ 一致的存在性定义或纯全称定义。

最后需要指出，鉴于上述结果，我们在定理 4.8 中给出的适用于所有数域的 $\mathbb{Z}$ 一致定义，就

算术层级而言已是最优的：如果把“∀∀∃ . . . ∃”替换为“∃ . . . ∃”，该定理的陈述就会不成立。

参考文献

[CVV20] Marianela Castillo、Xavier Vidaux 和 Carlos R. Videla，《二次多项式的朱莉娅·罗宾逊数与算术动力学》，Indiana Univ. Math. J. 69 (2020), no. 3, 873–885. ↑4[CF21] Sara Checcoli 和 Arno Fehm，《诺斯科特性质与局部次数》，美国数学会会刊 149 (2021), no. 6, 2403–2414. ↑4[Chu36] Alonzo Church，《初等数论中的一个不可解问题》，American Jour- nal of Mathematics 58 (1936), 345 –363. ↑3[CPZ05] Gunther Cornelissen、Thanases Pheidas 和 Karim Zahidi，《整数环的除法充足集与丢番图问题》，Journal de Th´eorie des Nombres Bordeaux 17 (2005), 727–735. ↑3[Dav73] Martin Davis，《希尔伯特第十问题不可解》，Amer. Math. Monthly 80(3) (1973), 233-269. ↑5[Den 75] Jan Denef，《二次环上的希尔伯特第十问题》，美国数学会会刊 48 (1975), 214–220. ↑3, 5, 14, 15[Den80] Jan Denef，《代数整数的丢番图集，II》，Transactions of American Math- ematical Society 257 (1980), no. 1, 227–236. ↑3, 5, 7[DL78] Jan Denef 和 Leonard Lipshitz，《某些代数整数环上的丢番图集》，Journal of London Mathematical Society 18 (1978), no. 2, 385–391. ↑3, 5[EG15] Jan-Hendrik Evertse 和 K ´alm´an Gy˝ory，《丢番图数论中的单位方程》，剑桥高等数学研究丛书，第146卷，剑桥大学出版社，剑桥，2015年。 ↑9, 10[FHV94] Michael D. Fried、Dan Haran 和 Helmut V¨ olklein，《实希尔伯特性与全实数域》，《算术几何》（亚利桑那州坦佩，1993），1994年，第1–34页。 ↑4[GFP20] Natalia Garcia-Fritz 和 Hector Pasten，《通过岩泽理论和海格纳点探索整数环上的希尔伯特第十问题》，Math. Ann. 377 (2020), no. 3-4, 989–1013. ↑3[GR19] Pierre Gillibert 和 Gabriele Ranieri，《朱莉娅·罗宾逊数》，Int. J. Number Theory 15 (2019), no. 8, 1565–1599. ↑4[G¨od31] Kurt G¨odel，《关于《数学原理》及相关系统中形式上不可判定的命题》，Monatshefte f¨ur Mathematik und Physik 38 (1931), 173 –198.↑3[Koe14] Jochen Koenigsmann，《数论中的不可判定性》，《代数、分析与算术中的模型论》，数学讲义，第2111卷，Springer，海德堡，2014年。↑9[MRUV20] Carlos Mart´ínez-Ranero、Javier Utreras 和 Carlos R. Videla，《不可判定性》，美国数学会会刊 148 (2020), no. 3, 961–964. ↑2, 4, 6[MR10] Barry Mazur 和 Karl Rubin，《椭圆曲线扭曲的秩与希尔伯特第十问题》，Inventiones Mathematicae 181 (2010), 541–575. ↑3[MR20] Barry Mazur 和 Karl Rubin，《并非大域的大域》，美国数学会会刊 Ser. B 7 (2020), 159–169. ↑4[MRS22] B Mazur、K Rubin 和 A Shlapentokh，《存在可定义性与丢番图稳定性》，2022年。 ↑3, 7, 14, 15[MP18] M. Ram Murty 和 Hector Pasten，《椭圆曲线、 L-函数与希尔伯特第十问题》，数论杂志 182 (2018), 1–18. ↑3[Pas23] Hector Pasten，《椭圆曲面与希尔伯特第十问题》，Rev. Mat. Teor. Apl. 30 (2023), no. 1, 113 –120. ↑3

[Phe88] Thanases Pheidas, 《一类代数整数环上的希尔伯特第十问题》, 美国数学会会刊 104 (1988), no. 2, 611–620. ↑3, 5[Rob49] Julia Robinson, 《算术中的可定义性与判定问题》, 符号逻辑杂志 14 (1949), 98–114. ↑3, 17[Rob62] Julia Robinson, 《代数环的判定问题》, 《数学分析及相关专题研究》, 1962年, 第297–304页。 ↑3, 4, 9[Ros36] Barkley Rosser, 《G ¨odel 和 Church 若干定理的推广》, 符号逻辑杂志 1 (1936), no. 3, 87–91, DOI 10.2307/2269028. ↑3[Rum86] Robert S. Rumely, 《全体代数整数环上的算术》, J. Reine Angew. Math. 368 (1986), 127–133. ↑4[SS89]Harold Shapiro 和 Alexandra Shlapentokh, 《代数数域之间的丢番图关系》, 纯粹与应用数学通讯 XLII (1989), 1113–1122. ↑3[Shl07] Alexandra Shlapentokh, 《全实域的2次扩张中的丢番图可定义性与可判定性》, 代数杂志 313 (2007), no. 2, 846–896. ↑3[Shl08] Alexandra Shlapentokh, 《在有限扩张中保持秩的椭圆曲线与代数数环上的希尔伯特第十问题》, Trans. Amer. Math. Soc. 360 (2008), no. 7, 3541–3555. ↑3[Shl09] Alexandra Shlapentokh, 《 $\mathbb{Q}$ 的无限扩张中的代数数环与保持秩的椭圆曲线》, 数学逻辑档案 48 (2009), no. 1, 77–114. ↑3[Shl18]Alexandra Shlapentokh, 《有理数的无限代数扩张中整数的一阶可判定性与可定义性》, 以色列数学杂志 226 (2018), no. 2, 579–633. ↑4, 5[Shl89] Alexandra Shlapentokh, 《希尔伯特第十问题向某些代数数域的推广》, 纯粹与应用数学通讯 XLII (1989), 939–962. ↑3, 5[Shl02] Alexandra Shlapentokh, 《全实数域的大子环及其2次全复扩张中的丢番图可定义性与可判定性》, 数论杂志 95 (2002), no. 2, 227–252. ↑6[Shl04] Alexandra Shlapentokh, 《某些 $\mathbb{Q}$的无限全实扩张中的丢番图可定义性与可判定性》, Trans. Amer. Math. Soc. 356 (2004), no. 8, 3189–3207.↑6[Shl94] Alexandra Shlapentokh, 《有理数域 Q 的无限全实扩张的某些代数数环中的丢番图不可判定性》, 纯粹与应用逻辑年刊 68 (1994), no. 3, 299–325.↑6[Spr20] Caleb Springer, 《不可判定性、单位群与某些 $\mathbb{Q}$的无限全虚扩张》, 美国数学会会刊 148 (2020), no. 11, 4705–4715. ↑4, 6[Spr23] Caleb Springer, 《全虚域中整数环的可定义性与可判定性》, 伦敦数学学会通报 (2023). ↑4, 6[Tar48] Alfred Tarski, 《初等代数与几何的判定方法》, 兰德公司报告 (1948). ↑2[vdD88] Lou van den Dries, 《代数整数环的消去理论》, J. Reine Angew. Math. 388 (1988), 189–205. ↑4, 17[VV15] Xavier Vidaux 和 Carlos R. Videla, 《嵌套平方根全实塔中自然数的可定义性》, 美国数学会会刊 143 (2015), no. 10, 4463–4477.↑4[VV16] Xavier Vidaux 和 Carlos R. Videla, 《关于诺斯科特性质与不可判定性的短札》, 伦敦数学学会通报 48 (2016), no. 1, 58–62. ↑4[Vid00a] Carlos Videla, 《数域的 pro-p 扩张中整数环的可定义性》, 以色列数学杂志 118 (2000), 1–14. ↑4

[Vid00b] Carlos R. Videla，分圆塔的不可判定性，美国数学会会刊 **128**(2000年)，第 12 期，3671–3674。 ↑4[Vid99] Carlos Videla，关于可作图数，美国数学会会刊 **127**(1999年)，第 3 期，851–860。 ↑[Vid89] Carlos Videla，关于希尔伯特第 ´十问题，第十届代数学校论文集（维多利亚，ES，巴西），巴西数学学会论文集 16，1989年，1989年，第 95–108 页。 ↑3，5

哈佛大学数学系，剑桥，MA 02138-2901电子邮箱：mazur@g.harvard.edu网址：http://www.math.harvard.edu/~mazur

加州大学欧文分校数学系，欧文，加利福尼亚州 92697，美国电子邮箱地址：krubin@uci.edu网址：https://math.uci.edu/~krubin

东卡罗来纳大学数学系，格林维尔，北卡罗来纳州 27858电子邮箱地址：shlapentokha@ecu.edu网址：myweb.ecu.edu/shlapentokha