arXiv:2304.12893v1 [math.GR] 25 Apr 2023

亚交换群中的半群算法问题

S

Ruiwen Dong*

摘要

我们研究有限生成亚交换群中的半群算法问题。本文聚焦于 Choffrut 和 Karhum¨aki 于 2005年 提出的三个判定问题：单位元问题 （半群是否包含单位元？）、群问题 （一个半群是否为群？）以及逆元问题 （半群是否包含某个生成元的逆元？）。我们证明，对于有限生成亚交换群的有限生成子半群，这三个问题均可判定。特别地，我们利用图论、凸多胞体、代数几何和数论之间的相互作用，建立了多项式半环与亚交换群子半群之间的对应关系。

由于已知在有限生成亚交换群中，半群成员问题 （半群是否包含给定元素？）是不可判定的，我们的结果完成了亚交换群中半群算法问题的可判定性刻画。

*计算机科学系，牛津大学，牛津，OX1 3QD，英国，电子邮件：ruiwen.dong@kellogg.ox.ac.uk

1 引言

1.1 群与半群中的算法问题。 1911 年，Max Dehn 提出了三个基本问题，这些问题后来成为计算群论的基础。给定一个群 G 的有限表示，需要确定是否存在能够解决以下问题的算法：字问题（某个元素是否为单位元）、共轭问题（两个元素是否共轭）以及同构问题（G 是否与另一个有限表示的群同构）。后来证明，这三个问题在一般群中都是不可判定的 [1, 33], ，从而首次给出了并非源自计算理论的不可判定问题实例。

自 20 世纪 40 年代以来，由于与数理逻辑的联系，成员问题 成为计算群论中活跃的研究领域。对于这些问题，我们在一个固定的群 G 中进行研究。输入是 G 中元素 $\mathcal{G} = \{g_1, \ldots, g_K\}$ 的有限集合，以及一个目标元素 $g \in G$。记由 $\mathcal{G}$ 生成的半群为 $\langle \mathcal{G} \rangle$，记由 $\mathcal{G}$ 生成的群为 $\langle \mathcal{G} \rangle_{grp}$。

(i) *(半群成员问题)* 判断 $\langle \mathcal{G} \rangle$ 是否包含 g。
(ii) *(群成员问题)* 判断 $\langle \mathcal{G} \rangle_{grp}$ 是否包含 g。

在 Markov [28], 的奠基性工作中，证明了对于六维矩阵群，半群成员问题是不可判定的。随后，Mikhailova [29] 证明了群 SL(4, $\mathbb{Z}$) 中群成员问题的不可判定性，其中该群由行列式为 1 的 4×4 整数矩阵组成。

作为计算代数中历史最悠久、发展最成熟的问题之一，成员问题在分析系统动力学方面发挥着至关重要的作用，并广泛应用于自动机理论、程序分析和交互式证明系统 [7, 11, 14, 21]。在大多数群类中，群成员问题往往比半群成员问题容易处理得多。例如，根据 Kopytov 的经典结果 [24]，在多循环群 类中，群成员问题是可判定的；而在幂零群 [34]的子类中，半群成员问题甚至是不可判定的。这一差距促使 Choffrut 和 Karhum¨aki 于 2005年 [12]引入了一系列中间问题:

(iii) *(单位元问题)* 判定 $\langle \mathcal{G} \rangle$ 是否包含 G的单位元。(iv) *(群问题)* 判定 $\langle \mathcal{G} \rangle$ 是否为群。(v) *(逆元问题)* 给定 $a \in \mathcal{G}$，判定 $a^{-1} \in \langle \mathcal{G} \rangle$。

除了是半群成员问题的一些重要特例之外，这些中间问题对于确定半群的结构性质至关重要，也推动了半群研究中众多工具的发展，涵盖从自动机理论和压缩字 [8, 9]到李代数 [15]等领域。不难看出，群问题的可判定性涵盖了单位元问题和逆元问题的可判定性（见第 2 节）。Bell 和 Potapov 最近的一项结果证明，SL(4，$\mathbb{Z}$) 中这三个问题都不可判定 [9]；而 SL(2，$\mathbb{Z}$) 中的单位元问题是 NP完全的 [8]。在 [3], Babai 等人著名地将阿贝尔矩阵群中的算法问题归约为格上的计算，因此，通过求解齐次线性丢番图方程，阿贝尔矩阵群中的这三个问题都能在多项式时间内判定。然而，对于更大的群类，这些中间问题的可判定性仍未解决，尤其是幂零群、多循环群和亚交换群；而这些群类中的成员问题的可判定性已有明确结论。

1.2 亚交换群与主要结果。 本文研究亚交换群中的算法问题。亚交换群是指其交换子为阿贝尔群的群。回顾一下，对于群 G，其交换子 $[G, G]$ 定义为由元素 $ghg^{-1}h^{-1}$、g、 $h \in G$生成的 G 的子群。自20世纪50年代以来，发展有限生成亚交换群的完整算法理论一直是深入研究的重点。关于近期进展的综述，请参见 [5, 23]。

按照计算群论中的惯例，有限生成亚交换群 G 总是作为输入的一部分，通过一个有限亚交换群表示给出（其定义见第2节）。每个有限生成亚交换群都具有一个有限亚交换群表示，因此它们自然成为算法方法的研究对象 [5,第629]页。

对于有限生成亚交换群的经典马克斯·戴恩问题，自20世纪50年代 Hall 的奠基性工作以来，字问题的可判定性已为人所知 [19]。Noskov 证明了共轭问题是可判定的 [32]。同构问题仍是一个悬而未决的重要问题 [6]。我们可以注意到，在可解群层级中，亚交换群（也称为二步可解群）处于可判定性的边缘。根据 Kharlampovich 的著名结果，三个马克斯·戴恩问题在三步可解群中都是不可判定的（这类群的交换子是亚交换群） [22], [23,定理 6.17，第 6 节8]。

在有限生成亚交换群中，群成员问题的可判定性是 Romanovskii 的经典结果 [35]；而对于许多情形，例如海森堡群的大直积幂 [34] 和缠绕积 $\mathbb{Z} \wr \mathbb{Z}$ [26]，半群成员问题是不可判定的。单位元问题、群问题和逆元问题的可判定性一直悬而未决。Dong 的一项最新结果 [16] 证明了一个重要的亚交换群实例中的群问题是可判定的，即 缠绕积 $\mathbb{Z} \wr \mathbb{Z}$。这提示了其他有限生成亚交换群也可能存在可判定性结果。我们的主要结果解决了这些开放问题：

定理 1.1. 所有有限生成的亚交换群上的群问题、单位元问题和逆元问题都是可判定的。

1.3 相关工作。 自 Hall 的研究以来，人们就注意到亚交换群与多项式环之间存在天然联系。事实上，这种联系是判定亚交换群中许多群 算法问题的关键。然而，半群的对应理论尚未建立。Dong [16] 近期的研究表明，某些半群、有向图和多项式半环之间存在联系。不过，这些联系十分复杂，尚未得到令人满意的刻画。我们在 Dong 的工作基础上，建立亚交换群的子半群 与多项式半环之间的完整联系。我们的许多想法受到 [16], 的启发，尤其是利用 $\mathcal{G}$-图 描述亚交换群上的词，以及探究半群、图和代数几何之间的相互作用。以下是我们的主要新贡献。

1. 我们提出一种系统化的方法，将亚交换群上的词转换为多项式半环中的元素。我们引入“位置多项式”这一概念，用以描述相应的$\mathcal{G}$-图。这些多项式足以描述图的一些有趣性质，例如“满像”和对称性。在 Dong 的工作中，这种转换是通过一种特设方法完成的，该方法将 $\mathbb{Z}$ 上的游走分解为“本原回路”。正如文中所指出的，这种方法无法推广到 $\mathbb{Z}^n$ 上的游走。我们在此发展的新方法克服了这一困难。
2. 使用“位置多项式”而非将游走分解为本原回路，其缺点是无法表达图的连通性。我们的第二个主要想法是引入一种新的图性质，称为“面可达性”。这种性质弱于连通性，但其优势在于可以用位置多项式来描述。随后我们证明，结合对称性，面可达性足以刻画欧拉图（相差平移并）。这一结论是通过凸几何和图论中的一系列推演得到的。

3. 得益于前两个思想，我们能够将半群问题化归为关于多项式半环的判定问题。我们的第三个新思想是对 Einsiedler、Mouat 和 Tuncel [17, 定理 1.3] 以及 Dong [16, 命题 3.4]中两个深刻结果的同时推广。这是

本文在数学上最深刻的部分：其中包含了代数几何工具的复杂应用，例如模上的 Gr¨obner 基，以及数论中的各种思想。

2 预备知识

2.1 词、半群和群。 本节所有省略的证明均可在附录 A 中找到。设 G 为任意一个群。设 $\mathcal{G} = \{g_1, \ldots, g_K\}$ 为 G 中元素的一个集合。将 $\mathcal{G}$ 视为字母表，记 $\mathcal{G}^*$ 为 $\mathcal{G}$ 上的词集。对于任意词 $w = g_{i_1} g_{i_2} \cdots g_{i_m} \in \mathcal{G}^*$，通过依次将 w 中出现的元素相乘，我们可以将 w 计算为 G 中的元素 $\pi(w)$。我们称词 w 表示 元素 $\pi(w)$。因此，由 $\mathcal{G}$ 生成的半群 $\langle \mathcal{G} \rangle$ 是 G 中由 $\mathcal{G}^*$ 上的非空 词表示的元素集合。字母表 $\mathcal{G}$ 上的词 w 称为满像 词，如果 $\mathcal{G}$ 中的每个字母在 w 中至少出现一次。

引理 2.1 ([16, 引理2。1])。 半群 $\langle \mathcal{G} \rangle$ 是一个群，当且仅当 G 的单位元由 $\mathcal{G}$ 上的一个满像词表示。

下面的引理是我们所考虑的算法问题之间的经典归约。根据引理 2.2，本文始终可以专注于群问题。

引理 2.2。 设 G 为一个群。如果群问题在 G中是可判定的，那么单位元问题和逆元问题在 G中也都是可判定的。

2.2 多胞体、劳朗多项式和模。 关于凸多面体的详细参考资料，见 [2]。设 C 为一个（闭）凸多面体。 C 的面 F 是指 C 与任意闭半空间的交集，其中该半空间的边界与 C的内部不相交。 C 的一个真面 是 C的一个面，且既不是空集，也不是 C 本身。例如，如果 C 的维数为二，那么C 的真面就是其边和顶点。

设 R 为一个交换环（例如 $\mathbb{Z}$或 $\mathbb{R}$）或半环（例如 $\mathbb{N}$ 或 $\mathbb{R}_{\geq 0}$）。记 $R[X_1^{\pm}, \ldots, X_n^{\pm}]$ 为关于 R 且含有 n 个变量的劳朗多项式环或半环：这是变量 X_1、X_1^{-1}、.....、X_n、X_n^{-1}的、系数属于 R的多项式集合。当 n 固定时，我们记

$$R[\overline{X}^{\pm}] \coloneqq R[X_1^{\pm}, \ldots, X_n^{\pm}], \quad R[\overline{X}^{\pm}]^* \coloneqq R[\overline{X}^{\pm}] \setminus \{0\}.$$

对于向量 $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$，用 X^a 表示单项式 $X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n}$。令 $\cdot$ 表示 $\mathbb{R}^n$中的点积。给定 $f \in R[X^{\pm}]$ 和向量 $v \in (\mathbb{R}^n)^* \coloneqq \mathbb{R}^n \setminus \{0\}$，定义其加权次数

$$\deg_v(f) \coloneqq \max\{v \cdot a \mid a \in \mathbb{Z}^n, c_a \neq 0\}, \quad \text{where } f = \sum c_a \overline{X}^a \neq 0.$$

此外，对所有 $v \in (\mathbb{R}^n)^*$，定义 $\deg_v(0) = -\infty$。

R 是一个交换环。一个 $R[X^{\pm}]$-模是阿贝尔群 $(M, +)$，并配有运算 $\cdot : R[X^{\pm}] \times M \to M$，满足 $f \cdot (a + b) = f \cdot a + f \cdot b$、$(f + g) \cdot a = f \cdot a + g \cdot a$、$fg \cdot a = f \cdot (g \cdot a)$ 和 $1 \cdot a = a$。例如，对于任意 $d \in \mathbb{N}$， $R[X^{\pm}]^d$ 通过$f \cdot (g_1, \ldots, g_d) = (fg_1, \ldots, fg_d)$构成一个 $R[X^{\pm}]$-模。

全文中，我们用粗体符号 $\boldsymbol{f}$ 表示向量 $(f_1, \ldots, f_d) \in R[X^{\pm}]^d$。

给定 $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m \in R[X^{\pm}]^d$，我们称它们生成 $R[X^{\pm}]$-模 $\sum_{i=1}^m R[X^{\pm}] \cdot \boldsymbol{g}_i \coloneqq \{\sum_{i=1}^m p_i \cdot \boldsymbol{g}_i \mid p_1, \ldots, p_m \in R[X^{\pm}]\}$。如果一个模可以由有限个元素生成，则称其为有限生成的。给定 N, M 中的两个有限生成子模 $R[X^{\pm}]^d$，满足$N \subseteq M$，我们可以定义商群 $M/N \coloneqq \{m \mid m \in M\}$，其中 $m_1 = m_2$ 当且仅当 $m_1 - m_2 \in N$。这个

商群也是一个 $R[X^{\pm}]$-模。如果一个 $R[X^{\pm}]$-模 $\mathcal{Y}$ 可以表示为 M/N 的商群，其中 $R[X^{\pm}]^d$ 的两个有限生成子模 $N \subseteq M$ 满足某个$d \in \mathbb{N}$，则称其为有限表示的。我们称 $\mathcal{Y}$ 的有限表示为这类 M， N 的相应生成元。

2.3 亚交换群的表示。亚交换群通常用有限亚交换群表示来表示。这里回顾其形式化定义。理解定义中的技术细节并非必要，因为本文将始终使用方程 (1)、(2) 和命题 2.4 给出的、更直观的表示。

令 F_s 为由 $s \geq 2$ 个生成元生成的自由群。商群 $M_s := F_s/[[F_s, F_s], [F_s, F_s]]$是亚交换群，称为由 s 个生成元生成的自由后元幂零群。令 $\{\underline{x}_1, \ldots, \underline{x}_s\}$ 为 F_s的生成元，则它们的等价类 $\{x_1, \ldots, x_s\}$ 是 M_s的生成元。 M_s 中的元素表示为由 $\{x_1, \ldots, x_s\}$构成的词。

定义 2.3（有限亚交换群表示）。令 G 为一个亚交换群。 G 的有限亚交换群表示由自由后元幂零群 $M_s, s \geq 2$的生成元以及有限集合中的元素 $r_1, \ldots, r_m$组成，使得 $G = M_s/\operatorname{ncl}^{M_s}(r_1, \ldots, r_m)$。这里，$\operatorname{ncl}^{M_s}(r_1, \ldots, r_m)$表示 $\{r_1, \ldots, r_m\}$的正规闭包，即包含 $\{r_1, \ldots, r_m\}$的 M_s 的最小正规子群。

根据 [19, 推论 1] 或 [5, 第 629] 页，每个有限生成亚交换群都有一个有限亚交换群表示。

给定一个有限表示的 $\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}]$-模 $\mathcal{Y}$，定义如下半直积:

$$\mathcal{Y} \rtimes \mathbb{Z}^n := \{(y, a) \mid y \in \mathcal{Y}, a \in \mathbb{Z}^n\}; \tag{1}$$

这是一个群，其乘法和求逆定义如下

$$(y, a) \cdot (y', a') = (y + \overline{X}^a \cdot y', a + a'), \quad (y, a)^{-1} = (-\overline{X}^{-a} \cdot y, -a). \tag{2}$$

$\mathcal{Y} \rtimes \mathbb{Z}^n$ 的单位元是 (0，0)。直观而言，元素 $(y,\ a)$ 可视为一个 2×2 矩阵$\begin{pmatrix} X^a & y \\ 0 & 1 \end{pmatrix}$，其中群乘法由矩阵乘法表示。[1] 下面的命题表明，只需在形如 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 的群中解决群问题。

命题 2.4. 假设给定群 G 的一个有限亚交换群表示，以及一个有限集合 $\mathcal{G} \subseteq G$。可以有效地构造一个有限表示的 $\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}]$-模 $\mathcal{Y}$，其中 $\sim$ 为某个 $n \in \mathbb{N}$；还可以构造群 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 的一个子集 $\mathcal{G}$，使得 $\langle\mathcal{G}\rangle$ 是一个群，当且仅当 $\sim$ $\sim$ $\sim\langle\mathcal{G}\rangle$ 是一个群。此外，构造出的集合 $\mathcal{G}$ 在典范投影 $\pi\colon\ \mathcal{Y} \rtimes \mathbb{Z}^n \to \mathbb{Z}^n$ 下满足 $\pi(\langle\mathcal{G}\rangle_{grp}) = \mathbb{Z}^n$。

证明概要。（完整证明见附录 B。）根据 [5, 定理 3.3], ，我们可以计算群 $\langle\mathcal{G}\rangle_{grp}$的一个表示，因此不失一般性，可以假设 $G = \langle\mathcal{G}\rangle_{grp}$。根据 [4,引理 3]， G 可以嵌入商群 $(\mathcal{Y} \rtimes \mathbb{Z}^n)\ /H$的一个子群中，其中 H 是 $\mathbb{Z}^n \leq \mathcal{Y} \rtimes \mathbb{Z}^n$的一个子群，且 H 中的元素与 $\mathcal{Y} \rtimes \mathbb{Z}^n$中的所有元素都可交换。因此，我们可以假设$G$ 给定为 $(\mathcal{Y} \rtimes \mathbb{Z}^n)\ /H$ 的一个子群，生成元集合 $\mathcal{G}$给定为 $\{g_1 H, \ldots, g_k H\}$，其中g_1，……，$g_k \in \mathcal{Y} \rtimes \mathbb{Z}^n$。设 h_1，……，h_M为 $H \subseteq \mathcal{Y} \rtimes \mathbb{Z}^n$ $\langle\mathcal{G}\rangle$ 作为半群的生成元。那么，当且仅当由 $\mathcal{G} := \{g_1, \ldots, g_k, h_1, \ldots, h_M\} \subseteq \mathcal{Y} \rtimes \mathbb{Z}^n$ 生成的半群是一个群时，才是群。由 [4, 引理 3] 中的构造不难证明，$\pi\ (\langle\mathcal{G}\rangle_{grp})\ = \mathbb{Z}^n$。最后，只需重溯 [5, 定理 3.3]和 [4, 引理 3] 的证明，即可说明该构造是有效的。 □

由命题 2.4，我们现在可以专注于解决 $\mathcal{Y} \rtimes$中的群问题 $\mathbb{Z}^n$.

[1] 当 $n = 0$ 时，多项式环 $\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}]$ 变为 $\mathbb{Z}$，群 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 退化为 $\mathbb{Z}$-模 $\mathcal{Y}$，它是一个阿贝尔群。

2.4 图论与 $\mathcal{G}$-图。 现在固定元素集合 $\mathcal{G} := \{(y_1, a_1) \ldots, (y_K, a_K)\} \subseteq \mathcal{Y} \rtimes \mathbb{Z}^n$。与 [16, 定义 4.1], 类似，我们定义 $\mathcal{G}$-图的概念。

定义 2.5 （$\mathcal{G}$-图）。 $\mathcal{G}$-图 是一个有向多重图 Γ，其顶点集合是 $\mathbb{Z}^n$ 的有限子集，并且每个顶点至少与一条边相连。 Γ的每条边都标有 $\{1, \ldots, K\}$ 中的一个索引。此外，如果一条从顶点 v 到顶点 w、标签为 i 的边满足 $v = w + a_i$，则.....

对于图 Γ，我们用 $V(\Gamma)$ 表示其顶点集合，用 $E(\Gamma)$ 表示其边集合。对于一条（有向）边 e，我们用 $s(e)$ 表示其起始顶点，用 $d(e)$ 表示其目的地顶点。如果一个图包含欧拉回路，我们称其为欧拉 图。如果对于每个顶点，其出度都等于入度，则称一个有向图为对称 图。当且仅当一个有向图是对称且连通的时，它才是欧拉图。

给定 $z \in \mathbb{Z}^n$ 和一个 $\mathcal{G}$-图 Γ，其平移 $\Gamma + z$ 是通过将 Γ 中的所有元素沿向量 z 移动所得到的图。图 1 展示了一个示例。

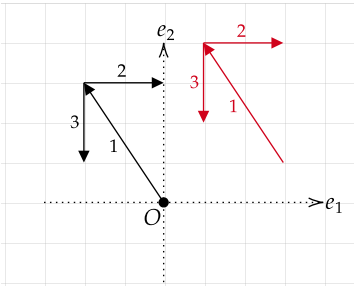

图 1：A $\mathcal{G}$-图 Γ （黑色）及其平移 $\Gamma +$ （3, 1）（红色）。

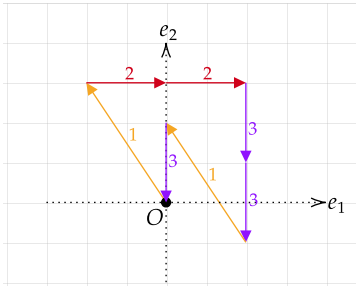

图 2：图 $\Gamma(w)$，其中$a_1 = (-2,\ 3)$ $a_2 = (2,\ 0)$ $a_3 = (0,\ -2)$，且 $w = (y_1,\ a_1)(y_2,\ a_2)(y_2,\ a_2)(y_3,\ a_3)(y_3,\ a_3)(y_1,\ a_1)(y_3,\ a_3)$。

定义 2.6 （由 $\mathcal{G}$-图表示的元素）。 对于边 $e \in E(\Gamma)$，用 $\ell(e)$ 表示 e 的标签。我们称 Γ 表示 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 的以下元素:

$$\left(\sum_{e \in E(\Gamma)} \overline{X}^{s(e)} \cdot y_{\ell(e)},\ \sum_{e \in E(\Gamma)} a_{\ell(e)} \right). \tag{3}$$

对于字母表 $\mathcal{G}$ 上的一个词 w，我们为其关联一个唯一的 $\mathcal{G}$-图 $\Gamma(w)$，定义如下。记 $w = (y_{i_1}, a_{i_1})(y_{i_2},\ a_{i_2}) \cdots (y_{i_p},\ a_{i_p})$。对于每个 $j = 0,\ \ldots\ldots,\ p-1$，我们添加一条边，从顶点 $a_{i_1} + \cdots + a_{i_j}$ 出发，到达顶点 $a_{i_1} + \cdots + a_{i_{j+1}}$，标签为 i_j。（如果 $j = 0$，则该边从 0 出发并到达 a_{i_1}。）随后取顶点 0 所在的连通分支，得到图 $\Gamma(w)$。图 2 展示了一个例子。

事实 2.7。 对于字母表 $\mathcal{G}$ 上的词 w，其关联图 $\Gamma(w)$ 所表示的 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 中的元素，等于词 w 所表示的 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 中的元素。

依次读取 w 中的字母，并沿着 $\Gamma(w)$ 中相应的边行进，即可得到 $\Gamma(w)$ 的一条欧拉路径。此外，如果词 w 表示单位元（或任何形式为 $(y,0)$ 的元素），那么这条欧拉路径就是一条欧拉回路。反过来，给定一个包含顶点 0 的欧拉 $\mathcal{G}$图Γ，我们可以从 0 出发沿一条欧拉回路行进，并读出一个词 w，使得 $\Gamma(w) = \Gamma$。

如果一个 $\mathcal{G}$图 Γ 对每个 $i \in \{1, \ldots, K\}$ 都包含一条标签为 i 的边，则称其为满像 。注意，对于字母表 $\mathcal{G}$ 上的词 w ，其关联图 $\Gamma(w)$ 是满像的，当且仅当词 w 是满像的。将引理 2.1 与上述词和欧拉图之间的对应关系结合起来，我们立即得到以下引理。注意，我们总可以平移一个 $\mathcal{G}$ 图，使其包含顶点 0；将一个 $\mathcal{G}$图平移向量 z ，会使其所表示元素的第一项乘以X^z。

—

引理 2.8。 半群 $\langle \mathcal{G} \rangle$ 是群，当且仅当存在一个表示单位元的满像欧拉 $\mathcal{G}$-图。

3 主要技术结果的证明

根据引理 2.2 和命题 2.4，我们的主要结果（定理 1.1）归结为证明下面的技术定理。

定理 3.1。 设 $\mathcal{Y}$ 是一个具有给定有限表示的 $\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}]$-模。假设给定半直积 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 的一个有限子集 $\mathcal{G}$ ，使得 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 的子群 $\langle \mathcal{G} \rangle_{grp}$ 在典范投影 $\mathcal{Y} \rtimes \mathbb{Z}^n \to \mathbb{Z}^n$ 下具有像 $\mathbb{Z}^n$ 。判断半群 $\langle \mathcal{G} \rangle$ 是否为群是可判定的。

本节概述定理 3.1 的证明。在小节 3.1 中，我们引入 $\mathcal{G}$-图的“面可达性”概念，以替代具有欧拉性质。在小节 3.2 中，我们引入“位置多项式”，将关于 $\mathcal{G}$-图的问题化为多项式半环上的算法问题。在小节 3.3 中，我们陈述一个关于多项式半环上算法问题的局部-整体原理。在小节 3.4 中，我们陈述关于多项式半环的可判定性结果。后文第 4、5 和 6 节将给出若干已陈述定理的证明。其他省略的证明可见附录 C。

3.1 从　半群到面可达图。现在固定元素集合

$$\mathcal{G} := \{(y_1, a_1), \ldots, (y_K, a_K)\} \subseteq \mathcal{Y} \rtimes \mathbb{Z}^n.$$

根据引理 2.8，判定群问题归结为寻找一个欧拉 $\mathcal{G}$-图。然而，将欧拉性质刻画为图论性质十分困难。事实上，具有欧拉性质等价于既对称又连通。虽然对称性易于进行局部描述（即在每个顶点处描述），但图的连通性是一种整体性质，因此难以描述。本小节的核心思想是引入一种称为“面可达性”的局部性质，以替代连通性。

令 Γ 为一个 $\mathcal{G}$-图。记 C 为 $V(\Gamma)$的凸包。若存在一条从该面内部出发并在其外部结束的边，则称真面 F 为可达 面。也就是说，如果存在一条边 $e \in E(\Gamma)$，从顶点 $s(e) \in F \cap V(\Gamma)$出发，并在顶点 $d(e) \in (C \setminus F) \cap V(\Gamma)$处结束，则称 F 是可达的。示例见图3。

如果 Γ 的每个真面都可达，则称图 Γ 为面可达 图。

观察 3.2。 欧拉图是面可达的。

相反，对称面可访问图不一定是欧拉图，因为它可能不连通。此外，对称图也不一定是面可访问图。反例见图4和图5。

顶点位于 $\mathbb{Z}^n$ 中的图 Γ 称为 $\mathbb{Z}^n$-生成的，如果向量集合 $\{d(e) - s(e) \mid e \in E(\Gamma)\}$作为半群生成 $\mathbb{Z}^n$ 。如果 Γ 是对称的，则该半群是一个群。因此，一个满像

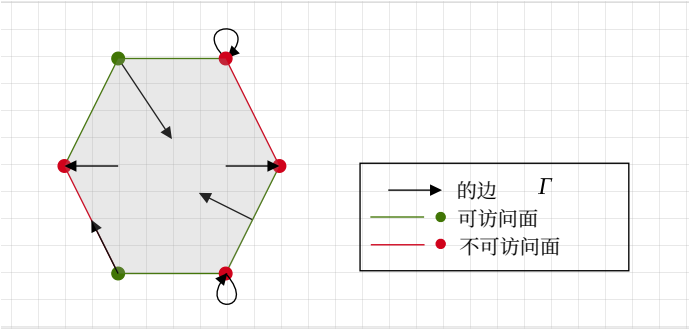

图3：可访问面和不可访问面。

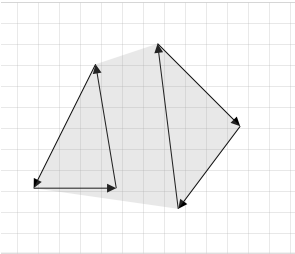

图4：一个因连通性而非欧拉的对称面可访问图。

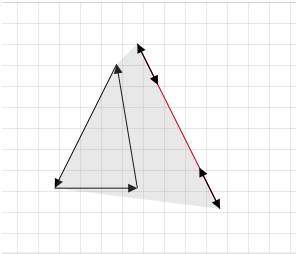

图5：一个不是面可访问图的对称图（红色面不可访问）。

对称的 $\mathcal{G}$-图是 $\mathbb{Z}^n$-生成的，当且仅当 $\{a_1,\ldots,a_K\}$ 作为群生成 $\mathbb{Z}^n$，根据定理 3.1 中的假设，这一点成立。

本小节的主要定理如下，它表明，面可达性可以通过取平移的有限并来刻画连通性。

定理 3.3。设 Γ 是一个具有对称性、面可达性并且由 $\mathbb{Z}^n$ 生成的 $\mathcal{G}$-图。则存在 z_1、……、$z_m \in \mathbb{Z}^n$，使得平移的并集 $\widehat{\Gamma} := \bigcup_{i=1}^m (\Gamma + z_i)$ 是一个欧拉图。

定理 3.3 的示意图见图6和图7。定理 3.3 的证明使用了凸几何与图论的复杂结合，将在第4节中给出。注意，定理 3.3 中的面可达性条件是必要的。图8和图9表明，如果没有面可达性，定理 3.3 不成立。

如果 Γ 表示单位元，那么并集 $\Gamma := \bigcup_{i=1}^m (\Gamma + z_i)$ 表示元素 $(\sum_{i=1}^m X^{z_i} \cdot 0,\ \sum_{i=1}^m 0) = (0, 0)$。因此，由引理 2.8 和定理 3.3，我们立即得到如下结论。

命题 3.4. 半群 $\langle \mathcal{G} \rangle$ 是群，当且仅当存在一个表示单位元的满像对称面可达 $\mathcal{G}$-图。

3.2 从面可访问图到正多项式。在本小节中，我们引入“位置多项式”来描述一个 $\mathcal{G}$-图，并将我们的图论问题归约为一个关于多项式的计算问题。回顾一下，对于 $\mathcal{G}$-图中的一条边 e，$\ell(e)$ 表示 e 的标签，而 $s(e) \in \mathbb{Z}^n$ 表示 e 的起始顶点。给定一个 $\mathcal{G}$- 图 Γ，按如下方式定义其位置元组

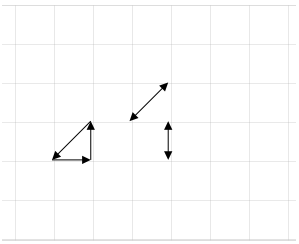

图 6：一个对称的面可达且 $\mathbb{Z}^n$-生成图 Γ，见定理 3.3。

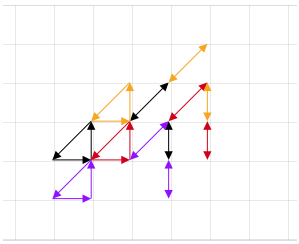

图 7：定理 3.3 中构造的欧拉图 Γ，由Γ的四个平移组成，每个平移都用不同颜色标出。

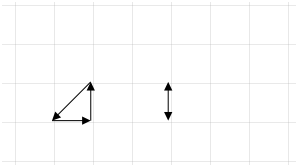

图 8：一个 Γ，它不是面可达的。

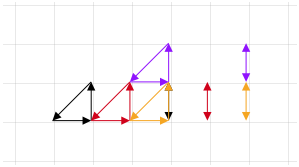

图 9：Γ的平移的并集不可能连通。

多项式 $\boldsymbol{f} = (f_1, \ldots, f_K)$：

$$f_i := \sum_{e \in E(\Gamma), \ell(e) = i} \overline{X}^{s(e)}, \quad i = 1, \ldots, K. \tag{4}$$

也就是说，f_i 是单项式 X^s的和，其中$\overline{s}$ 遍历 Γ中所有标签为 i 的边的起始顶点。这些多项式只有非负系数，因此属于 $\mathbb{N}[X^{\pm}]$。见图 10。

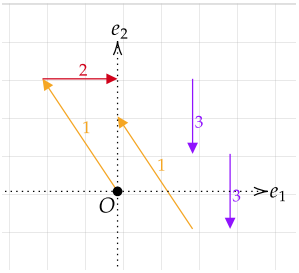

图 10：在这个例子中，$f_1 = 1 + X_1^2 X_2^{-1}$、$f_2 = X_1^{-2} X_2^3$、$f_3 = X_1^2 X_2^3 + X_1^3 X_2$。

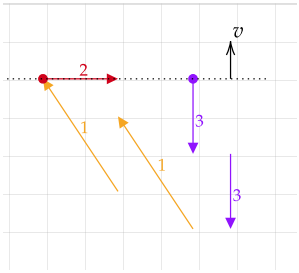

图 11：令 $v = (0, 1)$，我们有$M_v(\{1,2,3\}, \boldsymbol{f}) = \{2,3\}$、$O_v = \{1,3\}$。

反过来，给定任意一个多项式组 $\boldsymbol{f} = (f_1, \ldots, f_K) \in \mathbb{N}[X^{\pm}]^K$，可以构造一个$\mathcal{G}$-图 Γ，使得 $\boldsymbol{f}$ 恰好是其位置多项式。事实上，对于 f_i的每个单项式 cX^b，我们从顶点 b出发绘制 b 条标签为 i 的边。注意，f_i 必须是 $\mathbb{N}[X^{\pm}]$的元素，而不是 $\mathbb{Z}[X^{\pm}]$，这点至关重要，因为这样所有单项式才具有非负系数。

对于 $v \in (\mathbb{R}^n)^*$和 $I \subseteq \{1, \ldots, K\}$，定义

$$M_v(I, \boldsymbol{f}) := \left\{ i \in I \;\middle|\; \deg_v(f_i) = \max_{i' \in I} \{\deg_v(f_{i'})\} \right\}.$$

Th这是满足以下条件的指标集合：$i \in I$ $\deg_v(f_i)$ 在 $i \in I$ 中是最大的。定义

$$O_v := \{i \in \{1, \ldots, K\} \mid a_i \not\perp v\}.$$

这是满足以下条件的指标集合： $i \in \{1, \dots, K\}$ a_i 与 v 不正交。参见图 11。

下面的命题表明，我们可以利用位置多项式，完全刻画命题 3.4 中的图论性质。关键在于我们如何在 (iii) 中刻画面可达性。相比之下，无法利用位置多项式对连通性作出良好的刻画。

命题 3.5. 设 Γ 是一个 $\mathcal{G}$-图，其位置多项式为 $f_i \in \mathbb{N}[X^{\pm}], i = 1, \dots, K$。

(i) Γ 是满像的，当且仅当 $f_i \neq 0$ 对于 $i = 1, \dots, K$ 成立。

(ii) Γ 是对称的，当且仅当 $\sum_{i=1}^{K} f_i \cdot (X^{a_i} - 1) = \overline{0}$。*(iii)* Γ 是面可达的，当且仅当

$$O_v \cap M_v(\{1, \dots, K\}, \boldsymbol{f}) \neq \emptyset \quad \text{for every } v \in (\mathbb{R}^n)^* . \tag{5}$$

(iv) 假设 Γ 是对称的。Γ 表示单位元，当且仅当 $\sum_{i=1}^{K} f_i \cdot y_i = 0$。

证明。(i) 和 (iv) 很容易得到，直接利用位置多项式的定义 (4) 计算即可（详细内容见附录 C）。

(ii) 我们有

$$\sum_{i=1}^{K} f_i \cdot (\overline{X}^{a_i} - 1) = \sum_{i=1}^{K} \sum_{e \in E(\Gamma), \ell(e) = i} \overline{X}^{s(e)} (\overline{X}^{a_i} - 1) = \sum_{i=1}^{K} \sum_{e \in E(\Gamma), \ell(e) = i} (\overline{X}^{s(e) + a_i} - \overline{X}^{s(e)})$$
$$= \sum_{e \in E(\Gamma)} (\overline{X}^{d(e)} - \overline{X}^{s(e)}) = \sum_{e \in E(\Gamma)} \overline{X}^{d(e)} - \sum_{e \in E(\Gamma)} \overline{X}^{s(e)}.$$

这 当且仅当每个顶点的入度等于出度时，等于零 x.

(iii) 令 C 为 $V(\Gamma)$ 的凸包。对于 C 的每个真面 F，存在一个向量 $v \in (\mathbb{R}^n)^*$，使得 F 由 C 中所有满足 $v \cdot x$ 为最大的点 x 组成。反之，对于每个向量 $v \in (\mathbb{R}^n)^*$，所有满足 $v \cdot x$ 为最大的 C 中的点 x 所组成的集合 F 是 C 的一个真面。

设 F 为一个真面，则当且仅当从 F 出发的某条边不以 F 为终点时，F 是可达的。设 e 是一条从 F 出发、标签为 $\ell(e)$ 的边。则 $v \cdot s(e)$ 在所有 $e \in E(\Gamma)$ 中是最大的。由于单项式 $X^{s(e)}$ 包含于 $f_{\ell(e)}$ 中，这意味着 $\ell(e) \in M_v(\{1, \dots, K\}, \boldsymbol{f})$。

注意到，当且仅当 $a_{\ell(e)} = d(e) - s(e)$ 与 v 正交时，$d(e) \in F$，这等价于 $\ell(e) \notin O_v$。因此，当且仅当存在一条边 e 使得 $\ell(e) \in M_v(\{1, \dots, K\}, \boldsymbol{f})$ 且 $\ell(e) \in O_v$ 时，F 可达；也就是说，$O_v \cap M_v(\{1, \dots, K\}, \boldsymbol{f}) \neq \emptyset$。

根据面可达性的定义，当且仅当对每个 $v \in (\mathbb{R}^n)^*$，$O_v \cap M_v(\{1, \dots, K\}, \boldsymbol{f}) \neq \emptyset$ 都成立时，Γ 面可达。 □

令 $\mathcal{M}_{\mathbb{Z}}$ 为由所有满足 $\sum_{i=1}^{K} f_i \cdot (X^{a_i} - 1) = 0$ 且 $\sum_{i=1}^{K} f_i \cdot y_i = 0$ 的 $\boldsymbol{f} \in \mathbb{Z}[X^{\pm}]^K$ 组成的 $\mathbb{Z}[X^{\pm}]$-模：

$$\mathcal{M}_{\mathbb{Z}} \coloneqq \left\{ \boldsymbol{f} \in \mathbb{Z}[\overline{X}^{\pm}]^K \;\middle|\; \sum_{i=1}^{K} f_i \cdot (\overline{X}^{a_i} - 1) = 0 \text{ and } \sum_{i=1}^{K} f_i \cdot y_i = 0 \right\}. \tag{6}$$

然后，命题 3.5 表明：存在一个表示单位元的满像对称面可达 $\mathcal{G}$-图，当且仅当 $\mathcal{M}_{\mathbb{Z}}$ 包含满足性质（5）的元素 $\boldsymbol{f} \in \left(\mathbb{N}[X^{\pm}]^*\right)^K$。利用 $\mathbb{Z}[X^{\pm}]$上的线性代数，可以有效计算出 $\mathcal{M}_{\mathbb{Z}}$ 的生成元（附录 C 中给出了一个简单证明）：

引理 3.6。可以根据 y_i、a_i、$i = 1$、…、K 计算出 $\mathbb{Z}[X^{\pm}]$-模 $\mathcal{M}_{\mathbb{Z}}$ 的有限生成元集 $\boldsymbol{g}_1$、…、$\boldsymbol{g}_m \in \mathbb{Z}[X^{\pm}]^K$。

3.3 正多项式的局部-整体原理。现在我们开始构造一个算法，用于判定 $\mathcal{M}_{\mathbb{Z}}$ 是否包含满足性质（5）的元素 $\boldsymbol{f} \in \left(\mathbb{N}[X^{\pm}]^{*}\right)^{K}$。由于多项式的系数属于 $\mathbb{N}$ 而不是 $\mathbb{Z}$，这个问题非常复杂。事实上，已知在半环 $\mathbb{N}[X^{\pm}]$ 上求解线性方程是不可判定的 [31]。我们获得可判定性结果的关键在于利用线性方程的齐次性。

第一步是推广性质（5）。给定两个集合 I，$J \subseteq \{1,\dots,K\}$，我们的新目标是判定 $\mathcal{M}_{\mathbb{Z}}$ 是否包含满足以下条件的元素。

$$(O_v \cup J) \cap M_v(I, \boldsymbol{f}) \neq \emptyset, \quad \text{for every } v \in (\mathbb{R}^n)^{*}. \tag{7}$$

注意，性质（5）可以视为性质（7）在 $I = \{1,\dots,K\}$，$J = \emptyset$ 下的特殊情形。这一推广对于我们随后得到的可判定性结果至关重要。直观地说，标签属于 J 的边可以视为“沿着第 $(n+1)$ 个维数向外延伸”；而标签不属于 I 的边则可以视为“存在于第 $(n+1)$ 个维数中”。

第二步是从 $\mathbb{Z}$ 上的多项式环转到 $\mathbb{R}$ 上的多项式环，以便后续使用解析方法。令 $\mathcal{M}$ 为由引理 3.6 中的 $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m$ 生成的 $\mathbb{R}[X^{\pm}]$-子模，即

$$\mathcal{M} \coloneqq \left\{ \sum_{j=1}^{m} h_j \cdot \boldsymbol{g}_j \;\middle|\; h_1,\dots,h_m \in \mathbb{R}[\overline{X}^{\pm}] \right\}.$$

引理 3.7。存在满足性质 (7) 的元素 $\widetilde{\boldsymbol{f}} \in \mathcal{M}_{\mathbb{Z}} \cap \left(\mathbb{N}[X^{\pm}]^{*}\right)^{K}$，当且仅当存在满足性质 (7) 的 $\boldsymbol{f} \in \mathcal{M} \cap \left(\mathbb{R}_{\geq 0}[X^{\pm}]^{*}\right)^{K}$。 —

记 $\mathbb{A} \coloneqq \mathbb{R}[X^{\pm}], \mathbb{A}^{+} \coloneqq \mathbb{R}_{\geq 0}[X^{\pm}]^{*}$。给定 $f \in \mathbb{A}$ 和 $v \in (\mathbb{R}^n)^{*}$，f 的初始多项式 定义为 f 中所有具有最大次数 $\deg_v(\cdot)$ 的单项式之和：

$$\mathrm{in}_v(f) \coloneqq \sum\nolimits_{\deg_v(\overline{X}^b)=\deg_v(f)} c_b \overline{X}^b, \quad \text{where } f = \sum c_b \overline{X}^b.$$

对于 $\boldsymbol{f} = (f_1,\dots,f_K) \in \mathbb{A}^K$，自然记 $\mathrm{in}_v(\boldsymbol{f}) \coloneqq (\mathrm{in}_v(f_1),\dots,\mathrm{in}_v(f_K)) \in \mathbb{A}^K$。本小节的关键结果是以下局部-整体原理，它同时推广了 Einsiedler、Mouat 和 Tuncel [17,定理 1.3] 以及 Dong [16, 命题 3.4] 的两个深刻结果。

定理 3.8。令 $\mathcal{M}$ 为 $\mathbb{A}$的子模，且 I、J为 $\{1,\dots,K\}$的两个子集。存在$\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{A}^{+})^{K}$满足

$$(O_v \cup J) \cap M_v(I, \boldsymbol{f}) \neq \emptyset, \quad \textit{for every } v \in (\mathbb{R}^n)^{*}, \tag{8}$$

当且仅当以下两个条件得到满足：

1. **（LocR）：** 对于每个 $r \in \mathbb{R}^n_{>0}$，存在 $\boldsymbol{f}_r \in \mathcal{M}$ 使得 $\boldsymbol{f}_r(r) \in \mathbb{R}^K_{>0}$。 *2.* **（LocInf）：** 对于每个 $v \in (\mathbb{R}^n)^{*}$，存在 $\boldsymbol{f}_v \in \mathcal{M}$，使得

(a) 属于v $(\boldsymbol{f}_v) \in (\mathbb{A}^{+})^{K}$。*(b)* 记 $I' \coloneqq M_v(I, \boldsymbol{f}_v)$ $J' \coloneqq O_v \cup J$。我们有

$$\left(O_w \cup J'\right) \cap M_w(I', \mathrm{in}_v(\boldsymbol{f}_v)) \neq \emptyset \quad \textit{for every } w \in (\mathbb{R}^n)^{*}. \tag{9}$$

定理 3.8 的完整证明颇为复杂，见第 5 节。与所引用的结果相比，[16, 17], 这里新增的内容是纳入了性质（8）。由于我们对面可达性的刻画，这一性质至关重要。这一推广的主要难点在于集合 M_v, O_v与 $\boldsymbol{f}$之间复杂的相互作用，而所引用的两个结果中并不存在这种情况。

3.4 可判定性。 定理 3.8 是一种算法的关键，该算法可找到满足性质（7）的 $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{A}^+)^K$。事实上，我们有：

定理 3.9. 固定 $n \in \mathbb{N}$。假设输入为一个由 $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m \in \mathbb{A}^K$生成的集合，且其系数为整数，同时还给定向量 $a_1, \ldots, a_K \in \mathbb{Z}^n$ 以及 $\{1, \ldots, K\}$的两个子集 I, J。记 $\mathcal{M}$ 为由 $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m$生成的 $\mathbb{A}^K$ 的 $\mathbb{A}$-子模。可以判定是否存在满足以下条件的 $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{A}^+)^K$

$$(O_v \cup J) \cap M_v(I, \boldsymbol{f}) \neq \emptyset, \quad \textit{for every } v \in (\mathbb{R}^n)^* . \tag{10}$$

这里，如果 $n = 0$，则将 $\mathbb{A}$ 理解为 $\mathbb{R}$，而性质 (10) 视为平凡成立。

定理 3.9 的证明将在第 6 节给出。主要思路如下。我们对变量 n的个数进行归纳。定理 3.8 使我们能够将判定问题化为验证两个条件 (LocR) 和 (LocInf)。利用实数的一阶理论可以判定条件（LocR）。关键在于证明，只需针对可数多个 v判定条件（LocInf）即可。对于每个 v，我们都可以通过巧妙应用归纳假设来判定 (LocInf)。然后，我们并行运行两个过程：一个枚举 $\mathcal{M}_{\mathbb{Z}}$ 中的所有元素，并检查其中是否有元素属于 $(\mathbb{A}^+)^K$ 且满足性质 (10)；另一个枚举可数多个$v \in (\mathbb{R}^n)^*$，并检查条件（LocInf）是否不成立。定理 3.8 保证这两个过程必有一个会终止。

综合引理 2.2、命题 3.4、命题 3.5、引理 3.6、引理 3.7 和定理 3.9，我们得到主要技术结果：

定理 3.1。 设 $\mathcal{Y}$ 是一个具有给定有限表示的 $\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}]$-模。假设给定半直积 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 的一个有限子集 $\mathcal{G}$，使得 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 的子群 $\langle \mathcal{G} \rangle_{grp}$ 在典范投影 $\mathcal{Y} \rtimes \mathbb{Z}^n \to \mathbb{Z}^n$ 下具有像 $\mathbb{Z}^n$。则半群 $\langle \mathcal{G} \rangle$ 是否为群是可判定的。

证明。 注意到，$\mathbb{N}[X^{\pm}]^K$ 中的多项式元组与 $\mathcal{G}$-图之间存在一一对应关系。因此，命题 3.4 和命题 3.5 表明，只需判定模 $\mathcal{M}_{\mathbb{Z}}$ （定义见（6））是否包含满足性质（5）的元素 $\boldsymbol{f} \in \left(\mathbb{N}[X^{\pm}]^*\right)^K$。我们利用引理 3.6 计算 $\mathcal{M}_{\mathbb{Z}}$ 的一个基。然后，引理 3.7 表明，只需判定是否存在满足性质（5）的 $\boldsymbol{f} \in \mathcal{M} \cap \left(\mathbb{R}_{\geq 0}[X^{\pm}]^*\right)^K$。但是，性质（5）只不过是带有 $I = \{1, \ldots, K\}$，$J = \emptyset$ 的性质（8）。因此，定理 3.9 表明这是可判定的。 □

我们的主要结果由这一技术性结果推出。

定理 1.1。 在所有有限生成的亚阿贝尔群中，群问题、单位元问题和逆元问题都是可判定的。

证明。 令 G 为有限生成亚交换群。根据引理 2.2，只需判定 G 中的群问题。给定 G 中的有限子集 $\mathcal{G}$，我们使用命题 2.4 构造某个 $n \in \mathbb{N}$ 的有限表示的 $\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}]$-模 $\mathcal{Y}$，以及群 $\mathcal{Y} \rtimes \mathbb{Z}^n$, $\widetilde{\ }$ 的子集 $\widetilde{\mathcal{G}}$，使得 $\langle \mathcal{G} \rangle$ 是群当且仅当 $\langle \mathcal{G} \rangle$ 是群。此外，所构造的集合 $\mathcal{G}$ 在典范投影 $\pi\colon \mathcal{Y} \rtimes \mathbb{Z}^n \to \mathbb{Z}^n$ 下满足 $\widetilde{\ }\pi(\langle \mathcal{G} \rangle_{grp}) = \mathbb{Z}^n$。定理 3.1 表明，我们可以判定 $\widetilde{\ }\langle \mathcal{G} \rangle$ 是否为群。因此，可以判定 $\langle \mathcal{G} \rangle$ 是否为群。 □

4 从面可达性到连通性

本节给出定理 3.3 的证明。令 Γ 为一个具有对称性、面可达性且由 $\mathbb{Z}^n$ 生成的 $\mathcal{G}$-图。注意，在对称图中，从顶点 v 到 w 存在路径，当且仅当从 w 到 v 存在路径。因此，只需证明图 Γ 的无向版本具有连通性 $\widehat{}$。

令 x 为 $\mathbb{R}^n$ 中的任意一点。给定 $c \in \mathbb{R}^n$ 和 $r \in \mathbb{R}_{>0}$，用 $scale(x, c, r)$ 表示以 c 为中心、比率为 r 的 x 的缩放。也就是说，

$$scale(x, c, r) \coloneqq c + r \cdot (x - c).$$

令 S 为 $\mathbb{R}^n$ 中的任意集合，定义

$$scale(S, c, r) \coloneqq \{scale(x, c, r) \mid x \in S\}.$$

当中心为原点 0 时，我们通过定义来简化记号

$$NS \coloneqq scale(S, 0, N)$$

令 C 为 $V(\Gamma)$ 的凸包。由于 Γ 是 $\mathbb{Z}^n$-生成的，多面体 C 的维数为 n。对于任意 $N \in \mathbb{N}$，令 $NC \coloneqq scale(C, 0, N)$。定义

$$S_N \coloneqq \{z \in \mathbb{Z}^n \mid z + C \subset NC\}.$$

也就是说，S_N 是使 z 保持在 NC 中的平移向量集合。考虑图

$$\Gamma_N \coloneqq \sum_{z \in S_N} (\Gamma + z).$$

我们有 $V(\Gamma_N) \subseteq NC$。直观地说，Γ_N是图 Γ的平移的并集，这些图的凸包包含于 NC 中。图12和图13给出了示意图。我们的目标是证明，对于某个足够大的 N，图 Γ_N 是连通的。

首先，我们如下定义（无限）图 $\Gamma_{\mathbb{Q}}$。$\Gamma_{\mathbb{Q}}$ 的顶点为 $V(\Gamma_{\mathbb{Q}}) := C \cap \mathbb{Q}^n$。$\Gamma_{\mathbb{Q}}$ 的边为

$$E(\Gamma_{\mathbb{Q}}) \coloneqq \{scale(e, c, r) \mid e \in E(\Gamma), c \in C, r \in (0, 1) \cap \mathbb{Q}\}.$$

也就是说，$\Gamma_{\mathbb{Q}}$ 是所有完全落在 C 内的 Γ 的缩放版本的并集。直观地说，当 N 趋于无穷大时，可以将 $\Gamma_{\mathbb{Q}}$看作 Γ_N 的“极限”。图14给出了示意图。

将 面格 $\mathrm{Lat}(C)$ 定义为 C 的所有面的集合。对于 $F \in \mathrm{Lat}(C)$，其 相对内部$\mathrm{int}(F)$ 是 F 中不包含于 F 的任何子面中的点的集合：

$$\mathrm{int}(F) \coloneqq \{x \in F \mid \text{ for all faces } F' \subsetneq F, x \notin F'\}.$$

于是，面的相对内部构成了 C 的一个划分：

$$C = \bigcup_{F \in \mathrm{Lat}(C)} \mathrm{int}(F).$$

对于任意点 $x \in C$，定义 F_x 为 C 的面，使得 $x \in \mathrm{int}(F_x)$。这是包含 x 的最小面。对于 C 的任意面 F，当且仅当 $F_x \subseteq F$ 时，$x \in F$。定义

$$C_x \coloneqq \bigcup_{F \in \mathrm{Lat}(C), F \supseteq F_x} \mathrm{int}(F).$$

也就是说，集合 C_x 是所有包含 F_x 的面的内部的并集。图15对此进行了说明。这同样是所有包含 x 的面的内部的并集。如果 $y \in C_x$，那么 $F_y \supseteq F_x$，因此 $C_y = \bigcup_{F \in \mathrm{Lat}(C)\ F \subseteq F_y} \mathrm{int}(F) \subseteq \bigcup_{F \in \mathrm{Lat}(C)\ F \subseteq F_x} \mathrm{int}(F) = C_x$。

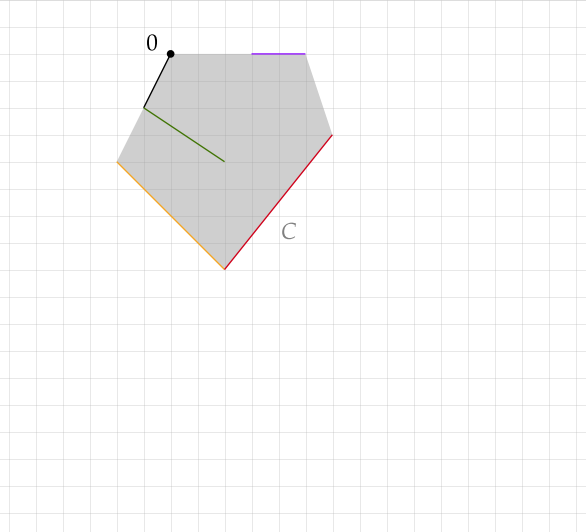

图12：图 Γ 的凸包 C 以灰色覆盖，每条边用不同颜色标示。

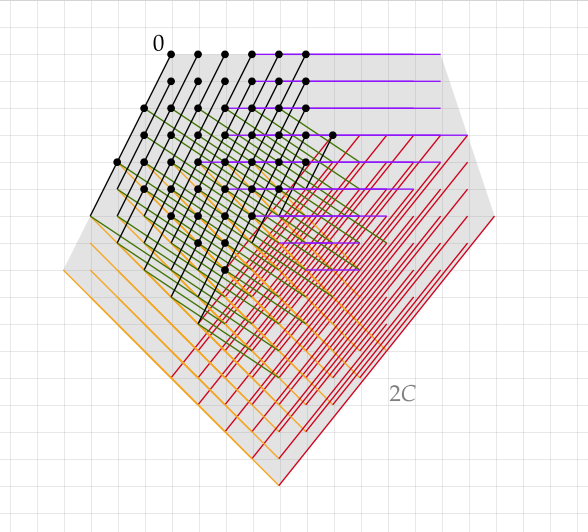

图13：由 Γ的平移构成的图 Γ_N，其中包含 $N = 2$。多面体 $2C$ 以灰色覆盖。

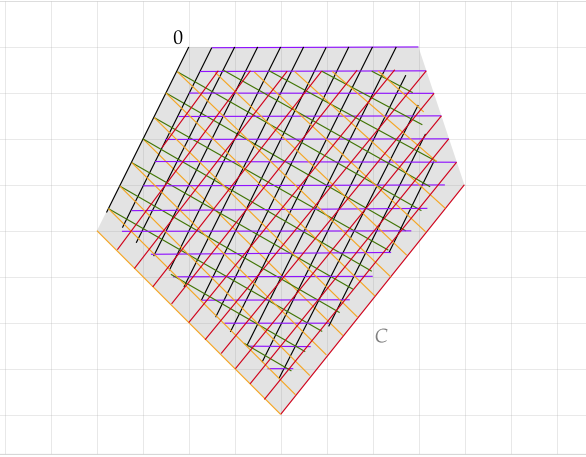

图14： $\Gamma_{\mathbb{Q}}$的示意图，其中 Γ 与图12中的相同。

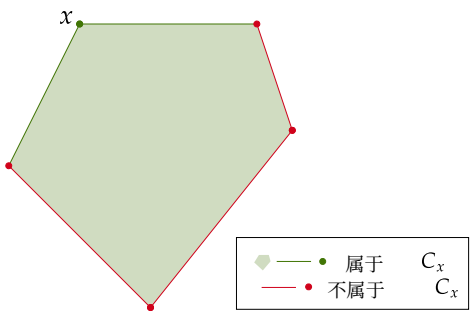

图15：集合 C_x的示意图。

引理 4.1。对于任意 $c \in C_x$ 和 $r \in (0,\ 1)$，有 $scale(C,\ c,\ r) \subset C_x$。

证明。令 $v \in C$，我们证明 $scale(v,\ c,\ r) \in C_x$。由于 $c \in C_x = \bigcup_{F \in \mathrm{Lat}(C)\ F \supseteq F_x} \mathrm{int}(F)$，我们有 $\mathrm{int}(F_c) \subset C_x$。因此 $F_c \supseteq F_x$。

将连接 c和 v 的闭线段记作 $seg(c,\ v)$，并将 $\mathrm{int}(seg(c,\ v))$ 记作：$= seg(c,\ v) \backslash \{c, v\}$。令 F 为包含 $seg(c,\ v)$ 的最小面，则 $F \supseteq F_c \supseteq F_x$。因此，$scale(v,\ c,\ r) \in \mathrm{int}(seg(c,\ v)) \subset \mathrm{int}(F) \subset C_x$。 □

由于 $C = \bigcup_{x \in C} C_x$，我们有 $E(\Gamma_{\mathbb{Q}}) = \bigcup_{x \in C} E_x(\Gamma_{\mathbb{Q}})$，其中

$$E_x(\Gamma_{\mathbb{Q}}) := \{scale(e, c, r) \mid e \in E(\Gamma), c \in C_x, r \in (0, 1) \cap \mathbb{Q}\}.$$

$E_x(\Gamma_{\mathbb{Q}})$ 中的每条边都包含在 C_x 中，这由引理 4.1 得出。

引理 4.2。 $\Gamma_{\mathbb{Q}}$ 的每个顶点 x 都通过一条有限路径 P_x 与 $\mathrm{int}(C)$ 连通，该路径由$E_x(\Gamma_{\mathbb{Q}})$中的边组成。

证明。 证明示意见图 16。我们首先证明， x 通过一条边$e_x \in E_x(\Gamma_{\mathbb{Q}})$与某个满足 $F_{x'} \supsetneq F_x$ 的 $x' \in C_x$ 相连。

由于 Γ 是面可达的，因此存在一条边 $e \in E(\Gamma)$ 连接 $w \in F_x$ 和 $w' \in C \setminus F_x$。由于 $x \in$ 属于 F_x 且 $w \in F_x$， 存在 $\varepsilon \in \mathbb{Q}_{>0}$ 使得 $c := scale(w, x, 1+\varepsilon) \in$ 属于 $F_x \subseteq C_x$。于是 $x = scale(w, c, \frac{\varepsilon}{1+\varepsilon})$，并且根据引理 4.1， $x' := scale(w', c, \overline{\frac{\varepsilon}{1+\varepsilon}}) \in C_x$。我们还知道 $x' \notin F_x$，因为 $w' \notin F_x$，所以 $F_{x'} \supsetneq F_x$。因此，边 $e_x := scale(e, c, \frac{\varepsilon}{1+\varepsilon})$ 位于 $E_x(\Gamma_{\mathbb{Q}})$ 中，并连接 x 和 x'。

注意到 $x' \in C_x$，因此 $C_{x'} \subseteq C_x$ 和 $E_{x'}(\Gamma_{\mathbb{Q}}) \subseteq E_x(\Gamma_{\mathbb{Q}})$。对 x' 重复此过程，我们可以分别在 $E_x(\Gamma_{\mathbb{Q}}) \subseteq E_{x'}(\Gamma_{\mathbb{Q}}) \subseteq \cdots$ 中找到一系列边 e_x， $e_{x'}$，……，，它们逐步将 x 与维数越来越高的面的内部连通。最终， x 通过路径 P_x 与 int(C) 连通。 □

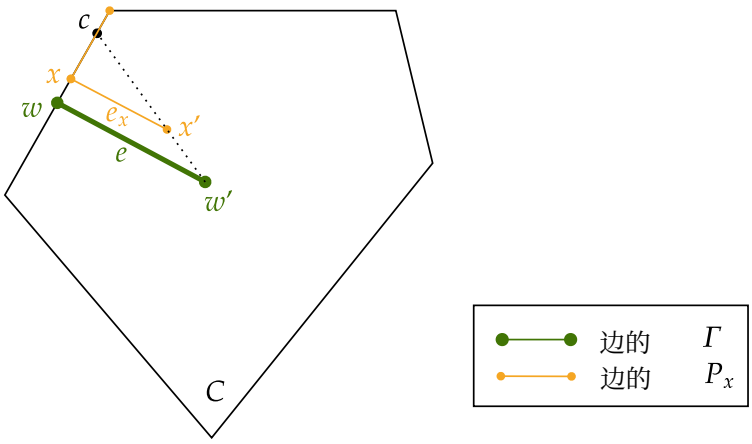

图 16：引理 4.2 的示意图。

设 x 是 C 中的任意点。对于 P_x 中的每条边 e'（引理 4.2 中定义的路径），记作 $e' = scale(e, c, r)$，其中 $e \in E(\Gamma)$ $c \in C_x$， $r \in (0, 1) \cap \mathbb{Q}$，定义多面体

$$C(e') := scale(C, c, r). \tag{11}$$

然后 $e' \subset C(e') \subset C_x$ 根据引理 4.1。因此，定义多面体的有限并

$$U_x := \bigcup_{e' \in P_x} C(e'),$$

我们有 $P_x \subset U_x \subset C_x$，且 U_x 是紧的。参见图17以了解示意图。

考虑从 $\mathbb{R}^n$ 的欧几里得拓扑继承的 C 的拓扑（即， C 的开子集具有 $C \cap U$ 的形式，其中 U 是 $\mathbb{R}^n$的一个开子集）。则在此拓扑下， C 是紧的。

事实 4.3。 对于每个 $x \in C$，集合 C_x 是 C的一个开子集。

证明。 只需证明 $C \setminus C_x$是闭集。事实上，$C \setminus C_x = \bigcup_{F \in \mathrm{Lat}(C)\ x \notin F}$内部$(F)$。对于任意$F \in$Lat$(C)$ $x \notin F$，对所有面 $F' \subseteq F$，我们都有 $x \notin F'$。因此$\bigcup_{F \in \mathrm{Lat}(C)\ x \notin F}$内部$(F) = \bigcup_{F \in \mathrm{Lat}(C)\ x \notin F} \bigcup_{F' \in \mathrm{Lat}(C)\ F' \subseteq F}$内部$(F') = \bigcup_{F \in \mathrm{Lat}(C)\ x \notin F} F$。所以$C \setminus C_x = \bigcup_{F \in \mathrm{Lat}(C)\ x \notin F} F$是有限个（闭）面的有限并，因而是闭集。 □

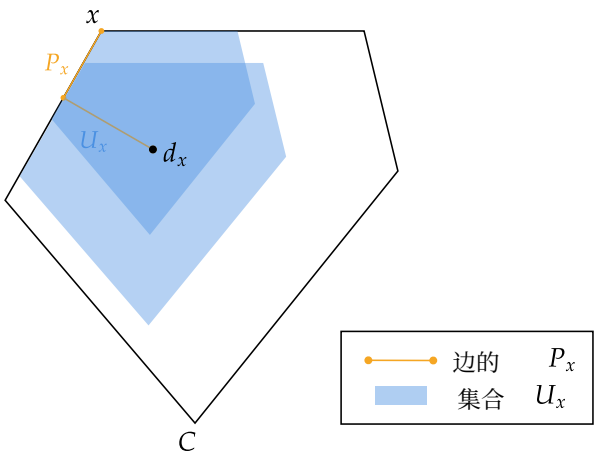

图17： U_x的示意图。

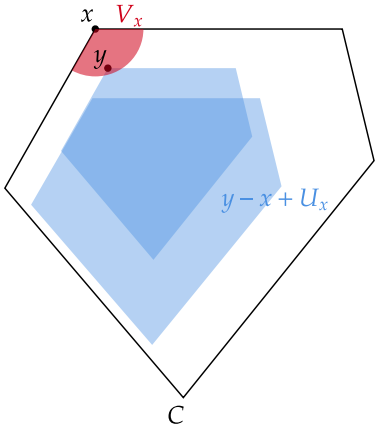

图18： V_x的示意图。

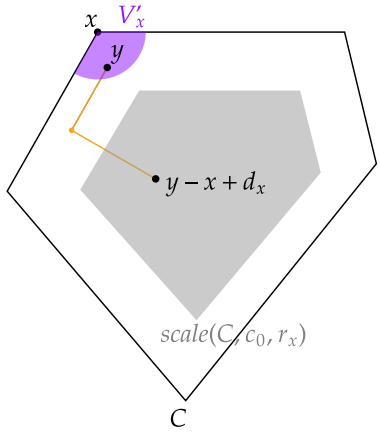

图19： V'_x的示意图。

将 $d_x := d(P_x) \in$ 内部(C) 记为 P_x的目的地。取定一点 c_0 在 C的内部。则d_x 包含于 $scale(C, c_0, r_x)$的内部，其中某个有理数为 $0 < r_x < 1$。

引理4.4。 *(1)* 存在 x的一个开邻域 $V_x \subset C$，使得对于所有 $y \in V_x$，都有 $(y-x)+U_x \subseteq C_x$。*(2)* 存在 x的一个开邻域 $V'_x \subset C$，使得对于所有 $y \in V'_x$，都有 $(y-x)+d_x \subseteq scale(C, c_0, r_x)$。示意见图*18*和图*19*。

证明。对于 $y \in C$， $r \in \mathbb{R}_{>0}$，记 $B(y, r)$ 为以 y 为中心、半径为 r 的开球。记$B_C(y, r) := C \cap B(y, r)$；它是 C 的开子集。

(1) 对于每个 $y \in U_x \subset C_x$，由于 C_x 在 C 中是开集，令 $r_y > 0$ 为满足 $B_C(y, r) \subset C_x$ 的实数r 的上确界。函数 $f: y \mapsto r_y$ 在 U_x 上连续，因为 $|r_y - r_{y'}| \leq |y - y'|$。由于 U_x 是紧集，f 在 U_x 上取得最小值 $r_{min} > 0$。然后令 $V_x := B_C(x, r_{min}/2)$，我们有 $(y-x)+U_x \subseteq C_x$。

(2) 由于 $scale(C、 c_0、 r_x)$ 是一个 n 维多面体，其内部是一个开集。由于 d_x 位于 $scale(C、 c_0、 r_x)$ 的内部，存在 $\rho_x > 0$，使得 $B(d_x、 \rho_x)$ 包含于其内部

其中 $scale(C,\ c_0,\ r_x)$。然后我们只需取 $V_x := B_C(x,\ \rho_x)$。 □

对每个 $x \in C$，记 $W_x := V_x \cap V'_x$。开集 W_x、$x \in C$ 覆盖紧集 C，因此我们可以选取有限个代表元 x_1、……、x_m，使得 $W_{x_1} \cup \cdots \cup W_{x_m} = C$。分别将路径 P_{x_1}、……、P_{x_m} 记为 P_1、……、P_m，并将集合 U_{x_1}、……、U_{x_m} 记为 U_1、……、U_m。令 $R := \max\{r_{x_1}, \ldots, r_{x_m}\}$。

因此，对于每个 $y \in C$，存在 x_i 使得 $y \in W_{x_i}$；集合 $U_i + (y - x_i)$ 包含于 C 中，并且路径 $P_i + (y - x_i)$ 从 y 通向 $scale(C,\ c_0,\ R)$ 的内部。

对于每条边 $e' = scale(e,\ c,\ r)$ $e \in E(\Gamma)$ $c \in C_x$，$r \in (0,\ 1) \cap \mathbb{Q}$，在路径 P_1、……、P_m 中的每一条路径上，令 $n(e') \in \mathbb{N}$ 满足 $n(e') \cdot r \in \mathbb{N}$ 且 $n(e') \cdot c \in \mathbb{Z}^n$。此外，令 $n_0 \in \mathbb{N}$ 满足$n_0 \cdot c_0 \in \mathbb{Z}^n$。定义

$$N_0 := n_0 \cdot \prod_{e' \in P_1 \cup \cdots \cup P_m} n(e').$$

于是特别地，$N_0 x_i$ 对于所有 $i = 1$、……、m 都只有整数项；并且 $N_0 \cdot s(e')$ 对所有 $e' \in P_1 \cup \cdots \cup P_m$ 也只有整数项。

引理 4.5。设 $N \in \mathbb{N}$ 满足 $N_0 \mid N$。则 Γ_N 中的每个顶点都与 $scale(NC、Nc_0、R) \cap V(\Gamma_N)$ 中的某个顶点连通。

证明。证明过程如图 20 和图 21 所示。

对于每个 $y \in \mathrm{conv}(\Gamma_N) \subseteq NC$，点 $y' := \frac{y}{N} \in \frac{1}{N}C$ 包含于 W_{x_1}，……，W_{x_m} 中的某一个集合内。不妨设 $y' \in W_{x_1}$，则 y' 通过 $\Gamma_{\mathbb{Q}}$ 中的路径 $(y' - x_1) + P_1$ 与 $(y' - x_1) + d(P_1) \in scale(C,\ c_0,\ R)$ 连通。我们将证明 $scale((y' - x_1) + P_1,\ 0,\ N)$ 是 Γ_N 中的一条路径。若确实如此，则它将 $Ny' = y$ 与 $N(y' - x_1 + d(P_1)) \in scale(NC,\ Nc_0,\ R)$ 连通，证毕。

现在我们证明，$scale((y' - x_1) + P_1, 0, N)$ 是 Γ_N 中的一条路径。只需证明，对于每条边 $e' \in P_1$，线段 $scale((y' - x_1) + e', 0, N)$ 都是 Γ_N 中若干条边的拼接。再次记$e' = scale(e, c, r)$ $e \in E(\Gamma)$ $c \in C_x, r \in (0, 1) \cap \mathbb{Q}$。考虑在（11）中定义的多面体 $C(e')$。根据集合 U_1 的定义，平移 $C'' := (y' - x_1) + C(e')$ 包含于 C 中。此外，~边 $e'' := (y' - x_1) + e'$ 包含于 C'' 中。因此，$\widetilde{C} := NC''$ 包含于 NC 中。注意，$s(e'')$ 在 C'' 中的相对正向与 $s(e)$ 在 C 中的相对正向相同，因此 $Ns(e'')$ 在 NC'' 中的相对正向与 $s(e)$ 在 C 中的相对正向相同。记~$\widetilde{s} := Ns(e'')$ $= y - Nx_1 + Ns(e') \in C \cap \mathbb{Z}^n$。对于每个 $k = 0,\ 1,\ \ldots,\ rN - 1$，定义

$$r_k := k(d(e) - s(e)) + \widetilde{s} - s(e) \in \mathbb{Z}^n.$$

考虑多胞体 $r_0 + C$，……，$r_{rN-1} + C$。对于每个 $k = 0$、1，……，$rN - 1$，

$$\widetilde{s} + \frac{krN}{rN - 1}(d(e) - s(e)) \in \widetilde{s} + rN(e - s(e)) = \widetilde{s} + N(e'' - s(e'')) = Ne'' \subset NC'' = \widetilde{C}.$$

因此

$$scale(\widetilde{C}, \widetilde{s} + \frac{krN}{rN - 1}(d(e) - s(e)), \frac{1}{rN}) \subset \widetilde{C} \subset NC.$$

因此，对于 $k = 0,\ 1$、.. .、$rN - 1$ 我们有

$$\begin{aligned} r_k + C = k(d(e) - s(e)) + \widetilde{s} - s(e) + C &= k(d(e) - s(e)) + scale(\widetilde{C}, \widetilde{s}, \frac{1}{rN}) \\ &= scale(\widetilde{C}, \widetilde{s} + \frac{krN}{rN - 1}(d(e) - s(e)), \frac{1}{rN}) \subset NC, \end{aligned}$$

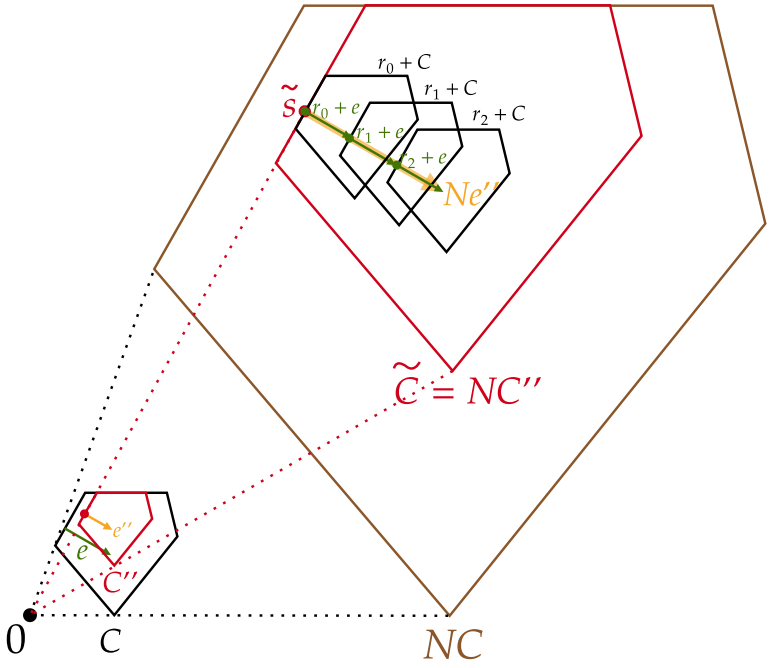

图 20：引理 4.5 的示意图1。

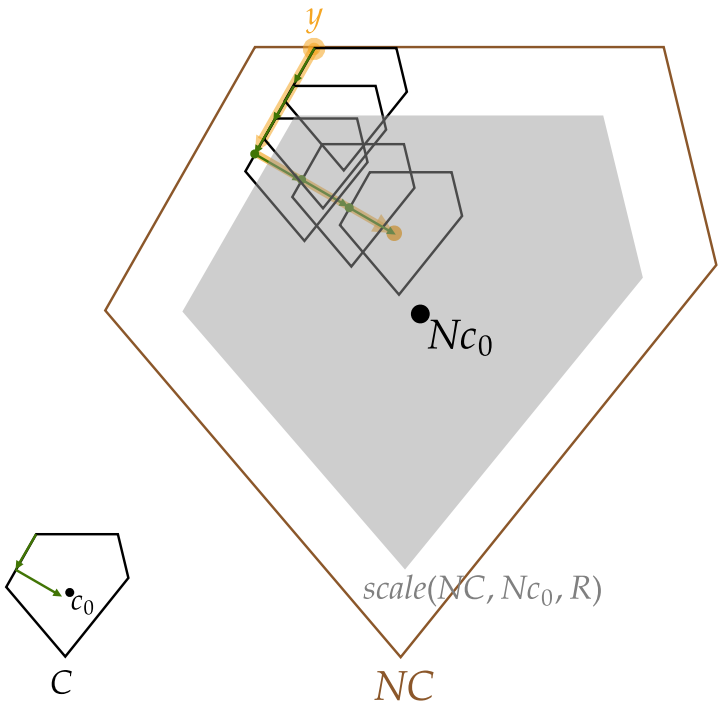

图 21：引理 4.5 的示意图2。

~其中，第二个等式源于以下事实：$\tilde{s}$ 在 C 中的相对正向相同

作为 C 中 $s(e)$ 的相对正向，因此 $scale(\widetilde{C},\ \widetilde{s},\ \frac{1}{rN})$ 是 $\frac{1}{rN}\widetilde{C}=C$ 的一个平移，其中 $\widetilde{s}$ 的相对正向与 C 中 $s(e)$ 的相对正向相同。因此，$r_k\in S_N$，且对于 $k=0,1,\ldots rN-1$，r_k+e 是 Γ_N 的一条边。拼接这些 rN 条边后，我们得到从 $\widetilde{s}$ 到 $\widetilde{s}+rN(d(e)-s(e))$ 的线段，这正是 $Ne''=scale((y'-x_1)+e',0,N)$。 □

对于 $k=1,\ldots\ldots,\ n$，令 e_k 表示 $\mathbb{Z}^n$ 的典范基中的第 k 个元素。由于 Γ 是 $\mathbb{Z}^n$-生成的，对于 $k=1,\ldots\ldots,\ n$，存在由 $E(\Gamma)$ 中各条边的平移拼接而成的 Q_k，将 0 与 e_k 连接起来。令 M_k 表示 Q_k 中出现的各条边的总长度，并令 $M:=\max_{1\le k\le n}\{M_k\}$。

记 ∂C 为 C的边界，即 C的真面之并。对于两个集合 $S,\ T\in\mathbb{R}^n$，定义它们的距离为 $dist(S,T):=\inf\{|t-s|\mid s\in S,t\in T\}$。$C$的直径定义为$diam(C):=\sup\{|t-s|\mid s,t\in C\}$。令 $N_1\in\mathbb{N}$ 满足

$$N_1\cdot dist(scale(C,c_0,R),\partial C)>M+\sqrt{n}+diam(C). \tag{12}$$

这样的 N_1 存在，这是因为 $scale(C,\ c_0,\ R)$ 与 ∂C 是不相交的闭集合，因此它们之间的距离大于零。

引理 4.6。令 $N\in\mathbb{N}$满足 $N>N_1$。$scale(NC,Nc_0,R)\cap V(\Gamma_N)$中的任意两个顶点在 Γ_N 中都是连通的。

证明。证明过程见图 22。

设 v_1、v_2 是 $scale(NC,Nc_0,R)\cap V(\Gamma_N)$ 中任意的两个顶点。在网格 $\mathbb{Z}^n$ 中存在一条从 v_1 到 v_2 的路径 $P_{\mathbb{Z}^n}(v_1,v_2)$，使得 $P_{\mathbb{Z}^n}(v_1,v_2)$ 中的每一点到$seg(v_1,v_2)$ 的距离至多为 $\sqrt{n}$ 。路径 $P_{\mathbb{Z}^n}(v_1,v_2)$ 由线段 $seg(0,e_k)$ $k=1$、……、n 的平移组成。对于 $k=1$、……、n，将 $P_{\mathbb{Z}^n}(v_1,v_2)$ 中线段 $seg(0,e_k)$ 的每个平移 $seg(0,e_k)+z$ 替换为路径 Q_k 的平移 Q_k+z，即可得到路径 $P_\Gamma(v_1,v_2)$。现在证明 $P_\Gamma(v_1,v_2)$ 的每条边都属于 $E(\Gamma_N)$。

$P_\Gamma(v_1,\ v_2)$ 中的每个点到线段 $seg(v_1,\ v_2)\subset scale(NC,\ Nc_0,\ R)$ 的距离至多为 $\sqrt{n}+M$，因此它到 $scale(NC,\ Nc_0,\ R)$ 的距离至多为 $\sqrt{n}+M$。根据 N_1 的定义 (12)，我们有

$$dist\left(scale(NC,Nc_0,R),\partial\left(NC\right)\right)=N\cdot dist(scale(C,c_0,R),\partial C)>M+\sqrt{n}+diam(C).$$

因此，$P_\Gamma(v_1,v_2)$ 中的每个点到边界 $\partial(NC)$ 的距离至少为 $diam(C)$。任取 $P_\Gamma(v_1,v_2)$ 中的一条边 e，它来自图 Γ 的某个平移 $\Gamma+z$。因此，e 包含于 $C+z$ 中。由于 e 到 $\partial(NC)$ 的距离至少为 $diam(C)$，多面体 $C+z$ 必须包含于 NC 中。因此，$z\in S_N$，所以 e 是 Γ_N 的一条边。我们已经证明，$P_\Gamma(v_1,v_2)$ 的每条边都在 $E(\Gamma_N)$ 中。因此，$scale(NC,Nc_0,R)\cap V(\Gamma_N)$ 中的任意两个顶点在 Γ_N 中连通。 □

定理 3.3。设 Γ 是一个具有对称性、面可达性且由 $\mathbb{Z}^n$ 生成的 $\mathcal{G}$-图。则存在 $z_1,\ldots,z_m\in\mathbb{Z}^n$，使得平移 $\widehat{\Gamma}:=\bigcup_{i=1}^m(\Gamma+z_i)$ 的并集是一个欧拉图。

证明。证明的示意见图 23。设 $N\in\mathbb{N}$，使得 $N_0\mid N$ 和 $N>N_1$。我们证明图 Γ_N 是连通的。任取图 Γ_N 的两个顶点 $v,\ w$。由于 $N_0\mid N$，引理 4.5 表明，v 和 w 分别与 v_1 和 v_2 中的两个顶点连通，即 $scale(NC,\ Nc_0,\ R)\cap V(\Gamma_N)$。由于 $N>N_1$，引理 4.6 表明，v_1 和 v_2 在 Γ_N 中连通。因此，v 和 w 在 Γ_N 中连通。 □

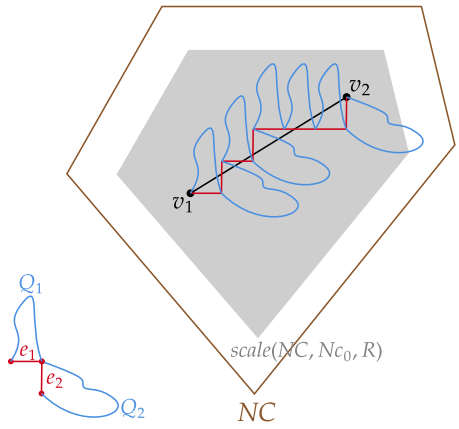

图 22：引理 4.6 的示意图。

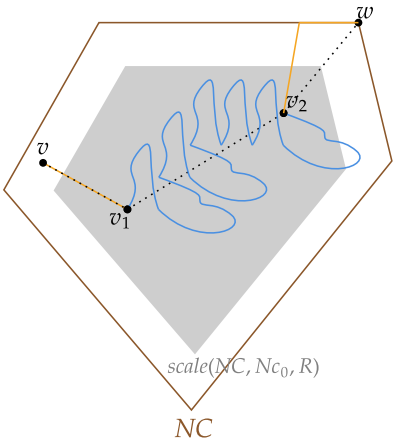

图 23：定理 3.3 证明的示意图。

5 证明局部-整体原理

在本节中，我们证明定理 3.8：

定理 3.8。 设 $\mathcal{M}$ 是 $\mathbb{A}^K$ 的一个 $\mathbb{A}$-子模， I和 J是 $\{1,\dots,K\}$的两个子集。存在$\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{A}^+)^K$ 满足

$$(O_v \cup J) \cap M_v(I, \boldsymbol{f}) \neq \emptyset, \quad \textit{for every } v \in (\mathbb{R}^n)^*, \tag{8}$$

当且仅当以下两个条件成立：

1. **(LocR)：** 对于每个 $r \in \mathbb{R}^n_{>0}$，存在 $\boldsymbol{f}_r \in \mathcal{M}$ 使得 $\boldsymbol{f}_r(r) \in \mathbb{R}^K_{>0}$。 *2.* **(LocInf)：** 对于每个 $v \in (\mathbb{R}^n)^*$，存在 $\boldsymbol{f}_v \in \mathcal{M}$，使得

(a) 属于$_v(\boldsymbol{f}_v) \in (\mathbb{A}^+)^K$. *(b)* 记 $I' := M_v(I, \boldsymbol{f}_v)$ J':
$= O_v \cup J$。我们有

$$\left(O_w \cup J'\right) \cap M_w(I', \mathrm{in}_v(\boldsymbol{f}_v)) \neq \emptyset \quad \textit{for every } w \in (\mathbb{R}^n)^*. \tag{9}$$

定理 3.8 可视为 Einsiedler、Mouat 和 Tuncel 的局部-整体原理 [17, 定理 1.3] 的推广。我们这篇论文的区别在于增加了约束（8）。请注意，这一性质源自命题 3.5 中的面可达性约束，因此对于我们研究亚交换群的子半群而言至关重要。原证明中的许多部分在 [17] 纳入性质（8）后都不再成立，尤其是 [17, 引理 3.2、引理 5.2]。为了考虑这一额外性质，我们需要引入新的论证，重新处理原证明中的许多部分。以下引理 5.1 是一个关键的新组成部分，它表明改变方向 v 一小段距离时，性质（8）具有某种“连续性”。

在陈述引理 5.1 之前，我们先作几点观察。定义商群

$$D_n := (\mathbb{R}^n)^* / \mathbb{R}_{>0}.$$

也就是说，D_n 中的元素形式为 $v\mathbb{R}_{>0}$，$v \in (\mathbb{R}^n)^*$，其中 $v\mathbb{R}_{>0} = v'\mathbb{R}_{>0}$ 当且仅当存在某个 $r \in \mathbb{R}_{>0}$使得 $v = r \cdot v'$。商群 D_n 可视为维数为 n 的单位球面，因为每个 $v\mathbb{R}_{>0}$ 都恰好等于一个满足 $||v'|| = 1$的 $v'\mathbb{R}_{>0}$。我们在 D_n 上赋予单位球面的标准拓扑。注意，在对 v 进行任意正实数缩放时，$v(\cdot)$ $M_v(\cdot)$ 和 O_v 保持不变。

引理 5.1。固定 $v \in (\mathbb{R}^n)^*$、集合 $I \subseteq \{1, \dots, K\}$ 和 $\boldsymbol{f} \in \mathbb{A}^K$。存在一个包含 $v\mathbb{R}_{>0}$的开邻域$U \subseteq D_n$，使得对于每个满足 $(v+w)\mathbb{R}_{>0} \in U$的 $w \in (\mathbb{R}^n)^*$，都有

$$\mathrm{in}_{v+w}(\boldsymbol{f}) = \mathrm{in}_w(\mathrm{in}_v(\boldsymbol{f})), \quad M_{v+w}(I, \boldsymbol{f}) = M_w(M_v(I, \boldsymbol{f}), \mathrm{in}_v(\boldsymbol{f})), \quad \textit{and} \quad O_{v+w} = O_v \cup O_w. \tag{13}$$

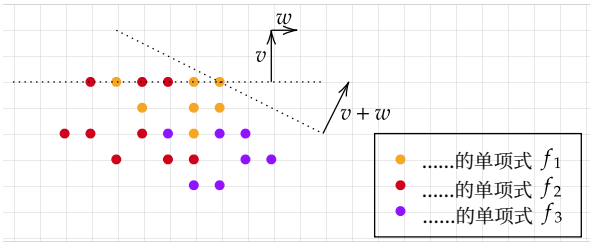

图 24：引理 5.1 的示意图。此处，$M_v(\{1,2,3\}, \boldsymbol{f}) = \{1,2\}$。

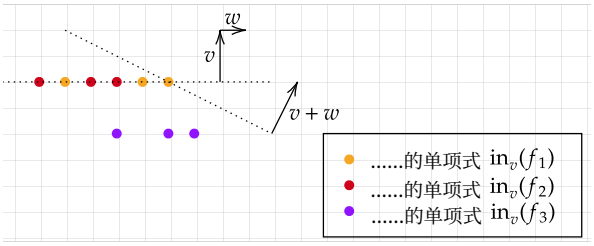

图 25：引理 5.1 的示意图。此处，$M_{v+w}(\{1,2,3\}, \boldsymbol{f}) = \{1\} = M_w(\{1,2\}, 在v(\boldsymbol{f})中)$。

证明。示意图见图 24 和图 25。对于满足 $f_i \neq 0$ 的每个 $i = 1, \dots, K$，记$f_i = g_i + h_i$，其中 $g_i :=$ 在$v(f_i)$中，且 $\deg_v(h_i) < \deg_v(g_i)$。

由于当 $v\mathbb{R}_{>0}$ 在 D_n中变化时，$\deg_v(h_i)$ 和 $\deg_v(g_i)$ 连续变化，因此存在一个包含 $v\mathbb{R}_{>0}$ 的开邻域 $U_i \subseteq D_n$，使得对于每个 $v'\mathbb{R}_{>0} \in U_i$，都有 $\deg_{v'}(h_i) < \deg_{v'}(g_i)$。因此，对于 $(v+w)\mathbb{R}_{>0} \in U_i$，我们有

$$\mathrm{in}_{v+w}(f_i) = \mathrm{in}_{v+w}(g_i) = \mathrm{in}_w(g_i) = \mathrm{in}_w(\mathrm{in}_v(f_i)).$$

其中$v+w(g_i)$中的 $=$ 在$w(g_i)$中可以如下论证。对于 g_i中出现的每个单项式 cX^b，我们有 $\overline{\deg}_{v+w}(cX^b)$ $= v \cdot b + w \cdot b = \overline{\deg}_v g_i + w \cdot b = \deg_v g_i + \deg_w(cX^b)$；因此，$g_i$ 中具有最大的$\overline{\deg}_{v+w}$ 的单项式，恰好是具有最大的 $\deg_w$的单项式。

注意，对于每个 $i \in M_v(I, \boldsymbol{f})$ $i' \in I \setminus M_v(I, \boldsymbol{f})$，我们都有 $\deg_v(f_i) > \deg_v(f_{i'})$。再次由 $\deg_v$ 关于 v 的连续性可知，存在 U' 的一个开邻域，使得对于 $v\mathbb{R}_{>0}$，

所有 $v'\mathbb{R}_{>0} \in U'$，我们都有 $\deg_{v'}(f_i) > \deg_{v'}(f_{i'})$，其中 $i \in M_v(I, \boldsymbol{f})$ $i' \in I \setminus M_v(I, \boldsymbol{f})$。于是，对于每个 $(v+w)\mathbb{R}_{>0} \in \cap_{i\in I,\ f_i\neq 0} U_i \cap U'$，我们有

$$
\begin{aligned}
&M_{v+w}(I, \boldsymbol{f}) \\
=&\left\{ i \in I \;\middle|\; \deg_{v+w}(f_i) = \max_{i'\in I}\{\deg_{v+w}(f_{i'})\} \right\} \\
=&\left\{ i \in M_v(I, \boldsymbol{f}) \;\middle|\; \deg_{v+w}(f_i) = \max_{i'\in M_v(I,\boldsymbol{f})}\{\deg_{v+w}(f_{i'})\} \right\} \quad (\text{since } (v+w)\mathbb{R}_{>0} \in U') \\
=&\left\{ i \in M_v(I, \boldsymbol{f}) \;\middle|\; \deg_{w}(\mathrm{in}_v(f_i)) = \max_{i'\in M_v(I,\boldsymbol{f})}\{\deg_{w}(\mathrm{in}_v(f_{i'}))\} \right\} \quad (\text{since } (v+w)\mathbb{R}_{>0} \in U_i, i \in I) \\
=&M_w(M_v(I, \boldsymbol{f}), \mathrm{in}_v(\boldsymbol{f}_v)).
\end{aligned}
$$

最后，取任意 $i \in \{1, \ldots, K\}$。若 $a_i \not\perp v$，则存在 $v\mathbb{R}_{>0}$ 的开邻域 $U_i'' \subseteq D_n$，使得对于每个 $v'\mathbb{R}_{>0} \in U_i''$，都有 $a_i \not\perp v'$。若 $a_i \perp v$，则对于每个 $w \in (\mathbb{R}^n)^*$，都有 $a_i \perp (v+w) \iff a_i \perp w$。取 $U'' := \cup_{i\in\{1,\ldots,K\},\ a_i\not\perp v} U_i''$。对于所有 $(v+w)\mathbb{R}_{>0} \in U''$，我们有

$$
\begin{aligned}
O_{v+w} &= \{i \in \{1, \ldots, K\} \mid a_i \not\perp (v+w)\} \\
&= \{i \in \{1, \ldots, K\} \mid (a_i \not\perp v \text{ and } a_i \not\perp (v+w)) \text{ or } (a_i \perp v \text{ and } a_i \not\perp (v+w))\} \\
&= \{i \in \{1, \ldots, K\} \mid (a_i \not\perp v) \text{ or } (a_i \perp v \text{ and } a_i \not\perp (v+w))\} \quad (\text{since } (v+w)\mathbb{R}_{>0} \in U_i'') \\
&= \{i \in \{1, \ldots, K\} \mid (a_i \not\perp v) \text{ or } (a_i \perp v \text{ and } a_i \not\perp w)\} \\
&= \{i \in \{1, \ldots, K\} \mid (a_i \not\perp v) \text{ or } (a_i \not\perp w)\} \\
&= O_v \cup O_w.
\end{aligned}
$$

取 $U = \cap_{i\in I,\ f_i\neq 0} U_i \cap U' \cap U''$，即可完成证明。 □

为了说明如何利用引理 5.1 将性质（8）纳入局部-整体原理，我们首先证明定理 3.8 的“仅当”部分。这是定理 3.8 中较为容易的蕴含关系。作为比较，所引用结果 [17, 定理 1.3] 和 [16,命题 3.4] 的“仅当”部分都可直接得出。

定理 *3.8* 的“仅当”部分的证明。设我们有满足性质（8）的 $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{A}^+)^K$。对于 LocR，只需对所有 $r \in \mathbb{R}^n_{>0}$ 取 $\boldsymbol{f}_r := \boldsymbol{f}$，则 $\boldsymbol{f}(r) \in \mathbb{R}^K_{>0}$。至于 LocInf，对于每个 $v \in (\mathbb{R}^n)^*$，我们证明 $\boldsymbol{f}_v := \boldsymbol{f}$ 满足性质（LocInf）（a）和（b）。根据 $\boldsymbol{f}$ 的定义，性质（LocInf）（a）成立。现在证明性质（LocInf）（b）。

当 $w \in v\mathbb{R}_{>0}$ 时，我们有 $O_w \cup J' = O_v \cup J$ 和 $M_w(I', \text{在} v(\boldsymbol{f})) = M_v(M_v(I, \boldsymbol{f}), \text{在} v(\boldsymbol{f})) = M_v(I, \boldsymbol{f})$，因此性质（LocInf）(b) 等价于 $(O_v \cup J) \cap M_v(I, \boldsymbol{f}) \neq \emptyset$。根据 $\boldsymbol{f}$ 的定义，这一点成立。

当 $w \notin v\mathbb{R}_{>0}$ 时，令 $U \subseteq D_n$ 为引理 5.1 中定义的 $v\mathbb{R}_{>0}$ 的开邻域。将 w 缩放一个足够小的正实数后，我们可以假设 $(v+w)\mathbb{R}_{>0} \in U$。我们有

$$
\mathrm{in}_{v+w}(\boldsymbol{f}) = \mathrm{in}_w(\mathrm{in}_v(\boldsymbol{f})), \quad M_{v+w}(I, \boldsymbol{f}) = M_w(I', \mathrm{in}_v(\boldsymbol{f})), \quad \text{and} \quad O_{v+w} = O_v \cup O_w,
$$

其中 $I' = M_v(I, \boldsymbol{f})$。因此 $(O_{v+w} \cup J) \cap M_{v+w}(I, \boldsymbol{f}) = (O_w \cup O_v \cup J) \cap M_w(I', \text{在} v(\boldsymbol{f})) = (O_w \cup J') \cap M_w(I', \text{在} v(\boldsymbol{f}))$。由于 $\boldsymbol{f}$ 满足性质（8），我们有 $(O_{v+w} \cup J) \cap M_{v+w}(I, \boldsymbol{f}) \neq \emptyset$。因此，对所有 $w \notin v\mathbb{R}_{>0}$，我们也有 $(O_w \cup J') \cap M_w(I', \text{在} v(\boldsymbol{f})) \neq \emptyset$。 □

我们现在开始着手证明定理 3.8 的“如果”部分。主要思路是采用受 Einsiedler 等人的原始证明启发的“粘合”过程 [17]。以下引理是这一粘合论证的基础。

引理 5.2。 假设 $v \in (\mathbb{R}^n)^*$和 $\boldsymbol{f}_v \in \mathcal{M}$满足定理 *3.8* 的 ***(LocInf)(a)*** 和 ***(b)*** 性质。那么存在一个包含 $v\mathbb{R}_{>0}$ 的开邻域 $U_v \subseteq D_n$，使得对于每个 $v'\mathbb{R}_{>0} \in U_v$,

(i) $\mathrm{in}_{v'}(\boldsymbol{f}_v) \in (\mathbb{A}^+)^K$.
(ii) $(O_{v'} \cup J) \cap M_{v'}(I, \boldsymbol{f}_v) \neq \emptyset$.

证明。 我们对 v, I和 $\boldsymbol{f}_v$应用引理 5.1，得到 $v\mathbb{R}_{>0}$的一个开邻域 $U_v \subseteq D_n$，使得对所有 $(v+w)\mathbb{R}_{>0} \in U_v$，我们都有

$$\mathrm{in}_{v+w}(\boldsymbol{f}_v) = \mathrm{in}_w(\mathrm{in}_v(\boldsymbol{f}_v)),\ M_{v+w}(I, \boldsymbol{f}_v) = M_w(M_v(I, \boldsymbol{f}_v), \mathrm{in}_v(\boldsymbol{f}_v)),\ \text{and } O_{v+w} = O_v \cup O_w.$$

注意，根据 $\boldsymbol{f}_v$的性质（LocInf）(a)，$\mathrm{in}_v(\boldsymbol{f}_v) \in (\mathbb{A}^+)^K$。由于对 $\mathbb{A}^+$中任意多项式取初始多项式都会得到 $\mathbb{A}^+$的一个元素，因此我们有 $\mathrm{in}_{v+w}(\boldsymbol{f}_v) = \mathrm{in}_w(\mathrm{in}_v(\boldsymbol{f}_v)) \in (\mathbb{A}^+)^K$。此外，$(O_{v+w} \cup J) \cap M_{v+w}(I, \boldsymbol{f}_v) = (O_w \cup J') \cap M_w(I', \mathrm{in}_v(\boldsymbol{f}_v))$，根据 $\boldsymbol{f}_v$的性质（LocInf）(b)，该集合非空。因此，(i) 和 (ii) 对 $v'\mathbb{R}_{>0} \in U_v$均成立。 □

以下引理是对引理 5.2]的加强。

引理 5.3。 假设定理 *3.8* 的条件（***LocInf***）成立。那么存在 $\boldsymbol{f} \in \mathcal{M}$ 满足

(i) $\mathrm{in}_v(\boldsymbol{f}) \in (\mathbb{A}^+)^K$ *for all* $v \in (\mathbb{R}^n)^*$.
(ii) $(O_v \cup J) \cap M_v(I, \boldsymbol{f}) \neq \emptyset$ *for all* $v \in (\mathbb{R}^n)^*$.

证明。 证明的主要步骤与 [17, 引理 5.2] 相同。图 26 展示了证明的示意图。对于每个 $v \in (\mathbb{R}^n)^*$，$||v|| = 1$，令 $\boldsymbol{f}_v \in \mathcal{M}$ 满足性质（LocInf）(a) 和 (b)。令 $U_v \subseteq D_n$ 为引理 5.2 中定义的 $v\mathbb{R}_{>0}$ 的一个开邻域。集合 $\{U_v \mid v \in (\mathbb{R}^n)^*,\ ||v|| = 1\}$ 构成紧集 D_n 的一个开覆盖。我们将 D_n 与 $\mathbb{R}^n$ 中的单位球面等同，并考虑 D_n 上由 $\mathbb{R}^n$ 诱导的度量。

令 $2\lambda < 1$ 为开覆盖 $\{U_v \mid v \in (\mathbb{R}^n)^*, ||v|| = 1\}$ 的一个勒贝格数 [30, 引理 7.2]，这意味着 D_n 中半径为 λ 的每个球都包含于某个 U_v 中。取有限个半径为 λ 的球覆盖 D_n，并将其中心标记为 $v_1, \ldots, v_m$。注意，每个球 $B(v_j, \lambda)$ $j = 1, \ldots, m$ 都包含于某个 $U_{v'_j}$ 中。令 $\boldsymbol{F}_j := \boldsymbol{f}_{v'_j}$，使得 $\mathrm{in}_v(\boldsymbol{F}_j) \in (\mathbb{A}^+)^K$ 且 $(O_v \cup J) \cap M_v(I, \boldsymbol{F}_j) \neq \emptyset$ 对所有 $v \in B(v_j, \lambda)$ 都成立（由引理 5.2）。令 2κ 为覆盖 $\{B(v_j, \lambda) \mid j = 1, \ldots, m\}$ 的一个勒贝格数。于是，对任意 $v \in D_n$，存在 $j \in \{1, \ldots, m\}$ 使得 $B(v, \kappa) \subset B(v_j, \lambda)$，特别地，$||v_j - v|| < \lambda - \kappa$。

令 δ 为.....的下确界

$$\left\{ v \cdot v_j - v \cdot v_{j'} \;\middle|\; ||v|| = 1, ||v_j - v|| < \lambda - \kappa, ||v_{j'} - v|| \geq \lambda, j, j' = 1, \ldots, m \right\}.$$

注意到 $\delta \geq \kappa(\lambda - \frac{\kappa}{2})$，因为对于所有范数为一的 v，w，w'，我们有

$$v \cdot w - v \cdot w' = \frac{1}{2}\left(||w' - v||^2 - ||w - v||^2 \right).$$

选择 r 足够大，使得对于所有 $v \in D_n$、$i = 1$、.....、K 以及 $j = 1$、.....、m，$\deg_v(F_{j,\,i}) < \frac{\delta}{2} r - \frac{\sqrt{n}}{2}$。对于 $j = 1$、.....、m，选取 $w_j \in \mathbb{Z}^n$ 使得 $||\overline{w}_j - r v_j|| \leq \frac{\sqrt{n}}{2}$。令

$$\boldsymbol{f} := \sum_{j=1}^{m} \overline{X}^{w_j} \boldsymbol{F}_j.$$

我们证明 $\boldsymbol{f}$ 满足条件 (i) 和 (ii)。任取范数为一的 $v \in (\mathbb{R}^n)^*$。令 $j \in \{1,\dots,m\}$ 满足 $||v - v_j|| < \lambda - \kappa$。对于满足 $||v - v_{j'}|| \geq \lambda$ 的 $j' \in \{1,\dots,m\}$，我们有

$$\begin{aligned}
\max_{1\leq i\leq K}\{\deg_v(\overline{X}^{w_{j'}}F_{j',i})\} &= v\cdot w_{j'} + \max_{1\leq i\leq K}\{\deg_v(F_{j',i})\}\\
&< v\cdot w_{j'} + \frac{\delta}{2}r - \frac{\sqrt{n}}{2}\\
&\leq rv\cdot v_{j'} + \frac{\delta}{2}r\\
&\leq rv\cdot v_j - r||v||\cdot||v_j - v_{j'}|| + \frac{\delta}{2}r\\
&\leq rv\cdot v_j - \frac{\delta}{2}r\\
&\leq v\cdot w_j + \frac{\sqrt{n}}{2} - \frac{\delta}{2}r\\
&< v\cdot w_j + \min_{1\leq i\leq K}\{\deg_v(F_{j,i})\}\\
&= \min_{1\leq i\leq K}\{\deg_v(\overline{X}^{w_j}F_{j,i})\}. \qquad (14)
\end{aligned}$$

对于满足 j' with $||v - v_{j'}|| < \lambda$ 的其余指标，我们已经知道，在 $v(\boldsymbol{F}_{j'})$ 中有 $\in (\mathbb{A}^+)^K$。由于这些初始部分不可能发生抵消，我们得到

$$\mathrm{in}_v(\boldsymbol{f}) = \mathrm{in}_v\left(\sum_{j'\colon ||v-v_{j'}||<\lambda}\overline{X}^{w_{j'}}\boldsymbol{F}_{j'}\right) \in \left(\mathbb{A}^+\right)^K.$$

因此，$\boldsymbol{f}$ 满足条件（i）。对于条件（ii），任取 $v \in (\mathbb{R}^n)^*$，令 $j' \in \{1,\dots,m\}$ 满足 $\max_{i\in I}\{\deg_v(X^{w_{j'}}F_{j',\,i})\} = \max_{1\leq j\leq m}\max_{i\in I}\{\deg_v(X^{w_j}F_{j,\,i})\}$。我们必有 $||v - v_{j'}|| < \lambda$。事实上，若有 $||v - v_{j'}|| \geq \lambda$，则存在 $j \in \{1,\dots,m\}$ 使得 $||v - v_j|| < \lambda - \kappa$，而由不等式（14）可得矛盾 $\max_{i\in I}\{\deg_v(X^{w_{j'}}F_{j',\,i})\} < \max_{i\in I}\{\deg_v(X^{w_j}F_{j,\,i})\}$。现在我们将证明 $M_v(I, \boldsymbol{F}_{j'}) \subset M_v(I, \boldsymbol{f})$. 取任意的 $i' \in M_v(I, \boldsymbol{F}_{j'})$，我们证明 $i' \in M_v(I, \boldsymbol{f})$.

一方面，由于 $||v - v_{j'}|| < \lambda$，所以在 $v(\boldsymbol{F}_{j'}) \in (\mathbb{A}^+)^K$ 中。我们有

$$\begin{aligned}
&\deg_v(\overline{X}^{w_{j'}}F_{j',i'}) = \max_{i\in I}\{\deg_v(\overline{X}^{w_{j'}}F_{j',i})\} = \max_{1\leq j\leq m}\max_{i\in I}\{\deg_v(\overline{X}^{w_j}F_{j,i})\}\\
&= \max_{i\in I}\max_{j:||v-v_j||<\lambda}\{\deg_v(\overline{X}^{w_j}F_{j,i})\} = \max_{i\in I}\deg_v\left(\sum_{j:||v-v_j||<\lambda}\overline{X}^{w_j}F_{j,i}\right) = \max_{i\in I}\deg_v\left(\sum_{j=1}^{m}\overline{X}^{w_j}F_{j,i}\right)\\
&= \max_{i\in I}\deg_v(f_i), \qquad (15)
\end{aligned}$$

因为在对 $v(X^{w_j}F_{j,i}) \in \mathbb{A}^+$ 求和时不可能发生抵消，对于 $j, ||v - v_j|| < \lambda$ 成立。另一方面，

$$\deg_v(\overline{X}^{w_{j'}}F_{j',i'}) = \max_{1\leq j\leq m}\max_{i\in I}\{\deg_v(\overline{X}^{w_j}F_{j,i})\} \geq \max_{1\leq j\leq m}\{\deg_v(\overline{X}^{w_j}F_{j,i'})\}.$$

因此，$\deg_v(\overline{X}^{w_{j'}}F_{j',i'}) = \max_{1\leq j\leq m}\{\deg_v(\overline{X}^{w_j}F_{j,i'})\}$。于是，

$$\deg_v(\overline{X}^{w_{j'}}F_{j',i'}) = \max_{1\leq j\leq m}\{\deg_v(\overline{X}^{w_j}F_{j,i'})\} = \max_{j:||v-v_j||<\lambda}\{\deg_v(\overline{X}^{w_j}F_{j,i'})\}$$

$$= \deg_v \left(\sum_{j:\|v-v_j\|<\lambda} \overline{X}^{w_j} F_{j,i'} \right) = \deg_v \left(\sum_{j=1}^{m} \overline{X}^{w_j} F_{j,i'} \right) = \deg_v(f_{i'})$$

因为在对$v(X^{w_j}F_{j,i'}) \in \mathbb{A}^+$求和时不可能发生抵消，$j, \|v - v_j\| < \lambda$。

因此 $\deg_v(f_{i'}) = \deg_v(X^{w_{j'}}F_{j',i'}) = \max_{i\in I}\deg_v(f_i)$，从而得到 $i' \in M_v(I, \boldsymbol{f})$。由于这对所有 $i' \in M_v(I, \boldsymbol{F}_{j'})$ 都成立，我们证明了 $M_v(I, \boldsymbol{F}_{j'}) \subseteq M_v(I, \boldsymbol{f})$。因此，$(O_v \cup J) \cap M_v(I, \boldsymbol{f}) \supseteq (O_v \cup J) \cap M_v(I, \boldsymbol{F}_{j'}) \neq \emptyset$。所以 $\boldsymbol{f}$ 满足条件 (ii)。 □

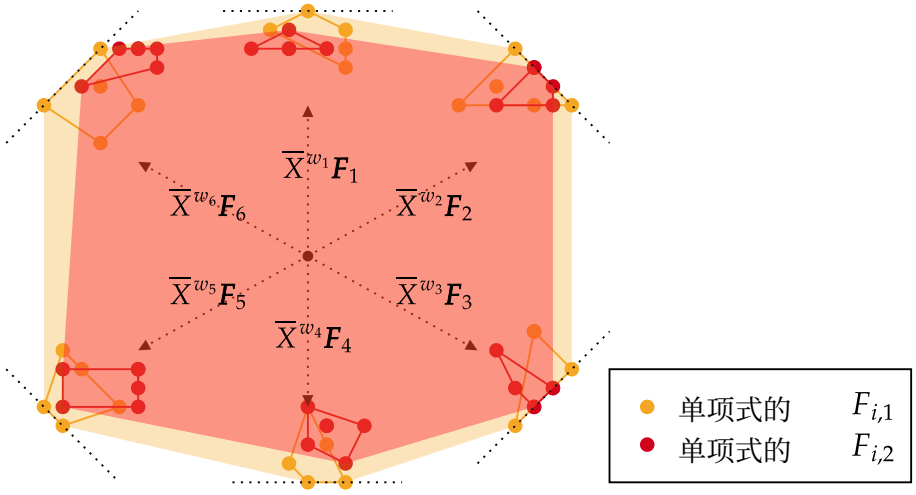

图 26：引理 5.3 证明的示意图。在此示例中，$a_1 = a_2 = (0, 0)$ $I = \{1, 2\}$，$J = \{1\}$。也就是说，条件 (ii) 要求对所有 $v \in (\mathbb{R}^n)^*$，均有 $1 \in M_v(\{1, 2\}, \boldsymbol{f})$

将引理 5.3 中得到的元素记为 $\boldsymbol{f}_\infty$ $\boldsymbol{f} \in \mathcal{M}$。由于对于所有 $v \in (\mathbb{R}^n)^*$，有 $\mathrm{in}_v(\boldsymbol{f}_\infty) \in (\mathbb{A}^+)$，因此存在 $c > 1$，使得对于所有 $x \in \mathbb{R}^n_{>0} \setminus [1/c, c]^n$，$\boldsymbol{f}_\infty(x) \in \mathbb{R}^K_{>0}$。定义紧集 $C := [1/(4nc)\ 4nc]^n$。

引理 5.4。设 $\mathcal{M}$ 是 $\mathbb{A}^K$ 的 $\mathbb{A}$-子模，且 $C \subset \mathbb{R}^n_{>0}$ 是一个紧集。假设对于所有 $r \in C$，存在 $\boldsymbol{f}_r \in \mathcal{M}$，使得 $\boldsymbol{f}_r(r) \in \mathbb{R}^K_{>0}$。那么存在 $\boldsymbol{f} \in \mathcal{M}$，使得对于所有 $x \in C$，$\boldsymbol{f}(x) \in \mathbb{R}^n_{>0}$。

证明。对于每个 $r \in C$，由多项式函数的连续性，存在一个以 r 为中心、半径为 b_r 的开球 $B(r, b_r)$，使得对于所有 $x \in B(r, b_r)$，$\boldsymbol{f}_r(x) \in \mathbb{R}^n_{>0}$。

考虑集合 C 的开覆盖 $B(r, \frac{b_r}{2})$ $r \in C$。由于 C 是紧的，因此存在一个有限子覆盖，我们将其记为 $B(r_1, \frac{b_{r_1}}{2}) \cdots, B(r_m, \frac{b_{r_m}}{2})$。

任取充分小的 $\delta > 0$。对于每个 $1 \le i \le m$，存在一个多项式 $q_i \in \mathbb{A}$，使得 $|q_i(x)| < \delta$ 对所有 $x \in C \setminus B(r_i, b_{r_i})$ 和 $|q_i(x)| > 1 - \delta$ 对所有 $x \in B(r_i, \frac{b_{r_i}}{2})$ 均成立。因此，对于充分小的 δ，和 $\boldsymbol{f} := \sum_{i=1}^m q_i \cdot \boldsymbol{f}_{r_i} \in \mathcal{M}$ 满足 $\boldsymbol{f}(x) \in \mathbb{R}^n_{>0}$，对所有 $x \in C$ 均成立。 □

将引理 5.4 中得到的元素记为 $\boldsymbol{f}_C$ $\boldsymbol{f} \in \mathcal{M}$。我们还需要 Handelman 提出的以下定理：

定理 5.5 (Handelman定理 [13], [20, V.6. 定理 C])。 设 $f \in \mathbb{A}$ 为一个多项式。当且仅当以下两个条件成立时，存在 $g \in \mathbb{A}^+$ 使得 $fg \in \mathbb{A}^+$：

(i) 对所有 $r \in \mathbb{R}^n_{>0}$，都有 $f(r) > 0$。*(ii)* 对所有 $v \in (\mathbb{R}^n)^*$ 以及 $r \in \mathbb{R}^n_{>0}$，都有 属于$v(f)(r) > 0$。

推论 5.6。 设 $\boldsymbol{f} \in \mathbb{A}^K$。存在 $g \in \mathbb{A}^+$，使得 $g\boldsymbol{f} \in (\mathbb{A}^+)^K$ 当且仅当以下两个条件成立：

(i) 对所有 $r \in \mathbb{R}^n_{>0}$，都有 $\boldsymbol{f}(r) \in \mathbb{R}^K_{>0}$。*(ii)* 对所有 $v \in (\mathbb{R}^n)^*$ 以及 $r \in \mathbb{R}^n_{>0}$，都有 属于$v(\boldsymbol{f})(r) \in \mathbb{R}^K_{>0}$。

证明。如果存在 存在 $g \in \mathbb{A}^+$ 使得 $g \cdot \boldsymbol{f} \in (\mathbb{A}^+)^K$，那么显然 (i) 和 (ii) 都成立 d.

另一方面，设 $\boldsymbol{f} \in \mathbb{A}^k$ 满足 (i) 和 (ii)。根据 Handelman定理（定理 5.5），存在 $g_1, \ldots, g_K \in \mathbb{A}^+$，使得 $f_1 g_1 \in \mathbb{A}^+, \ldots, f_K g_K \in \mathbb{A}^+$。设 $g := g_1 g_2 \cdots g_n$，则 $g\boldsymbol{f} \in (\mathbb{A}^+)^K$。 □

现在，我们可以通过将分别在引理 5.3 和 5.4 中得到的元素$\boldsymbol{f}_\infty$、$\boldsymbol{f}_C \in \mathcal{M}$ 粘合起来，证明定理 3.8 的“若”部分。

定理 *3.8* 的“若”部分的证明。设 $\boldsymbol{f}_\infty$、$\boldsymbol{f}_C \in \mathcal{M}$ 分别为引理 5.3 和 5.4 中得到的元素。定义多项式

$$q := \frac{1}{2nc} \sum_{i=1}^{n} (X_i + X_i^{-1}) \in \mathbb{A}.$$

令 $\epsilon > 0$ 满足

$$\epsilon \cdot \boldsymbol{f}_\infty(x) + \boldsymbol{f}_C(x) \in \mathbb{R}^n_{>0} \tag{16}$$

对所有 $x \in C$均成立。由 C的紧性可知，这样的 ϵ 存在。我们断言，存在 $N \in \mathbb{N}$，使得向量 $\boldsymbol{f} := \epsilon q^N \cdot \boldsymbol{f}_\infty + \boldsymbol{f}_C$同时满足推论 5.6 中的条件 (i) 和 (ii)。

令 $M \in \mathbb{N}$ 满足：对于所有 $v \in (\mathbb{R}^n)^*$、$||v|| = 1$ 和 $i = 1, \ldots, K$，$\deg_v(f_{\infty,i}) + M \cdot \min_{||w||=1} \deg_w(q) > \deg_v(f_{C,i})$。由单位球面的紧性可知，这样的 M存在。令 $\boldsymbol{g} := \epsilon q^M \cdot \boldsymbol{f}_\infty + \boldsymbol{f}_C$。那么，对于所有 $v \in (\mathbb{R}^n)^*$、$i = 1, \ldots, K$，我们有 $\deg_v(\epsilon q^M \cdot f_{\infty,i}) = M \cdot \deg_v(q) + \deg_v(f_{\infty,i}) > \deg_v(f_{C,i})$。因此，对于所有 $v \in (\mathbb{R}^n)^*$，有$v(\boldsymbol{g}) = \mathrm{in}_v(\boldsymbol{f}_\infty) \in (\mathbb{A}^+)^K$。因此，存在另一个紧集 $[1/d, d]^n \supset C$，使得对于所有 $x \in \mathbb{R}^n_{>0} \setminus [1/d, d]^n$，$\boldsymbol{g}(x) \in \mathbb{R}^K_{>0}$。由于 $[1/d, d]^n \supset C = [1/(4nc)\ 4nc]^n$，我们有 $d \geq 4nc$。由于 $[1/d, d]^n$是紧集，存在 $N > M$使得

$$\epsilon f_{\infty,i}(x) \cdot 2^N + f_{C,i}(x) > 0 \tag{17}$$

对于所有 $i = 1$、.....、K 以及所有 $x \in [1/d, d]^n$，我们证明，对于这个 N，向量 $\boldsymbol{f} := \epsilon q^N \cdot \boldsymbol{f}_\infty + \boldsymbol{f}_C$ 同时满足推论 5.6 中的条件 (i) 和 (ii)。

Fi任意 x $i \in \{1, \ldots, K\}$。对于每个 $x \in \mathbb{R}^n_{>0} \setminus [1/d, d]^n$，我们有 $q(x) > \frac{d}{2nc} \geq 1$，因此

$$f_i(x) := \epsilon q(x)^N \cdot f_{\infty,i}(x) + f_{C,i}(x) \geq \epsilon q(x)^M \cdot f_{\infty,i}(x) + f_{C,i}(x) = g_i(x) > 0.$$

Fo对于每个 $x \in [1/d, d]^n \setminus C$，至少有一个 $i' \in \{1, \ldots, K\}$ 满足 $x_{i'} \geq 4nc$，因此

$$f_i(x) = \epsilon f_{\infty,i}(x) \cdot \left(\sum_{i'=1}^{n} \frac{x_{i'} + x_{i'}^{-1}}{2nc} \right)^N + f_{C,i}(x) \geq \epsilon f_{\infty,i}(x) \cdot 2^N + f_{C,i}(x) > 0$$

根据不等式（17）和 $\sum_{i=1}^{n}(x_i+x_i^{-1}) > x_{i'} \geq 4nc$。

对于每个 $x \in C \setminus [1/c,c]^n$,

$$f_i(x) = \epsilon q(x)^N \cdot f_{\infty,i}(x) + f_{C,i}(x) > 0$$

由于 $f_{\infty,\,i}(x) > 0$ 对所有 $x \notin [1/c,c]^n$ 和 $f_{C,\,i}(x) > 0$ 对所有 $x \in C$。

对于每个 $x \in [1/c,c]^n$,

$$f_i(x) = \epsilon f_{\infty,i}(x) \cdot \left(\sum_{i=1}^{n} \frac{x_i + x_i^{-1}}{2nc}\right)^N + f_{C,i}(x) \geq \min\{\epsilon f_{\infty,i}(x), 0\} + f_{C,i}(x) > 0$$

由 $\sum_{i=1}^{n}(x_i+x_i^{-1}) < 2nc$。事实上，如果 $f_{\infty,\,i}(x) \geq 0$ 那么 $f_{\infty,\,i}(x) \cdot \left(\sum_{i=1}^{n} \frac{x_i+x_i^{-1}}{2nc}\right)^N \geq 0$，否则 $\left(\sum_{i=1}^{n} \frac{x_i+x_i^{-1}}{2nc}\right)^N \leq 1$ 因此 $f_{\infty,\,i}(x) \cdot \left(\sum_{i=1}^{n} \frac{x_i+x_i^{-1}}{2nc}\right)^N \geq f_{\infty,\,i}(x)$。因此，对于每个 $x \in \mathbb{R}^n_{>0}$，我们有 $f_i(x) > 0$。换言之， $\boldsymbol{f}$ 满足推论 5.6 中的条件 (i)。

此外，由于 $N > M$我们有，对于 $i = 1,\ldots,K, v \in (\mathbb{R}^n)^*$，$\deg_v(q^N \cdot f_{\infty,i}) > \deg_v(f_{C,i})$。因此，$\mathrm{in}_v(\boldsymbol{f}) = \mathrm{in}_v(\boldsymbol{f}_\infty) \in (\mathbb{A}^+)^K$，并且对于所有 $v \in (\mathbb{R}^n)^*$，$M_v(I,\boldsymbol{f}) = M_v(I,\boldsymbol{f}_\infty)$。因此，$\boldsymbol{f}$满足推论 5.6 中的条件 (ii)。

因此，根据推论 5.6，我们找到了 $g \in \mathbb{A}^+$，使得 $g\boldsymbol{f} \in (\mathbb{A}^+)^K$。同时，我们还有 $g\boldsymbol{f} \in \mathcal{M}$ 以及 $(O_v \cup J) \cap M_v(I, g\boldsymbol{f}) = (O_v \cup J) \cap M_v(I, \boldsymbol{f}) = (O_v \cup J) \cap M_v(I, \boldsymbol{f}_\infty) \neq \emptyset$ 对所有 $v \in (\mathbb{R}^n)^*$ 都成立。因此，我们找到了所需的元素 $\boldsymbol{f}_v := g\boldsymbol{f}$。 □

6 局部条件的可判定性

本节致力于证明定理 3.9。根据局部-整体原理（定理 3.8），这归结为证明两个“局部”条件（LocR）和（LocInf）的可判定性。

6.1 正实数处局部条件（LocR）的可判定性。在本小节中，我们证明定理 3.8 的条件（LocR）是可判定的。设 $\mathcal{M}$ 是 $\mathbb{A}^K$ 的一个 $\mathbb{A}$-子模。

引理 6.1。设 $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m$ 是 $\mathcal{M}$ 的生成元。定理 *3.8* 的条件（*LocR*）等价于以下条件：

1. **（LocRLin）**对于每个 $r \in \mathbb{R}^n_{>0}$，存在 $x_1, \ldots, x_m \in \mathbb{R}$，使得 $\sum_{i=1}^{m} x_i \boldsymbol{g}_i(r) \in \mathbb{R}^K_{>0}$。

证明。（LocR） $\Longrightarrow$（LocRLin）：假设定理 3.8 的条件（LocR）成立。对于 $r \in \mathbb{R}^n_{>0}$，条件（LocR）表明存在 $p_1, \ldots, p_m \in \mathbb{A}$，使得 $\sum_{i=1}^{m} p_i \boldsymbol{g}_i = \boldsymbol{f}_r$，其中 $\boldsymbol{f}_r(r) \in \mathbb{R}^K_{>0}$。于是令 $x_1 := p_1(r), \ldots, x_m := p_m(r)$，我们有 $\sum_{i=1}^{m} x_i \boldsymbol{g}_i(r) = \boldsymbol{f}_r(r) \in \mathbb{R}^K_{>0}$。

(LocRLin) $\Longrightarrow$ (LocR)：假设条件（LocRLin）成立。对于任意 $r \in \mathbb{R}^n_{>0}$，条件（LocRLin）表明存在 $x_1, \ldots, x_m \in \mathbb{R}_{>0}$，使得 $\sum_{i=1}^{m} x_i \boldsymbol{g}_i(r) \in \mathbb{R}^K_{>0}$。于是 $\boldsymbol{f}_r := \sum_{i=1}^{m} x_i \boldsymbol{g}_i \in \mathcal{M}$ 满足 $\boldsymbol{f}_r(r) \in \mathbb{R}^K_{>0}$。 □

命题 6.2。给定 $\mathcal{M}$ 的生成元 $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m$，可以判定定理 *3.8* 的条件（*LocR*）是否成立。

证明。根据引理 6.1，只需判定条件（LocRLin）即可。该条件可以用实数的一阶理论表达：

$$\forall r_1 > 0, \cdots \forall r_n > 0, \exists x_1 \cdots \exists x_m, \left(\sum_{i=1}^{m} x_i g_{i,1}(r_1,\ldots,r_n) > 0\right) \wedge \cdots \wedge \left(\sum_{i=1}^{m} x_i g_{i,K}(r_1,\ldots,r_n) > 0\right).$$

根据塔斯基定理 [37],该句子的真值是可判定的。 □

6.2 无穷远处的局部条件：从（LocInf）到移位初始项（LocInfShift）。在本小节中，我们引入移位初始项，以便用新的条件（LocInfShift）替代定理 3.8 的条件（LocInf）。我们的定义遵循 [17,第 1]节中的定义。

假设给定了 $\boldsymbol{f} \in \mathbb{A}^K$, $v \in (\mathbb{R}^n)^*$ 和 $\boldsymbol{\alpha} = (\alpha_1, \ldots\ldots, \alpha_K) \in \mathbb{R}^K$。那么，$v,\alpha(\boldsymbol{f}) =$ 中的 移位初始项（$\mathrm{in}_{v,\alpha}(\boldsymbol{f})_1, \ldots, \mathrm{in}_{v,\alpha}(\boldsymbol{f})_K$）定义为

$$\mathrm{in}_{v,\alpha}(\boldsymbol{f})_i \coloneqq \begin{cases} \mathrm{in}_v(f_i) & \text{if } \deg_v(f_i) + \alpha_i = \max_{1 \le i' \le K}\{\deg_v(f_{i'}) + \alpha_{i'}\}, \\ 0 & \text{if } \deg_v(f_i) + \alpha_i < \max_{1 \le i' \le K}\{\deg_v(f_{i'}) + \alpha_{i'}\}. \end{cases}$$

引理 *6.3*。设 $\boldsymbol{f} \in \mathbb{A}^K$ 和 $v \in (\mathbb{R}^n)^*$。当且仅当存在 $\boldsymbol{\alpha} \in \mathbb{R}^K$ 使得 $\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f}) \in (\mathbb{A}^+)^K$ 时，$\mathrm{in}_v(\boldsymbol{f}) \in (\mathbb{A}^+)^K$。此外，在这种情况下，$\mathrm{in}_v(\boldsymbol{f}) = \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})$，并且 $\alpha_1 + \deg_v(f_1) = \cdots = \alpha_K + \deg_v(f_K)$。

证明。如果 $\mathrm{in}_v(\boldsymbol{f}) \in (\mathbb{A}^+)^K$，那么令 $\alpha_1 \coloneqq -\deg_v(f_1)$，……，$\alpha_K \coloneqq -\deg_v(f_K)$。我们有 $\deg_v(f_1) + \alpha_1 = \cdots = \deg_v(f_K) + \alpha_K = \max_{1 \le i \le K}\{\deg_v(f_i) + \alpha_i\}$，因此 $\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f}) = \mathrm{in}_v(\boldsymbol{f}) \in (\mathbb{A}^+)^K$。

若 $\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f}) \in (\mathbb{A}^+)^K$，则 $\mathrm{in}_v(f_i) = \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})_i \in \mathbb{A}^+$ 对 $i = 1, \ldots, K$ 均成立。因此 $\mathrm{in}_v(\boldsymbol{f}) = \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f}) \in (\mathbb{A}^+)^K$。

此外，在这种情况下，由于 $\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})_i \neq 0$ 对 $i = 1, \ldots, K$ 均成立，我们有 $\deg_v(f_i) + \alpha_i = \max_{1 \le i' \le K}\{\deg_v(f_{i'}) + \alpha_{i'}\}$。因此 $\alpha_1 + \deg_v(f_1) = \cdots = \alpha_K + \deg_v(f_K)$。 □

给定 $v = (v_1, \ldots, v_n) \in (\mathbb{R}^n)^*$，定义以下实数集合：

$$\sum_{k=1}^{n} \mathbb{Z} v_k \coloneqq \left\{ \sum_{k=1}^{n} z_k v_k \;\middle|\; z_1, \ldots, z_n \in \mathbb{Z} \right\}.$$

那么，对每个 $f \in \mathbb{A}$，我们都有 $\deg_v(f) \in \sum_{k=1}^n \mathbb{Z} v_k$。

Prop命题 6.4. 定理 *3.8* 的条件（LocInf）等价于以下条件 *：*

2. **（LocInfShift）：** 对于每个 $v \in (\mathbb{R}^n)^*$，都存在 $\boldsymbol{f} \in \mathcal{M}$ 以及 $\boldsymbol{\alpha} \in \left(\sum_{k=1}^n \mathbb{Z} v_k\right)^K$，满足以下性质：

(a) 属于$_{v,\ \boldsymbol{\alpha}}(\boldsymbol{f}) \in (\mathbb{A}^+)^K$。*(b)* 记 $I' \coloneqq \{i \in I \mid \alpha_i = \min_{i' \in I} \alpha_{i'}\}$，
$J' \coloneqq O_v \cup J$。我们有

$$\left(O_w \cup J'\right) \cap M_w(I', \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})) \neq \emptyset \quad \textit{for every } w \in (\mathbb{R}^n)^*.$$

证明。（LocInf）蕴含（LocInfShift）。假设定理 3.8 的条件（LocInf）成立。固定一个向量 $v \in (\mathbb{R}^n)^*$。那么存在 $\boldsymbol{f} \in \mathcal{M}$，使得 $\mathrm{in}_v(\boldsymbol{f}) \in (\mathbb{A}^+)^K$ 满足性质（LocInf）(b)。如引理 6.3 中所述，我们可以令 $\alpha_i \coloneqq -\deg_v(f_i)$，其中 $i = 1, \ldots, K$，于是 $\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f}) = \mathrm{in}_v(\boldsymbol{f}) \in (\mathbb{A}^+)^K$，满足（LocInfShift）(a)。此外，根据 $\alpha_i = -\deg_v(f_i)$ 的定义，我们有 $\boldsymbol{\alpha} \in (\sum_{k=1}^n \mathbb{Z} v_k)^K$。最后，$\{i \in I \mid \alpha_i = \min_{i' \in I} \alpha_{i'}\} = \{i \in I \mid \deg_v(f_i) = \max_{i' \in I} \deg_v(f_{i'})\} = M_v(I, \boldsymbol{f})$，因此（LocInf）(b)蕴含（LocInfShift）(b)。

（LocInfShift） $\Longrightarrow$ **（LocInf）**。假设条件（LocInfShift）成立。固定一个向量 $v \in (\mathbb{R}^n)^*$。那么存在 $\boldsymbol{f} \in \mathcal{M}$ 以及 $\boldsymbol{\alpha} \in (\mathbb{R}^n)^*$，使得在$_{v,\ \boldsymbol{\alpha}}(\boldsymbol{f}) \in (\mathbb{A}^+)^K$ 满足性质（LocInfShift）（b）。根据引理 6.3，我们有在$_v(\boldsymbol{f}) =$在$_{v,\ \boldsymbol{\alpha}}(\boldsymbol{f}) \in (\mathbb{A}^+)^K$，以及 $\alpha_1 + \deg_v(f_1) = \cdots = \alpha_K + \deg_v(f_K)$。因此我们有 $\{i \in I \mid \alpha_i = \min_{i' \in I} \alpha_{i'}\} = \{i \in I \mid \deg_v(f_i) = \min_{i' \in I} \deg_v(f_{i'})\} = M_v(I, \boldsymbol{f})$，所以（LocInfShift）(b) 蕴含（LocInf）(b)。 □

6.3 维数约化：特殊情形。 在本小节及后续小节中，我们将进一步把条件（LocInfShift）约化为条件（LocInfD）（见命题 6.11）。在本小节中，我们首先考虑这样一种特殊情形：条件（LocInfShift）中的向量 $v \in (\mathbb{R}^n)^*$ in 的形式为 $(0, \ldots\ldots, 0, v_{d+1}, \ldots\ldots, v_n)$，其中 $v_{d+1}, \ldots\ldots, v_n \in \mathbb{R}$ 是 $\mathbb{Q}$-线性无关的。

现在我们定义一个 $\mathbb{A}$-模 $\mathcal{M}$ 的超 *Gr¨obner* 基。注意，我们的定义与 [17, 第 2], 节不同，尽管直观理解相同。设 $v \in (\mathbb{R}^n)^*, \boldsymbol{\alpha} \in \mathbb{R}^K$。定义 $\mathrm{in}_{v,\alpha}(\mathcal{M})$ 为由 $\mathrm{in}_{v,\alpha}(\boldsymbol{f})$ $\boldsymbol{f} \in \mathcal{M}$ 中的元素生成的 $\mathbb{A}$-模：

$$\mathrm{in}_{v,\alpha}(\mathcal{M}) \coloneqq \sum_{\boldsymbol{f}\in\mathcal{M}} \mathbb{A} \cdot \mathrm{in}_{v,\alpha}(\boldsymbol{f}) = \left\{ \sum_{j=1}^{q} p_j \cdot \mathrm{in}_{v,\alpha}(\boldsymbol{f}_j) \;\middle|\; q \in \mathbb{N}, p_1, \ldots p_q \in \mathbb{A}, \boldsymbol{f}_1, \ldots, \boldsymbol{f}_q \in \mathcal{M} \right\}.$$

定义 6.5 （超 Gr¨obner 基）。 模 $\mathcal{M}$ 的一组生成元 $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m$ 称为超 *Gr¨obner* 基，如果对于所有 $v \in (\mathbb{R}^n)^*, \boldsymbol{\alpha} \in \mathbb{R}^K$，集合 $\{\mathrm{in}_{v,\alpha}(\boldsymbol{g}_1) \ldots, \mathrm{in}_{v,\alpha}(\boldsymbol{g}_m)\}$ 都生成 $\mathrm{in}_{v,\alpha}(\mathcal{M})$ 这个 $\mathbb{A}$-模。

引理 6.6 （ [17, 引理 2。1]的重述）。 假设给定模 $\mathcal{M}$ 的任意一组生成元。那么可以有效地计算出 $\mathcal{M}$ 的超 *Gr¨obner* 基。

证明。 设 $\mathbb{R}[\overline{X}] \coloneqq \mathbb{R}[X_1, \ldots, X_n]$ 是以 n 个变量为基础的正则多项式环（注意，目前我们不考虑劳朗多项式环 $\mathbb{A} = \mathbb{R}[\underline{X^{\pm}}]$）。设 $e_1, \ldots, e_K$ 是 $\mathbb{R}[X]^K$的规范 $\underline{\mathbb{R}[X]}$-基。$\mathbb{R}[X]^K$ 的一个单项式是形如 $X^u e_i$ 的元素，其中$u \in \mathbb{Z}^n_{\geq 0}, i \in \{1, \ldots, K\}$。 $\mathbb{R}[X]^K$的单项式上的一个项序 是全序 $\prec$，并满足

(i) $e_i \prec \overline{X}^u e_i$,
(ii) $\overline{X}^u e_i \prec \overline{X}^{u'} e_{i'} \implies \overline{X}^{u+w} e_i \prec \overline{X}^{u'+w} e_{i'}$,

对所有 $i, i' \in \{1, \ldots, K\}$ 和 $u, u', w \in \mathbb{Z}^n_{\geq 0}$均成立。

设 N 是 $\underline{\mathbb{R}[X]^K}$的一个 $\mathbb{R}[X]$-子模。元素 $\boldsymbol{f} \in \mathbb{R}[X]^K$ 可唯一地写成和 $\sum_{u,i} c_{u,i} X^u e_i$，其系数 $c_{u,i}$ 属于 $\mathbb{R}$。在这个和中， $\mathbb{R}[X]^K$ 的非零系数单项式只有有限多个，其中按照项序 $\prec$ 最大的单项式记作 $\mathrm{in}_{\prec}(\boldsymbol{f})$。定义 $\mathrm{in}_{\prec}(N)$ 为 N关于 $\prec$的初始模，即由所有 $\mathrm{in}_{\prec}(\boldsymbol{f})$ $\boldsymbol{f} \in N$生成的$\mathbb{R}[X]$-模。若元素 $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_l \in N$关于 $\prec$构成 Gr¨obner 基，意即 $\mathrm{in}_{\prec}(N)$ 作为 $\mathbb{R}[X]$-模由 $\mathrm{in}_{\prec}(\boldsymbol{f}_1) \ldots, \mathrm{in}_{\prec}(\boldsymbol{f}_l)$ 生成。

一个通用 *Gr¨obner* 基由 N中的元素 $\boldsymbol{f}_1$、……、 $\boldsymbol{f}_l$给出；这些元素关于每个项序都构成 N 的 Gr¨obner 基。N 的通用 Gr¨obner 基存在，并且可以按照 [17, 引理 21]中的描述，由 N 的生成元集合有效地计算出来。

固定 $\left(\mathbb{R}[\overline{X^{\pm}}]\right)^K$的一个 $\mathbb{R}[X^{\pm}]$-子模 $\mathcal{M}$。找出 $\boldsymbol{f}_1$、……、 $\boldsymbol{f}_l$，使其作为一个 $\mathbb{R}[X^{\pm}]$-模生成 $\mathcal{M}$。令 $\delta = (\delta_1$、 ……、 $\delta_n) \in \{-1, 1\}^n$。选取 $u \in \mathbb{Z}^n$ 使得

$$\overline{X}^u \boldsymbol{f}_1, \ldots, \overline{X}^u \boldsymbol{f}_l \in \left(\mathbb{R}[X_1^{\delta_1}, \ldots, X_n^{\delta_n}]\right)^K,$$

并令 $\boldsymbol{f}_{\delta,\ 1}$、……、 $\boldsymbol{f}_{\delta,\ l_\delta}$为由 $X^u \boldsymbol{f}_1$、……、 $X^u \boldsymbol{f}_l$生成的 $\mathbb{R}[X_1^{\delta_1}, \ldots, X_n^{\delta_n}]$-子模的通用 Gr¨obner 基。将 $\overline{\{\boldsymbol{f}_{\delta,1}, \ldots, \boldsymbol{f}_{\delta,l_\delta}\}}$在 $\delta \in \{-1, 1\}^n$上的并列为 $\boldsymbol{g}_1$、……、 $\boldsymbol{g}_m$。根据 [17,引理 21], , 这是 $\mathcal{M}$的超 Gr¨obner 基。 □

由证明可轻易看出以下结论：如果给定的 $\mathcal{M}$ 生成元仅包含整数系数多项式，那么引理 6.6 计算出的超 Gr¨obner 基也仅包含整数系数多项式。

设 $0 \le d \le n-1$ 为一个整数。从现在起，我们记

$$\mathbb{A}_d \coloneqq \mathbb{R}[X_1^{\pm}, \dots, X_d^{\pm}], \quad \mathbb{A}_d^+ \coloneqq \mathbb{R}_{\ge 0}[X_1^{\pm}, \dots, X_d^{\pm}]^*.$$

特别是， $\mathbb{A}_0 = \mathbb{R}$， $\mathbb{A}_0^+ = \mathbb{R}_{>0}$。

正如本小节开头所述，我们现在考虑具有特殊形式的向量 $v \in (\mathbb{R}^n)^*$，即 $(0, \dots, 0, v_{d+1}, \dots, v_n)$，其中 $v_{d+1}, \dots, v_n$ 是 $\mathbb{Q}$-线性无关的。下面的引理可以看作是 [17,引理 6.2] 的推广。

引理 *6.7*（[17, 引理 *6.2*] 的推广）。设 $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m$ 是 $\mathcal{M}$ 的一个超 *Gr¨obner* 基。设 $v = (0, \dots, 0, v_{d+1}, \dots, v_n) \in (\mathbb{R}^n)^*$，使得 $0 \le d \le n-1$ 和 $v_{d+1}, \dots, v_n$ 是 $\mathbb{Q}$-线性无关的。设 $\boldsymbol{\alpha} \in \mathbb{R}^K$。则存在 $b_i \in \{0\}^d \times \mathbb{Z}^{n-d}$ 和 $c_j \in \{0\}^d \times \mathbb{Z}^{n-d}$，使得 $X^{b_i} X^{c_j}$ 属于 v 中，$\boldsymbol{\alpha}(\boldsymbol{g}_j)_i \in \mathbb{A}_d$ 对于 $i = 1, \dots, K$ 以及 $j = 1, \dots, m$。

证明。设 $j \in \{1, \dots, m\}$， $i \in \{1, \dots, K\}$，使得在 v, $\boldsymbol{\alpha}(\boldsymbol{g}_j)_i \ne 0$ 中。由于 $v_{d+1}, \dots\dots, v_n$ 是 $\mathbb{Q}$-线性无关的，存在一个开邻域 $U \subseteq \mathbb{R}^{n-d}$，其包含 $(v_{d+1}, \dots\dots, v_n)$，使得每个 $v' \in \{0\}^d \times U$ 都满足在 v' (在 v, $\boldsymbol{\alpha}(\boldsymbol{g}_j)_i$) $=$ 在 v(在 v, $\boldsymbol{\alpha}(\boldsymbol{g}_j)_i$)。这表明，对于某个 $z_{ij} \in \{0\}^d \times \mathbb{Z}^{n-d}$， $X^{z_{ij}}$ 在 v, $\boldsymbol{\alpha}(\boldsymbol{g}_j)_i \in \mathbb{A}_d$。

令 $F \coloneqq \{(i, j) \mid \text{在 } v, \boldsymbol{\alpha}(\boldsymbol{g}_j)_i \ne 0\}$ 中，这就为所有 $(i, j) \in F$ 定义了 z_{ij}。注意，对于 $(i, j) \in F$，我们有

$$\max_{1 \le i' \le K} \{\deg_v(\boldsymbol{g}_{j,i'}) + \boldsymbol{\alpha}_{i'}\} = -v \cdot z_{ij} + \alpha_i.$$

考虑一个序列

$$(i_0, j_0), (i_1, j_0), (i_1, j_1), \dots, (i_l, j_{l-1}), (i_l, j_l), (i_0, j_l) \tag{18}$$

在 F 中，并记 $i_{l+1} = i_0$，我们得到

$$0 = \sum_{s=0}^{l} \left(\max_{1 \le i' \le K} \{\deg_v(\boldsymbol{g}_{j,i'}) + \boldsymbol{\alpha}_{i'}\} - \max_{1 \le i' \le K} \{\deg_v(\boldsymbol{g}_{j,i'}) + \boldsymbol{\alpha}_{i'}\} \right) = \sum_{s=0}^{l} \left(v \cdot z_{i_{s+1} j_s} - v \cdot z_{i_s j_s} \right).$$

由于 $v = (0, \dots, 0, v_{d+1}, \dots, v_n)$，其中 $v_{d+1}, \dots, v_n$ 是 $\mathbb{Q}$-线性无关的，且 $z_{ij} \in \{0\}^d \times \mathbb{Z}^{n-d}$，上述方程给出

$$\sum_{s=0}^{l} \left(z_{i_{s+1} j_s} - z_{i_s j_s} \right) = 0 \tag{19}$$

对于 F 中的每个允许的序列（18）。

现在我们将 z_{ij} 和方程（19）扩展到所有的对 $(i, j) \in \{1, \dots, K\} \times \{1, \dots, m\}$。假设 z_{ij} 已在集合 $E \supseteq F$ 上定义，并且（19）在 E 上成立。取 $(i, j) \notin E$。如果存在一个序列

$$(i_1, j), (i_1, j_1), \dots, (i_l, j_{l-1}), (i_l, j_l), (i, j_l) \in E,$$

我们令 $i_{l+1} = i$ 并定义

$$z_{ij} \coloneqq z_{i_1 j} - \sum_{s=1}^{l} \left(z_{i_s j_s} - z_{i_{s+1} j_s} \right).$$

容易验证，方程（19）随后对 $E \cup \{(i, j)\}$ 中的每个允许的序列（18）都成立。如果不存在序列

$$(i_1, j_0), (i_1, j_1), \dots, (i_l, j_{l-1}), (i_l, j_l), (i_0, j_l)$$

位于 E 中，我们可以将 z_{ij} 取为 $\{0\}^d \times \mathbb{Z}^{n-d}$ 的任意元素，并使方程（19）对 $E \cup \{(i,\ j)\}$ 中的所有序列（18）成立。

由此将 z_{ij} 扩展到所有的对 $(i,\ j) \in \{1,\dots,K\} \times \{1,\dots,m\}$，我们定义

$$b_i \coloneqq z_{i1},$$

and

$$c_j \coloneqq z_{ij} - z_{i1},$$

根据方程（19），该式与 i 无关。事实上，对允许的序列 $(i,\ j)$，$(i',\ j)$，$(i',\ 1)$，$(i,\ 1)$ 使用方程（19），可得 $z_{ij} - z_{i1} = z_{i'j} - z_{i'1}$。因此，$z_{ij} = b_i + c_j$，引理得证。

□

设 $v \in (\mathbb{R}^n)^*$ 满足 $v = (0,\ \dots,\ 0,\ v_{d+1},\ \dots,\ v_n)$，其中 $v_{d+1},\ \dots,\ v_n$ 是 $\mathbb{Q}$-线性无关的。令 $\boldsymbol{\alpha} \in \mathbb{R}^K$。对于每个 $j = 1,\ \dots,\ m$，在 $\operatorname{in}^d_{v,\ \boldsymbol{\alpha}}(\boldsymbol{g}_j)$ 中定义 $=$（在 $\operatorname{in}^d_{v,\ \boldsymbol{\alpha}}(\boldsymbol{g}_j)_1,\ \dots,\ \operatorname{in}^d_{v,\ \boldsymbol{\alpha}}(\boldsymbol{g}_j)_K$ 中），其中

$$\operatorname{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i \coloneqq \overline{X}^{b_i}\overline{X}^{c_j} \operatorname{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i \in \mathbb{A}_d, \quad i = 1,\dots,K.$$

这里，b_i 和 c_j 的定义与引理 6.7 中相同。注意，向量 $b_i, c_j \in \{0\}^d \times \mathbb{Z}^{n-d}$ 不一定是唯一确定的。然而，当 $d, v, \boldsymbol{\alpha}$ 固定时，$\operatorname{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i$ 中的多项式由 $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m$ 唯一确定。事实上，根据引理 6.7，$\operatorname{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i$ 中的每一个都可以唯一地写成 $X^s \cdot p$，其中 $X^s \in \mathbb{R}[X^{\pm}_{d+1}, \dots, X^{\pm}_n]$ 和 $p \in \mathbb{R}[X^{\pm}_1, \dots, X^{\pm}_d]$。因此，$\operatorname{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i$ 在分解中作为多项式 p 被唯一确定。

注意，如果 $\operatorname{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i \neq 0$，则 $\deg_v(g_{j,i}) = -v \cdot (b_i + c_j)$；否则，$\deg_v(g_{j,i}) < -v \cdot (b_i + c_j)$。在这两种情况下，

$$\deg_v(g_{j,i}) \leq -v \cdot (b_i + c_j), \tag{20}$$

当且仅当 $\operatorname{in}^d_{v,\ \boldsymbol{\alpha}}(\boldsymbol{g}_j)_i \neq 0$ 时等式成立。

引理 6.8。如果存在 $j \in \{1,\dots,m\}$ 使得 $\operatorname{in}^d_{v,\ \boldsymbol{\alpha}}(\boldsymbol{g}_j)_{\ i} \neq 0$，$\operatorname{in}^d_{v,\ \boldsymbol{\alpha}}(\boldsymbol{g}_j)_{\ i'} \neq 0$，那么 $\alpha_i - v \cdot b_i = \alpha_{i'} - v \cdot b_{i'}$。

证明。如果 $\operatorname{in}^d_{v,\ \boldsymbol{\alpha}}(\boldsymbol{g}_j)_i \neq 0$，$\operatorname{in}^d_{v,\ \boldsymbol{\alpha}}(\boldsymbol{g}_j)_{i'} \neq 0$，那么 $\operatorname{in}_{v,\ \boldsymbol{\alpha}}(\boldsymbol{g}_j)_i \neq 0$，$\operatorname{in}_{v,\ \boldsymbol{\alpha}}(\boldsymbol{g}_j)_{i'} \neq 0$，因此 $\deg_v(\operatorname{in}_{v,\ \boldsymbol{\alpha}}(\boldsymbol{g}_j)_i) + \alpha_i = \deg_v(\operatorname{in}_{v,\ \boldsymbol{\alpha}}(\boldsymbol{g}_j)_{i'}) + \alpha_{i'}$。

但是 $\deg_v(\operatorname{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i) = \deg_v(\overline{X}^{-b_i} \cdot \operatorname{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i) = -v \cdot (b_i + c_j)$。对 i' 推导相同的方程可得 $-v \cdot (b_i + c_j) + \alpha_i = -v \cdot (b_{i'} + c_j) + \alpha_{i'}$。这就得到 $\alpha_i - v \cdot b_i = \alpha_{i'} - v \cdot b_{i'}$。

□

定义 $\operatorname{in}^d_{v,\boldsymbol{\alpha}}(\mathcal{M})$ 为由 $\operatorname{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_1) \dots, \operatorname{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_m) \in \mathbb{A}_d^K$ 生成的 $\mathbb{A}_d$-模：

$$\operatorname{in}^d_{v,\boldsymbol{\alpha}}(\mathcal{M}) \coloneqq \sum_{j=1}^m \mathbb{A}_d \cdot \operatorname{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j) = \left\{ \sum_{j=1}^m p_j \cdot \operatorname{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j) \;\middle|\; p_1, \dots p_m \in \mathbb{A}_d \right\}.$$

证明 Einsiedler 等人的原始结果的一个关键部分 [17]是 [17, 引理 3。2], 它表明，在 $\operatorname{in}^d_{v,\boldsymbol{\alpha}}(\mathcal{M}) \cap \left(\mathbb{A}_d^+\right)^K \neq \emptyset$ 蕴含 $\mathcal{M} \cap (\mathbb{A}^+)^K \neq \emptyset$。然而，若额外施加性质（8），这一结论便不再成立：满足性质（8）的 $\mathcal{M} \cap (\mathbb{A}^+)^K$ 中的一个元素，未必能由满足类似性质的 $\operatorname{in}^d_{v,\boldsymbol{\alpha}}(\mathcal{M}) \cap \left(\mathbb{A}_d^+\right)^K$ 中的一个元素得到。事实上，若将 [17,引理 3。2] 直接应用于我们的情形，主要问题会出现在证明的最后一段：其中将多项式的不同“层级”组合起来，以构造一个正元素。加入次数约束后，这种方法便不再奏效。下面的引理表明，若施加额外约束 $\boldsymbol{\alpha} \in \left(\sum_{k=d+1}^n \mathbb{Z} v_k\right)^K$，则 [17, 引理 3。2]仍可在一定程度上与性质（8）相容。

引理 6.9。 设 $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m$ 是 $\mathcal{M}$的一个超 *Gröbner* 基。设 $v = (0, \ldots, 0, v_{d+1}, \ldots, v_n)$ 满足 $0 \le d \le n-1$，且 $v_{d+1}, \ldots, v_n$ 线性无关（系数属于 $\mathbb{Q}$）。设 $\boldsymbol{\alpha} \in \left(\sum_{k=d+1}^{n} \mathbb{Z} v_k\right)^K$。记 $I' := \{i \in I \mid \alpha_i = \text{最小值}_{i' \in I}\, \alpha_{i'}\}$, $J' := O_v \cup J$。将到前 d 个坐标的投影记为 $\pi_d \colon \mathbb{Z}^n \to \mathbb{Z}^d$。对于每个 $u \in (\mathbb{R}^d)^*$，定义 $O'_u := \{i \in \{1, \ldots, K\} \mid \pi_d(a_i) \not\perp u\}$。以下两个条件等价:

(i)（LocInfShift 中的条件）：存在 $\boldsymbol{f} \in \mathcal{M}$ 使得 在$_{v,\,\boldsymbol{\alpha}}$（$\boldsymbol{f}$）$\in$ $(\mathbb{A}^+)^K$ 且

$$\left(O_w \cup J'\right) \cap M_w(I', \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})) \neq \emptyset \quad \textit{for every } w \in (\mathbb{R}^n)^*. \tag{21}$$

(ii) 我们有 $J' \cap I' \neq \emptyset$，并且存在 $\boldsymbol{f}^d \in$在$^d_{v,\,\boldsymbol{\alpha}}(\mathcal{M}) \cap \left(\mathbb{A}^+_d\right)^K$，使得

$$\left(O'_u \cup J'\right) \cap M_u(I', \boldsymbol{f}^d) \neq \emptyset \quad \textit{for every } u \in (\mathbb{R}^d)^*. \tag{22}$$

当 $d = 0$ 时，性质 （22） 被认为是平凡成立的。

证明。 **(i)** $\Longrightarrow$ **(ii)**。假设（i）成立。令 $\boldsymbol{f} \in \mathcal{M} \cap$ $(\mathbb{A}^+)^K$ 满足（21）。现在证明（ii）。

性质 $J' \cap I' \neq \emptyset$由在$_{v,\,\boldsymbol{\alpha}}$（$\boldsymbol{f}$）$\in$ $(\mathbb{A}^+)^K$以及（21）推出，取 $w := v$ 即可。事实上，我们有 $O_v \cup J' = O_v \cup J$并且

$$\begin{aligned} M_v(I', \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})) &= \left\{ i \in I' \;\middle|\; \deg_v(\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})_i) = \max_{i' \in I'} \deg_v(\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})_{i'}) \right\} \\ &= \left\{ i \in I' \;\middle|\; -\alpha_i = \max_{i' \in I'} (-\alpha_{i'}) \right\} = I', \end{aligned}$$

其中第二个等式来自于$_{v,\,\boldsymbol{\alpha}}(\boldsymbol{f}) \in (\mathbb{A}^+)^K$。因此，根据性质（21），取 $w := v$ 可得 $J' \cap I' \neq \emptyset$。

由于 $\boldsymbol{g}_1, \ldots\ldots, \boldsymbol{g}_m$ 是一个超 Gröbner 基，我们可以写成

$$\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f}) = \sum_{j=1}^{m} h_j \cdot \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j). \tag{23}$$

Let

$$S := \left\{ 1 \le j \le m \;\middle|\; \deg_v(h_j) + \max_{1 \le i \le K} (\deg_v(\boldsymbol{g}_{j,i}) + \alpha_i) \text{ is maximal} \right\}.$$

不妨设 $\sum_{j \in S} \mathrm{in}_v(h_j) \cdot \mathrm{in}_{v,\,\boldsymbol{\alpha}}(\boldsymbol{g}_j) \neq 0$；否则，我们可以通过在 $_v(h_j)$ 中令 $h_j -$，将每个 h_j 替换为 $j \in S$，同时（23）仍然成立。于是我们有

$$\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f}) = \mathrm{in}_{v,\boldsymbol{\alpha}} \left(\sum_{j=1}^{m} h_j \cdot \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j) \right) = \sum_{j \in S} \mathrm{in}_v(h_j) \cdot \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j).$$

事实上，根据$_{v,\,\boldsymbol{\alpha}}$中平移初项的定义，上述右侧的元素是唯一能够对中间和式的平移初项作出贡献的元素。因此，不妨设对于所有 $j = 1, \ldots\ldots, m$, $S = \{1, \ldots, m\}$ 和 $h_j = \mathrm{in}_{\,v}(h_j)$。记 $D := \deg_v(h_j) + \max_{1 \le i' \le K}(\deg_v(\boldsymbol{g}_{j,\,i'}) + \alpha_{i'})$；这与 $j \in \{1, \ldots, m\}$ 的选择无关。

由于 $v = (0, \ldots\ldots, 0, v_{d+1}, \ldots\ldots, v_n)$ 使得 $v_{d+1}, \ldots\ldots, v_n$ 是 $\mathbb{Q}$-线性无关的，并且 $h_j =$属于$_v(h_j)$，因此我们可以写成 $h_j = X^{z_j} p_j$，其中 $p_j \in \mathbb{A}_d$ 且 $z_j \in \{0\}^d \times \mathbb{Z}^{n-d}$。注意，对于满足 $\mathrm{in}^d_{v,\,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i \neq 0$ 的所有 $(i,\ j)$，都有 $D = \deg_v(h_j) + \max_{1 \le i' \le K}(\deg_v(\boldsymbol{g}_{j,\,i'}) + \alpha_{i'}) = v \cdot z_j - v \cdot (b_i + c_j) + \alpha_i$。由于

$\boldsymbol{\alpha} \in \left(\sum_{k=d+1}^{n} \mathbb{Z} v_k\right)^K$，每个 α_i，$i = 1, \ldots\ldots, K$，都可以写成 $\alpha_i = v \cdot z_i'$，其中某个 $z_i' \in \{0\}^d \times \mathbb{Z}^{n-d}$。因此，对于满足 $\mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i \neq 0$ 的所有 (i, j)，都有 $D = v \cdot (z_j - b_i - c_j + z_i')$。

由于 $\mathbb{Q}$ 中 v 的各项线性无关，因此存在唯一的 $z \in \{0\}^d \times \mathbb{Z}^{n-d}$，使得对所有满足 ${}^d_v$ 中 $z = z_j - b_i - c_j + z_i'$ 的 (i, j)，都有 $\boldsymbol{\alpha}(\boldsymbol{g}_j)_i \neq 0$。于是

$$\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})_i = \sum_{j=1}^{m} \overline{X}^{z_j} p_j \, \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i = \sum_{j=1}^{m} p_j \overline{X}^{z_j - b_i - c_j} \, \mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i = \overline{X}^{z - z_i'} \sum_{j=1}^{m} p_j \, \mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i$$

Let

$$\boldsymbol{f}^d \coloneqq \sum_{j=1}^{m} p_j \, \mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j) \in \mathrm{in}^d_{v,\boldsymbol{\alpha}}(\mathcal{M}).$$

于是，对 $i = 1, \ldots\ldots, K$，

$$f_i^d = \overline{X}^{z_i' - z} \, \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})_i \in \mathbb{A}^+ \cap \mathbb{A}_d = \mathbb{A}_d^+.$$

因此 $\boldsymbol{f}^d \in \left(\mathbb{A}_d^+\right)^K$。接下来只需证明 $\boldsymbol{f}^d$ 满足性质（22）。若 $d = 0$，则性质（22）显然成立。设 $d \geq 1$。对于每个 $u \in (\mathbb{R}^d)^*$，令 $w \coloneqq (u, 0^{n-d})$ 为式（21）中的项。于是

$$\left(O_w \cup J'\right) \cap M_w(I', \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})) \neq \emptyset.$$

此外，对于每个 $i \in \{1, \ldots, K\}$，由于 $(z - z_i') \in \{0\}^d \times \mathbb{Z}^{n-d}$ 且 $w \in \mathbb{Z}^d \times \{0\}^{n-d}$，我们有 $\mathrm{deg}_w(\text{在 } v \text{ 中的 }, \boldsymbol{\alpha}(\boldsymbol{f})_i)^{-} = \mathrm{deg}_w(X^{z - z_i'} \boldsymbol{f}_i^d) = \mathrm{deg}_u(\boldsymbol{f}_i^d)$。因此，

$$\begin{aligned} M_w(I', \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})) &= \left\{ i \in I' \;\middle|\; \deg_w(\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})_i) = \max_{i' \in I'} \deg_w(\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})_{i'}) \right\} \\ &= \left\{ i \in I' \;\middle|\; \deg_u(f_i^d) = \max_{i' \in I'} \deg_u(f_{i'}^d) \right\} = M_u(I', \boldsymbol{f}^d). \end{aligned}$$

此外，由于 v 的最后 $n - d$ 个 $\mathbb{Q}$线性无关，当且仅当 $a_i \perp v \, a_i \in \sum_{k=1}^{d} \mathbb{Z} e_k$时，我们有

$$\begin{aligned} O_u' \cup J' &= O_u' \cup O_v \cup J = \{i \mid \neg(\pi_d(a_i) \perp u \wedge a_i \perp v)\} \cup J \\ &= \left\{ i \;\middle|\; \neg\left(\pi_d(a_i) \perp u \wedge a_i \in \sum_{i=1}^{d} \mathbb{Z} e_i\right) \right\} \cup J = \left\{ i \;\middle|\; \neg\left(a_i \perp w \wedge a_i \in \sum_{i=1}^{d} \mathbb{Z} e_i\right) \right\} \cup J \\ &= \{i \mid \neg(a_i \perp w \wedge a_i \perp v)\} \cup J = O_w \cup O_v \cup J = O_w \cup J' \end{aligned} \tag{24}$$

因此，$(O_u' \cup J') \cap M_u(I', \boldsymbol{f}^d) = (O_w \cup J') \cap M_w(I', \text{ 在 } v, \boldsymbol{\alpha}(\boldsymbol{f}) \text{中})$，根据（21），该集合非空。由此我们证明了 $\boldsymbol{f}^d$ 满足性质（22）。

(ii) $\Longrightarrow$ (i). 假设(ii)成立。将 $\boldsymbol{f}^d = \sum_{j=1}^{m} p_j$ 写作 ${}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)$中的元素，其中 $p_j \in \mathbb{A}_d$ 对 $j = 1, \ldots, m$成立。

对于每个 $i \in \{1, \ldots, K\}$，将 $\alpha_i = v \cdot z_i$ 写作某个 $z_i \in \{0\}^d \times \mathbb{Z}^{n-d}$。由于 v的各项 $\mathbb{Q}$线性无关，这样的 z_i 是唯一的。

对于每个 $j \in \{1, \ldots, m\}$，取任意满足 $\mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_{i_j} \neq 0$ 的 $i_j \in \{1, \ldots, K\}$，注意到向量 $c_j + b_{i_j} - z_{i_j}$ 不依赖于 i_j 的选择。事实上，取另一个满足 $\mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_{i_j'} \neq 0$ 的 $i_j' \in \{1, \ldots, K\}$，则由引理 6.8 可得 $\alpha_{i_j} - v \cdot b_{i_j} = \alpha_{i_j'} - v \cdot b_{i_j'}$。由于 $\alpha_{i_j} = v \cdot z_{i_j}$，$\alpha_{i_j'} = v \cdot z_{i_j'}$，我们有 $v \cdot (z_{i_j} - b_{i_j}) = v \cdot (z_{i_j'} - b_{i_j'})$。由 v 的各项具有 $\mathbb{Q}$-线性无关性可得$z_{i_j} - b_{i_j} = z_{i_j'} - b_{i_j'}$。因此，向量 $c_j + b_{i_j} - z_{i_j}$ 不依赖于 i_j 的选择。

对于所有 $i \in \{1,\dots,K\}$，我们有

$$\deg_v(g_{j,i}) + \alpha_i \le \deg_v(g_{j,i_j}) + \alpha_{i_j}, \tag{25}$$

当且仅当 $\mathrm{in}^d_{v,\ \boldsymbol{\alpha}(\boldsymbol{g}_j)_i} \neq 0$ 时等式成立。

Take

$$\boldsymbol{f} \coloneqq \sum_{j=1}^{m} \overline{X}^{c_j+b_{i_j}-z_{i_j}} p_j \cdot \boldsymbol{g}_j \in \mathcal{M}.$$

对于每个 $i \in \{1,\dots,K\}$ 和 $j \in \{1,\dots,m\}$，我们有

$$\begin{aligned}\deg_v(\overline{X}^{c_j+b_{i_j}-z_{i_j}} p_j g_{ji}) + \alpha_i &= v\cdot(c_j+b_{i_j}) - v\cdot z_{i_j} + \deg_v(g_{j,i}) + \alpha_i \\ &\le -\deg_v(g_{j,i_j}) - \alpha_{i_j} + \deg_v(g_{j,i}) + \alpha_i \le 0 \end{aligned}\tag{26}$$

第一个不等式来自（20）和 $\alpha_{i_j} = v\cdot z_{i_j}$，而第二个不等式来自（25）。此外，根据（20）和（25）中的等式条件，（26）中的等式当且仅当 $\mathrm{in}^d_{v,\ \boldsymbol{\alpha}(\boldsymbol{g}_j)_i} \neq 0$ 时成立。

因此，对于每个 $i \in \{1,\dots,K\}$，我们有

$$\begin{aligned}\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})_i &= \sum_{j:\mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i\neq 0} \overline{X}^{c_j+b_{i_j}-z_{i_j}}\,\mathrm{in}_v(p_j g_{j,i}) = \sum_{j:\mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i\neq 0} \overline{X}^{c_j+b_i-z_i} p_j\,\mathrm{in}_v(g_{j,i}) \\ &= \sum_{j:\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i\neq 0} \overline{X}^{c_j+b_i-z_i} p_j\,\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i = \sum_{j=1}^{m} \overline{X}^{c_j+b_i-z_i} p_j\,\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i = \overline{X}^{-z_i}\sum_{j=1}^{m} p_j\,\mathrm{in}^d_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j)_i \\ &= \overline{X}^{-z_i} f_i^d \in \mathbb{A}^+. \end{aligned}\tag{27}$$

在第一个等式中，初始多项式不会相互抵消，因为它们的和为 $X^{-z_i} f_i^d \in \mathbb{A}_d^+$。因此 $\mathrm{in}_{v,\ \boldsymbol{\alpha}(\boldsymbol{f})} \in (\mathbb{A}^+)^K$。

现在我们证明性质（21）。回顾 $I' \coloneqq \{i \in I \mid \alpha_i = \min_{i'\in I}\alpha_{i'}\}$。对于 $i,\ i' \in I'$，我们有 $v\cdot z_i = \alpha_i = \alpha_{i'} = v\cdot z_{i'}$。由 $\mathbb{Q}$-线性无关性可知，v 的各项满足

$$z_i = z_{i'} \text{ for all } i, i' \in I'. \tag{28}$$

任取一个 $w \in (\mathbb{R}^n)^*$。

如果 $w \in \sum_{k=d+1}^n \mathbb{R}e_k$，那么

$$\begin{aligned} M_w(I', \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})) &= \left\{ i\in I' \;\middle|\; \deg_w(\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})_i) = \max_{i'\in I'} \deg_w(\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})_{i'}) \right\} \\ &= \left\{ i\in I' \;\middle|\; -w\cdot z_i = \max_{i'\in I'}\{-w\cdot z_{i'}\} \right\} \qquad \text{(by (27))} \\ &= I'. \qquad \text{(by (28))} \end{aligned}$$

So

$$\big(O_w \cup J'\big) \cap M_w(I', \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})) = \big(O_w \cup J'\big) \cap I' \supseteq J' \cap I' \neq \emptyset.$$

如果 $w \notin \sum_{k=d+1}^n \mathbb{R}e_k$ 且 $d \ge 1$，则写成 $w = w' + u$，其中 $w' \in \sum_{k=d+1}^n \mathbb{R}e_k$ 且 $u \in \sum_{k=1}^d \mathbb{R}e_k$。于是

$$M_w(I', \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f}))$$

$$
\begin{aligned}
&= \left\{ i \in I' \;\middle|\; \deg_w(\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})_i) = \max_{i' \in I'} \deg_w(\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})_{i'}) \right\} \\
&= \left\{ i \in I' \;\middle|\; -w' \cdot z_i + \deg_u(f_i^d) = \max_{i' \in I'} \{-w' \cdot z_{i'} + \deg_u(f_{i'}^d)\} \right\} \qquad \text{(by (27))} \\
&= \left\{ i \in I' \;\middle|\; \deg_u(f_i^d) = \max_{i' \in I'} \{\deg_u(f_{i'}^d)\} \right\} \qquad \text{(by (28))} \\
&= M_u(I', \boldsymbol{f}^d).
\end{aligned}
$$

由于 v 的最后 $n-d$ 个元素是 $\mathbb{Q}$-线性无关的，因此当且仅当 $a_i \in \sum_{k=1}^{d} \mathbb{Z} e_k$ 时有 $a_i \notin O_v$。所以，如（24）所示，$O'_u \cup J' = O_w \cup J'$。因此，

$$
\big(O_w \cup J'\big) \cap M_w(I', \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})) = \big(O'_u \cup J\big) \cap M_u(I', \boldsymbol{f}^d) \neq \emptyset.
$$

如果 $w \notin \sum_{k=d+1}^{n} \mathbb{R} e_k$ 和 $d = 0$。对于 $i = 1$、……、K，我们有 $f_i^d \in \mathbb{R}$，因此

$$
\begin{aligned}
M_w(I', \mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})) &= \left\{ i \in I' \;\middle|\; \deg_w(\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})_i) = \max_{i' \in I'} \deg_w(\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f})_{i'}) \right\} \\
&= \left\{ i \in I' \;\middle|\; -w' \cdot z_i = \max_{i' \in I'} \{-w' \cdot z_{i'}\} \right\} \qquad \text{(by (27))} \\
&= I' \qquad \text{(by (28))}
\end{aligned}
$$

因此 $(O_w \cup J') \cap M_w(I', \text{在}_{v,\,\boldsymbol{\alpha}}(\boldsymbol{f})) = (O_w \cup J') \cap I' \supset J' \cap I' \neq \emptyset$。

这证明了性质（21）。 □

6.4 维数约化：一般情形。本小节延续上一小节的工作。我们的目标是将条件（LocInfShift）转化为条件（LocInfD）（见命题 6.11）。在上一小节中，我们考虑了这样一种特殊情形：条件（LocInfShift）中的向量 $v \in (\mathbb{R}^n)^*$ 具有（0、……、0，v_{d+1}、……、v_n）的形式。在本小节中，我们考虑一般情形。处理 $v \in (\mathbb{R}^n)^*$ 的一般情形时，关键思想是进行如下坐标变换。

给定矩阵 $A = (a_{ij})_{1 \le i,\, j \le n} \in \mathrm{GL}(n, \mathbb{Z})$，定义新变量 $X'_1, \ldots, X'_n$，其中 $X'_i := X_1^{a_{i1}} X_2^{a_{i2}} \cdots X_n^{a_{in}}$。于是

$$
\mathbb{R}[X_1, \ldots, X_n] = \mathbb{R}[X'_1, \ldots, X'_n].
$$

换言之，我们可以定义环自同态

$$
\varphi_A \colon \mathbb{A} \to \mathbb{A}, \quad X_i \mapsto X_1^{a_{i1}} X_2^{a_{i1}} \cdots X_n^{a_{in}},
$$

使得 $\varphi_A(X^b) = X^{bA}$。自同态 φ_A 逐项延拓到 $\mathbb{A}^K \to \mathbb{A}^K$。

对于每个 $A \in \mathrm{GL}(n, \mathbb{Z})$，记 $A^{-\top}$ 为其转置矩阵的逆。则对于所有 $v \in (\mathbb{R}^n)^*, b \in \mathbb{Z}^n$，有 $(vA^{-\top}) \cdot (bA) = v \cdot b$。因此，对于任意 $f \in \mathbb{A}$，我们有 $\mathrm{in}_{vA^{-\top}}(\varphi_A(f)) = \varphi_A(\mathrm{in}_v(f))$，而对于任意 $\boldsymbol{f} \in \mathbb{A}^K$，我们有 $M_v(I, \boldsymbol{f}) = M_{vA^{-\top}}(I, \varphi_A(\boldsymbol{f}))$。此外，如果我们将向量 a_1、…、$a_K \in \mathbb{Z}^n$ 替换为向量 $a_1 A$、…、$a_K A \in \mathbb{Z}^n$，那么集合 O_v 就变为 $O_{vA^{-\top}}$。容易验证，如果 $\boldsymbol{g}_1$、…、$\boldsymbol{g}_m$ 是 $\mathcal{M}$ 的超 Gr¨obner 基，那么 $\varphi_A(\boldsymbol{g}_1)$ …、$\varphi_A(\boldsymbol{g}_m)$ 仍然是 $\varphi_A(\mathcal{M}) := \{\varphi_A(\boldsymbol{f}) \mid \boldsymbol{f} \in \mathcal{M}\}$ 的超 Gr¨obner 基。

设 $v \in (\mathbb{R}^n)^*$，并令 $A \in \mathrm{GL}(n, \mathbb{Z})$ 满足 $vA^{-\top} = (0, \ldots, 0, v_{d+1}, \ldots, v_n)$，其中 $v_{d+1}, \ldots, v_n$ 是 $\mathbb{Q}$-线性无关的。于是，如同上一小节中所做的那样，我们将 $\overset{d}{\mathrm{in}}_{vA^{-\top},\boldsymbol{\alpha}}(\varphi_A(\mathcal{M}))$ 中的模定义为由 $\overset{d}{\mathrm{in}}_{vA^{-\top},\boldsymbol{\alpha}}(\varphi_A(\boldsymbol{g}_1)), \ldots, \overset{d}{\mathrm{in}}_{vA^{-\top},\boldsymbol{\alpha}}(\varphi_A(\boldsymbol{g}_m))$ 生成的模。

上述观察说明了以下事实。固定 $v \in (\mathbb{R}^n)^*$，使其属于定理 3.8 的 (LocInfShift)。给定任意坐标变换 $A \in \mathrm{GL}(n,\mathbb{Z})$，我们可以同时将 $A^{-\top}$（右）乘以 v，并将 A（右）乘以所有 $a_1,\dots,a_K$，同时将 φ_A 应用于 $\mathcal{M}$ 的超 Gr¨obner 基 $\boldsymbol{g}_1,\dots,\boldsymbol{g}_m$。那么，原有的性质 (LocInfShift)(a)(b) 对 $\boldsymbol{f}$ 成立，当且仅当坐标变换后它们对 $\varphi_A(\boldsymbol{f})$ 成立。我们将利用这一观察，把 v 的一般情形归约到上一小节所考察的特殊情形。

事实 6.10。对于每个 $v \in (\mathbb{R}^n)^*$，存在 $A \in \mathrm{GL}(n,\mathbb{Z})$，使得 $vA^{-\top} = (0,\dots,0,v_{d+1},\dots,v_n)$，其中 $v_{d+1},\dots,v_n$ 是 $\mathbb{Q}$-线性无关的。

证明。只需证明以下内容即可。如果 $v \in (\mathbb{R}^n)^*$ 的形式为 $(0,\dots,0,v_d,\dots,v_n)$，$1 \le d \le n$，其中 $v_d,\dots,v_n$ 是 $\mathbb{Q}$-线性相关的，那么我们可以找到一个矩阵 $A_d \in \mathrm{GL}(n,\mathbb{Z})$，使得 $vA_d = (0,\dots,0,v_{d+1},\dots,v_n)$。事实上，如果这成立，那么我们可以找到一系列矩阵 $A_r,\dots,A_{r+s}$，使得 $vA_rA_{r+1}\cdots A_{r+s}$ 的形式为 $(0,\dots,0,v_{r+s+1},\dots,v_n)$，其中 $v_{r+s+1},\dots,v_n$ 是 $\mathbb{Q}$-线性无关的。于是令 $A := (A_rA_{r+1}\cdots A_{r+s})^{-\top}$。

现在假设 $v = (0,\dots,0,v_d,\dots,v_n)$，$1 \le d \le n$ 其中 $v_d,\dots,v_n$ 是 $\mathbb{Q}$-线性相关的。设 $z_d,\dots,z_n \in \mathbb{Q}$ 不全为零，且满足 $z_dv_d + \cdots + z_nv_n = 0$。将它们乘以一个公分母后，可假设 $z_d,\dots,z_n \in \mathbb{Z}$。利用高斯主元法，可以找到一个 $\widetilde{\ }$ $\widetilde{\ }$ 矩阵 $A_d \in \mathrm{GL}(n-d+1,\mathbb{Z})$，使得 $(z_d,\dots,z_n)A_d = (z,0,\dots,0)$，其中某个 $z \in \mathbb{Z}^*$。于是我们有

$$0 = (z_d,\dots,z_n)\cdot(v_d,\dots,v_n) = (z_d,\dots,z_n)\widetilde{A_d}\cdot(v_d,\dots,v_n)\widetilde{A_d}^{-\top} = (z,0,\dots,0)\cdot(v_d,\dots,v_n)\widetilde{A_d}^{-\top}.$$

因此 $(v_d,\dots,v_n)\widetilde{A_d}^{-\top}$ 具有 $(0,v'_{d+1},\dots,v'_n)$ 的形式。接着令 $A_d := diag(I_{d-1},\widetilde{A_d}^{-\top})$。也就是说，$A_d$ 是一个分块对角矩阵，其分块 I_{d-1} 是 $(d-1)$ 维单位矩阵，分块 $\widetilde{A_d}^{-\top}$ 是 $(n-d+1)$ 维矩阵。于是 $vA_d = (0,\dots,0,v'_{d+1},\dots,v'_n)$。

□

命题 6.11. 命题 *6.4* 的(LocInfShift) 条件等价于以下内容：

2. **(LocInfD):** 对于每个 $v \in (\mathbb{R}^n)^*, A \in \mathrm{GL}(n,\mathbb{Z})$，使得 $vA^{-\top} = (0,\dots,0,v_{d+1},\dots,v_n)$，$0 \le d \le n-1$，且 $v_{d+1},\dots,v_n$ 线性无关，存在 $\boldsymbol{\alpha} \in \left(\sum_{k=d+1}^n \mathbb{Z}v_k\right)^K$ 和 $\boldsymbol{f}^d \in$ 属于$^d_{vA^{-\top}}$，$\boldsymbol{\alpha}$ $(\varphi_A(\mathcal{M}))$ 满足以下性质：

(a) $\boldsymbol{f}^d \in \left(\mathbb{A}^+_d\right)^K$. *(b1)* 记 $I' := \{i \in I \mid \alpha_i = $最小值$_{i' \in I}\,\alpha_{i'}\}$, $J' := (O_v \cup J)$，则有

$$J' \cap I' \neq \emptyset. \tag{29}$$

(b2) 记 $\pi_d := \mathbb{Z}^n \to \mathbb{Z}^d$ 为投影到前 d 个坐标的投影。对于 $u \in (\mathbb{R}^d)^*$，定义 $O'_u := \{i \in \{1,\dots,K\} \mid \pi_d(Aa_i) \not\perp u\}$，我们有

$$\left(O'_u \cup J'\right) \cap M_u(I', \boldsymbol{f}^d) \neq \emptyset \quad \textit{for every } u \in (\mathbb{R}^d)^*. \tag{30}$$

如引理 *6.9* 所述，当 $d = 0$ 时，性质 (30) 被视为显然成立。

证明。固定一个 $v=(v_1,\dots,v_n)\in(\mathbb{R}^n)^*$。任取 $A\in\mathrm{GL}(n,\mathbb{Z})$，使得 $vA^{-\top}=(0,\dots,0,v'_{d+1},\dots,v'_n)$，并满足 $v'_{d+1},\dots,v'_n$ 是 $\mathbb{Q}$-线性无关的。注意，由于 $A\in\mathrm{GL}(n,\mathbb{Z})$，因此 $\sum_{k=1}^n\mathbb{Z}v_k=\sum_{k=d+1}^n\mathbb{Z}v'_k$。所以，我们可以将引理 6.9 应用于超 Gr¨obner 基 $\varphi_A(\boldsymbol{g}_1)\dots,\varphi_A(\boldsymbol{g}_m)$、向量 $vA^{-\top}=(0,\dots,0,v'_{d+1},\dots,v'_n)$ 以及向量 $a_1A,\dots,a_KA\in\mathbb{Z}^n$。这表明，存在 $\boldsymbol{\alpha}\in\left(\sum_{k=d+1}^n\mathbb{Z}v'_k\right)^K$ 和 $\boldsymbol{f}^d\in$ 属于 $\overset{d}{}_{vA^{-\top}}$，$\boldsymbol{\alpha}($ $\varphi_A(\mathcal{M}))$ 满足 (LocInfD)(a)(b1)(b2)，当且仅当存在 $\boldsymbol{\alpha}\in(\sum_{k=1}^n\mathbb{Z}v_k)^K$ 和 $\boldsymbol{f}\in\mathcal{M}$ 满足 (LocInfShift)(a)(b)。 □

6.5 无穷远处的局部条件：计算胞腔（LocInfCell）。在本小节中，我们将条件（LocInfD）进一步简化为条件（LocInfCell），只需针对每个坐标变换矩阵 $A\in\mathrm{GL}(n,\mathbb{Z})$ 验证有限个 $v\in(\mathbb{R}^n)^*$。

设 $v\in(\mathbb{R}^n)^*,\boldsymbol{\alpha}\in\mathbb{R}^K$。用 $e_1,\dots,e_K$ 表示 $\mathbb{A}$-模 $\mathbb{A}^K$ 的典范基。我们引入新变量 $T_1,\dots,T_K$，并定义一个 $\mathbb{A}$-模同态

$$\phi:\mathbb{A}^K\to\mathbb{R}[X_1^{\pm},\dots,X_n^{\pm},T_1^{\pm},\dots,T_K^{\pm}],\quad \overline{X}^ue_i\mapsto\overline{X}^uT_i.$$

对于每个 $\boldsymbol{f}\in\mathbb{A}^K$，我们有 $\phi(\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{f}))=\mathrm{in}_{(v,\boldsymbol{\alpha})}(\phi(\boldsymbol{f}))$。

与前面的小节一样，设 $\boldsymbol{g}_1,\dots,\boldsymbol{g}_m$ 是 $\mathcal{M}$ 的一个超 Gr¨obner 基。由于 $\phi(\boldsymbol{g}_i)$ 是 $\mathbb{R}[X_1^{\pm},\dots,X_n^{\pm},T_1^{\pm},\dots,T_K^{\pm}]$ 中的一个多项式，因此存在 $(\mathbb{R}^n)^*\times\mathbb{R}^K$ 的一个划分，使得同一划分部分中的任意两个方向所对应的 $\phi(\boldsymbol{g}_i)$ 的初始部分相同。设 $\mathcal{L}_{\mathcal{M}}$ 为与多项式 $\phi(\boldsymbol{g}_1)\dots,\phi(\boldsymbol{g}_m)$ 相关的划分的公共细化。

从现在起，我们用“胞腔”来称呼给定划分中的元素。固定 $I\subseteq\{1,\dots,K\}$。存在 $\mathbb{R}^K$ 的一个划分 $\mathcal{L}_I$，使得对于同一胞腔中的任意两个向量 $(\alpha_1,\dots,\alpha_K)$、$(\alpha'_1,\dots,\alpha'_K)$，都有 $\alpha_i>\alpha_j\iff\alpha'_i>\alpha'_j$ 和 $\alpha_i<\alpha_j\iff\alpha'_i<\alpha'_j$，对所有 $i,\ j\in I$ 均成立。定义 $(\mathbb{R}^n)^*\times\mathbb{R}^K$ 的划分 $\mathcal{L}'_I:=(\mathbb{R}^n)^*\times\mathcal{L}_I$，其中每个胞腔均形如 $(\mathbb{R}^n)^*\times P,\ P\in\mathcal{L}_I$。

最后，存在 $(\mathbb{R}^n)^*$ 的一个划分 $\mathcal{L}_O$，使得同一胞腔中的任意两个向量 $v,\ v'$ 对所有 $i\in\{1,\dots,K\}$ 均满足 $v\perp a_i\iff v'\perp a_i$。通过细分 $\mathcal{L}_O$，我们可以假设每个胞腔都是凸多面体。类似于 $\mathcal{L}'_I$ 的定义，我们定义 $(\mathbb{R}^n)^*\times\mathbb{R}^K$ 的划分 $\mathcal{L}'_O:=\mathcal{L}_O\times\mathbb{R}^K$。

对于同一个集合 S 的任意两个划分 $\mathcal{A}$，$\mathcal{B}$，定义 $\mathcal{A}\vee\mathcal{B}$ 为 S 的划分，其元素具有如下形式 $A\cap B,\ A\in\mathcal{A},\ B\in\mathcal{B}$。考虑由下式定义的 $(\mathbb{R}^n)^*\times\mathbb{R}^K$ 的划分 $\mathcal{L}$：

$$\mathcal{L}:=\mathcal{L}_{\mathcal{M}}\vee\mathcal{L}'_I\vee\mathcal{L}'_O.$$

我们指出，根据划分 $\mathcal{L}_{\mathcal{M}},\ \mathcal{L}'_I,\ \mathcal{L}'_O$ 的定义，$\mathcal{L}$ 的胞腔在正实数缩放下保持不变，这意味着对于所有胞腔 $Q\in\mathcal{L}$ 和 $r\in\mathbb{R}_{>0}$，都有 $x\in Q\iff r\cdot x\in Q$。

令 $\pi\colon(\mathbb{R}^n)^*\times\mathbb{R}^K\to(\mathbb{R}^n)^*$，$(v,\ \boldsymbol{\alpha})\mapsto v$ 为典范投影。对于每个 $Q\in\mathcal{L}$，定义二元划分 $\{\pi(Q),\ (\mathbb{R}^n)^*\setminus\pi(Q)\}$，并定义

$$\mathcal{P}:=\bigvee_{Q\in\mathcal{L}}\{\pi(Q),(\mathbb{R}^n)^*\setminus\pi(Q)\}.$$

根据此定义，任取满足 $\pi^{-1}(P)\cap Q\neq\emptyset$ 的 $P\in\mathcal{P}$ 和 $Q\in\mathcal{L}$；则对于 $v,\ v'\in P$，存在 $\boldsymbol{\alpha}\in\mathbb{R}^K$ 使得 $(v,\ \boldsymbol{\alpha})\in Q$，当且仅当存在 $\boldsymbol{\alpha}'\in\mathbb{R}^K$ 使得 $(v',\ \boldsymbol{\alpha}')\in Q$。

需要注意的是，划分 $\mathcal{L}_{\mathcal{M}}$、$\mathcal{L}_I$、$\mathcal{L}_O$ 均由系数为有理数 的等式和不等式定义。此外，每个不等式都是严格的，因此每个胞腔 $Q\in\mathcal{L}$ 和$P\in\mathcal{P}$ 都是相对开集（如果一个多面体在包含它的最小线性空间中是开集，则称其为相对开多面体）。换言之，每个胞腔都由等式和严格不等式的组合定义。我们还要指出，与 $\mathcal{L}$ 的胞腔一样，$\mathcal{P}$ 的胞腔在正实数缩放下是不变的，这意味着 $x\in P\iff r\cdot x\in P$对于所有胞腔 $P\in\mathcal{P}$和 $r\in\mathbb{R}_{>0}$均成立。

设 $Q \in \mathcal{L}$。对于 $(v, \boldsymbol{\alpha}), (v', \boldsymbol{\alpha}') \in Q$，我们有

$$\mathrm{in}_{v,\boldsymbol{\alpha}}(\boldsymbol{g}_j) = \mathrm{in}_{v',\boldsymbol{\alpha}'}(\boldsymbol{g}_j)$$

对于所有 $j = 1, \ldots\ldots, d$。因此，如果 $v = (0, \ldots\ldots, 0, v_{d+1}, \ldots\ldots, v_n)$ 满足 $v_{d+1}, \ldots\ldots, v_n$ 关于 $\mathbb{Q}$ 线性无关，那么在 $\overset{d}{v,}\ \boldsymbol{\alpha}(\mathcal{M})$ 中，$\mathcal{M}$ 仅取决于包含 $(v, \boldsymbol{\alpha})$ 的胞腔 $Q \in \mathcal{L}$。因此，我们可以记作

$$\mathrm{in}_Q^d(\boldsymbol{g}_j) \coloneqq \mathrm{in}_{v,\boldsymbol{\alpha}}^d(\boldsymbol{g}_j), \quad j = 1, \ldots, m, \quad \mathrm{in}_Q^d(\mathcal{M}) \coloneqq \mathrm{in}_{v,\boldsymbol{\alpha}}^d(\mathcal{M}), \quad \text{where } (v, \boldsymbol{\alpha}) \in Q.$$

对于任意坐标变换 $A \in \mathrm{GL}(n, \mathbb{Z})$，我们类似地根据超 Gr¨obner 基 $\varphi_A(\boldsymbol{g}_1) \ldots\ldots \varphi_A(\boldsymbol{g}_m)$ 以及向量 $a_1 A, \ldots\ldots, a_K A$ 定义划分 $\mathcal{L}A^{-\top}$ 和 $\mathcal{P}A^{-\top}$。特别地，$\mathcal{L}A^{-\top}$ 的每个胞腔都具有 $Q \cdot diag(A^{-\top}, I_K)$ $Q \in \mathcal{L}$ 的形式，而 $\mathcal{P}A^{-\top}$ 的每个胞腔都具有 $P \cdot A^{-\top}, P \in \mathcal{P}$ 的形式。如果 $vA^{-\top} = (0, \ldots\ldots, 0, v_{d+1}, \ldots\ldots, v_n)$ 满足 $v_{d+1}, \ldots\ldots, v_n$ 关于 $\mathbb{Q}$ 线性无关，那么在 $\overset{d}{vA^{-\top}}$ 中，$\boldsymbol{\alpha}(\varphi_A(\mathcal{M}))$ 仅取决于包含 $(vA^{-\top}, \boldsymbol{\alpha})$ 的胞腔 $Q \in \mathcal{L}A^{-\top}$。类似地，对于 $j = 1, \ldots\ldots, m$，我们可以记作

$$\mathrm{in}_Q^d(\varphi_A(\boldsymbol{g}_j)) \coloneqq \mathrm{in}_{vA^{-\top},\boldsymbol{\alpha}}^d(\varphi_A(\boldsymbol{g}_j)),\ \mathrm{in}_Q^d(\varphi_A(\mathcal{M})) \coloneqq \mathrm{in}_{vA^{-\top},\boldsymbol{\alpha}}^d(\varphi_A(\mathcal{M})),\ \text{where } (vA^{-\top}, \boldsymbol{\alpha}) \in Q.$$

定理 3.9 的输入是模 $\mathcal{M}$ over $\mathbb{A} = \mathbb{R}[X_1^{\pm}, \ldots, X_n^{\pm}]$ 的生成元、向量a_1、……、a_K in $\mathbb{Z}^n$ 以及两个集合 I、J。我们的策略是对 n 使用归纳法来证明定理 3.9。基例 $n = 0$ 归结为线性规划。事实上，当 $n = 0, \mathbb{A} = \mathbb{R}$、$\mathbb{A}^+ = \mathbb{R}_{>0}$ 时，性质 (10) 显然成立；问题转化为：给定 $\mathbb{R}^K$ 的一个 $\mathbb{R}$-子模 $\mathcal{M}$，判定 $\mathcal{M} \cap \mathbb{R}^K_{>0}$ 是否包含一个元素。由于 $\mathcal{M}$ 的给定生成元都具有整数系数，因此可以使用线性规划判定。

下面的观察表明，具有更小 n 的定理 3.9 的判定过程可以帮助我们判定哪些胞腔 $Q \in \mathcal{L}$ 包含满足性质 (LocInfD)(a)(b1)(b2) 的 $\boldsymbol{f}^d$。

引理 6.12。固定一个坐标变换 $A \in \mathrm{GL}(n, \mathbb{Z})$ 和一个数 $0 \le d \le n-1$。假设对于所有 n_0，$0 \le n_0 \le n-1$，定理 *3.9* 均成立。那么对于每个胞腔 $Q \in \mathcal{L}A^{-\top}$，我们可以判定 $\mathrm{in}_Q^d(\varphi_A(\mathcal{M}))$ 是否包含满足性质（*LocInfD*）*(a)*、*(b1)* 和 *(b2)* 的元素 $\boldsymbol{f}^d$。

证明。假设对于所有 $0 \le n_0 \le n-1$，定理 3.9 均成立。固定一个胞腔 $Q \in \mathcal{L}A^{-\top}$。

根据划分 $\mathcal{L}$ 的定义，集合 $I' \coloneqq \{i \in I \mid \alpha_i = \min_{i' \in I} \alpha_{i'}\}, J' \coloneqq O_v \cup J$ 仅取决于包含 $(v, \boldsymbol{\alpha})$ 的胞腔 Q。因此，我们可以计算 I', J'，并验证性质（LocInfD）(b1)、$J' \cap I' \neq \emptyset$ 是否满足。

在 (LocInfD) 中，$\mathbb{A}_d$-子模 $\mathrm{in}_{\overset{d}{vA^{-\top},}\ \boldsymbol{\alpha}}(\varphi_A(\mathcal{M})) = \mathrm{in}_Q^d(\varphi_A(\mathcal{M}))$ 由 $\mathbb{A}_d^K$ 中的 $\mathrm{in}_Q^d(\varphi_A(\boldsymbol{g}_j))$ $j = 1, \ldots\ldots, m$生成。回顾一下，$\pi_d \coloneqq \mathbb{Z}^n \to \mathbb{Z}^d$ 表示投影到前 d 个坐标。因此，利用定理 3.9，将 n 替换为 $d < n$，将 $\mathbb{A}$-模 $\mathcal{M}$ 替换为$\mathbb{A}_d$-模 $\mathrm{in}_Q^d(\varphi_A(\mathcal{M}))$，并将向量 $a_1, \ldots\ldots, a_K$ 替换为向量 $\pi_d(a_1 A)\ldots\ldots, \pi_d(a_K A)$，我们可以判定 $\mathrm{in}_Q^d(\varphi_A(\mathcal{M}))$ 是否包含满足性质 (LocInfD)(a) 和 (b2) 的元素 $\boldsymbol{f}^d$。

□

记 $Op(A, d)$ 为所有满足以下条件的胞腔 $Q \in \mathcal{L}A^{-\top}$ 的并：$\mathrm{in}_Q^d(\varphi_A(\mathcal{M}))$ 包含满足性质 (LocInfD)(a)(b1)(b2) 的元素$\boldsymbol{f}^d$。根据引理 6.12，集合 $Op(A, d)$ 可有效地计算为由有理系数定义的多面体的有限并（假设定理 3.9 对所有 $0 \le n_0 \le n-1$ 都成立）。图 27 展示了 $Op(A, d)$ 的示意图。

命题 6.13. 命题 6.11 的（LocInfD）条件等价于以下内容：

2. （**LocInfCell**）：对于每个 $A \in \mathsf{GL}$（n、$\mathbb{Z}$）以及每个数 $0 \leq d \leq n-1$，以下结论成立：

(a) 对于每个 $v = (0, \ldots, 0, v_{d+1}, \ldots, v_n) \in \{0\}^d \times (\mathbb{R}^{n-d})^*$，其中 $v_{d+1}, \ldots, v_n$ 是 $\mathbb{Q}$-线性无关的，存在 $\boldsymbol{\alpha} \in \left(\sum_{k=d+1}^{n} \mathbb{Z} v_k\right)^K$，使得 $(v, \boldsymbol{\alpha}) \in Op(A, d)$。

证明。 这直接由 $Op(A, d)$ 的定义得出。 □

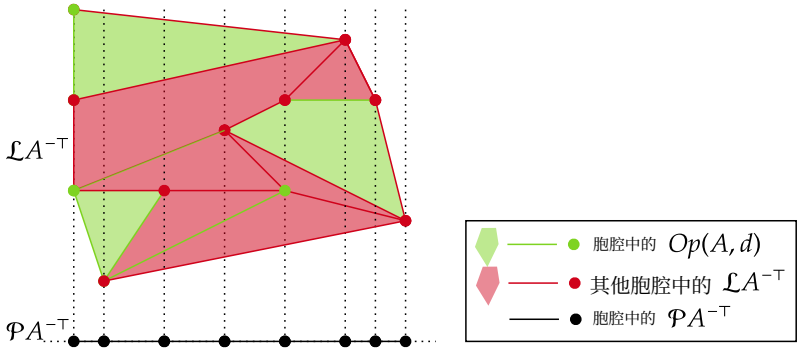

图 27： $Op(A, d)$ 的示意图。

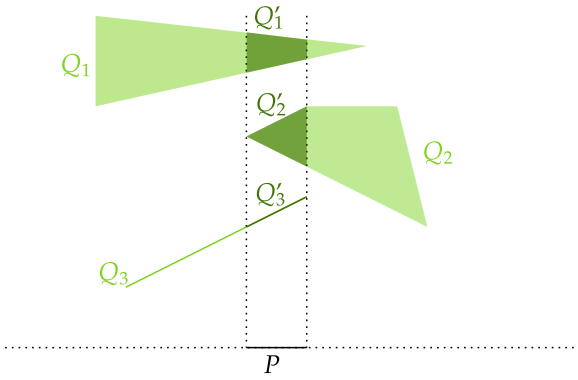

图 28：引理 6.14 的示意图

引理 6.14。 给定 $A \in \mathsf{GL}(n, \mathbb{Z})$ $d \in \mathbb{N}$，以及给定 $Op(A, d)$ 为由有理系数定义的多面体的有限并，可以判定陈述 (LocInfCell)(a) 是否为真。

证明。 将 Q 中的每个胞腔替换为其与 $\{0\}^d \times (\mathbb{R}^{n-d})^* \times \mathbb{R}^K$ 的交集；并将 $P \in \mathcal{P}A^{-\top}$ 中的每个胞腔替换为其与 $\{0\}^d \times (\mathbb{R}^{n-d})^*$ 的交集。我们可以假设 $\mathcal{P}A^{-\top}$ 是 $(\mathbb{R}^{n-d})^*$ 的划分， $\mathcal{L}A^{-\top}$ 是 $(\mathbb{R}^{n-d})^* \times \mathbb{R}^K$ 的划分， $Op(A, d) \subseteq (\mathbb{R}^{n-d})^* \times \mathbb{R}^K$ 是 $\mathcal{L}A^{-\top}$ 中的胞腔之并，并且对我们考虑的所有 v 都有 $v \in \left(\mathbb{R}^{n-d}\right)^*$。我们分两种情况讨论。

(1) 当 $d = n-1$。在这种情况下，由于这些划分在缩放下保持不变，我们可以假设 $v_n \in \{1,-1\}$。于是，对于每种情况 $v_n = 1$ 和 $v_n = -1$，判断是否存在$\boldsymbol{\alpha} \in (\mathbb{Z}v_n)^K = \mathbb{Z}^K$，使得 $(v, \boldsymbol{\alpha}) \in Op(A, d)$。由于 $Op(A, d)$ 是使用有理数定义的多面体的有限并，因此可以利用整数规划判定。

（2）当 $d \le n-2$ 时。图 28 展示了此情形的示意图。每当 $v = (v_{d+1}, \dots, v_n)$ 且 $v_{d+1}, \dots, v_n$ 线性独立于 $\mathbb{Q}$ 时，v 必须落在维数为 $n-d$ 的胞腔 $P \in \mathcal{P}A^{-\top}$ 中。对于每个维数为 $n-d$ 的胞腔 $P \in \mathcal{P}A^{-\top}$，考虑所有满足 $\pi(Q) \cap P \neq \emptyset$ 的胞腔 $Q \subseteq Op(A, d)$。如果不存在这样的胞腔 Q，则命题（LocInfCell）（a）为假。事实上，由于 $P \in \mathcal{P}A^{-\top}$ 的维数为 $n-d$，其中包含一个元素 $v = (v_{d+1}, \dots, v_n)$，且 $v_{d+1}, \dots, v_n$ 线性独立于 $\mathbb{Q}$。因此，对于这个 v，不存在任何 $\boldsymbol{\alpha} \in \mathbb{R}^K$ 使得 $(v, \boldsymbol{\alpha}) \in Op(A, d)$，所以命题（LocInfCell）（a）为假。

现在假设，对于每个维数为 $n-d$ 的胞腔 $P \in \mathcal{P}$，都存在胞腔 $Q \subseteq Op(A, d)$，使得 $\pi(Q) \cap P \neq \emptyset$。固定一个胞腔 $P \in \mathcal{P}$，令 $Q_1, \dots, Q_\ell$ 表示 $Op(A, d)$ 中满足 $\pi(Q) \cap P \neq \emptyset$ 的所有胞腔。定义 $Q'_t := Q_t \cap \pi^{-1}(P)$，其中 $t = 1, \dots, \ell$。每个 Q'_t 都是一个相对开多面体。

T取任意一个 Q'_t，它由以下方程和不等式定义：

$$(v_{d+1}, \dots, v_n) \in P \tag{31}$$
$$\beta_{j,1}\alpha_1 + \cdots + \beta_{j,K}\alpha_K = \gamma_{j,d+1}v_{d+1} + \cdots + \gamma_{j,n}v_n, \quad j = 1, \dots, m_0, \tag{32}$$
$$\delta_{j,1}\alpha_1 + \cdots + \delta_{j,K}\alpha_K < \epsilon_{j,d+1}v_{d+1} + \cdots + \epsilon_{j,n}v_n, \quad j = 1, \dots, m_1. \tag{33}$$

其中 $\beta_{j,\,i}$，$\gamma_{j,\,i}$，$\delta_{j,\,i}$，$\epsilon_{j,\,i}$ 都是有理数。注意，根据 P 的定义，对于 v，$v' \in P$，存在 $\boldsymbol{\alpha} \in \mathbb{R}^K$ 使得 $(v, \boldsymbol{\alpha}) \in Q$，当且仅当存在 $\boldsymbol{\alpha}' \in \mathbb{R}^K$ 使得 $(v', \boldsymbol{\alpha}') \in Q$。因此，$\pi(Q'_t) = P$，我们可以假设（32）和（33）的左端不为零（因此，除了（31）之外，不会对（v_{d+1}，……，v_n）施加额外的约束）。

使用高斯主元法，并可根据需要交换 $\alpha_i, i = 1, \dots, K$ 的顺序，我们可以将上述方程和不等式改写为以下形式

$$(v_{d+1}, \dots, v_n) \in P \tag{34}$$
$$\alpha_i = \beta_{i,D+1}\alpha_{D+1} + \cdots + \beta_{i,K}\alpha_K + \gamma_{i,d+1}v_{d+1} + \cdots + \gamma_{i,n}v_n, \quad i = 1, \dots, D, \tag{35}$$
$$\delta_{j,D+1}\alpha_{D+1} + \cdots + \delta_{j,K}\alpha_K < \epsilon_{j,d+1}v_{d+1} + \cdots + \epsilon_{j,n}v_n, \quad j = 1, \dots, m_1. \tag{36}$$

特别地，数 $D \in \mathbb{N}$ 满足：Q'_t 是一个维数为 $n-d+K-D$ 的多面体。设 $M \in \mathbb{N}$ 为所有 $\beta_{i,j}, \gamma_{i,k}, i = 1, \dots, D, j = D+1, \dots, K, k = d+1, \dots, n$ 的公分母。我们将方程 (35) 两边乘以 M，并假设 Q'_t 定义为

$$(v_{d+1}, \dots, v_n) \in P \tag{37}$$
$$M\alpha_i = \beta_{i,D+1}\alpha_{D+1} + \cdots + \beta_{i,K}\alpha_K + \gamma_{i,d+1}v_{d+1} + \cdots + \gamma_{i,n}v_n, \quad i = 1, \dots, D, \tag{38}$$
$$\delta_{j,D+1}\alpha_{D+1} + \cdots + \delta_{j,K}\alpha_K < \epsilon_{j,d+1}v_{d+1} + \cdots + \epsilon_{j,n}v_n, \quad j = 1, \dots, m_1, \tag{39}$$

其中 $\beta_{i,j}, \gamma_{i,k}, i = 1, \dots, D, j = D+1, \dots, K, k = d+1, \dots, n$, 均为整数。
固定任意一个 $v = (v_{d+1}, \dots, v_n) \in P$，其中 $v_{d+1}, \dots, v_n$ 是 $\mathbb{Q}$-线性无关的。我们声明如下：存在 $\boldsymbol{\alpha} \in \left(\sum_{k=d+1}^{n} \mathbb{Z}v_k\right)^K$，使得 $(v, \boldsymbol{\alpha}) \in Q'_t$，当且仅当以下 $(n-d)D$ 个方程组成的方程组具有整数解 $z_{i,\,k}$，$i = 1, \dots, D, D+1, \dots, K$，$k = d+1, \dots, n$。

$$Mz_{i,d+1} = \beta_{i,D+1}z_{D+1,d+1} + \cdots + \beta_{i,K}z_{K,d+1} + \gamma_{i,d+1}, \quad i = 1, \dots, D,$$

$$
\begin{aligned}
&Mz_{i,d+2} = \beta_{i,D+1}z_{D+1,d+2} + \cdots + \beta_{i,K}z_{K,d+2} + \gamma_{i,d+2}, \quad i = 1, \ldots, D,\\
&\quad\vdots\\
&Mz_{i,n} = \beta_{i,D+1}z_{D+1,n} + \cdots + \beta_{i,K}z_{K,n} + \gamma_{i,n}, \quad i = 1, \ldots, D.
\end{aligned} \tag{40}
$$

现在证明这一声明。对于“仅当”蕴含，假设存在 $\boldsymbol{\alpha} \in \left(\sum_{k=d+1}^{n} \mathbb{Z}v_k\right)^K$ 使得 $(v, \boldsymbol{\alpha}) \in Q'_t$。对于每个 $i \in \{1, \ldots, K\}$，记 $\alpha_i = \sum_{k=d+1}^{n} z_{i,k} v_k$，则方程 (38) 变为

$$
M\sum_{k=d+1}^{n} z_{i,k}v_k = \beta_{i,D+1}\sum_{k=d+1}^{n} z_{D+1,k}v_k + \cdots + \beta_{i,K}\sum_{k=d+1}^{n} z_{K,k}v_k + \gamma_{i,d+1}v_{d+1} + \cdots + \gamma_{i,n}v_n, \quad i = 1, \ldots, D. \tag{41}
$$

由于 v_{d+1}、……、v_n 是关于 $\mathbb{Q}$ 线性无关的，当且仅当对于所有 $k = d+1$、……、n，v_k 两边的系数相等时，方程（41）成立。也就是说，

$$
Mz_{i,k} = \beta_{i,D+1}z_{D+1,k} + \cdots + \beta_{i,K}z_{i,k} + \gamma_{i,k}, \quad i = 1, \ldots, D, \quad k = d+1, \ldots, n.
$$

这正是方程组（40）。

对于“若”蕴含，假设方程组 (40) 具有整数解 $z_{i,k}, i = 1, \ldots, D, D+1, \ldots, K, k = d+1, \ldots, n$。

对于每个整数元组 $c_{i,k}, i = D+1, \ldots, K, k = d+1, \ldots, n$，我们可以通过令 $z'_{i,k} := z_{i,k} + Mc_{i,k}, i = D+1, \ldots, K, k = d+1, \ldots, n$，构造方程组（40）的一个新解，并且

$$
\begin{aligned}
&z'_{i,d+1} := z_{i,d+1} + \beta_{i,D+1}c_{D+1,d+1} + \cdots + \beta_{i,K}c_{K,d+1}, \quad i = 1, \ldots, D,\\
&z'_{i,d+2} = z_{i,d+2} + \beta_{i,D+1}c_{D+1,d+2} + \cdots + \beta_{i,K}c_{K,d+2}, \quad i = 1, \ldots, D,\\
&\quad\vdots\\
&z'_{i,n} = z_{i,n} + \beta_{i,D+1}c_{D+1,n} + \cdots + \beta_{i,K}c_{K,n}, \quad i = 1, \ldots, D.
\end{aligned} \tag{42}
$$

由于 $z'_{i,k}$、$i = 1$、……、D、$D+1$、……、K、$k = d+1$、……、n 是（40）的一个解，因此很容易验证，$\alpha_i := \sum_{k=d+1}^{n} z'_{i,k} v_k$、$i = 1$、……、$K$ 构成（38）的一个解。现在我们证明，对于每个元组（v_{d+1}、……、v_n）$\in P$，实际上都可以找到整数 $c_{i,k}$、$i = D+1$、……、K、$k = d+1$、……、n，使得 $\alpha_i = \sum_{k=d+1}^{n} (z_{i,k} + Mc_{i,k}) v_k$、$i = D+1$、……、$n$ 也满足（39）。

由于 Q'_t 是相对开且非空的，因此集合 $\pi^{-1}(v_{d+1}, \ldots, v_n) \cap Q'_t$ 也非空。因此，不等式（39）关于 $(\alpha_{D+1}, \ldots, \alpha_K) \in \mathbb{R}^{K-D}$ 的解集 $\mathcal{A}$ 非空。该解集 $\mathcal{A}$ 是 $\mathbb{R}^{K-D}$ 的一个开子集，因为它由严格不等式定义。由于 $v_{d+1}, \ldots, v_n$ 是 $\mathbb{Q}$-线性无关的，集合

$$
\left\{ \alpha_i := \sum_{k=d+1}^{n} (z_{i,k} + Mc_{i,k}) v_k \;\middle|\; c_{i,d+1}, \ldots, c_{i,n} \in \mathbb{Z} \right\}
$$

对每个 $i \in \{D+1, \ldots, K\}$，$\mathbb{R}$ 中都是稠密的。因此，我们可以找到 $c_{D+1,d+1}$、……、$c_{D+1,n} \in \mathbb{Z}$，使得 $\alpha_{D+1} := \sum_{k=d+1}^{n} (z_{D+1,k} + Mc_{D+1,k}) v_k$ 对某些 x_{D+2}、……、$x_n \in \mathbb{R}$ 满足（α_{D+1}、x_{D+2}、……、x_n）$\in \mathcal{A}$。类似地，由于 $\mathcal{A}$ 是开集，我们随后可以找到 $c_{D+2,d+1}$、……、$c_{D+2,n} \in \mathbb{Z}$，使得 $\alpha_{D+2} := \sum_{k=d+1}^{n} (z_{D+2,k} + Mc_{D+2,k}) v_i$ 对某些 x_{D+3}、……、$x_n \in \mathbb{R}$ 满足（α_{D+1}、α_{D+2}、x_{D+3}、……、x_n）$\in \mathcal{A}$。继续以此方式进行，我们将找到整数 $c_{i,k}$、$i = D+1$、……、K、$k =$

$d+1$、...、n，使得（α_{D+1}、...、α_n）$\in \mathcal{A}$。这个元组（α_{D+1}、...、α_n）满足（39）。由于无论选择$c_{i,k}$如何，$\alpha_i = \sum_{k=d+1}^{n} z'_{i,k} v_k$、$i=1$、...、$K$、都是（38）的解，因此（38）和（39）现在都得到满足。我们证明了这一断言。

注意到，方程组（40）是否有整数解只取决于系数$\beta_{i,k}$、$\gamma_{i,k}$、$i=1$、.....、D、$j=D+1$、.....、K、$k=d+1$、.....、n。这些系数由多面体 Q'_t决定，而与 v的选择无关。对于每个 Q'_t、$t=1$、.....、ℓ，我们都可以判定其方程组（40）是否有整数解。如果对某个 $t \in \{1,\dots,\ell\}$，其方程组（40）有整数解，那么上述断言表明，对于所有 $v=$（v_{d+1}、.....、v_n）$\in P$withv_{d+1}、.....、v_n为 $\mathbb{Q}$-线性无关的，都存在 $\boldsymbol{\alpha} \in \left(\sum_{k=d+1}^{n} \mathbb{Z} v_k\right)^K$使得（$v$、$\boldsymbol{\alpha}$）$\in Q'_t$。否则，如果对于所有 $t \in \{1,\dots,\ell\}$，其方程组（40）都没有整数解，那么对于任意$v=$（v_{d+1}、.....、v_n）$\in P$ with v_{d+1}、.....、v_n为 $\mathbb{Q}$-线性无关的，都不存在$\boldsymbol{\alpha} \in \left(\sum_{k=d+1}^{n} \mathbb{Z} v_k\right)^K$使得（$v$、$\boldsymbol{\alpha}$）$\in Q'_t$。

总而言之，为了判定命题（LocInfCell）（a）是否成立，只需枚举所有维数为 $n-d$ 的胞腔 $P \in \mathcal{P}A^{-\top}$。对于一个胞腔 P，如果不存在胞腔 $Q \subseteq Op$（A，d）使得 π（Q）$\cap P \neq \emptyset$，则命题（LocInfCell）（a）为假；否则，对于每个 Q'_1，.....，Q'_ℓ，检查方程组（40）是否有整数解；如果某个Q'_t 存在整数解，我们就称胞腔 P 为“可操作的”。如果每个维数为 $n-d$ 的胞腔 $P \in \mathcal{P}$ 都是可操作的，则命题（LocInfCell）（a）为真，否则为假。

□

6.6 证明定理 3.9：归纳法与双重过程。在本小节中，我们最终证明定理 3.9。总体策略是对 n 使用归纳法，同时判定定理 3.8 中的条件 (LocR) 和 (LocInf)。

定理 3.9。固定 $n \in \mathbb{N}$。假设给定一组生成元 $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m \in \mathbb{A}^K$，其系数为整数，以及向量 $a_1, \dots, a_K \in \mathbb{Z}^n$ 和 $\{1,\dots,K\}$ 的两个子集 I, J。记 $\mathcal{M}$ 为由 $\boldsymbol{g}_1, \dots, \boldsymbol{g}_m$ 生成的 $\mathbb{A}^K$ 的 $\mathbb{A}$- 子模。判断是否存在满足条件的 $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{A}^+)^K$ 是可判定的

$$(O_v \cup J) \cap M_v(I, \boldsymbol{f}) \neq \emptyset, \quad \textit{for every } v \in (\mathbb{R}^n)^* . \tag{10}$$

这里，如果 $n=0$，则将 $\mathbb{A}$ 理解为 $\mathbb{R}$，而性质 (10) 被视为平凡成立。

证明。我们对 n使用归纳法。如小节 6.5 中所述，基例 $n=0$ 可归结为线性规划问题（给定 $\mathbb{R}^K$ 的一个 $\mathbb{R}$-子模 $\mathcal{M}$，判断 $\mathcal{M} \cap \mathbb{R}^K_{>0}$ 是否包含一个元素）。假设我们对所有 $n_0 < n$都有一个判定过程，现在构造一个针对 n的判定过程。

根据定理 3.8，只需判定条件 (LocR) 和 (LocInf) 是否同时满足。首先利用命题 6.2 检查 (LocR) 是否成立。如果 (LocR) 不成立，则返回 False，并得出不存在满足 (10) 的 $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{A}^+)^K$。如果 (LocR) 成立，则继续。

现在我们并行运行以下两个过程：

1. **过程 A：** 我们枚举 $\mathbb{Z}[X_1^{\pm}, \dots, X_n^{\pm}]$-模的所有元素：

$$\mathcal{M}_{\mathbb{Z}} := \left\{ \sum_{j=1}^{m} h_j \cdot \boldsymbol{g}_j \;\middle|\; h_1, \dots, h_m \in \mathbb{Z}[X_1^{\pm}, \dots, X_n^{\pm}] \right\}.$$

对于每个元素 $\boldsymbol{f} \in \mathcal{M}_{\mathbb{Z}}$，检查 $\boldsymbol{f}$ 是否属于 $(\mathbb{A}^+)^K$ 且满足性质 (10)。如果 $\boldsymbol{f} \in (\mathbb{A}^+)^K$，则可以通过查看 $\boldsymbol{f}$的对应 $\mathcal{G}$-图 Γ 来检查性质 (10)。考虑通过仅保留 Γ 中标签属于集合 I的边而得到的图 Γ_I。当且仅当 conv($V(\Gamma_I)$) 的每个真面 F都包含以下任一条边的起点时，$\boldsymbol{f}$满足性质 (10)：标签属于 J 的边，或从 F出发的边。如果某个元素 $\boldsymbol{f} \in \mathcal{M}_{\mathbb{Z}}$ 属于 $(\mathbb{A}^+)^K$ 且满足性质 (10)，则我们停止该过程并返回 True。

2. **过程 B：** 我们枚举所有 $A \in \mathrm{GL}(n, \mathbb{Z})$ 和 $d \in \{0, 1, \ldots, n-1\}$。对于每个 A和d，使用引理 6.12 和归纳假设计算 $Op(A, d)$。利用引理 6.14，我们检查命题 6.13 中的命题（LocInfCell）（a）是否为假。如果对于某个 A, d，命题（LocInfCell）（a）为假，则停止该过程并返回 False。

我们断言，上述两个过程中的一个必定会停止。

事实上，如果 $\mathcal{M}$ 包含一个属于 $(\mathbb{A}^+)^K$ 且满足性质 (10) 的元素，那么存在一个元素$\boldsymbol{f} \in \mathcal{M}_{\mathbb{Z}} \cap (\mathbb{A}^+)^K$ 满足性质 (10)（见引理 3.7）。在这种情况下，过程 A 通过找到一个属于 $\mathcal{M}_{\mathbb{Z}} \cap (\mathbb{A}^+)^K$ 且满足性质 (10) 的元素而终止。

如果 $\mathcal{M}$ 不包含一个属于 $(\mathbb{A}^+)^K$ 且满足性质 (10) 的元素，那么根据定理 3.8，条件（LocInf）必定为假（因为我们已经检查过（LocR）为真）。根据命题 6.4、6.11 和 6.13 构成的链，必定存在某个 $A \in \mathrm{GL}(n, \mathbb{Z})$ 和 $d \in \{0, 1, \ldots, n-1\}$，使得命题（LocInfCell）（a）为假。在这种情况下，过程 B 通过找到 $A \in \mathrm{GL}(n, \mathbb{Z})$ 和$d \in \{0, 1, \ldots, n-1\}$（其中命题（LocInfCell）（a）为假）而终止。

因此，通过并行运行过程 A 和过程 B，我们得到一个对于 n 总能终止的算法。

□

参考文献

[1] S. I. Adyan。《群的某些性质的识别问题的算法不可解性》。载于*Dokl. Akad. Nauk SSSR (N.S.)*，第 103 卷，第 533–535 页，1955年。[2] A. D. Alexandrov。《style id='5'>凸多面体，第 109 卷。Springer，2005年。[3] L. Babai、R. Beals、J.-y. Cai、G. Ivanyos 和 E. M. Luks。交换矩阵上的乘法方程。载于第七届 *ACM-SIAM*离散算法研讨会论文集，第 498–507 页，1996 年。[4] G. Baumslag。有限表示的亚交换群的子群。*Journal of the AustralianMathematical Society*，16(1):98–110，1973 年。[5] G. Baumslag、F. B. Cannonito 和 D. J. Robinson。有限生成亚交换群的算法理论。*Transactions of the American Mathematical Society*，344(2):629–648，1994 年。[6] G. Baumslag、R. Mikhailov 和 K. E. Orr。局部化、亚交换群与同构问题。*Transactions of the American Mathematical Society*，369(10):6823–6852，2017 年。[7] R. Beals 和 L. Babai。矩阵群的拉斯维加斯算法。载于*1993* 年 *IEEE* 第 *34* 届计算机科学基础年会论文集，第 427–436 页。IEEE，1993 年。

[8] P. C. Bell、M. Hirvensalo 和 I. Potapov。在$SL_2(\mathbb{Z})$中的矩阵半群单位元问题是 NP完全。载于《第二十八届 ACM-SIAM离散算法研讨会论文集》，第 187–206 页。SIAM，2017 年。[9] P. C. Bell 和 I. Potapov。论单位对应问题的不可判定性及其在词半群和矩阵半群中的应用。《International Journal of Foundations of Computer Science》，21(06):963–978，2010 年。[10] C. Berkesch 和 F.-O. Schreyer。极小生成关系、有限长度模与随机曲线。《交换代数与非交换代数几何》，1:25–52，2015 年。[11] V. D. Blondel、E. Jeandel、P. Koiran 和 N. Portier。关于量子自动机的可判定和不可判定问题。《SIAM Journal on Computing》，34(6):1464–1473，2005年。[12]C. Choffrut 和 J. Karhum¨aki。关于整数矩阵的一些判定问题。《RAIRO-Theoretical Informatics and Applications-Informatique Théorique et Applications》，39(1):125–131，2005年。[13] V. De Angelis 和 S. Tuncel。关于带有正倍数的多项式的Handelman定理。《Codes, systems, and graphical models》（明尼阿波利斯，明尼苏达州，1999 年），第 439–445 页，2001 年。[14] H. Derksen、E. Jeandel 和 P. Koiran。量子自动机与代数群。《Journal of Symbolic Computation》，39(3-4):357–371，2005年。[15] R. Dong。幂零群上的单位元问题和群问题，2022 年。已投稿。[16] R. Dong。在 $\mathbb{Z} \wr \mathbb{Z}$ 中单位元问题是可判定的。arXiv 预印本 arXiv:2302.05939，2023 年。[17] M. Einsiedler、R. Mouat 和 S. Tuncel。$(\mathbb{R}[x_1, \ldots, x_k])^n$ 的子模何时包含正元素？《Monatshefte für Mathematik》，140(4):267–283，2003 年。[18]D. Eisenbud。《交换代数：以代数几何为视角》，第 150 卷。Springer Science & Business Media，2013 年。[19] P. Hall。可解群的有限性条件。《Proceedings of the London Mathematical Society》，s3-4(1):419–436，1954 年 1 月。[20] D. Handelman。紧群的正多项式与乘积型作用，第 320 卷。American Mathematical Soc.，1985 年。[21] E. Hrushovski、J. Ouaknine、A. Pouly 和 J. Worrell。仿射程序的多项式不变量。载于《第 33 届 ACM/IEEE 计算机科学逻辑研讨会论文集》，第 530–539 页，2018 年。[22] O. G. Kharlampovich。一个具有不可解字问题的有限表示可解群。《Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya》，45(4):852–873，1981 年。[23] O. G. Kharlampovich 和 M. V. Sapir。簇中的算法问题。《International Journal of Algebra and Computation》，5(04n05):379–602，1995 年。[24] V. M. Kopytov。代数数域上矩阵的有限生成可解群中的出现问题的可解性。《Algebra and Logic》，7(6):388–393，1968 年。

[25] J. C. Lennox 和 D. J. Robinson。《无限可解群理论》。克拉伦登出版社，2004 年。[26] M. Lohrey、B. Steinberg 和 G. Zetzsche。群花环积的有理子集与子幺半群。《Information and Computation》，243：191–204，2015 年。[27] W. Magnus。关于 Marshall Hall 的一个定理。《Annals of Mathematics》，第 764–768 页，1939 年。[28] A. Markov。关于矩阵的某些不可解问题。《苏联科学院学报》，57(6)：539–542，1947 年。[29] K. A. Mikhailova。群的直积的出现问题。《Matematicheskii Sbornik》，112(2)：241–251，1966 年。[30] J. R. Munkres。《拓扑学：入门教程》。Prentice-Hall，1974 年。[31] P. Narendran。多项式半环上的线性方程求解。载于《第 11 届 IEEE 计算机科学逻辑年度研讨会论文集》，第 466–472 页。IEEE，1996 年。[32] G. A. Noskov。亚交换群中的共轭问题。《苏联科学院数学札记》，31：252–258，1982 年。[33] P. S. Novikov。论群论中字问题的算法不可解性。《以 V. A. 斯捷克洛夫命名的数学研究所论文集》，44：3–143，1955 年。[34] V. Roman'kov。海森堡群足够大的有限直幂的子幺半群成员问题的不可判定性。《arXiv 预印本 arXiv:2209.14786》，2022 年。[35]N. S. Romanovskii。可解群的一些算法问题。《Algebra and Logic》，13(1)：13–16，1974 年。[36] F.-O. Schreyer。利用广义 Weierstrass 除法定理计算 syzygy。硕士论文，汉堡大学数学系，1980 年。[37] A. Tarski。《初等代数与几何的判定方法》。修订版第二版，加利福尼亚大学出版社，伯克利，1951 年。

引理 2.2 和 2.8 的证明

引理 2.2。 设 G 为一个群。如果 G中的群问题是可判定的，那么 G中的单位元问题和逆元问题也是可判定的。

证明。 固定群 G。设 $\mathcal{G}$ 是 G的一个有限子集。对于单位元问题，我们断言，半群 $\langle \mathcal{G} \rangle$ 包含单位元 e，当且仅当 $\mathcal{G}$存在某个非空子集 $\mathcal{H}$ 使得 $\langle \mathcal{H} \rangle = \langle \mathcal{H} \rangle_{grp}$。事实上，如果 $\langle \mathcal{G} \rangle$ 包含单位元 e，设 e 由词 $w \in \mathcal{G}^*$表示。令 $\mathcal{H} \subseteq \mathcal{G}$ 为出现在 w中的字母所组成的集合，则 w 是字母表 $\mathcal{H}$ 上的一个满像词，因此根据引理 2.1，$\langle \mathcal{H} \rangle = \langle \mathcal{H} \rangle_{grp}$。反之，如果 $\langle \mathcal{H} \rangle = \langle \mathcal{H} \rangle_{grp}$，则 $e \in \langle \mathcal{H} \rangle_{grp} = \langle \mathcal{H} \rangle \subseteq \langle \mathcal{G} \rangle$。

因此，要判定单位元问题，只需检查 $\mathcal{G}$的每个非空子集 $\mathcal{H}$ 所对应的群问题即可。

对于逆元问题，设 $\mathcal{G} = \{g_1, \ldots, g_K\}$。不失一般性，假设我们要判定 $g_1^{-1} \in \langle \mathcal{G} \rangle$。我们断言，$g_1^{-1} \in \langle \mathcal{G} \rangle$ 当且仅当存在 $\mathcal{G}$ 的某个子集 $\mathcal{H}$，使得 $\langle \mathcal{H} \cup \{g_1\} \rangle = \langle \mathcal{H} \cup \{g_1\} \rangle_{grp}$。事实上，若 $g_1^{-1} \in \langle \mathcal{G} \rangle$，假设 g_1^{-1} 可由以下词表示

$w \in \mathcal{G}^*$。设 $\mathcal{H}$ 为出现在 w 中的字母所组成的集合，则 $g_1 w$ 是字母表$\mathcal{H} \cup \{g_1\}$上的一个表示单位元的满像词，因此由引理 2.1 可得 $\langle \mathcal{H} \cup \{g_1\} \rangle = \langle \mathcal{H} \cup \{g_1\} \rangle_{grp}$。反过来，若 $\langle \mathcal{H} \cup \{g_1\} \rangle = \langle \mathcal{H} \cup \{g_1\} \rangle_{grp}$，则 $g_1^{-1} \in \langle \mathcal{H} \cup \{g_1\} \rangle_{grp} = \langle \mathcal{H} \cup \{g_1\} \rangle \subseteq \langle \mathcal{G} \rangle$。

因此，要判定逆元问题，只需针对 $\mathcal{G}$ 的每个子集 $\mathcal{H} \cup \{g_1\}$ 检查群问题。

□

引理 2.8。半群 $\langle \mathcal{G} \rangle$ 是群，当且仅当存在一个表示单位元的满像欧拉 $\mathcal{G}$-图。

证明。如果半群 $\langle \mathcal{G} \rangle$ 是群，那么根据引理 2.1，存在一个表示单位元的满像词 w。于是，与之关联的 $\mathcal{G}$-图 $\Gamma(w)$ 是满像的、欧拉的，并且表示单位元。

如果 Γ 是一个表示单位元的满像欧拉 $\mathcal{G}$-图。设 $z \in V(\Gamma)$ 是 Γ 的任意一个顶点。现在考虑平移 $\Gamma - z$：它表示元素 $(X^z \cdot 0,\ 0) = (0,\ 0)$，并包含一条从 0 出发的欧拉回路。我们从这条欧拉回路读出一个词 w，于是 w 表示单位元。此外，w 是满像的，因为 $\Gamma - z$ 是满像的。因此，根据引理 2.1，半群 $\langle \mathcal{G} \rangle$ 是群。

□

B 命题 2.4 的证明

现在给出命题 2.4 的完整证明。我们首先陈述 Baumslag 的一个引理。

引理 B.1 ([5, 定理 3。3], [25, 定理 9.5。3])。给定一个有限元后承表示 G 以及一个有限子集 $\mathcal{G} \subseteq G$，存在一种算法可以找出子群 $\langle \mathcal{G} \rangle_{grp}$的有限亚交换群表示。

[25, 定理 9.5。3] 的证明表明，集合 $\mathcal{G}$ 由 $\langle \mathcal{G} \rangle_{grp}$的有限亚交换群表示的生成元给出。[2] 由于我们的目标是判定群问题（即 $\langle \mathcal{G} \rangle = \langle \mathcal{G} \rangle_{grp}$），根据引理 B.1，我们不妨假设 $G = \langle \mathcal{G} \rangle_{grp}$。

现在回顾<style id='1'>缠绕积的<style id='1'>定义。给定两个群 A, T，它们的（限制）缠绕积 $A \wr T$定义为半直积 $A^T \rtimes T$。这里，A^T是 A关于指标集 T的直和，称为<style id='12'>基群。也就是说，A^T是序列 $(a_s)_{s \in T}, a_s \in A$的集合，其中对于除有限多个 $s \in T$ 之外的所有 $a_s = 0$。它在逐点乘法下构成一个群。缠绕积 $A \wr T = A^T \rtimes T$是由形如 $((a_s)_{s \in T}, t)$的有序对组成的集合，其中 $(a_s)_{s \in T} \in A^T, t \in T$，其乘法定义为

$$((a_s)_{s \in T}, t) \cdot \left((a'_s)_{s \in T}, t'\right) = \left((a_s a'_{t^{-1}s})_{s \in T}, tt'\right).$$

缠绕积 $A \wr T$自然地包含以下子群：$T \cong \{ ((e_{A^T}, t)) \mid t \in T \}$，其中 e_{A^T}是 A^T的单位元；以及基群 $A^T \cong \{ ((a_s)_{s \in T}, e_T) \mid (a_s)_{s \in T} \in A^T \}$，其中$e_T$ 是 T的单位元。

当 $A = \mathbb{Z}^n$ 和 T 为阿贝尔群时，缠绕积的一个重要特殊情形是：此时，基群 A^T 同构于群环的直幂 $(\mathbb{Z}[T])^n$

$$\mathbb{Z}[T] := \left\{ \sum_{t \in T} z_t t \;\middle|\; z_t \in \mathbb{Z},\ \text{and } z_t = 0 \text{ except for a finite number of } t \right\}.$$

[2]事实上，令 $H = \langle \mathcal{G} \rangle_{grp}$和 $G' = [G, G]$。[25, 定理 9.53] 的证明计算出了 $H \cap G'$作为 $\mathbb{Z}[HG'/G']$-模的一个有限表示，其中使用了 $H \cap G'$的生成元。随后，它利用这一表示计算出 H的一个有限亚交换群表示。该计算使用了 [25, 第 9 节 5], 开头所概述的过程，其中 H 的有限亚交换群表示的生成元是 H 的生成集 $\mathcal{G}$。

这里，$\sum_{t\in T} z_t t$ 表示一个具有有限支集的形式和。于是，缠绕积 $A \wr T$ 变为半直积 $(\mathbb{Z}[T])^n \rtimes T$，由形如 $(y,\ t)$ 的有序对组成，其中 $y \in (\mathbb{Z}[T])^n$，$t \in T$，其乘法定义为 $(y,\ t)\cdot(y',\ t') = (y + t\cdot y',\ tt')$。

此外，如果 $A = \mathbb{Z}^n$ 和 $T = \mathbb{Z}^d$，那么缠绕积 $A \wr T$ 就是方程 (1) 中定义的半直积 $\left(\mathbb{Z}[X_1^{\pm},\dots,X_d^{\pm}]\right)^n \rtimes \mathbb{Z}^d$。Magnus 的以下经典结果给出了将自由群的商群显式嵌入缠绕积的方法。

引理 B.2（Magnus嵌入定理 [4, 引理 2], [27]）。设 F 是由集合 $X = \{x_i \mid i \in I\}$ 自由生成的自由群，且 R 是 F 的正规子群。设映射 $x_i R \mapsto t_i$、$i \in I$ 定义了从 F/R 到由 t_i、$i \in I$ 生成的群 T 的同构。此外，设 A 是由元素 a_i、$i \in I$ 自由生成的自由阿贝尔群。那么映射

$$x_i[R,R] \mapsto a_i t_i,\ \ i \in I,$$

定义了一个从 $F/[R,R]$ 到缠绕积 $W = A \wr T$ 的单射。

回顾一下，半直积 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 以规范方式包含子群 $\mathbb{Z}^n \cong \{(0,\ a) \mid a \in \mathbb{Z}\}$。下一个引理表明，有限生成亚交换群可以有效地嵌入商群 $(\mathcal{Y} \rtimes \mathbb{Z}^n)/H$ 中，其中 H 是 $\mathbb{Z}^n \cong \{(0,\ a) \mid a \in \mathbb{Z}\}$ 的子群。

引理 B.3（[4, 引理 3] G G 的推论）。设 是一个有限生成亚交换群。那么 与商群 $(\mathcal{Y} \rtimes \mathbb{Z}^n)/H$ 的子群 G 同构，其中

(*i*) $n \in \mathbb{N}$ 和 $\mathcal{Y}$ 是一个有限表示的 $\mathbb{Z}[X_1^{\pm},\dots,X_n^{\pm}]$-模。(*ii*) H 是 $\mathbb{Z}^n \le \mathcal{Y} \rtimes \mathbb{Z}^n$ 的子群，且 H 中的元素与 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 中的所有元素交换。(*iii*) 在投影 $\pi\colon (\mathcal{Y} \rtimes \mathbb{Z}^n)/H \to \mathbb{Z}^n/H$ 下，$\pi(G)$ 的像等于 $\mathbb{Z}^n/H$。此外，给定 G 的有限亚交换群表示、整数 n、$\mathcal{Y}$ 的有限表示、H 的生成元以及同构 $G \xrightarrow{\sim} \widetilde{G}$，所有这些对象都可以有效地计算得到。

证明。该引理是对 [4, 引理 3] 的简单推广。我们叙述其证明，以说明其有效性以及条件 (ii) 和 (iii)。

设 $\{g_1,\dots,g_n\}$ 为 G 的生成元，设 F 为由 $x_1,\dots,x_n$ 自由生成的自由群，使得 $M_n = F/[[F,F],[F,F]]$ 且 $G = M_n/\operatorname{ncl}^{M_n}(\widetilde{r_1},\dots,\widetilde{r_m})$ 是 G 的给定有限亚交换群表示。这里，$\widetilde{r_i} = r_i[[F,F],[F,F]], i = 1,\dots,m$，其中 r_i 作为自由群 F 的一个元素给出。设 ϕ 为从 F 到 G 的满同态，其定义为

$$\phi\colon x_i \mapsto g_i,\quad (i = 1,\dots,n).$$

设 K 为 ϕ 的核，设 R 为 $[G,G]$ 在 ϕ 下的原像。由于 $\phi([F,F]) = [G,G]$，我们有 $R = \phi^{-1}([G,G]) = K[F,F]$。此外，$K$ 是由 $r_1,\dots,r_m$ 和 $[[F,F],[F,F]]$ 生成的 F 的正规子群。于是 $R/K \cong [G,G]$，因而是阿贝尔的。因此 $[R,R] \le K$，这意味着

$$[R,R] \le K \le R.$$

现在设 A 是由 a_1、……、a_n 生成的自由阿贝尔群，并考虑缠绕积 $A \wr T$，其中 $T = F/R$。阿贝尔群 T 的结构可以通过 $T = F/R = F/(K[F,F]) \cong (F/[F,F])/(K[F,F]/[F,F])$ 有效地计算出来。换言之，记 $r_j = x_{i_{j1}}^{e_{j1}} \cdots x_{i_{j\ell_j}}^{e_{j\ell_j}}$，$j$ =1、……、m，并记 $t_i = x_i R$，i = 1、……、n，那么 T 是商群 F_{ab}/H，其中 $F_{ab} = F/[F,F]$ 是由 t_1、……、t_n 生成的自由阿贝尔群，而 $H = K[F,F]/[F,F]$ 是由 $t_{i_{j1}}^{e_{j1}} \cdots t_{i_{j\ell_i}}^{e_{j\ell_i}}$，$j = 1$、……、$m$ 生成的 F_{ab} 的子群。

设 ψ 是从 F 到 $A \wr T$ 的同态，定义为

$$\psi(x_i) = a_i t_i, \quad (i = 1, \ldots, n).$$

根据引理 B.2， ψ的核是 $[R, R]$。因此， ψ诱导出一个同构 ψ_*： $x_i[R, R] \mapsto a_i t_i$，将$F/[R, R]$ 映入 $A \wr T$。

我们令 $N = \psi_*\left(K/[R, R]\right)$ 。现在 $N \leq \psi_*\left(F/[R, R]\right)$ 。因此， N被元素 $a_i t_i$， $i = 1$，... ...， n正规化。但由 ψ_*的定义可知， N包含在 $A \wr T$的基群 $B = A^T$ 中。由于 B 是阿贝尔群， N 被 B 正规化，因而也被元素t_i正规化，所以被 $A \wr T$中的所有元素正规化。换言之， N 是正规子群，并由$\psi_*\left(r_1[R, R]\right)$ ....., $\psi_*\left(r_m[R, R]\right)$ 正规生成。这是因为 $N = \psi_*\left(K/[R, R]\right)$ ，且 K 由r_1，....., r_m 以及集合 $[[F, F], [F, F]] \leq [R, R]$正规生成。注意

$$\psi_*(r_j[R, R]) = \left(a_{i_{j_1}} t_{i_{j_1}}\right)^{e_{j_1}} \cdots \left(a_{i_{j_{\ell_j}}} t_{i_{j_{\ell_j}}}\right)^{e_{j_{\ell_j}}}, j = 1, \ldots, m. \tag{43}$$

现在， G通过映射 $g_i \mapsto a_i t_i N$同构于 $(A \wr T) /N$的子群 $G := \psi_*(F/[R, R])/N$。

注意， $(A \wr T) /N = \left(A^T/N\right) \rtimes T$，其中 N是正规子群，因此 N是由$\psi_*(r_1[R, R]) \ldots, \psi_*(r_m[R, R])$ 生成的 $\mathbb{Z}[T]$-模。此外，由于 G 包含元素 $a_i t_i N, i = 1, \ldots, n$，其在 T上的投影包含元素 $t_i, i = 1, \ldots, n$，因此就是 T本身。

我们记 $T = F_{ab}/H = \mathbb{Z}^n/H$ ，因为 F_{ab} 是由 n 个生成元生成的自由阿贝尔群。典范投影 $\mathbb{Z}^n \to T$ 诱导出环同态 $\mathbb{Z}[\mathbb{Z}^n] \to \mathbb{Z}[T]$，因此 $\mathbb{Z}[T]$-模A^T/N自然也是一个 $\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}] = \mathbb{Z}[\mathbb{Z}^n]$-模，其中形如 X^h、 $h \in H$的元素作用平凡。取 $\mathcal{Y} := A^T/N$，我们将 $\mathcal{Y} = A^T/N$视为一个 $\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}]$-模，并据此定义半直积 $\mathcal{Y} \rtimes \mathbb{Z}^n$。我们证明， H中的元素与 $\mathcal{Y} \rtimes \mathbb{Z}^n$中的每个元素交换。这是相当直接的：由于形如 X^h、 $h \in H$的元素在 $\mathcal{Y} = A^T/N$上的作用平凡，我们有 $(0, h)(y, a)(0, h^{-1}) = (X^h \cdot y, a) = (y, a)$。因此， H中的元素与 $\mathcal{Y} \rtimes \mathbb{Z}^n$中的每个元素交换，从而证明了 (ii)。更进一步，这说明 H 是 $\mathcal{Y} \rtimes \mathbb{Z}^n$的正规子群。

最后，我们有

$$\widetilde{G} = \left(A^T/N\right) \rtimes T = \mathcal{Y} \rtimes \left(\mathbb{Z}^n/H\right) = \left(\mathcal{Y} \rtimes \mathbb{Z}^n\right)/H,$$

并且，(iii) 直接由投影 $\widetilde{G} = \left(A^T/N\right) \rtimes T \to T = \mathbb{Z}^n/H$具有满像这一事实得到。现在我们证明， $\mathcal{Y} = A^T/N$ 可以有效地写成一个有限表示的$\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}]$-模。首先，我们按以下方式将 A^T写成一个有限表示的 $\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}]$-模。令 h_1、.....、 h_m为 H作为 $\mathbb{Z}^n$的子群的生成元。由于 $A \cong \mathbb{Z}^n$，我们有$A^T = (\mathbb{Z}[T])^n$，并且 $\mathbb{Z}[T]$是 $\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}] = \mathbb{Z}[\mathbb{Z}^n]$关于由元素 $X^{h_i} - 1$、 $i = 1$、.....、 m生成的理想的商群。因此，我们得到 $\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}]$-模$\mathbb{Z}[T]$的一个有限表示，并由此得到模 $A^T = (\mathbb{Z}[T])^n$的一个有限表示。 $N \subseteq A^T$作为 $\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}]$-模的生成元与其作为 $\mathbb{Z}[T]$-模的生成元相同，这些生成元由 (43) 中的元素给出。因此，我们得到 $\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}]$-模 $\mathcal{Y} = A^T/N$的一个有限表示，(i) 得证。

□

因此，我们可以假设 G 是 $\left(\mathcal{Y} \rtimes \mathbb{Z}^n\right)/H$ 的一个子群，而生成元集合 $\mathcal{G}$ 是 $\left(\mathcal{Y} \rtimes \mathbb{Z}^n\right)/H$的一个子集。记作 $\mathcal{G} = \{g_1 H, \ldots, g_k H\}$，其中 g_1， ... ， g_k 是 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 的元素，并令 h_1， ... ， h_M 为 $H \subseteq \mathcal{Y} \rtimes \mathbb{Z}^n$ 作为半群的生成元。于是

引理 B.4。 半群 $\langle \mathcal{G} \rangle$ 是群，当且仅当由 g_1、.....、 g_k、h_1、.....、 $h_M \in \mathcal{Y} \rtimes \mathbb{Z}^n$ 生成的半群是群。

Proof. 假设 $\langle \mathcal{G} \rangle$ 是群。那么根据引理 2.1，存在一个满像 word

$$w = g_{i_1} H g_{i_2} H \cdots g_{i_p} H$$

在字母表 $\mathcal{G}$ 上表示 $(\mathcal{Y} \rtimes \mathbb{Z}^n)/H$ 中单位元的词。由于 H 的元素与 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 的每个元素都可交换，这意味着 $g_{i_1} g_{i_2} \cdots g_{i_p} \in H$。因此，存在一个字母表 $\mathcal{H}$ 上的词 $v := \{h_1, \ldots, h_M\}$，使得 $g_{i_1} g_{i_2} \cdots g_{i_p} \cdot v$ 表示 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 中的单位元。由于 $\mathcal{H}$ 作为半群生成群 H，存在一个字母表 $\mathcal{H}$ 上表示 $H \leq \mathcal{Y} \rtimes \mathbb{Z}^n$ 的单位元的满像词 v'。于是，词 $g_{i_1} g_{i_2} \cdots g_{i_p} \cdot v \cdot v'$ 是字母表 $\{g_1, \ldots, g_k, h_1, \ldots, h_M\}$ 上的满像词，并且表示 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 中的单位元。根据引理 2.1，由 $\{g_1, \ldots, g_k, h_1, \ldots, h_M\}$ 生成的半群是一个群。

对于另一个蕴含方向，现设由 $\{g_1, \ldots, g_k, h_1, \ldots, h_M\}$ 生成的半群是一个群。根据引理 2.1，存在一个在字母表 $\{g_1, \ldots, g_k, h_1, \ldots, h_M\}$ 上的满像词 $\widetilde{w}$，表示单位元。由于元素 $h_1, \ldots, h_M$ 与所有其他元素交换，我们可以将它们移到 $\widetilde{w}$ 的最右侧，并设

$$\widetilde{w} = g_{i_1} g_{i_2} \cdots g_{i_p} h_{j_1} h_{j_2} \cdots h_{j_q}.$$

则词 $g_{i_1} H \cdot g_{i_2} H \cdot \cdots \cdot g_{i_p} H$ 是字母表 $\mathcal{G}$ 上的满像词，并表示 $(\mathcal{Y} \rtimes \mathbb{Z}^n)/H$ 的单位元。根据引理 2.1，半群 $\langle \mathcal{G} \rangle$ 是一个群。 □

命题 2.4 由引理 B.1、B.3 和 B.4 得出：

命题 2.4。 设给定群 G 的有限亚交换群表示以及有限集合 $\mathcal{G} \subseteq G$。可以有效地构造一个有限表示的 $\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}]$-模 $\mathcal{Y}$，使得对于某个 $n \in \mathbb{N}$，以及群 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 的一个子集 $\mathcal{G}$，满足 $\langle \mathcal{G} \rangle$ 是一个群当且仅当 $\sim\langle \mathcal{G} \rangle$ 是一个群。此外，在典范投影 $\pi\colon \mathcal{Y} \rtimes \mathbb{Z}^n \to \mathbb{Z}^n$ 下，所构造的集合 $\mathcal{G}$ 满足 $\pi(\langle \mathcal{G} \rangle_{grp}) = \mathbb{Z}^n$。

证明。 根据引理 B.1，我们可以计算出群 $\langle \mathcal{G} \rangle_{grp}$ 的有限元后承表示。由于生成元 $\mathcal{G}$ 在此表示下已明确给出，不妨设 $G = \langle \mathcal{G} \rangle_{grp}$。根据引理 B.3，$G$ 可以有效地嵌入商群 $(\mathcal{Y} \rtimes \mathbb{Z}^n)/H$ 的一个子群中，其中 H 是 $\mathbb{Z}^n \leq \mathcal{Y} \rtimes \mathbb{Z}^n$ 的子群，并且 H 中的元素与 $\widetilde{\ }$ 的所有元素 $\mathcal{Y} \rtimes \mathbb{Z}^n$ 交换。因此，不妨设 $G = G$ 是 $(\mathcal{Y} \rtimes \mathbb{Z}^n)/H$ 的子群，且生成元集合 $\mathcal{G}$ 给定为 $\{g_1 H, \ldots, g_k H\}$，其中 $g_1, \ldots, g_k \in \mathcal{Y} \rtimes \mathbb{Z}^n$。设 $h_1, \ldots, h_M$ 是 $H \subseteq \mathcal{Y} \rtimes \mathbb{Z}^n$ 作为一个半群的生成元。

Let $\widetilde{\ }$ 投影 $\{g_1, \ldots, g_k, h_1, \ldots, h_M\} \subseteq (\mathcal{Y} \rtimes \mathbb{Z}^n)/H$ 下等于 根据引理 B.3，$\langle \mathcal{G} \rangle_{grp}$ 的像生成 H 这个 $\widetilde{\ }$ 半群，因此由 $\mathcal{G}$ 生成的群在典范投影 $\mathcal{Y} \rtimes \mathbb{Z}^n \to \mathbb{Z}^n$ 下的像为 $(\mathbb{Z}^n/H) + H = \mathbb{Z}^n$。最后，根据引理 B.4，半群 $\langle \mathcal{G} \rangle$ 是群，当且仅当由 $\mathcal{G}$ 生成的 $\widetilde{\ }$ 半群是群。命题得证。

□

C 第 3 节中省略的证明

命题 3.4。 半群 $\langle \mathcal{G} \rangle$ 是群，当且仅当存在一个表示单位元的满像对称面可达 $\mathcal{G}$-图。

证明。 根据引理 2.8 和观察 3.2，只需证明“如果”方向。设 Γ 是一个表示单位元的满像对称面可达 $\mathcal{G}$-图，我们构造一个表示单位元的满像欧拉 $\mathcal{G}$-图。根据定理 3.3，存在

$\widehat{\ }$ $\sim z_1$、.....、 $z_m \in \mathbb{Z}^n$，使得 $\Gamma := \bigcup_{i=1}^m ($ $\Gamma + z_i)$ 是一个欧拉图。由于 Γ 包含 Γ 的一个平移$\widehat{\ }$，因此它是满像的。每个平移 $\Gamma + z_i$ 都表示元素 $X^{z_i} \cdot 0 = 0$，所以并集 Γ 也表示单位元。 □

命题 3.5。设 Γ 是一个 $\mathcal{G}$-图，其位置多项式为 $f_i \in \mathbb{N}[X^{\pm}]$、$i = 1$、.....、$K$。

(i) Γ 是满像的，当且仅当对于 $i = 1$、.....、K，$f_i \neq 0$。
(ii) Γ 是对称的，当且仅当 $\sum_{i=1}^K f_i \cdot \overline{(X^{a_i} - 1)} = 0$。*(iii)* Γ 是面可达的，当且仅当

$$O_v \cap M_v(\{1, \ldots, K\}, \boldsymbol{f}) \neq \emptyset \quad \textit{for every } v \in (\mathbb{R}^n)^* . \tag{5}$$

(iv) 假设 Γ 是对称的。当且仅当 $\sum_{i=1}^K f_i \cdot y_i = 0$ 时，Γ 表示单位元。

证明。(i) Γ 是满像的，当且仅当每个标签至少出现一次，即对于所有 i，$f_i \neq 0$。(ii) 我们有

$$\sum_{i=1}^K f_i \cdot (\overline{X}^{a_i} - 1) = \sum_{i=1}^K \sum_{e \in E(\Gamma), \ell(e) = i} \overline{X}^{s(e)} (\overline{X}^{a_i} - 1) = \sum_{i=1}^K \sum_{e \in E(\Gamma), \ell(e) = i} (\overline{X}^{s(e) + a_i} - \overline{X}^{s(e)})$$
$$= \sum_{e \in E(\Gamma)} (\overline{X}^{d(e)} - \overline{X}^{s(e)}) = \sum_{e \in E(\Gamma)} \overline{X}^{d(e)} - \sum_{e \in E(\Gamma)} \overline{X}^{s(e)}.$$

这等于零，当且仅当每个顶点处的入度等于出度 x.

(iii) 令 C 为 $V(\Gamma)$ 的凸包。对于 C 的每个真面 F，存在一个向量 $v \in (\mathbb{R}^n)^*$，使得 F 由 C 中满足 $v \cdot x$ 为最大的所有点 x 组成。反之，对于每个向量 $v \in (\mathbb{R}^n)^*$，F （即 C 中满足 $v \cdot x$ 为最大的所有点 x 的集合）构成 C 的一个真面。

设 F 为一个真面，则当且仅当从 F 出发的某条边不以 F 为终点时，F 是可达的。设 e 是一条从 F 出发、标签为 $\ell(e)$ 的边。则 $v \cdot s(e)$ 在所有 $e \in E(\Gamma)$ 中是最大的。由于单项式 $X^{s(e)}$ 包含于 $f_{\ell(e)}$ 中，这意味着 $\ell(e) \in M_v(\{1, \ldots, K\}, \boldsymbol{f})$。

注意到，当且仅当 $a_{\ell(e)} = d(e) - s(e)$ 与 v 正交时，$d(e) \in F$，这等价于 $\ell(e) \notin O_v$。因此，当且仅当存在一条边 e，使得 $\ell(e) \in M_v(\{1, \ldots, K\}, \boldsymbol{f})$ 且 $\ell(e) \in O_v$ 时，F 是可达的；也就是说，$O_v \cap M_v(\{1, \ldots, K\}, \boldsymbol{f}) \neq \emptyset$。

根据面可达性的定义，Γ 是面可达的，当且仅当对于每个 $v \in (\mathbb{R}^n)^*$，$O_v \cap M_v(\{1, \ldots, K\}, \boldsymbol{f}) \neq \emptyset$ 成立。

(iv) 假设 Γ 是对称的，则 $\sum_{e \in E(\Gamma)} a_{\ell(e)} = 0$。根据方程（3），$\Gamma$ 表示元素

$$\left(\sum_{e \in E(\Gamma)} \overline{X}^{s(e)} \cdot y_{\ell(e)}, \sum_{e \in E(\Gamma)} a_{\ell(e)} \right) = \left(\sum_{i=1}^K \sum_{e \in E(\Gamma), \ell(e) = i} \overline{X}^{s(e)} \cdot y_i, 0 \right) = \left(\sum_{i=1}^K f_i \cdot y_i, 0 \right),$$

当且仅当 $\sum_{i=1}^K f_i \cdot y_i = 0$时，它是单位元。 □

引理 3.6. 可以根据 $y_i, a_i, i = 1, \ldots, K$计算出 $\mathbb{Z}[X^{\pm}]$-模 $\mathcal{M}_{\mathbb{Z}}$ 的有限生成元集 $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m \in \mathbb{Z}[X^{\pm}]^K$。

证明。回忆一下，$\mathcal{Y}$ 被给定为商群 M/N，其中 N 和 M 分别是由 $\boldsymbol{m}_1, \ldots, \overline{\boldsymbol{m}}_{\ell'}$ 和 $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_\ell \in \mathbb{Z}[\overline{X}^{\pm}]^d$ 生成的 $\mathbb{Z}[X^{\pm}]$-子模。对于 $i = 1, \ldots, K$，元素 $\underline{y_i}$被给定为 $y_i = \overline{\widetilde{\boldsymbol{y}}_i} + N$，其中 $\widetilde{\boldsymbol{y}}_i \in M \subseteq \mathbb{Z}[X^{\pm}]^d$。

方程 $\sum_{i=1}^{K} f_i \cdot y_i = 0$ 可以写成 $\sum_{i=1}^{K} f_i \cdot \widetilde{\boldsymbol{y}}_i \in N$，这等价于

$$\sum_{i=1}^{K} f_i \cdot \widetilde{\boldsymbol{y}}_i = \sum_{j=1}^{\ell} g_j \cdot \boldsymbol{n}_j \text{ for some } g_1, \ldots, g_\ell \in \mathbb{Z}[\overline{X}^{\pm}]. \tag{44}$$

令 $\widetilde{\mathcal{M}}$ 为以下齐次线性方程组的解集（f_1，…，f_K，g_1，…，g_ℓ）$\in \mathbb{Z}[X^{\pm}]^{K+\ell}$：

$$\sum_{i=1}^{K} f_i \cdot \widetilde{\boldsymbol{y}}_i - \sum_{j=1}^{\ell} g_j \cdot \boldsymbol{n}_j = 0$$
$$\sum_{i=1}^{K} f_i \cdot (\overline{X}^{a_i} - 1) = 0.$$

集合 $\mathcal{M}$ 也称为 Syzygy 模。线性代数中的经典结果表明，在诺特环上，可以有效地计算出 $\mathcal{M}$ 的有限生成元集（$\boldsymbol{f}_1$，$\boldsymbol{g}_1$）…，（$\boldsymbol{f}_s$，$\boldsymbol{g}_s$）（见 [10, 36] 或 [18, 定理 15.10]）。令 $\pi\colon \mathbb{Z}[X^{\pm}]^{K+\ell} \to \mathbb{Z}[X^{\pm}]^{K}$，（$f_1$，…，$f_K$，$g_1$，…，$g_\ell$）$\mapsto$（$f_1$，…，$f_K$）为投影到前 K 个坐标的投影。则 $\mathcal{M}_{\mathbb{Z}} = \pi(\mathcal{M})$，而 $\mathcal{M}_{\mathbb{Z}}$ 的有限生成元集就是 $\{\pi((\boldsymbol{f}_1, \boldsymbol{g}_1)), \ldots, (\pi(\boldsymbol{f}_s, \boldsymbol{g}_s))\} = \{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s\}$。

□

引理 3.7。存在满足性质（7）的元素 $\widetilde{\boldsymbol{f}} \in \mathcal{M}_{\mathbb{Z}} \cap \left(\mathbb{N}[X^{\pm}]^*\right)^K$，当且仅当存在满足性质（7）的 $\boldsymbol{f} \in \mathcal{M} \cap \left(\mathbb{R}_{\geq 0}[X^{\pm}]^*\right)^K$。

证明。满足性质（7）的元素 $\widetilde{\boldsymbol{f}} \in \mathcal{M}_{\mathbb{Z}} \cap \left(\mathbb{N}[X^{\pm}]^*\right)^K$ 显然是 $\mathcal{M} \cap \left(\mathbb{R}_{\geq 0}[X^{\pm}]^*\right)^K$ 中的一个元素。因此，只需证明“若”蕴含。

设有一个满足性质（7）的元素 $\boldsymbol{f} \in \mathcal{M} \cap \left(\mathbb{R}_{\geq 0}[X^{\pm}]^*\right)^K$，我们证明存在一个满足性质（7）的元素 $\widetilde{\boldsymbol{f}} \in \mathcal{M}_{\mathbb{Z}} \cap \left(\mathbb{N}[X^{\pm}]^*\right)^K$。

写成 $\boldsymbol{f} = (f_1, \ldots, f_K)$，其中对于 $i = 1, \ldots, K$，

$$f_i = \sum_{b \in B_i} c_{i,b} \overline{X}^b.$$

这里，支集 B_i 是 $\mathbb{Z}^n$ 的非空有限子集，并且对于所有 $b \in B_i$，$c_{i,\,b} \in \mathbb{R}_{>0}$。由于性质（7）只取决于支集 $B_1, \ldots, B_K$，因此只需证明存在 $\boldsymbol{f} = (\widetilde{f}_1, \ldots, \widetilde{f}_K) \in \mathcal{M}_{\mathbb{Z}} \cap \left(\mathbb{N}[X^{\pm}]^*\right)^K$，使得

$$\widetilde{f}_i = \sum_{b \in B_i} \widetilde{c}_{i,b} \overline{X}^b$$

并且对于所有 $b \in B_i$，$\widetilde{c}_{i,\,b} \in \mathbb{Z}_{>0}$。

由于 $\boldsymbol{f} \in \mathcal{M}$，对于某些 $h_1, \ldots, h_m \in \mathbb{R}[X^{\pm}]$，我们有 $\boldsymbol{f} = \sum_{j=1}^{m} h_j \cdot \boldsymbol{g}_j$。对于每个 $j \in \{1, \ldots, m\}$，写成 $h_j = \sum_{b \in H_j} h_{j,\,b} X^b$，其中 H_j 是 $\mathbb{Z}^n$ 的有限子集。于是，方程 $\boldsymbol{f} = \sum_{j=1}^{m} h_j \cdot \boldsymbol{g}_j$ 可以改写为 $\mathbb{R}$ 上的有限线性方程组，其中左端为 0 或 $c_{i,\,b}$，$b \in B_i$，$i = 1, \ldots, K$，右端是变量 $h_{j,\,b}$，$j \in \{1, \ldots, m\}$，$b \in H_j$ 的 $\mathbb{Z}$-线性组合（因为对于所有 j，$\boldsymbol{g}_j$ 的系数都是整数）。

由于这个线性方程组是齐次的，且系数全都属于 $\mathbb{Z}$，因此它有解 $h_{j,\,b} \in \mathbb{R}$，$j \in \{1, \ldots, m\}$，$b \in H_j$ 和 $c_{i,\,b} \in \mathbb{R}_{>0}$，$b \in B_i$，$i = 1, \ldots, K$，当且仅当它有

一个解，使得对于所有 i, j, b，$h_{j,b} \in \mathbb{Q}, c_{i,b} \in \mathbb{Q}_{>0}$ 均成立。将所有 $h_{j,b}, c_{i,b}$ 乘以它们的公分母后，我们得到一个解 $\widetilde{h}_{j,b} \in \mathbb{Z}, \widetilde{c}_{i,b} \in \mathbb{Z}_{>0}$，适用于所有 i, j, b。于是，$\widetilde{f}_i := \sum_{b \in B_i} \widetilde{c}_{i,b} X^b, i = 1, \ldots, K$ 和 $\widetilde{h}_j = \sum_{b \in H_j} \widetilde{h}_{j,b} X^b, j = 1, \ldots, m$ 满足 $\widetilde{\boldsymbol{f}} = \sum_{j=1}^{m} \widetilde{h}_j \cdot \boldsymbol{g}_j$。因此，$\widetilde{\boldsymbol{f}} = (\widetilde{f}_1, \ldots, \widetilde{f}_K) \in \mathcal{M}_{\mathbb{Z}} \cap \left(\mathbb{N}[\overline{X}^{\pm}]^*\right)^K$。元素 $\widetilde{\boldsymbol{f}}$ 满足性质（7），因为条件仅取决于支集 $B_1, \ldots, B_K$。

□