arXiv:2303.02037v1 [math.NT] 3 Mar 2023

代数数的对数矩阵的秩 I：Baker 和 Waldschmidt–Masser 定理

Samit Dasgupta

2023年3月6日

摘要

令 $\mathscr{L}$ 表示代数数的对数所构成的 Q-向量空间。在这篇综述性文章中，我们介绍对系数属于 $\mathscr{L}$ 的矩阵秩的研究。我们首先考虑一个略有不同的问题，即给出 Baker定理的一种弱形式的证明。该定理指出， $\mathscr{L}$ 中一组元素若在 Q 上线性无关，则事实上在 Q 上线性无关。接着，我们回顾 Schanuel猜想，并证明它在 C((*t*)) 上的 Ax类比。

然后，我们考虑系数属于 $\mathscr{L}$ 的任意矩阵，并陈述“结构秩猜想”，该猜想给出了系数属于 $\mathscr{L}$ 的一般矩阵秩的猜想。我们证明 Waldschmidt 和 Masser 定理，该定理给出了一个下界，为结构秩猜想提供了部分结果。最后，我们陈述一个新的猜想，称为矩阵系数猜想；它给出了系数属于 $\mathscr{L}$ 的方阵为奇异矩阵的一个必要条件。

目录

1 引言 **2**

2 Baker定理 **4**

2.1 辅助多项式的构造.6 2.2 Baker 引理.10 2.3 代数整数的离散性.11 2.4 逐步推进.12

3 阿克斯定理 **13**

3.1 导子.14 3.2 Kähler微分上的导子.15

4 StructuralRank 猜想 19
4.1 p-进设置.20 4.2 数论中的应用.21 4.2.1 Leopoldt猜想.21 4.2.2 Gross–Kuz'min 猜想.23 4.2.3 表示论考量.24 4.3 Roy定理.25

5 Waldschmidt和Masser定理 28
5.1 应用.28 5.2 辅助多项式.30 5.3 Waldschmidt 定理.31 5.3.1 Waldschmidt 定理的证明 1.31 5.3.2 Waldschmidt 定理的证明 2.33 5.4 Masser 定理.36

6 矩阵系数猜想 43

1 引言

在1900年的国际数学家大会上，David Hilbert提出了23个未解决问题，这些问题一直激励着一代又一代的数学家。作为其问题列表中的第7个问题，Hilbert提出了以下问题：

Hilbert第七问题。设 a、$b \in \mathbf{Q}$，且 $\overline{a} \neq 0$、1 和 $b \notin \mathbf{Q}$。值 a^b 是否必为超越的?

Gelfond（1934年）和Schneider（1935年）分别独立证明了Hilbert的问题具有肯定答案。Gelfond–Schnieder定理也可等价地表述如下。设

$$\mathscr{L} = \{x \in \mathbf{C} \colon e^x \in \overline{\mathbf{Q}}\}$$

表示由代数数的对数组成的Q-向量空间。

定理 1.1（格尔丰德–施奈德）。如果 $\mathscr{L}$ 中的两个元素在 Q 上线性相关，那么它们在 $\overline{\mathbf{Q}}$ 上线性相关。

30 年后，艾伦·贝克取得了一项了不起的突破 [3], ，他将两个元素推广到了 $\mathscr{L}$ 中任意数量的元素。

定理 1.2（Baker，1966年）。如果 $n \geq 1$ 的元素在 $\mathscr{L}$ 上线性相关，那么它们在 $\overline{\mathbf{Q}}$ 上线性相关。

事实上，Baker 证明了这一结果的一个有效加强形式，为 $\mathscr{L}$ 中在 Q 上线性无关的元素的任意代数线性组合的大小给出了一个很强的下界。在本文中，我们将给出 Baker定理 一个略弱于定理 1.2 的版本的证明。

接下来，我们将关注点从单个对数线性形式转向 $\mathscr{L}$ 中的任意矩阵。这一方向的主要猜想是结构秩猜想。在应用中，考虑由 $\mathscr{L}$ 和有理数域 Q 张成的 Q-向量空间往往很有用，我们将其记为 $\mathscr{L}+\mathbf{Q}$。给定一个系数属于任意特征为零的域的 $m\times n$矩阵 M，我们如下定义 M 的结构秩。选取一个 Q-基 $\ell_1,\dots,\ell_r$，使其张成 M 的系数，并写作 $M=\sum_{i=1}^{r}\ell_i M_i$，其中 $M_i\in M_{m\times n}(\mathbf{Q})$。写作 $M_x=\sum_{i=1}^{r}x_i M_i$，其中的$x_i$是不定元。于是，$M_x$是一个系数属于有理函数域 $F=\mathbf{Q}(x_1,\dots,x_n)$ 的 $m\times n$ 矩阵。我们将 M 的结构秩定义为 M_x 在F 上的秩。可以验证，这一定义与所选基 ℓ_i 无关。

猜想 1.3（结构秩猜想）。矩阵 $M\in M_{m\times n}(\mathscr{L}+$有理数域) 的秩等于 M 的结构秩。

对代数数的对数和指数函数的特殊值的超越数理论而言，“终极猜想”是以下Schanuel猜想。

猜想 1.4。设 y_1，……，$y_n\in$复数域 线性无关。则

$$\operatorname{trd}_{\mathbf{Q}}\mathbf{Q}(y_1,\dots,y_n,e^{y_1},\dots,e^{y_n})\geq n.$$

特别地，如果 y_1，……，$y_n\in\mathscr{L}$ 线性无关，则

$$\operatorname{trd}_{\mathbf{Q}}\mathbf{Q}(y_1,\dots,y_n)=n. \tag{1}$$

Schanuel猜想在（1）中给出的特殊情形蕴含结构秩猜想，这或许并不令人惊讶；然而，Roy定理的一个优美结论是，反之亦然。

定理 1.5（Roy）。结构秩猜想等价于（1）中给出的 Schanuel猜想的特殊情形。

定理 1.5 在第4节中得到证明。关于结构秩猜想，最有力的无条件证据是以下Waldschmidt和Masser 定理。

定理 1.6（Waldschmidt–Masser）。设 $M\in M_{m\times n}(\mathscr{L})$。假设

$$rank(M)<mn/(m+n)$$

于是存在 $P\in\mathrm{GL}_m(\mathbf{Q})$ 和 $Q\in\mathrm{GL}_n(\mathbf{Q})$，使得 $PMQ=\begin{pmatrix}M_1 & 0\\ M_2 & M_3\end{pmatrix}$ 其中零块的维数为 $m'\times n'$，且 $m'/m+n'/n>1$。

超越性结果在代数数论中有许多重要应用。尤其是在岩泽理论中，这些论述的 p-进类比最为相关。例如，Leopoldt猜想关注数域 F 中一组单位基的 p-进对数矩阵的秩。Waldschmidt–Masser 定理的 p-进类比为这一猜想提供了最有力的依据。比如，对于全实域 F，可以推知 Leopoldt 矩阵的秩至少达到预期值的一半。我们在 §5 证明 Walsdschmidt–Masser 定理的 p-进版本，因为文献中对阿基米德情形的研究更为常见。

致谢。我谨向 Damien Roy 致以衷心的感谢；他详细审阅了本文的早期草稿，并提出了许多宝贵建议，大大改进了文章的阐述。我还要感谢 Mahesh Kakde，我与他合作并在他的帮助下学习了这些材料；同时也感谢 Michel Waldschmidt 的有益讨论。我们非常感谢 Alan Harper；对于 Baker定理，我们遵循了他的论述 [11]；也感谢 Eric Stansifer，他的论述 [18] 对我们讨论 Waldschmidt–Masser 定理产生了很大影响。

本笔记源于我在 2020年春季于杜克大学在线讲授的一门专题课程；我感谢参加课程的各位同学所进行的热烈讨论。

2 Baker定理

在概述 Baker定理的证明之前，让我们先讨论一下如何有望推导出该定理的结论。给定代数数 α_1，……，$\alpha_n \in$ 有理数域*、复数 x_i，满足 $e^{x_i} = \alpha_i$，以及一个线性相关关系

$$\beta_1 x_1 + \cdots + \beta_n x_n = 0 \tag{2}$$

与 $\beta_i \in \mathbb{Q}$ 一起。我们将证明，这意味着存在整数 λ_1、……、λ_n，且不全为零，使得

$$\alpha_1^{\lambda_1} \alpha_2^{\lambda_2} \ldots \alpha_n^{\lambda_n} = 1. \tag{3}$$

这意味着 x_i 与复数 $2\pi i$ 在 $\mathbb{Q}$ 上线性相关。因此，我们将要证明的 Baker定理的一个稍弱版本如下：

定理 2.1。如果 x_1、$\ldots x_n$、$2\pi i \in \mathscr{L}$ 在 $\mathbb{Q}$ 上线性无关，那么 x_1、……、x_n 在 $\mathbb{Q}$ 上线性无关。

除了我们将介绍的方法之外，只需稍加努力，便可去掉 $2\pi i$，并证明上述定理 1.2 中所述的 Baker定理版本。不过，为了简化论述并突出要点，我们在定理 2.1 的证明中加入了 $2\pi i$。

那么，如何从 β_i 的存在性推导出 λ_i 的存在性呢？人们或许会很想证明 λ_i 可以取为等于 β_i，也就是说， β_i 是有理数（或者更一般地说，可以通过某种直接方式从 β_i 中提取出 λ_i ）。然而，实践中采用更间接的方法更为有效。

定理 2.2。设 α_1，……， $\alpha_n \in \mathbf{C}^*$。假设存在一个非零多项式

$$f(t_1, \ldots, t_n) \in \mathbf{C}[t_1, \ldots, t_n]$$

其关于每个变量 t_i 的次数为 $\leq L$ ，使得

$$f(\alpha_1^z, \ldots, \alpha_n^z) = 0$$

对于 $z = 1$、2、……、$(L+1)^n$。那么存在整数 λ_1、……、 λ_n，且不全为零，使得

$$\alpha_1^{\lambda_1} \alpha_2^{\lambda_2} \ldots \alpha_n^{\lambda_n} = 1.$$

*Pr*证明。考虑方阵 M ，其行由整数标记 s

$$z = 1, \ldots, (L+1)^n$$

其列由整数的元组 $\lambda = (\lambda_1, \ldots\ldots, \lambda_n)$ 标记，其中 $0 \leq \lambda_i \leq L$，相应的矩阵元素为

$$\alpha^{\lambda z} := \alpha_1^{\lambda_1 z} \cdots \alpha_n^{\lambda_n z}.$$

多项式 f 的存在等价于存在一个列向量 v ，使得 $Mv = 0$。事实上， v 的各个分量恰好是 f 的系数。

因此， f 非零的存在意味着 $\det(M) = 0$。但是， M 是与元素 $\alpha^\lambda = \alpha_1^{\lambda_1} \cdots \alpha_n^{\lambda_n}$相关联的范德蒙德矩阵，其中元组 λ 遍历所有 $(L+1)^n$ 种可能。因此，行列式为零意味着存在两个不同的元组 λ, λ' ，使得 $\alpha^\lambda = \alpha^{\lambda'}$。因此，我们得到了所需的 $\alpha^{\lambda - \lambda'} = 1$ 。 □

因此，Baker定理的核心是利用方程 (2) 构造一个辅助多项式 f ，使其满足定理 2.2 的条件。我们先概述 Baker 构思巧妙的这一方法。

1. 狄利克雷盒子原理是运用鸽巢原理构造具有某些指定零点的多项式 f 的一种方法。我们可以将其应用于定理 2.2 的陈述中出现的元素 α^z。当然，这种方法得到的多项式零点数不会足够多（也就是说，我们可能会对某个 A找出 $z = 1$、……、 A的零点，但 A 会小于 $(L+1)^n$ ）。Baker 的巧妙洞见在于，条件 (2) 使我们能够确保 f 的某些导数也在与这些 z相对应的值处为零。

2. 随后，Baker 证明了一个复分析引理。该引理是经典施瓦茨引理的定量强化，它表明，f 及其许多导数为零，意味着 f 及其数量只有一半的导数的大小具有一个很强的上界；不过，这一结论适用于数量为其 B 倍的整数 z（其中 $B > 1$ 取决于一些参数，我们稍后会对这些参数作出明确说明）。

3. 利用 α_i 和 β_i 是代数数这一事实，Baker 推出这些有界值（即 f 的值，以及当 $z = 1, \ldots, AB$ 时其许多导数的值）实际上必定为 0。其基本思想是，绝对值小于 1 的整数必定为零；将这一初等结论推广到次数和高度有界的代数数后，即可应用。

4. 有了更多的零值之后，我们回到第 2 步，再次证明，对于另一个因子 B 倍数量的 z 个值，有一半数量的导数很小。我们重复这一过程 N 次，直到 $AB^N > (L+1)^n$，从而证明辅助多项式 f 有足够多的零点，可以应用定理 2.2。

本节余下部分将详细介绍这些步骤。

2.1 辅助多项式的构造

对于每个 α_i，令 c_i 表示 α_i的整最小多项式的首项系数，并令 d 表示任意 α_i的最高次数。

Lemma 2.3. 存在整数 $a_{i,j,s}$，使得对每个整数 $j \geq 0$，都有

$$(c_i\alpha_i)^j = \sum_{s=0}^{d-1} a_{i,j,s}\alpha_i^s.$$

证明。为简化记号，我们省略下标 i。因此，我们考虑次数至多为 d 的 $\alpha \in \overline{\mathbb{Q}}$，并令 c 表示 α 的整最小多项式的首项系数。于是存在整数 $b_0, \ldots, b_{d-1}$，使得

$$c\alpha^d = b_{d-1}\alpha^{d-1} + \cdots + b_1\alpha + b_0. \tag{4}$$

我们对 j 使用归纳法证明该结论。基例 $0 \leq j < d$ 显然成立。对于 $j \geq d$，我们假设根据归纳法，存在整数 $a_{j-1,s}$，使得

$$(c\alpha)^{j-1} = \sum_{s=0}^{d-1} a_{j-1,s}\alpha^s.$$

两边乘以 $c\alpha$，得到

$$(c\alpha)^j = \left(\sum_{s=0}^{d-2} c \cdot a_{j-1,s}\alpha^{s+1}\right) + a_{j-1,d-1}(c\alpha^d). \tag{5}$$

将 (4) 中的 $c\alpha^d$ 代入 (5) 右侧，得到所需的表达式

$$(c\alpha)^j = \sum_{s=0}^{d-1} a_{j,s}\alpha^s$$

其中

$$a_{j,s} = \begin{cases} a_{j-1,d-1}b_0 & s = 0 \\ a_{j-1,d-1}b_s + c \cdot a_{j-1,s-1} & 1 \le s \le d-1. \end{cases}$$

□

Let

$$f(t) = \sum_{\lambda=(\lambda_1,\ldots,\lambda_n)} p_\lambda t^\lambda := \sum_{\lambda} p_\lambda t_1^{\lambda_1}\cdots t_n^{\lambda_n}$$

是一个关于每个变量 t_i 次数为 $\le L$ 的多项式。根据引理 2.3 中的 c_i 和 $a_{i,\ j,\ s}$，我们计算得

$$\begin{aligned}(c_1\cdots c_n)^{Lz} f(\alpha^z) &= (c_1\cdots c_n)^{Lz}\sum_{\lambda} p_\lambda \alpha^{\lambda z} \\ &= \sum_{\lambda} p_\lambda c^{Lz-\lambda z}(c\alpha)^{\lambda z} \\ &= \sum_{\lambda} p_\lambda c^{Lz-\lambda z}\prod_{i=1}^{n}\sum_{s=0}^{d-1}(\alpha_i)^s a_{i,\lambda_i z,s} \\ &= \sum_{s_1,s_2,\ldots,s_n=0}^{d-1} \alpha^s \sum_{\lambda} p_\lambda c^{L-\lambda z}\prod_{i=1}^{n} a_{i,\lambda_i z,s}.\end{aligned}$$

因此，我们可以通过对系数 p_λ 施加整数线性条件，使 $f(\alpha^z) = 0$，具体而言，对每个 z，我们要求

$$\sum_{\lambda} p_\lambda c^{L-\lambda z}\prod_{i=1}^{n} a_{i,\lambda_i z,s} = 0. \tag{6}$$

这一观察使得我们可以利用 Siegel 的下述引理，初步构造一个辅助多项式 f。该引理通常称为“狄利克雷抽屉原理”。

引理2.4（Siegel）。设 $N > 2M > 0$ 为整数，且 $A = (a_{i,\ j})$ 是一个 $M \times N$ 的整数矩阵，使得 $|a_{i,\ j}| < H.$。则存在一个非零向量 $b \in \mathbf{Z}^N$，使得 $Ab = 0$，并且 b 的每个坐标的绝对值都小于 $2NH$。

证明。考虑所有坐标绝对值为 $\le NH$ 的向量 $b \in \mathbf{Z}^N$。这样的向量共有 $(2NH+1)^N > (2NH)^N$ 个。对于每个这样的 b，Ab 的每个坐标的大小至多为 $(NH)^2$。可能的向量 Ab 的总数小于 $(2(NH)^2)^M$。由于 $N > 2M$，鸽巢原理说明，必有两个不同的 b 得到相同的 Ab 值。它们的差即为所需的向量。

□

将西格尔引理应用于 (6) 中的线性方程组，无法得到定理 2.2 所要求的足够多的零点。事实上，我们尚未使用假设 (2)！Baker 注意到一个关键技巧：只要 f 及其足够多的导数为零即可。精确表述如下。

定理 2.5. 对每个充分大的参数 h，以下结论成立。令

$$L = h^{2-1/(4n)}.$$

存在一个多项式

$$f(t) = \sum_{\lambda} p_\lambda t^\lambda \in \mathbf{Z}[t_1, \ldots, t_n]$$

其关于每个变量 t_i 的次数均为 $\leq L$，使得 $|p_\lambda| < e^{h^3}$，并且由下式定义的单变量复解析函数 $z \in \mathbf{C}$

$$\phi(z) = \sum_{\lambda} p_\lambda e^{z(\lambda_1 x_1 + \ldots + \lambda_n x_n)} \tag{7}$$

满足

$$\phi^{(m)}(z) = 0 \qquad for\ m = 0, \ldots, h^2 - 1, \quad z = 1, \ldots, h.$$

证明。注意，$\phi(z)$ 的定义使得，对于整数z，$\phi(z) = f(\alpha^z) = f(\alpha_1^z, \ldots, \alpha_n^z)$。将线性相关关系 (2) 除以 $-\beta_n$（必要时重新排序以确保其非零），并重新命名系数后，可写为

$$x_n = \beta_1 x_1 + \cdots + \beta_{n-1} x_{n-1}$$

其中 $\beta_i \in$ 属于有理数域。于是有

$$\phi(z) = \sum_{\lambda} p_\lambda e^{z[(\lambda_1 + \lambda_n \beta_1) x_1 + \ldots + (\lambda_{n-1} + \lambda_n \beta_{n-1}) x_{n-1}]}. \tag{8}$$

注意，$\phi^{(m)}(z)$与 $\phi(z)$的求和相同，只是其中以 λ为指标的项乘以

$$\left((\lambda_1 + \lambda_n \beta_1) x_1 + \cdots + (\lambda_{n-1} + \lambda_n \beta_{n-1}) x_{n-1}\right)^m.$$

展开后，只需证明

$$\sum_{\lambda} p_\lambda \alpha^{\lambda z} (\lambda_1 + \lambda_n \beta_1)^{m_1} \cdots (\lambda_{n-1} + \lambda_n \beta_{n-1})^{m_{n-1}} = 0 \tag{9}$$

对所有满足条件的非负整数元组

$$m_1 + \cdots + m_{n-1} = m.$$

令 d 表示由所有 α_i 和 β_i 生成的数域的次数。令 c_i 表示 α_i 的整最小多项式的首项系数。根据引理 2.3，对于每个非负整数 j，都存在整数 $a_{i,\ j,\ s}$，使得

$$(c_i\alpha_i)^j = \sum_{s=0}^{d-1} a_{i,j,s}\alpha_i^s.$$

令 d_i 和 $b_{i,\ j,\ s}$ 对于 β_i起相同的作用。

若满足以下条件，表达式 (9) 将为零

$$\sum_{\mu_1=0}^{m_1}\cdots\sum_{\mu_{n-1}=0}^{m_{n-1}}\sum_{\lambda_1,\cdots\lambda_n=0}^{L} p_\lambda\left(\prod_{i=1}^{n} c_i^{Lz-\lambda_i z}a_{i,\lambda_i z,s_i}\right)\times \left(\prod_{j=1}^{n-1}\binom{m_j}{\mu_j}(d_j\lambda_j)^{m_j-\mu_j}\lambda_n^{\mu_j}b_{j,\mu_j,t_j}\right)$$

对于满足 $0 \le s_i, t_i \le d$ 的所有元组 $(s_1, \ldots, s_n)$ 和 $(t_1, \ldots, t_{n-1})$，该式均为零。

在我们要寻找的系数 p_λ 中，这对应多少个线性方程？我们希望当 $0 \le m < h^2$ 和 $1 \le z \le h$时该式为零。因此，这类方程的数量为

$$M = (h^2)^{n-1}hd^{2n-1} = h^{2n-1}d^{2n-1}.$$

注意，d 和 n 是固定的，但我们可以任意增大 h。

变量 p_λ 的数量为 $(L+1)^n$，因此，为了确保当 h 足够大时该数量大于 $2M$，我们令 $L = h^{2-1/(4n)}$ 如定理陈述中所示。最后，我们估计系数的大小。由简单的归纳法可知，存在一个常数 C，它仅依赖于α_i 和 β_i，使得

$$|a_{i,j,s}| \le C^j \qquad |b_{i,j,t}| \le C^j.$$

因此，对于某个仅取决于 α_i、β_i、n 的常数 K，我们有

$$\prod_{i=1}^{n}\left|c_i^{Lz-\lambda_i z}a_{i,\lambda_i z,s_i}\right| \le K^{Lz} \le K^{Lh}$$

类似地

$$\prod_{j=1}^{n-1}\left|\binom{m_j}{\mu_j}(d_j\lambda_j)^{m_j-\mu_j}\lambda_n^{\mu_j}b_{j,\mu_j,t_j}\right| \le K^{h^2\log(h)}.$$

根据西格尔引理，存在一个非平凡的整数解 p_λ，使得

$$|p_\lambda| \le 2K^{Lh+h^2\log(h)}(L+1)^n \ll e^{h^3}.$$

□

2.2 Baker 引理

本节介绍 Baker 的一个复分析引理，它强化了经典的 Schwarz 引理。这将使我们能够界定 f 及其许多导数的大小，其中 f 是 z 在 A 个取值处的某个倍数；我们已确保辅助多项式 f 在这些取值处为零。

引理 2.6。设 f：复数域 $\longrightarrow$ C 是一个整函数，设 $\epsilon > 0$，并设 A, B, C, T, U 是较大的正整数，使得

$$\frac{\epsilon}{2}C > \frac{2T + UAB}{A(\log A)^{1/2}} + \frac{UBA^{\epsilon}}{\log A}. \tag{10}$$

假设

- $|f(z)| \leq e^{T+U|z|}$ 对于 $z \in$ C。
- $f_{(t)}(z) = 0$ 对于 $t = 0, \ldots, C-1$ 和 $z = 1, 2, \ldots, A$。

Then

$$|f(z)| \leq e^{-(T+Uz)(\log A)^{1/2}} \text{ for } z = 1, \ldots, AB.$$

证明。函数

$$h(z) = \frac{f(z)}{(z-1)^C \cdots (z-A)^C}$$

根据第二个假设，它是整函数。由以原点为圆心、半径为 $A^{1+\epsilon}B$ 的圆上的最大模原理，对于 $|z| \leq AB$，有：

$$|h(z)| \leq \max_{|w|=A^{1+\epsilon}B} |h(w)|,$$

因此

$$|f(z)| \leq \max_{|w|=A^{1+\epsilon}B} |f(w)| \cdot \max_{|w|=A^{1+\epsilon}B} \left| \frac{(z-1)(z-2)\cdots(z-A)}{(w-1)(w-2)\cdots(w-A)} \right|^C,$$

Now

$$\left| \frac{(z-1)(z-2)\cdots(z-A)}{(w-1)(w-2)\cdots(w-A)} \right| \leq \frac{(AB)^A}{(A^{1+\epsilon/2}B)^A} = e^{-(\epsilon/2)A\log A}.$$

与此同时

$$|f(w)| \leq e^{T+UA^{1+\epsilon}B}.$$

Our 目标是证明 $|f(z)| \leq e^{-(T+UAB}{}_{)(\log A)^{1/2}}$，因此只需证明

$$-(\epsilon/2)AC\log A + (T + UA^{1+\epsilon}B) \leq -(T + UAB)(\log A)^{1/2}.$$

不难看出，这由引理的假设推出，

$$\frac{\epsilon}{2}C > \frac{2T + UAB}{A(\log A)^{1/2}} + \frac{UBA^{\epsilon}}{\log A}.$$

□

现在让我们将 Baker 引理应用于我们的辅助多项式及其导数。按照式 (7) 和 (8) 中的 $\phi(z)$，我们有

$$\phi^{(m)}(z) = \sum_{m_i} \binom{m}{m_1, \ldots, m_{n-1}} \prod_{i=1}^{n-1} x_i^{m_i} f_{m_1,\ldots,m_{n-1}}(z)$$

其中

$$f_{m_1,\ldots,m_{n-1}}(z) = \sum_{\lambda} p_\lambda \alpha^{\lambda z} (\lambda_1 + \lambda_n \beta_1)^{m_1} \cdots (\lambda_{n-1} + \lambda_n \beta_{n-1})^{m_{n-1}}. \tag{11}$$

从最后这个表达式显然可知

$$|f_{m_1,\ldots,m_{n-1}}(z)| < K^{h^3 + L|z|} \tag{12}$$

对于一个仅取决于 n、 α_i和 β_i的适当常数 K，成立。事实上， p_λ 有上界e^{h^3}。 m_i 和 λ_i 有上界 h^2。我们选取常数 K，使得不等式 (12) 对 α_i 或 β_i 分别替换为其任一共轭元时也成立。

现在，我们对函数$f_{m_1,\ldots,m_{n-1}}(z)$逐一应用 Baker 引理，其中

$$\begin{aligned} &T = h^3 \log K, \quad U = L \log K, \\ &C = h^2/2 \\ &A = h, \quad B = h^{1/(8n)}, \quad \epsilon = 1/(8n). \end{aligned}$$

我们假设常数 K和 h 的选取使得 T、 U、 A、 B、 C均为整数。注意，对于 $m_1 + \cdots + m_{n-1} \le h^2/2$和$t \le h^2/2$， $f_{m_1,\ldots,m_{n-1}}(z)$的第 t阶导数是$f_{m'_1,\ldots,m'_{n-1}}(z)$的一个线性组合，其中 $m'_1 + \cdots + m'_{n-1} \le h^2$，根据多项式 f的构造，这使得 $z = 0, \ldots, h$ 按要求消失。

此外，根据我们对参数的选择，所需的不等式 (10) 写作

$$\frac{h^2}{32n} > \frac{2(\log K)h^3 + (\log K)h^{2-1/(4n)} \cdot h \cdot h^{1/(8n)}}{h(\log h)^{1/2}} + \frac{(\log K)h^{2-1/4n} \cdot h^{1/(8n)} \cdot h^{1/(8n)}}{\log h},$$

很容易看出，当 h 足够大时该不等式成立。因此，Baker 引理给出

$$|f_{m_1,\ldots,m_{n-1}}(z)| < K^{-(h^3 + Lz)(\log h)^{1/2}} \tag{13}$$

对于 $m_1 + \ldots + m_{n-1} \le h^2/2$ 和 $z = 1$、.....、 $h^{1+1/(8n)}$。

2.3 代数整数的离散性

我们应用以下基本的初等原理。

引理 2.7. 假设 $a \in \mathbb{Q}$ 满足条件,¯即对某个正整数 d， da 是代数整数。假设 $|a| < \epsilon$，其中 ϵ 是某个正实数，并且每个共轭元 $\sigma(a)$ 都满足 $|\sigma(a)| < M$，其中 M 是某个正实数。最后假设 $[\mathbb{Q}(\alpha) : \mathbb{Q}] \le n$，且 $\epsilon M^{n-1} d^n < 1$。那么 $a = 0$。

证明。我们对代数整数 da 的范数作如下估计:

$$\begin{aligned}|\mathrm{N}_{\mathbf{Q}(a)/\mathbf{Q}}(da)| &= \prod_{\sigma:\ \mathbf{Q}(a)\hookrightarrow\mathbf{C}} |\sigma(da)| \\ &\le d^n|a| \cdot \prod_{\sigma\neq 1} |\sigma(a)| \\ &\le d^n \epsilon M^{n-1} < 1.\end{aligned}$$

绝对值小于 1 的整数必定为 0。因此 $\mathrm{N}_{\mathbf{Q}(a)/\mathbf{Q}}(da) = 0$，所以 $a = 0$。 □

我们将引理 2.7 应用于式 (11) 中定义的每个代数数 $f_{m_1,\ldots,m_{n-1}}(z)$，其中

$$m_1 + \ldots + m_{n-1} \le h^2/2, \qquad z = 0, 1, \ldots, h^{1+1/(8n)}.$$

在式 (13) 中，我们证明了

$$|f_{m_1,\ldots,m_{n-1}}(z)| < \epsilon := K^{-(h^3+Lz)(\log h)^{1/2}}. \tag{14}$$

我们还在式 (12) 中看到

$$|\sigma(f_{m_1,\ldots,m_{n-1}}(z))| < M := K^{h^3+Lz} \tag{15}$$

对每个 σ 均成立。从定义容易看出，$f_{m_1,\ldots,m_{n-1}}(z)$ 的分母可以用一个大小至多为.....的整数消去

$$d := K^{h^2+Lz}, \tag{16}$$

必要时增大 K，使其仅取决于 α_i 和 β_i。

由于 (14) 的指数中多出了因子 $(\log h)^{1/2}$，因此很容易看出，当 h 足够大时，不等式 $\epsilon M^{n-1} d^n < 1$ 成立，所以我们得出

$$f_{m_1,\ldots,m_{n-1}}(z) = 0$$

对于 $m_1 + \ldots + m_{n-1} \le h^2/2$ 和 $z = 0$，1，.....，$h^{1+1/(8n)}$。

2.4 逐步提升

我们反复进行上述过程，在第 k 次迭代中，使用 Baker 引理处理函数 $f_{m_1,\ldots,m_{n-1}}(z)$，其中 $m_1 + \cdots + m_{n-1} \le h^2/2^{k+1}$ 的参数为:

$$\begin{aligned}&T = h^3 \log K, \quad U = L \log K, \\ &C = h^2/2^{k+1} \\ &A = h^{1+k/(8n)}, \quad B = h^{1/(8n)}, \quad \epsilon = 1/(8n).\end{aligned}$$

我们假设 K 和 h 最初的选取使得上述量为整数。在第 k 次迭代中，我们得到：

$$|f_{m_1,\ldots,m_{n-1}}(z)| < K^{-(h^3+Lz)(\log(h+k/(8n)))^{1/2}}$$

for

$$m_1 + \ldots + m_{n-1} \le h^2/2^{k+1}, \qquad z = 0, 1, \ldots, h^{1+(k+1)/(8n)}.$$

（15）和（16）中的量保持不变，因此引理 2.7 再次推出，值$f_{m_1,\ldots,m_{n-1}}(z)$均为零。因此，我们可以继续讨论下一个 k。

每次迭代都会使零点的数量乘以 $B = h^{1/(8n)}$。经过 $16n^2$ 次迭代后，我们将得到超过 h^{2n} 个零点。由于 $L = h^{2-1/(4n)}$ 和 h 很大，我们有

$$h^{2n} > (L+1)^n,$$

因此，多项式$f = f_{0,0,\ldots,0}$ 满足定理 2.2 的条件。因此，存在整数 $\lambda_1, \ldots, \lambda_n$，不全为零，使得

$$\alpha_1^{\lambda_1} \cdots \alpha_n^{\lambda_n} = 1.$$

至此，Baker定理的证明完成。

3 阿克斯定理

从 $\mathscr{L}$ 中的元素的线性形式转向任意多项式，我们提醒读者注意引言中陈述的 Schanuel 猜想。

Schanuel猜想。设 $y_1, \ldots, y_n \in$ 复数域 中的元素 Q线性无关。那么

$$\operatorname{trd}_{\mathbf{Q}} \mathbf{Q}(y_1, \ldots, y_n, e^{y_1}, \ldots, e^{y_n}) \ge n.$$

尽管人们对这个猜想知之甚少，但我们有以下由 James Ax [2] 证明的函数域类比结果。

T定理 3.1（Ax）。设 $y_1, \ldots, y_n \in t$复数域$[[t]]$ 中的元素 Q线性无关。则 n

$$\operatorname{trd}_{\mathbf{C}(t)} \mathbf{C}(t)(y_1, \ldots, y_n, e^{y_1}, \ldots, e^{y_n}) \ge n.$$

本节证明阿克斯定理。本节内容自成一体，对函数域情形不感兴趣的读者可以跳过。

3.1 导子

定义 3.2. 设 A 是一个交换环， B 是一个交换 A-代数。 B 到 B-模 M 的一个 A-导子是一个 A 线性映射

$$D\colon B \longrightarrow M$$

使得

$$D(ab) = aD(b) + D(a)b, \qquad a, b \in B, \tag{17}$$

wh此处我们将 M 同时视为左 B-模和右 B-模，因为 B 是交换的 .

存在一对 $(d = d_{B/A}, \Omega^{B/A})$，其中 $\Omega^{B/A}$ 是一个 B-模，且配有一个 A-导子

$$d\colon B \longrightarrow \Omega_{B/A}$$

它具有如下普遍性：任意 A-导子 $D\colon B \longrightarrow M$ 都可以通过将 $d_{B/A}$ 与一个 B-模同态 $\Omega^{B/A} \longrightarrow M$复合而得到。K¨ahler 微分形式 $\Omega^{B/A}$ 的模定义为自由 B-模对下列元素取商所得的模：对于每个 $b \in B$，以形式生成元 db 为生成元，并满足关系 $da = 0$（对 $a \in A$、 $d(b+b') = db + db'$以及 $d(bb') = b \cdot db' + b' \cdot db$）。泛导子 $d_{B/A}\colon B \longrightarrow \Omega^{B/A}$ 定义为 $d_{B/A}(b) = db$。

引理 3.3. 设 F/K 是一个域扩张，且 $x \in F$ 在 K上是可分代数的。那么 $dx = 0$属于 $\Omega_{F/K}$。

证明。令 $f(x) \in K[x]$ 为 x 的最小多项式。于是

$$0 = d(f(x)) = f'(x)dx.$$

由于 x 是可分的， $f'(x) \neq 0$，因此 $dx = 0$。 □

同时，若 $F(t)$ 表示域 F 上的一元函数域，则 $\Omega^{F(t)/F}$ 是由 dt 生成的 1 维 $F(t)$-向量空间，其中 $d(f(t)) = f'(t)dt$。

引理 3.4。设 $K \subset F \subset L$ 为特征为 0 的域。设 $D\colon F \longrightarrow F$ 是一个 K-导子。则 D 可以扩张为一个 K-导子 $L \longrightarrow L$。

证明。对于 $f \in F[t]$，令 f^D 表示对 f 的系数应用 D 后所得的多项式。我们说明如何扩张导子 d。令 $z \in L, z \notin F$。若 z 在 F 上代数，则令 $p(x)$ 为其最小多项式。定义

$$u = -\frac{p^D(z)}{p'(z)}, \quad \tilde{D}(g(z)) = g^D(z) + g'(z)u. \tag{18}$$

如果 z 在 F上是超越的，我们定义

$$\tilde{D}(g(z)) = g^D(z) + g'(z)u \tag{19}$$

˜对任意 $u \in L$。留给读者验证：令 $D|_F = D$ ，并使用 (18) 或˜(19) 将其扩展到 $F(z)$，即可得到一个导子 D。现在利用佐恩引理将 D 一直扩展到 L。

□

推论 3.5。设 $K \subset L$ 为特征为 0 的域。则

$$\dim_L \Omega_{L/K} = \mathrm{trd}_K L.$$

更一般地，若 $K \subset F \subset L$，则

$$\dim_L (L \cdot d_{L/K}(F)) = \mathrm{trd}_K F.$$

证明。令 $f_1, \ldots, f_n$ 为 F/K的一个超越基。假设

$$\sum_{i=1}^{n} a_i d_{L/K} f_i = 0$$

其中 $a_i \in L$。由 $d_{L/K}$的泛性质可得

$$\sum_{i=1}^{n} a_i D(f_i) = 0$$

对于任意 K-导子 $D_i\colon L \to L$。因此，若能证明对每个 i，都存在一个 K-导子 $D_i\colon L \to L$，使得 $D_i(f_j) = \delta_{ij}$，则可得对所有 i均有 $a_i = 0$。由此得到 $d_{L/K} f_i$ 在 L上的线性无关性。

D_i 的存在性可由引理 3.4 的证明得出。首先，我们可以将 K 上的零导子延拓到 $K(f_i)$，方法是在 (19) 中令 $z = f_i, u = 1 - f_i$；随后，通过对 $j \neq i$令 $z = f_j, u = -f_j$，逐步将其延拓到 $K(f_1, \ldots, f_n)$。最后，再次使用引理 3.4 将 D_i 延拓到 L。 □

3.2 Kähler微分上的导子

设 A 是一个交换环， B 是一个 A-代数。设 $D\colon B \longrightarrow B$ 是一个导子，满足 $D(A) \subset A$。存在一个 A-线性映射

$$D^1\colon \Omega_{B/A} \longrightarrow \Omega_{B/A}$$

满足

$$D^1(f dg) = (Df)dg + f d(Dg). \tag{20}$$

我们将其验证留给读者，但要指出一个更一般的事实也成立。若考虑微分的分次代数

$$\Omega^*_{B/A} = \bigoplus_{n=0}^{\infty} \bigwedge_B^n \Omega_{B/A},$$

那么微分 $D\colon B \longrightarrow B$ 延拓为一个分次导子

$$D^*\colon \Omega^*_{B/A} \longrightarrow \Omega^*_{B/A}$$

满足 (17)，其中第 0 个分次分量为 D ，第 1 个分次分量为 D^1。在阿克斯定理的证明中，我们只需要映射 D^1，但请注意，规则 (20) 可以推广：对于任意 $f \in B$ 和 $\omega \in \Omega^{B/A}$，都有

$$D^1(f\omega) = (Df)\omega + fD^1(\omega). \tag{21}$$

引理 3.6。设 $y \in t\mathbb{C}[[t]]$, $z = e^y$，且设 $D\colon \mathbb{C}((t)) \longrightarrow \mathbb{C}((t))$ 是一个形如 $D(f(t)) = f'(t) \cdot g(t)$ 的 $\mathbb{C}$-导子，其中 $g(t) \in \mathbb{C}((t))$ 固定。则

$$D^1(dy - z^{-1}dz) = 0$$

属于 $\Omega^{\mathbb{C}((t))/\mathbb{C}}$。

证明。一次 根据定义 (20) 直接计算可得，一般而言，我们有

$$D^1(dy - z^{-1}dz) = d(Dy - z^{-1}Dz).$$

然而，当 $z = e^y$ 时，对于导子 $D(f(t)) = f'(t) \cdot g(t)$，项 $Dy - z^{-1}Dz$ 消失。结论得证。 □

引理 3.7。设 $K \subset L$ 是域， $D\colon L \longrightarrow L$ 是一个导子，且 $\ker D = K$。则映射

$$L \otimes_K \ker D^1 \longrightarrow \Omega_{L/K}, \qquad f \otimes \omega \mapsto f\omega,$$

是单射的。

证明。假设存在

$$f_1, \ldots, f_n \in L^*, \qquad \omega_1, \ldots, \omega_n \in \ker D^1$$

使得

$$\sum_{i=1}^{n} f_i \otimes \omega_i \mapsto 0, \qquad \text{i.e. } \sum_{i=1}^{n} f_i\omega_i = 0. \tag{22}$$

进行缩放，使得 $f_1 = 1$. 如果所有 f_i 都属于 K，那么

$$\sum_{i=1}^{n} f_i \otimes \omega_i = 1 \otimes \sum_{i=1}^{n} f_i\omega_i = 1 \otimes 0 = 0,$$

因此得证。假设情况并非如此，并取这样的最小消去线性组合。根据极小性，不妨设 ω_i 在 L上 D^1 线性无关。将 D^1 应用于表达式 (22)。利用 (21)，我们得到

$$0 = \sum_{i=1}^{n}((Df_i)\omega_i + f_iD^1(\omega_i)) = \sum_{i=1}^{n}(Df_i)\omega_i,$$

其中第二个等式成立是因为 $\omega_i \in \ker D^1$。由 L上的 ω_i 线性无关性，我们看到对于所有 i 都有 $Df_i = 0$ ，因此根据假设，对于所有 i都有 $f_i \in K$ 。这就得到了所需的结果。 □

下面给出一个技术代数引理，它将使我们能够将问题归约到曲线的函数域情形。

引理 3.8。设 $K \subsetneq L$ 是域扩张，且 K 在 L 中相对代数闭。设

$$W = \{F\colon K \subset F \subset L,\ \ \mathrm{trd}_F\, L = 1,\\ F \text{ relatively algebraically closed in } L\}.$$

Then

$$\bigcap_{F\in W} F = K.$$

证明。设 $t \in L$、 $t \notin K$。我们需要证明存在 $F \in W$ 使得 $t \notin F$。由于 K 在 L 中相对代数闭，元素 t 在 K 上超越。

选取 L/K 的一个超越基，由 t 和一组不属于 $K(t)$ 的元素 B 组成。令 F 为 $K(B)$ 在 L 中的相对代数闭包，即

$$F = \{x \in L\colon x \text{ algebraic over } K(B)\}.$$

于是 $F \in W$，因为 L 在 $F(t)$ 上代数。由于 $t \notin F$，证明完毕。 □

从某种意义上说，下面的引理是 Ax 的证明的主要动力。

引理 3.9。设 L/K 是特征为 0 的域。用 dL 表示由 $f \in L$ 的所有 df 张成的 $\Omega^{L/K}$ 的 K-子空间。用 dL/L 表示由 $f \in L^*$ 的所有 $f^{-1}df$ 张成的 $\Omega^{L/K}$ 的整数环 Z-子模。那么， K 向量空间之间的典范映射

$$K \otimes_{\mathbf{Z}} dL/L \longrightarrow \Omega_{L/K}/dL, \qquad k \otimes \frac{df}{f} \mapsto \frac{k}{f}df, \tag{23}$$

是单射，其中 $\Omega_{L/K}/dL$ 表示 $\Omega^{L/K}$ 除以由 df在 $f \in L$上张成的 K-子空间所得的商。

证明。取一个元素

$$\sum_{i=1}^{n} k_i \otimes f_i^{-1}df_i \tag{24}$$

它属于映射 (23) 的核，且 n 最小。由最小性可知， k_i 在有理数域 Q 上线性无关。我们将证明每个 f_i 都属于 $\overline{K}_L$，即 K 在 L 中的相对代数闭包。由引理 3.3，这将推出 $df_i = 0$，从而得到所需的单射性。

如果 $L = \overline{K}_L$，则无需证明。否则，令 $F \in W$，其中 W 如引理 3.8 中所述。因此， $K \subset F \subset L$， $\mathrm{trd}_F\, L = 1$，且 $\overline{F}_L = F$。由于式 (24) 中的元素属于式 (23) 的核，我们有

$$\sum_{i=1}^{n} k_i f_i^{-1}df_i = \sum_{i=1}^{m} k_i' df_i'. \tag{25}$$

对于某些 $f_i' \in L^*$、 $k_i' \in K$。现在，我们希望使用曲线的函数域的性质，但遗憾的是，我们不知道 L 在 F上是有限生成的。为此，我们考虑域 L'，它是在 F上由 f_i、 f_i'以及在 $\Omega^{L/K}$ 中用于得到式 (25) 的任意关系中所使用的元素生成的。域 L' 在 F 上仍具有超越次数 1，并且在 F 上有限生成。因此，我们可以将 L' 认定为 F 上某条光滑射影代数曲线的函数域。此外，按照构造，式 (25) 在 $\Omega^{L'/K}$ 中仍然成立，因此它在 $\Omega^{L'/F}$ 中也成立。

曲线上的点 P 对应于赋值

$$\operatorname{ord}_P \colon (L')^* \longrightarrow \mathbf{Z}.$$

与 P 相关联的还有一个剩余映射

$$\operatorname{res}_P \colon \Omega_{L'/F} \longrightarrow F.$$

剩余映射与赋值映射满足以下众所周知的性质。对于所有的 $g \in (L')^*$，我们有

$$\operatorname{res}_P(g^{-1}dg) = \operatorname{ord}_P(g), \qquad \operatorname{res}_P(dg) = 0.$$

对 (25) 应用 res_P，得到

$$\sum_{i=1}^{n} k_i \operatorname{ord}_P(f_i) = 0.$$

由 k_i 的 Q-线性无关性可得，对于所有 P, i，$\operatorname{ord}_P(f_i) = 0$。然而，光滑射影曲线上没有零点或极点的函数必为常数，因此对于所有 i， $f_i \in F$。由于这对所有 F 都成立，根据引理 3.8 可得 $f_i \in \overline{K}_L$。这就是所需的结果。

□

现在我们可以完成阿克斯定理的证明。

定理 3.1 的证明。设 $y_1, \ldots, y_n \in t\mathbf{C}[[t]]$，并令 $z_i = e^{y_i} \in \mathbf{C}[[t]].$。设

$$L = \mathbf{C}(y_1, \ldots, y_n, z_1, \ldots, z_n).$$

只需证明，若 $\operatorname{trd}_{\mathbf{C}} L \leq n$，则 $y_1, \ldots, y_n$ 在 Q 上线性相关。假设 $\operatorname{trd}_{\mathbf{C}} L \leq n$。那么根据推论 3.5，这些微分形式

$$\omega_i = dy_i - z_i^{-1} dz_i \in \Omega_{L/\mathbf{C}}$$

对于 $i = 1, \ldots, n$，连同 dy_1，它们在 L 上必须线性相关：

$$\sum_{i=1}^{n} f_i \omega_i + g dy_1 = 0, \tag{26}$$

其中 $f_i, g \in L$ 不全为零。注意，如果 $y_1'(t) = 0$，那么 y_1 是一个常数；又因为 $y_1 \in t\mathbf{C}[[t]]$，我们将得到 $y_1 = 0$。于是 y_i 显然线性相关；因此此后我们可以假设 $y_1'(t) \neq 0$。定义一个 C-导子

$$D\colon L \longrightarrow L, \qquad D(f(t)) = f'(t)/y_1'(t).$$

由引理 3.6 可得 $D^1(\omega_i) = 0$。此外，直接计算可得

$$D^1(dy_1) = d(Dy_1) = d(1) = 0.$$

因此，我们有

$$\sum f_i \otimes \omega_i + g \otimes dy_1 \in \ker((L \otimes_{\mathbf{C}} \ker D^1) \longrightarrow \Omega_{L/\mathbf{C}}).$$

由引理 3.7，我们不妨设 $f_i, g \in$ 属于复数域。

将方程 $\sum f_i\omega_i + gdy_1 = 0$ 改写为

$$\sum_{i=1}^{n} f_i \cdot (-z_i^{-1}dz_i) = -\sum_{i=1}^{n} f_i dy_i - gdy_1.$$

引理 3.9 表明，要么所有 $f_i = 0$，要么 $z_i^{-1}dz_i$ 在 Q 上线性相关。在第一种情况下，由 (26) 以及 f_i, g 不全为零这一事实可得 $dy_1 = 0$。因此， y_1是一个常数；如前所述，这意味着 $y_1 = 0$。所以我们假设属于第二种情况，即

$$\sum m_i(dz_i)/z_i = 0$$

其中 $m_i \in$不全为零。这意味着

$$d\left(\prod z_i^{m_i}\right) / \left(\prod z_i^{m_i}\right) = 0,$$

因此 $\prod z_i^{m_i} = e^{\sum m_i y_i}$ 是一个常数。考察常数项可知，这个常数必为 1。因此

$$\sum m_i y_i = 0,$$

从而得到 y_i 在有理数域 Q 上的所需线性相关关系。 □

4 StructuralRank 猜想

现在我们回到复数域 C 上的经典情形，而非函数域情形，并继续考察由 $\mathscr{L}$中的元素构成的矩阵。 2×2 矩阵的最简单情形引出了以下四指数猜想。

猜想 4.1. 设 $M \in M_{2\times 2}(\mathscr{L})$。那么 $\det(M) = 0$ 当且仅当 M的行或列在 Q 上线性相关。

这一猜想最早由 Schneider 于 1957 年公开发表 [16], ，不过在此前二十年间，Selberg、Siegel、Alaoglu–Erdos [1], 等人已考虑过它的不同版本。该猜想至今仍未解决。支持这一猜想的最有力理论证据是以下六指数定理。

定理 4.2。设 $M \in M_{2\times 3}(\mathscr{L})$。那么，$\operatorname{rank}(M) < 2$ 当且仅当 M的行或列在 Q 上线性相关。

六指数定理由 Lang [13] 和 Ramachandra[15] 于 20 世纪 60 年代末独立证明。关于四指数猜想和六指数定理的历史详情及参考文献，请参阅 Waldschmidt [20] 生动有趣的个人记述。

六指数定理是 Waldschmidt–Masser 定理的一个特例，我们将在本文后文讨论该定理。将四指数猜想简单推广到任意维数的矩阵并不成立——一般而言，即使矩阵的行和列在 Q 上线性无关，矩阵的秩也可能低于最大秩。例如，注意到

$$\det \begin{pmatrix} x & z & 0 \\ 0 & y & -x \\ y & 0 & z \end{pmatrix} = 0.$$

因此，若用 $\mathscr{L}$ 中任意线性无关的元素替换 x、 y和 z，就会得到一个秩为 < 3 的矩阵，其行和列在 Q 上线性无关。诸如此类的例子促使我们提出结构秩猜想，该猜想已在引言中作了精确表述。上面的矩阵的结构秩等于 2。

4.1 p进设置

超越数理论中的大多数论述在 p进设置下都有对应的类比。如下文所述，这些类比在岩泽理论中尤为重要。设 p 为一个素数，并令 $\mathbf{C}_p = \mathbf{Q}_p$ 表示 $\mathbf{Q}_p$的代数闭包的完备化。下文的论述在 $\mathbf{Q}_p$上同样适用，但使用 $\mathbf{C}_p$ 可以提供更广泛的适用性。存在一个 p进对数和一个 p 进指数函数

$$\begin{aligned} \log_p \colon \{x \in \mathbf{C}_p \colon |x-1| < 1\} &\longrightarrow \mathbf{C}_p \\ \exp_p \colon \{x \in \mathbf{C}_p \colon |x| < p^{-1/(p-1)}\} &\longrightarrow \mathbf{C}_p \end{aligned} \tag{27}$$

由通常的幂级数定义

$$\log_p(1-x) = -\sum_{n=1}^{\infty} \frac{x^n}{n}, \qquad \exp_p(x) = \sum_{n=1}^{\infty} \frac{x^n}{n!}.$$

函数 $\log_p$ 和 $\exp_p$ 在（27）给出的定义域上是单射群同态。 p-进对数唯一地延拓为连续同态

$$\log_p \colon \{x \in \mathbf{C}_p \colon |x| = 1\} \longrightarrow \mathbf{C}_p$$

因为每个满足 $|x| = 1$ 的 $x \in$ 复数域$_p$ 都满足 $|x^n - 1| < 1$，其中 n 是适当的正整数，因此我们可以定义 log$_p(x) = \frac{1}{n}$ log$_p(x^n)$。接下来，我们将 log$_p$ 延拓为连续同态

$$\log_p \colon \mathbf{C}_p^* \longrightarrow \mathbf{C}_p$$

通过固定 Iwasawa 的（非典范）选择 log$_p(p) = 0$。log$_p$ 在复数域$_p^*$ 上的核由形如 $p^a \cdot u$ 的元素组成，其中 $a \in$ 属于有理数域，且 u 是单位根。

我们定义代数数的 p-adic 对数所构成的 Q-向量空间：

$$\mathscr{L}_p = \{\log_p(x) \colon x \in \overline{\mathbf{Q}}^*\} \subset \mathbf{C}_p.$$

p-adic 版本的 Baker定理由 Brumer 按照贝克方法证明。

定理 4.3（Baker–Brumer）。设 $y_1, \ldots, y_n \in \mathscr{L}_p$ 在有理数域上线性无关，则$y_1, \ldots, y_n$ 在有理数域上线性无关。

类似地，在 p-adic 情形下，也有 Schanuel猜想和结构秩猜想的自然类比。确切地说，我们陈述后者：

猜想 4.4（p-adic 结构秩猜想）。设

$$M \in M_{m\times n}(\mathscr{L}_p + \mathbf{Q}) \subset M_{m\times n}(\mathbf{C}_p).$$

M 的秩等于 M的结构秩。

4.2 数论中的应用

超越数理论中的结论在代数数论中有重要应用。本节介绍岩泽理论中的两个重要猜想，它们是 p-进结构秩猜想的特例。这些猜想是我们开展本研究的个人动机。

4.2.1 Leopoldt猜想

固定一个素数 p 和一个嵌入 Q $\hookrightarrow \overline{\text{C}}_p$。

猜想 4.5（Leopoldt猜想）。设 F 是一个次数为 n 的数域，且其定义在 Q 上；令 σ_1、…、σ_n表示 Q 的嵌入 $F \hookrightarrow$。令 u_1、…、 u_r为 $\mathcal{O}_F^*/\mu(F)$的一组 Z-基。令

$$M = (\log_p \sigma_j(u_i)) \in M_{r\times n}(\mathscr{L}_p).$$

那么秩$_{\text{C}_p}(M) = r$。

命题 4.6。 p-进结构秩猜想蕴含 Leopoldt猜想。

证明。这里的关键在于，Leopoldt猜想的陈述的阿基米德类比已知为真；这就是数域的调节子不为零这一经典结果。更确切地说，若固定一个嵌入 $\mathbf{Q} \hookrightarrow \mathbf{C}$，并令 $N = (\log|\sigma_j(u_i)|)$，其中绝对值表示 $\mathbf{C}$ 上通常的绝对值，则有

$$\operatorname{rank}_{\mathbf{C}}(N) = r.$$

这是利用 $\log|\cdot|$ 取值于有序域 $\mathbf{R}$ 这一事实证明的（而 $\log_p$ 则不是）。因此，p-进情形的结论远比阿基米德情形深刻。

结构秩定义中出现的域 $\mathbf{Q}(x_1, \ldots, x_k)$ 搭起了 p-进情形与复数情形之间的桥梁，其中 p-进结构秩猜想发挥了主要作用。

设 $\{c_1, \ldots, c_k\} \subset \{\sigma_j(u_i)\}$，使得 $\{\log_p(c_i)\}$ 是由 $\log_p(\sigma_j(u_i))$ 张成的 $\mathbf{Q}$-向量空间的一组 $\mathbf{Q}$-基。记

$$M = (\log_p \sigma_j(u_i)) = \sum_{i=1}^{k} M_i \log_p(c_i)$$

且 $M_i \in M_{r\times n}(\mathbf{Q})$。$p$-进结构秩猜想蕴含

$$\begin{aligned} \operatorname{rank}_{\mathbf{C}_p} M &= \operatorname{rank}_{\mathbf{Q}(x_1,\ldots,x_k)} \left(\sum_{i=1}^{k} M_i x_i \right) \\ &\geq \operatorname{rank}_{\mathbf{C}} \left(\sum_{i=1}^{k} M_i \log|c_i| \right) \\ &= \operatorname{rank}_{\mathbf{C}} (\log|\sigma_j(u_i)|) \\ &= r. \end{aligned} \tag{28}$$

因此 $\operatorname{rank}_{\mathbf{C}_p} M \geq r$，所以必定取等号。注意，在等式 (28) 中，我们隐含地使用了以下事实：若 $u_i \in \mathbf{Q}^*$ 是 p-进单位，且 $m_i \in \mathbf{Z}$ 是整数，则

$$\sum m_i \log_p(u_i) = 0 \Longrightarrow \prod u_i^{m_i} \text{ is a root of unity } \Longrightarrow \sum m_i \log|u_i| = 0.$$

□

让我们介绍 Leopoldt猜想的两个应用。

代数的（岩泽理论）。根据类域论，Leopoldt猜想意味着：F 在 p 之外非分歧的最大 pro-p 阿贝尔扩张的 $\mathbf{Z}_p$-秩等于 $r_2 + 1$，其中 $2r_2$ 是嵌入 $F \hookrightarrow$ 复数域 $\mathbf{C}$ 且其像不包含于 $\mathbf{R}$ 中的嵌入数。

解析（p-进 L-函数）。设 F 是一个全实域，因此

$$r = \operatorname{rank} \mathcal{O}_F^* = [F : \mathbf{Q}] - 1.$$

存在经典 Dedekind ζ 函数的一个 p-进类比，它定义在 F 上，记为 $\zeta_{F,\,p}$。Colmez 的一个定理 [6]指出

$$\lim_{s\to 1}(s-1)\zeta_{F,p}(s) = (*)R_p(F),$$

其中

$$R_p(F) = \det(\log_p(\sigma_j(u_i))_{i,j=1,\dots,r}$$

而（$*$）表示一个具体但此处不作精确定义的非零代数数。这是一个 p-进“类数公式”。因此，$\zeta_{F,\,p}(s)$ 在 $s=1$ 处有极点，当且仅当 Leopoldt猜想成立。

4.2.2 Gross–Kuz'min 猜想

Gross 和 Kuz'min 各自独立提出了一个类似于 Leopoldt猜想的猜想，涉及 $s=0$ 处而非 $s=1$ 处的 p-进 L-函数。不同于经典 L-函数的情形，p-进 L-函数没有联系 0 和 1 处函数值的函数方程。

关于 Gross–Kuz'min 猜想的更多细节（超出下文所述内容），请读者参阅 Gross 的文章 [10] 。为陈述该猜想，设 H 是一个 CM 域，H^+ 是其极大全实子域。令

$$U_p^- = \{u \in H^* \colon |u|_w = 1 \text{ for all } w \nmid p\}.$$

此处 w 遍历 H 中所有不整除 p 的赋值，包括阿基米德赋值。于是 $\operatorname{rank}(U_p^-) = r$，其中 r 是 H^+ 中位于 p 之上且完全分裂于 H 的素理想数。

令 X_p 表示一个以 H 上方的 p 的赋值为指标集的 $\mathbf{C}_p$-向量空间。令 c 表示 $\operatorname{Gal}(H/H^+)$ 的非平凡元素，即 $c=$ 复共轭。令 X_p^- 表示 X_p 的最大商，使得 c 在其上的作用为 -1。那么 X_p^- 的维数为 r。我们定义两个映射

$$\ell_p, o_p \colon U_p^- \longrightarrow X_p^-.$$

$o_p(u)$ 在对应于 H 的赋值 $\mathfrak{P}$ 的分量上的坐标为 $\operatorname{ord}_{\mathfrak{P}}(u)$，而 $\ell_p(u)$ 的坐标为 $\log_p(\mathrm{N}_{H_{\mathfrak{P}}/\text{有理数域}_p}(u))$。我们将 ℓ_p 和 o_p 延拓为 $\mathbf{C}_p$-线性映射

$$U_p^- \otimes \mathbf{C}_p \longrightarrow X_p^-.$$

利用 Dirichlet 单位定理不难证明 o_p 是一个同构，并定义

$$R_p^-(H) = \det(\ell_p \circ o_p^{-1}).$$

猜想 4.7（Gross–Kuz'min）。我们有 $R_p^-(H) \neq 0$。

通过与命题 4.6 的证明类似的证明可知，p-进结构秩猜想蕴含 Gross–Kuz'min 猜想（此处用 ord_p 代替 $\log|\cdot|$）。同样，这个猜想有代数和解析解释。

代数解释（岩泽理论）。根据类域论，Gross–Kuz'min 猜想蕴含对 H 的圆分整环 p-扩张中各域的类群的 p-部分增长的一个上界。详见 [9, 命题 3.9]。

解析的（p-进 L-函数）。令 χ 表示 Gal(H/H^+) 的非平凡特征。则已知

$$\operatorname{ord}_{s=0} L_p(\chi\omega, s) \geq r.$$

对于奇数 p，这由 Wiles [22]的工作得到；在 Spiess 的论证基础上，[4] 和 [17] 给出了一个利用 Eisenstein 余循环、适用于所有 p 的另一种证明。在论文 [7]（与 Darmon 和 Pollack 合作）和 [8]（与 Kakde 和 Ventullo 合作）中，我们证明了

$$L_p^{(r)}(\chi\omega, 0) = (*)R_p^-(H)$$

其中（$*$）是一个特定的非零有理数。这是在 $s = 0$处的一个 p-进类数公式。因此，当且仅当 Gross-Kuz'min 猜想成立时，$L_p(\chi\omega, s)$ 在 $s = 0$ 处的零点阶数恰好为 r。

4.2.3 表示论考量

保持 Gross–Kuz'min 猜想的设定，现设 H 包含一个全实域 F，使得 H/F 是伽罗瓦的。令 $G = \text{Gal}(H/F)$。对于 G 在 $\mathbf{C}_p$上的任意表示M，以及 V的不可约表示的特征 χ，令 M^χ 表示 M 的χ-等型分量（即由 M 中同构于 V的子表示张成的空间）。

Then

$$U_p^- = \bigoplus_\chi U_p^\chi, \qquad X_p^- = \bigoplus_\chi X_p^\chi,$$

其中求和遍历 χ 的不可约表示 V的特征，这些表示中 G 上的c 作用为 -1。映射 ℓ_p 和 o_p 也可分解为映射之和

$$\ell_p^\chi, o_p^\chi \colon U_p^\chi \longrightarrow X_p^\chi.$$

我们定义

$$R_p^\chi(H) = \det(\ell_p^\chi \circ (o_p^\chi)^{-1}).$$

于是有

$$R_p^-(H) = \prod_\chi R_p^\chi(H). \tag{29}$$

现在，对于如上所述的 χ，

$$r_p^\chi := \dim_{\mathbf{C}_p} U_p^\chi = \dim_{\mathbf{C}_p} X_p^\chi = \sum_{\mathfrak{p}|p} \dim_{\mathbf{C}_p} V^{G_\mathfrak{p}},$$

其中求和遍及 F 中位于 p 上方的素理想，$G_\mathfrak{p} \subset G$ 表示 H 中位于 $\mathfrak{p}$ 上方的一个素理想的分解群，而 $V^{G_\mathfrak{p}}$ 表示 V 中在 F 作用下不变的最大子空间

$G_{\mathfrak{p}}$。当 $r_p^{\chi} = 1$ 时，调节子 $R_p^{\chi}(H)$ 是代数数的 p-进对数的有理数域上线性组合。正如 Gross 在 [10, 命题 2.13], 中指出的，在这种情况下，$R_p^{\chi}(H)$ 的非零性可由 Brumer–Baker 定理（定理 4.3）推出。

定理 4.8. 若 $r_p^{\chi} = 1$，则 $R_p^{\chi}(H) \neq 0$。

有一种特殊情形，此时每个 $r_p^{\chi} \leq 1$。若 F 在 p 上方仅有一个素数（例如 $F =$ 有理数域），且 G 是阿贝尔的（因此每个 V 的维数都是 1），那么显然 $r_p^{\chi} \leq 1$。将定理 4.8 与分解式 (29) 结合，我们得到：

推论 4.9. 设 F 是一个全实域，且在 p上方恰有一个素数；设 H 是 F的一个 CM 阿贝尔扩张。那么 Gross–Kuz'min 猜想对 H成立。

对 Leopoldt猜想也可以进行类似的分析，从而得到：

定理 4.10. Leopoldt猜想对有理数域的阿贝尔扩张成立。

4.3 Roy 的一个定理

Damien Roy 在超越数理论中证明了许多优美的结果。现在我们来证明其中一个。

定理4.11（Roy）。结构秩猜想等价于 Schanuel猜想的以下特殊情形：若 $y_1, \ldots, y_n \in \mathscr{L}$ Q 线性无关，则

$$\mathrm{trd}_{\mathbf{Q}}\, \mathbf{Q}(y_1, \ldots, y_n) = n.$$

类似地， p-进结构秩猜想等价于 Schanuel猜想特殊情形的 p-进版本，但这里我们只讨论阿基米德情形。定理4.11在 [12]中得到了证明。

Roy定理的一个方向相对初等。

引理 4.12。Schanuel猜想的特殊情形蕴含结构秩猜想。

证明。我们假设 Schanuel猜想的特殊情形成立。首先考虑一个系数属于 $\mathscr{L}$ 的矩阵M。令 $M = \sum M_i c_i$ 满足 $M_i \in M_{m\times n}$(Q)，且 $c_i \in \mathscr{L}$ 在 Q 上线性无关。写作

$$M_x = \sum M_i x_i \in M_{m\times n}(\mathbf{Q}(x_1, \ldots, x_n))$$

并令 $r =$ rank(M_x)。令 J_x 为 M_x 的一个 $r \times r$ 子矩阵，使得

$$\det(J_x) = P(x_1, \ldots, x_n) \neq 0$$

在 $\mathbb{Q}[x_1, \ldots, x_n]$. 中， M的对应子矩阵的行列式等于 $P(c_1, \ldots, c_n)$，因此不可能为零，因为根据 Schanuel猜想的特殊情形， c_i 是代数独立的。因此，$\operatorname{rank}(M) \geq r$。显然，$\operatorname{rank}(M) \leq r$，所以两者相等。

现在假设 M 的系数属于 $\mathscr{L} + \mathbb{Q}$，但不属于 $\mathscr{L}$。有两种情况。

情况 1：1 不在 M的系数的 Q线性张成中。这个张成空间的 Q-基可取为 $1 + c_1, c_2, \ldots, c_n$，其中 $c_i \in \mathscr{L}$。容易验证 c_i必定 Q线性无关，因此根据 Schanuel猜想的特殊情形，它们是代数独立的。因此， $1 + c_1, c_2, \ldots, c_n$也具有同样的性质。于是，前面的证明可应用于这个基。

情况 2：1 在 M的系数的 Q线性张成中。我们可以取这个张成空间的一个 Q-基，其形式为 $c_0 = 1, c_1, \ldots, c_n$，其中对于 $i \geq 1$， $c_i \in \mathscr{L}$。我们照前面的方法继续。写作

$$M = \sum_{i=0}^{n} M_i c_i, \quad M_x = \sum_{i=0}^{n} M_i x_i.$$

设 $r = \operatorname{rank}(M_x)$，且 J_x 是 M_x 的一个 $r \times r$ 子矩阵，其中

$$\det(J_x) = P(x_0, \ldots, x_n) \neq 0.$$

对应子矩阵 J的行列式为 $P(1, c_1, \ldots, c_n)$。由于 P是一个次数为 r的非零齐次多项式，其特化 $P(1, x_1, \ldots, x_n)$也非零，因此根据 c_i的代数独立性，$\det(J) = P(1, c_1, \ldots, c_n) \neq 0$。所以 $\operatorname{rank}(M) \geq r$ ，得证。

□

逆命题的主要内容包含在以下引理中。

引理 4.13。设 k是一个交换环，并设 $P \in k[x_1, \ldots, x_n]$。存在一个方阵 N ，其系数取自

$$k + kx_1 + \cdots + kx_n$$

使得 $\det(N) = P$。

暂且先假定该引理成立，并证明 Roy定理。

定理4.11的证明。假设结构秩猜想成立。设 $c_1, \ldots, c_n \in \mathscr{L}$ 在有理数域 Q 上线性无关，并且对于某个非零的 $P \in \mathbb{Q}[x_1, \ldots, x_n]$，有 $P(c_1, \ldots, c_n) = 0$。如引理 4.13 所示，取一个系数属于 $\mathbb{Q} + \mathbb{Q}x_1 + \cdots + \mathbb{Q}x_n$ 的方阵 N，使得 $\det(N) = P$。

令 M 为将 x_i 替换为 c_i 后得到的矩阵 N 。于是有 $\det(M) = 0$。注意，结构秩猜想中的矩阵 M_x 是矩阵 N 的齐次化，其系数属于 $\mathbb{Q}x_0 + \mathbb{Q}x_1 + \cdots + \mathbb{Q}x_n$。这里我们利用了 c_i 与 1 在 Q 上线性无关，因为 e 是超越的。该猜想意味着 $\det(M_x) = 0$，因此通过对 $x_0 = 1$ 进行特化可得 $\det(N) = 0$ ，这就产生了矛盾。

□

现在还需证明引理 4.13。首先要指出的是，这条引理实际上是理论计算机科学一个重要研究方向的起点；在该领域，这条引理通常归功于 Valiant。已有众所周知的高效算法可用于计算矩阵的行列式，因此，将一般多项式表示为一个行列式，就能得到一种高效计算多项式取值的算法。表示给定多项式为行列式所需矩阵的最小维数，称为该多项式的行列式复杂度。研究多项式族中行列式复杂度的增长，是一个已有大量文献探讨的课题。

我们沿用 Roy 对引理 4.13 的证明。我们需要证明两个子引理。

引理 4.14. 对于一个非负整数 d，令 $P_d \subset k[x_1, \ldots, x_n]$ 表示次数为 $\leq d$ 的多项式的 k-子空间。给定 $N \in M_{m\times m}(P_d)$ 且满足 $d \geq 1$，存在一个整数 s和矩阵

$$A \in M_{m\times s}(P_{d-1}), \quad B \in M_{s\times m}(P_1)$$

使得 $N = AB$。

证明。令 $N = (a_{i,\ j})$ 且满足 $a_{i,\ j} \in P_d$。我们可以写成

$$a_{i,j} = \sum_{\ell=1}^{n} c_{i,j,\ell} x_\ell + c_{i,j,n+1}$$

其中，对于 $1 \leq \ell \leq n+1$，有 $c_{i,\ j,\ \ell} \in P_{d-1}$。令

$$c_{i,j} = (c_{i,j,\ell}) \in M_{1\times(n+1)}(P_{d-1}), \quad x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \\ 1 \end{pmatrix} \in M_{(n+1)\times 1}(P_1).$$

定义

$$A = (c_{i,j}) \in M_{m\times m(n+1)}(P_{d-1}), \quad B = x \otimes 1_{m\times m} \in M_{(n+1)m\times m}(P_1).$$

于是可计算得 $N = AB$。 □

引理 4.14 中的矩阵 A 和 B 不是方阵，因此我们无法递归地应用该引理。以下观察可以解决这个问题。

引理 4.15. 设 $A \in M_{m\times s}, B \in M_{s\times m}$。则

$$\det(AB) = \det \begin{pmatrix} I_s & B \\ -A & 0 \end{pmatrix},$$

其中右侧的矩阵是一个维数为 $m+s$ 的方阵。

证明。我们只需注意到

$$\begin{pmatrix} I_s & 0 \\ A & I_m \end{pmatrix} \begin{pmatrix} I_s & B \\ -A & 0 \end{pmatrix} \begin{pmatrix} I_s & -B \\ 0 & I_m \end{pmatrix} = \begin{pmatrix} I_s & 0 \\ 0 & AB \end{pmatrix}$$

并对等式两边取行列式。 □

现在我们可以证明主要引理。

引理 4.13 的证明。更一般地，现在通过对 d 进行归纳可得：对于任意矩阵$N \in M_{m\times m}($$P_d$)，都存在一个矩阵 $N' \in M_{m'\times m'}(P_1)$，使得行列式($N$) =行列式($N'$)。

基例 $d = 1$ 是显然的。对于 $d > 1$，我们利用引理 4.14 将 $N = AB$ 写成$A \in M_{m\times s}(P_{d-1})$和 $B \in M_{s\times m}(P_1)$。于是由引理 4.15 可得行列式 (N) = 行列式 (N')，其中 $N' \in M_{(m+s)\times(m+s)}($$P_{d-1}$)。归纳法至此完成。

该引理对应于从复数域中的一个 1×1 矩阵出发的情形。 □

5 Waldschmidt 和 Masser 定理

据我们所知，关于结构秩猜想，最强的一般性无条件结果是引言中陈述的 Waldschmidt和Masser 的定理 1.6 [21]。为求变化，本节将证明该猜想的 p-进版本，不过阿基米德版本的证明基本相同。 p-进版本的陈述与阿基米德版本完全相同，只需将 $\mathscr{L}$ 替换为 $\mathscr{L}_p$。

定理 5.1（Waldschmidt–Masser）。设 m, n 为正整数，且令 $M \in M_{m\times n}(\mathscr{L}_p)$。假设

$$rank(M) < mn/(m + n).$$

那么存在 $P \in$ GL$_m$(有理数域) 和 $Q \in$ GL$_n$(有理数域)，使得 $PMQ = \begin{pmatrix} M_1 & 0 \\ M_2 & M_3 \end{pmatrix}$ 其中，0 块的维数为 $m' \times n'$，且 $m'/m + n'/n > 1$。

5.1 应用

下面陈述复数域和 p-进 Waldschmidt–Masser 定理的一些应用。六指数定理早在 20 世纪 60 年代就已得到证明，它是 Waldschmidt–Masser 定理的一个推论。

定理 4.2 的证明。 $M = 0$ 的情形是平凡的。因此设 $M \in M_{2\times 3}(\mathscr{L})$ 的秩为 1。由于 $1 < 6/5$，Waldschmidt–Masser 定理表明，经过左右两侧的有理基变换后，矩阵 M 具有分块矩阵形式

$$PMQ = \begin{pmatrix} M_1 & 0 \\ M_2 & M_3 \end{pmatrix}$$

其中 0 块的维数为 1×2 或 2×1。在第一种情况下，我们的矩阵具有如下形式

$$PMQ=\begin{pmatrix} * & 0 & 0\\ * & * & *\end{pmatrix}.$$

这样的矩阵秩为 1，当且仅当它具有以下形式

$$PMQ=\begin{pmatrix} 0 & 0 & 0\\ * & * & *\end{pmatrix}\quad\text{or}\quad PMQ=\begin{pmatrix} * & 0 & 0\\ * & 0 & 0\end{pmatrix}.$$

在第一种情形下，我们看到 PM 具有相同的形状，这说明 M 的行在 Q 上线性相关。在第二种情形下，我们看到 MQ 具有相同的形状，这说明 M 的列在 Q 上线性相关。原来的零块维数为 2×1 的情形也类似。

□

对于方阵，Waldschmidt–Masser 定理可简化为以下结论。

推论 5.2. 设 $M\in M_{n\times n}(\mathscr{L})$ 或 $M_{n\times n}(\mathscr{L}_p)$。假设秩$(M)<n/2$。那么存在 $P,Q\in \mathrm{GL}_n(\mathbb{Q})$，使得

$$PMQ=\begin{pmatrix} M_1 & 0\\ M_2 & M_3\end{pmatrix}\quad \textit{(block matrix)}$$

其中零块的维数为 $m\times m'$，且 $m+m'>n$。

推论 5.3. Leopoldt 调节子矩阵和 Gross–Kuz'min 调节子矩阵的秩至少为其预期秩的一半。

证明。设 r 为 Leopoldt 矩阵的预期秩。设

$$M'=(\log|\sigma_j(u_i)|)_{i,j=1,\dots,r}$$

为阿基米德调节子的一个 $r\times r$ 子矩阵，且 $\det(M')\neq 0$。设

$$M=(\log_p\sigma_j(u_i))_{i,j=1,\dots,r}$$

为 Leopoldt 矩阵中相应的子矩阵。

若 Leopoldt 矩阵的秩小于 $r/2$，则 M也满足同样的情况。由此，Waldschmidt–Masser 定理推出存在 $P,Q\in\mathrm{GL}_r(\text{有理数域})$，使得 PMQ具有一个维数为 $m\times m'$的右上角零块，其中 $m+m'>r$。但这样一来， $PM'Q$ 也具有相同的性质。这意味着 $\det(M')=0$，矛盾。

对于 Gross 调节子，同样的证明也成立，只需用 ord_p 代替 $\log|\cdot|$. □

5.2 辅助多项式

与 Baker定理 的证明一样，Waldschmidt–Masser 定理的证明是在定理的假设下构造一个合适的辅助多项式，其存在性蕴含定理的结论。Waldschmidt 的结果表明该辅助多项式存在，而 Masser 定理则表明这个多项式能得出所需结论。下面我们对此作更详细的说明。

我们有 $M = (a_{i,\ j})$，其中 $a_{i,\ j} = \log_p(x_{i,\ j}) \in \mathscr{L}_p$。这里 $x_{i,\ \overline{j}} \in$ 有理数域*。必要时缩放 M，我们可以假设 $|x_{i,\ j} - 1|_p < 1$。对于 $i = 1$，……，m，令

$$x_i = (x_{i,j})_{j=1,\ldots,n} \in (\overline{\mathbf{Q}}^*)^n \subset (\mathbf{C}_p^*)^n.$$

令 $X = \langle x_i \rangle \subset$ (有理数域*)^n 为由 x_i生成的子群。对于每个正整数 N，定义

$$X(N) = \left\{ \prod_{i=1}^{m} x_i^{a_i} : 0 \le a_i \le N \right\}.$$

对于多个变量的多项式 P，我们用 deg(P) 表示 P的总次数。

定理5.4（Waldschmidt）。设 $r =$ rank(M) $< mn/(m+n)$。存在 $\epsilon > 0$，使得对于所有充分大的 N，存在一个非零的 $P \in$ 整数环$[t_1, \ldots, t_n]$，满足 deg(P) $< N^{m/n-\epsilon}$，且对于所有 $x \in X(N)$，$P(x) = 0$。

Waldschmidt 定理是定理 1.6 中关于“超越性”的部分。Masser 定理是一个纯粹的代数几何命题，它以存在如上所述的辅助多项式P 为前提，推导出对原矩阵 M给出所需结论所必需的关系。我们稍后会准确描述 Masser 定理的表述，但首先让我们评论一下定理5.4表述中有关辅助多项式的数值关系。我们可以将存在具有指定零点的多项式看作关于该多项式系数的线性方程组。每个零点给出一个这样的线性方程。如果 $x_{i,j}$ 是一般的，则 $X(N)$的大小为 $(N+1)^m$。次数为 $< d$ 的多项式的系数少于 d^n 个。因此，如果 $x_{i,j}$ 是一般的，我们预计多项式要存在就需要 $d^n \ge (N+1)^m$，特别是 $d > N^{m/n}$。因此，定理5.4中的辅助多项式 P 的存在性对于一般的$x_{i,j}$并不成立。

现在让我们精确陈述 Masser 定理。设 k 为一个特征为零的域，设 $(x_{i,\ j}) \in M_{m\times n}($$k^*$)。按上述方式定义 X和 $X(N)$。定义一个配对

$$\mathbf{Z}^m \times \mathbf{Z}^n \longrightarrow k^*$$
$$\langle (a_i), (b_j) \rangle = \prod_{i,j} x_{i,j}^{a_i b_j}.$$

定理 5.5（Masser）。设 $N > 0$，并假设存在 $P \in k[t_1, \ldots, t_n]$ 使得 deg(P) $<(N/n)^{m/n}$，且对所有 $x \in X(N)$，$P(x) = 0$。那么存在子群 $A \subset \mathbf{Z}^m$、$B \subset \mathbf{Z}^n$，其秩分别为 m'、n'，且满足 $\langle A$、$B \rangle = 1$ 和 $m'/m + n'/n > 1$。

定理 5.4 和定理 5.5 合起来便得到定理 5.1。本节余下部分将证明这两个定理。

5.3 Waldschmidt 定理

我们将给出 Waldschmidt 定理的两种证明。

5.3.1 Waldschmidt 定理的证明 1

我们的第一种证明在思路上与 Waldschmidt 的原始证明相似。为简单起见，我们假设 $x_{i,j} \in \mathbf{Z}$ 且 $x_{i,j} \equiv 1 \pmod{p}$。标准技巧（乘以一个整数以得到代数整数，并取范数以得到整数）可以处理一般情形，但我们希望避免所需的额外记号。

令 r 表示矩阵 $M \in M_{m\times n}(\mathbf{Z}_p)$ 的秩。必要时重新排列列后，我们可以假设 M 的最后 $n-r$ 列属于前 r 列的 $\mathbf{Z}_p$-线性张成。于是，对每个 $i > r$，存在 $\lambda_{i,1}, \ldots, \lambda_{i,r} \in \mathbf{Z}_p$，使得若 $z = (z_1, \ldots, z_n) \in X$，则有

$$z_i = z_1^{\lambda_{i,1}} z_2^{\lambda_{i,2}} \cdots z_r^{\lambda_{i,r}}, \qquad i > r. \tag{30}$$

为理解这个等式右边的含义，注意，对于 $\lambda \in \mathbf{Z}_p$，函数

$$t^\lambda = (1 + (t-1))^\lambda = \sum_{i=0}^{\infty} \binom{\lambda}{i} (t-1)^i \tag{31}$$

是收敛的幂级数。因而，若 $t \in 1 + p\mathbf{Z}_p$，则 (31) 在 $\mathbf{Z}_p$ 中收敛。

我们的目标是找到一个多项式 $P \in \mathbf{Z}[t_1, \ldots, t_n]$，使得 $P(z) = 0$ 对于 $z \in X(N)$ 成立。定义 $u_i = t_i - 1$，并考虑典范映射

$$\begin{aligned} \varphi\colon \mathbf{Z}[t_1, \ldots, t_n] &\longrightarrow \mathbf{Z}_p[[u_1, \ldots u_n]]/(t_i - t_1^{\lambda_{i,1}} \cdots t_r^{\lambda_{i,r}})_{i=r+1}^n \\ &\cong \mathbf{Z}_p[[u_1, \ldots, u_r]]. \end{aligned} \tag{32}$$

元素 (32) 中的 s 通过 (31) 被视为 u_i 中的幂级数。

固定一个正整数 c。定义 φ_c 为 φ 与典范约化的复合

$$\mathbf{Z}_p[[u_1, \ldots, u_r]] \longrightarrow (\mathbf{Z}/p^c\mathbf{Z})[[u_1, \ldots, u_r]]/(u_1^c, \ldots, u_r^c). \tag{33}$$

如果多项式 $P \in \mathbf{Z}[t_1, \ldots, t_n]$ 满足 $\varphi_c(P) = 0$，那么对于任意 $z \in X$，$P(z)$ 都能被 p^c 整除。事实上，对于 $z \in X$，$\varphi(P)(z) = P(z)$ 是良定义的，因为 φ 的核在 X 上消失。接下来，显然，$\varphi(P)(z) \pmod{p^c}$ 仅取决于 $\varphi(P)$ 的系数模 p^c。最后，我们注意到 $z_i \equiv 1 \pmod{p} \implies u_i \equiv 0 \pmod{p} \implies u_i^c \equiv 0 \pmod{p^c}$。

现在，(33) 右侧的环是有限的。在 $u_1, \ldots, u_r$ 模 $(u_1^c, \ldots, u_r^c)$ 下单项式的总数为 c^r，因此这些系数模 p^c 的可能取值总数为

$$(p^c)^{c^r} = p^{c^{r+1}}.$$

因此，根据鸽巢原理，如果我们有一个大小大于 $p^{c^{r+1}}$ 的 $\mathbf{Z}[t_1, \ldots, t_n]$ 子集，那么该子集中的某两个元素（设为 P_1 和 P_2）在 φ_c 下的像相同，且它们的差 $P = P_1 - P_2$ 将满足 $P(z) \equiv 0$（模 p^c），对所有 $z \in X$ 均成立。

我们取所有多项式构成的子集：每个变量的次数都小于某个常数 d，且系数为小于某个常数 h 的非负整数 p^h。这个子集的大小为 p^{hd^n}，因此我们所需的条件是

$$hd^n > c^{r+1}. \tag{34}$$

现在，我们还想运用 Baker定理 证明中讨论的“整数的离散性”原理，以确保当 $z \in X(N)$ 时，条件 $P(z) \equiv 0$ (模 p^c) 能推出 $P(z) = 0$。为此，我们需要对 $|P(z)|$（阿基米德绝对值）给出一个粗略的上界。假设 A 是 $|x_{i,\ j}|$ 的上界。那么，对每个 $z = (z_1, \ldots, z_n) \in X(N)$，都有 $|z_i| < A^{Nm}$。因此， $P(z)$ 的取值中每个单项式的绝对值至多为 $p^h A^{Ndmn}$，总计可得

$$|P(z)| < d^n p^h A^{Ndmn}.$$

因此，如果

$$d^n p^h A^{Ndmn} < p^c \tag{35}$$

那么我们确实可以得到蕴含关系

$$P(z) \equiv 0 \pmod{p^c} \Longrightarrow P(z) = 0.$$

为证明该定理，令 $d = \lfloor N^{m/n-\epsilon}/n \rfloor$，这样构造出的多项式 P 的次数将小于 $N^{m/n-\epsilon}$，正如所要求的那样。我们寻找参数 h 和 c，使得 (34) 和 (35) 均成立。不出所料，这些不等式的要求方向相反——第一个不等式表明，相对于 c 而言， h 较大；第二个不等式则表明，相对于 c 而言， h 较小。当 N 较大时，如果

$$h \cdot N^{m-n\epsilon} \gg c^{r+1}, \qquad c > k(\log N) + h + k' N^{(m+n)/n-\epsilon}$$

对于适当的常数 k、k'，

如果令 $c = N^{(m+n)/n+\epsilon}$ 和 $h = cN^{-\delta}$ 为一个较小的 $\delta > 0$，那么显然，当 N 足够大时，第二个不等式将成立。将这些参数代入第一个不等式可得

$$m - \delta > \left(\frac{m}{n} + 1 + \epsilon\right) r.$$

I显然，我们可以选择满足该不等式的较小正数 δ、ϵ f

$$m > \left(\frac{m}{n} + 1\right) r, \qquad \text{i.e.,} \qquad r < \frac{mn}{m+n}.$$

至此，证明完成。

5.3.2 Waldschmidt 定理的证明 2

在第二种证明中，我们将回到完全一般的情形，也就是说，不假设 $x_{i,j} \in \mathbf{Z}$，只假设 $x_{i,j} \in \mathbf{Q}^*$。给出第二种证明的动机在于，它引入了超越数理论中一个此前未曾讨论的重要主题，即由 Michel Laurent 开创的插值行列式理论。在 [14], Laurent 利用他的新理论给出了六指数定理的一种新证明。基本思想是，我们将把所需多项式 P 的存在视为关于该多项式系数的线性方程组的解，并证明相应的行列式为零。

再次，我们将构造一个多项式 P，使得每个变量的次数都小于$d = \lfloor N^{m/n-\epsilon}/n \rfloor$，且对所有 $z \in X(N)$，都有 $P(z) = 0$。考虑如下矩阵，其行由我们希望得到的零点 $z \in X(N)$ 索引，列由

$$y \in \mathbf{Z}^n(d-1) = \{(y_1, \ldots, y_n) \colon 0 \le y_i \le d-1\}.$$

我们希望得到的多项式的单项式的指数索引：

$$L = (z^y) \in M_{(N+1)^m \times d^n}(\mathbf{C}_p).$$

只需证明秩$(L) < N^{m-n\epsilon}/n^m < d^n$，因为这样一来，其核中的任意非零向量都将是我们希望得到的多项式的系数。当然，只要让 ϵ 更小，我们就可以忽略常数 n^m，因为当 N 足够大时，$N^\epsilon \gg n^m$。

下面不加证明地陈述矩阵秩的一种初等解释。

引理 5.6. 设 k 是一个域，并设有一个矩阵

$$(a_{i,j}) \in M_{m \times n}(k)$$

秩等于 r。那么存在向量

$$\beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_n \in k^r$$

使得 $a_{i,j} = \langle \beta_i, \gamma_j \rangle$。

In 在我们的情形中，我们有 $M = \log_p(x_{i,j}) \in M_{m \times n}$(复数域$_p$)，其秩为 r。我们记 e

$$\log_p(x_{i,j}) = \langle \beta_i, \gamma_j \rangle \qquad \text{for } \beta_i, \gamma_j \in \mathbf{C}_p^r.$$

不失一般性，我们可以对所有的 β_i, γ_j 进行缩放，使其所有坐标的绝对值均为 $< p^{-1}$。（这只是缩放矩阵 M，既不影响定理的假设，也不影响其结论。）

若 $z = \prod_{i=1}^m x_i^{\ell_i}$属于 $\ell \in$ 整数环^m，则对于 $y \in$ 整数环^n，我们有

$$z^y = \exp\left\langle \sum \beta_i \ell_i, \sum \gamma_j y_j \right\rangle.$$

接下来我们需要一个 p-进 Schwarz 引理。对于正整数 d 和实数 $R > 0$，定义

$$B_d(R) = \{(z_1, \ldots, z_d) \colon |z_i| \leq R \text{ for all } i\} \subset \mathbf{C}_p^d.$$

对于解析函数 $f\colon B_d(R) \longrightarrow \mathbf{C}_p$，定义

$$|f|_R = \max_{z \in B_d(R)} |f(z)|. \tag{36}$$

引理 5.7. 假设 $f\colon B_1(R) \longrightarrow \mathbf{C}_p$ 是解析函数，且在 $z = 0$ 处有阶数至少为 n 的零点。那么对于任意 $0 < R' < R$，有

$$|f|_{R'} \leq \left(\frac{R}{R'}\right)^{-n} |f|_R.$$

证明. 令 $g(z) = f(z)/z^n$。由于 f 在 $z = 0$ 处有阶数至少为 n 的零点，因此它在 $B_1(R)$ 上是解析的。对于任意 $z \in B_1(R')$，有

$$\begin{aligned} |f(z)| &\leq (R')^n |g(z)| \\ &\leq (R')^n |g|_R \\ &= \left(\frac{R'}{R}\right)^n |f|_R. \end{aligned}$$

最后一个等式用到了 p-进最大模原理，该原理指出 (36) 中的最大值在边界 $|z| = R$ 上取得。证明这一解析事实，请参见 [5, 定理 1.4.1] 或 [18, 定理 7] 。

□

现在我们给出 Laurent 主定理关于插值行列式的论述。

定理 5.8 (Laurent). 设 $0 < R' < R$，并设 $f_1, \ldots, f_d$ 是解析函数

$$B_r(R) \longrightarrow \mathbf{C}_p.$$

设 $z_1, \ldots, z_d \in B_r(R')$. 则 $L = \det(f_j(z_i))$ 满足

$$|L| \leq \left(\frac{R}{R'}\right)^{-\Theta_r(d)} \prod_{i=1}^{d} |f_i|_R,$$

其中对于相对于 r 足够大的 d ，

$$\Theta_r(d) > \frac{r}{6e} d^{(r+1)/r}. \tag{37}$$

证明。定义 $\Delta(z) = \det(f_j(z_i z))$，它在 $|z| \leq R/R'$ 上解析。我们将证明，对于某个满足（37）的组合函数 Θ_r ， $\Delta(z)$ 在 $z = 0$ 处具有至少 $\Theta_r(d)$ 阶数为.....的零点；该函数将在下面立即定义。由 Schwarz 引理，结论随即成立：

$$|L| = |\Delta(1)| \leq \left(\frac{R}{R'}\right)^{-\Theta_r(d)} |\Delta|_{R/R'}$$

利用平凡上界

$$|\Delta|_{R/R'} \le \prod_{i=1}^{d} |f_i|_R.$$

（注意，在复数情形下，右侧需要乘以 $d!$ ；但在非阿基米德情形下，由于强三角不等式，无需乘以这个因子。）

将每个 f_i 写成变量 u_1、.....、$u_r \in \mathbf{C}_p$ 的幂级数。由行列式的多重线性，只需考虑 $f_j(u) = u^{v_j} = u_1^{v_{1j}} u_2^{v_{2j}} \cdots u_r^{v_{rj}}$（其中 v_{ij} 为非负整数）的情形。于是

$$\Delta(z) = z^{\sum_j ||v_j||} \det(z_i^{v_j}),$$

其中 $||v_j|| = v_{j1} + v_{j2} + \cdots + v_{jr}$。如果两个元组 v_j 相等，那么该行列式为零，且 $\Delta(z)$ 恒等于 0。否则，消失阶至少为

$$\Theta_r(d) := \text{the minimum of } \sum_{j=1}^{d} ||v_j|| \text{ as } v_j \text{ ranges}$$
$$\text{over all distinct tuples of elements of } (\mathbf{Z}^{\ge 0})^r.$$

例如，$\Theta_1(d) = d(d-1)/2$. 组合不等式（37）的证明见[19,引理 4.3]。

□

现在我们可以应用 Laurent 定理，完成 Waldschmidt 定理的证明。我们要证明，L 的任意一个维数为 $d^n \approx N^{m-n\epsilon}$ 的方形子矩阵 $L' = (z_i^y)$ 的行列式都为零，其中

$$z_1, \ldots, z_d \in X(N), \quad y \in \mathbf{Z}^n(d-1), \quad d = \lfloor N^{m/n-\epsilon} \rfloor.$$

如前所述，矩阵 L' 的各项可以写成 $\exp(\langle \sum \beta_i \ell_i, \sum \gamma_i y_i \rangle)$，其中 $\ell \in \mathbf{Z}^m(N)$ 对应于 z。对每个 y，我们都有函数

$$f_y(u_1, \ldots, u_r) = \exp(\langle u, \sum \gamma_i y_i \rangle)$$

我们将 Laurent 定理应用于插值行列式，其中取 $R = 1$ 和 $R' = 1/p$。于是得到

$$|L'| \le C^{-N^{(m-n\epsilon)(r+1)/r}}$$

其中 $C > 1$ 是一个常数。

现在我们要对 L' 的阿基米德绝对值给出一个上界。令

$$A = \max_{i,j} |x_{i,j}|_\infty.$$

于是 $|z^y|_\infty \le A^{N \cdot N^{(m/n)-\epsilon} n}$。因此

$$|L'|_\infty \le (N^{m-n\epsilon})! \cdot D^{N^{(m/n)+1+m-(n+1)\epsilon}}.$$

阶乘的增长被另一项压过，因此可以忽略。通过缩放使其满足整性，只会缩放 D。从由 $x_{i,j}$ 生成的域向下取范数到有理数域 Q，以得到一个整数环 Z 中的元素，情况也一样。

因此，当 $L' = 0$ 时，我们有

$$C^{N^{(m-n\epsilon)(r+1)/r}} > D^{N^{(m/n)+1+m-(n+1)\epsilon}}.$$

当然，要使这个不等式对较大的 N 成立， C 和 D 的具体取值并不重要；重要的是满足相应的指数不等式。

因此，只需满足

$$(m - n\epsilon)\frac{r+1}{r} > \frac{m}{n} + 1 + m - (n+1)\epsilon.$$

这可化简为

$$\frac{1}{r} > \frac{m+n}{mn} + \epsilon\left(\frac{n-r}{r}\right).$$

存在满足此不等式的 $\epsilon > 0$，当且仅当

$$r < \frac{mn}{m+n}.$$

由此可得 det(L') 如所需为零，并完成 Waldschmidt 定理的第二个证明。

5.4 Masser 定理

我们通过证明上文定理 5.5 中陈述的 Masser 定理来结束本节。这是一个纯粹的代数几何命题，不涉及对数或指数函数。特别地，我们在任意特征零域 k 上进行讨论。回顾 §5.2 中建立的记号。令群 $X \subset (k^*)^n$ 作用于多项式环 $R = k[t_1, \ldots, t_n]$，其作用为

$$z \cdot f = f(z_1 t_1, z_2 t_2, \ldots, z_n t_n).$$

回顾一下，子群 X 由元素 x_1、.....、x_m 生成。如果 $a \in \mathbf{Z}^m$，我们记作 $x^a = \prod_{i=1}^m x_i^{a_i} \in X$。对于素理想 $\mathfrak{p} \subset R$，令

$$\mathrm{Stab}_X(\mathfrak{p}) = \{a \in \mathbf{Z}^m \colon x^a \cdot \mathfrak{p} = \mathfrak{p}\}.$$

在深入证明之前，先考察最简单的情形 $n = m = 2$ 是很有启发性的。令 $N > 0$，并假设存在 $P \in k[t_1, t_2]$，使得 deg(P) $< N$，且对于所有 $x \in X(2N)$，都有 $P(x) = 0$。我们要证明以下两种情况必有一种成立：

(A) 存在一个非零的 $a \in$ 整数环^2，使得 $x^a =$ (1, 1)（这对应于 $m' = 1, n' = 2$），或者

(B) 存在一个非零的 $b \in$ 整数环[2]，使得 $z^b = z_1^{b_1} z_2^{b_2} = 1$ 对所有 $z \in X$（这对应于 $m' = 2, n' = 1$）。

我们将 P 分解为不可约因子的乘积 $\prod P_i$。可以假设其中没有任何 P_i是单项式，因为单项式在（k^*）[2]中没有零点。我们首先证明，如果某个 P_i满足 $\mathrm{rank}(\mathrm{Stab}_X((P_i))) = 2$，那么我们就处于上述第二种情形。这由下面的引理 5.9 得出，但在此情形下也很容易直接看出。事实上，如果 $t_1^{a_1} t_2^{a_2}$ 是 P_i中出现的一个单项式，那么关于 $z \in X$ 和 $\lambda \in k^*$ 的方程 $zP_i = \lambda P_i$ 给出

$$z_1^{a_1} z_2^{a_2} = \lambda.$$

令 $t_1^{a_1'} t_2^{a_2'}$为 P_i 中出现的另一个单项式（回忆一下，我们可以假设 P_i 不是单项式），得到一个类似的方程；将这两个方程相除后，λ 被约去，于是得到

$$z_1^{b_1} z_2^{b_2} = 1,$$

其中，对于 $i = 1$而言，$b_i = a_i - a_i'$、2 不同时为零。如果 $\mathrm{rank}(\mathrm{Stab}_X((P_i))) = 2$，那么这对有限指数子群 X中的所有 z 都成立，因此将（b_1，b_2）替换为适当的倍数后，我们处于情形（B）。

因此，我们只需考虑这样的情形：每个不可约因子 P_i of P 都满足 $\mathrm{rank}(\mathrm{Stab}_X((P_i))) \leq 1$. 在这种情形下，我们将证明存在一个形如

$$Q = \sum_{i=1}^{k} a_i (z_i \cdot P),$$

其中 $a_i \in \mathbf{Z}$ 且 $z_i \in X(N)$，使得 P 和 Q 互素。我们先说明为何这就完成了证明。由于 P 在 $X(2N)$ 上为零，因此每个满足 $z \cdot P \,\mathrm{with} z \in X(N)$ 的多项式都在 $X(N)$ 上为零，从而多项式 Q 在 $X(N)$ 上为零。因此，P和 Q 都在 $X(N)$ 上为零。集合 $X(N)$ 的大小为 $(N+1)^2$，除非我们处于上面的情形 (A) 中。但是 $\deg Q \leq \deg P < N$，且这些多项式互素，所以如果这些多项式有 $(N+1)^2$ 个公共零点，根据贝祖定理就会得到矛盾。因此，我们必定处于情形 (A) 中。

为证明多项式 Q 的存在性，我们首先证明，对于每个不可约多项式 P_i，都存在 z_i，使得 $z_i^{-1} \cdot P_i$ 不整除 P；等价地，P_i 不整除 $z_i \cdot P$。这可通过计数得到。由于 $\mathrm{rank}_X((P_i)) \leq 1$，当 z 遍历 $X(N)$ 时，集合 $(z^{-1} \cdot P_i)$ 中至少有 $N+1$ 个不同的理想。证明见下文的引理 5.12。但是 P 的次数小于 N，而 N 是不可约因子个数的上界，因此必有某个 $z^{-1} \cdot P_i$ 不是 P 的因子。有了这些 z_i，线性组合 Q 的存在性便可通过鸽巢原理用一个简单的归纳论证得出；见下文的引理 5.13。

现在我们回到一般情形。回顾一下，素理想 $\mathfrak{p}$ 的高度 $\mathrm{ht}(\mathfrak{p})$ 是满足以下条件的最大整数 r：存在一条由互不相同的素理想组成的链

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_r = \mathfrak{p}.$$

引理 5.9. 设 $\mathfrak{m} = (t_1 - 1, \ldots, t_n - 1)$。设 $\mathfrak{p} \subset \mathfrak{m}$ 是高度为 n' 的素理想，并设$A = \mathrm{Stab}_X(\mathfrak{p})$。存在一个秩为 $\geq n'$ 的子群 $B \subset \mathbf{Z}^n$，使得 $\langle A, B\rangle_X = 1$。

证明。令 $B = \{y \in \mathbf{Z}^n\colon \ \langle A, y\rangle_X = 1\}$. 取 $Z \subset \mathbf{Z}^n$ 使得

$$\mathbf{Q}^n = \mathbf{Q}B \oplus \mathbf{Q}Z.$$

我们要证明: $s := \mathrm{rank}(Z) \leq n - n'$。令 $z_1, \ldots, z_s$ 为 Z 的一组基。将$z_i = (z_{i,\ 1}, \ldots, z_{i,\ n})$写作。

对于 $i = 1, \ldots, s$，令 $u_i = \prod_{j=1}^n t^{z_{i,\ j}}{}^{\ j} \in R' = k[t_1^{\pm 1}, \ldots, t_n^{\pm 1}]$。由于

$$\mathrm{trd}_k \operatorname{Frac}(R'/\mathfrak{p}R') = n - n',$$

若 $s > n - n'$，则存在一个系数属于 k 的非零多项式 Q，使得$Q(u_1, \ldots, u_s) \in \mathfrak{p}R'$。假设情况如此，并将 $Q(u_1, \ldots, u_s)$ 写成多项式$Q'(t_1, \ldots, t_n) \in \mathfrak{p}R'$。

对于任意 $a \in A$，我们有 $x^a \cdot Q' \in \mathfrak{p}R'$，因此

$$\begin{aligned} Q'(x^a t) \in \mathfrak{p}R' \subset \mathfrak{m}R' &\Longrightarrow Q'(x^a) = 0 \\ &\Longrightarrow Q(\langle a, z_1\rangle_X, \ldots, \langle a, z_s\rangle_X) = 0. \end{aligned}$$

固定 a，并将 a 替换为 da，其中 $d = 0$、1、.....。利用 Baker定理中的范德蒙德技巧，我们得到 z_i 的某个 Z-线性组合与 a正交。更确切地说，对于某个

$$w \in S = \left\{ \sum_{i=1}^s w_i z_i \neq 0,\ |w_i| \leq \deg(Q) \right\}.$$

因此

$$A = \bigcup_{w \in S} w^{\perp}.$$

但是 A 是有限生成自由阿贝尔群，不能表示为真子群的有限并。因此，存在 $w \in S$ 使得 $\langle A、\ w\rangle = 1$。但这样一来，$w \in B$，这与 $w \in Z$矛盾。因此，$s \leq n - n'$，如所需。 □

根据引理 5.9，我们现在的任务是证明存在一个素理想 $\mathfrak{p}$，其高度为 n'，满足 $\mathrm{Stab}_X(\mathfrak{p})$ 的秩 $= m'$，其中 $m'/m + n'/n > 1$。下面的定理给出了这一点。

定理 5.10。设 $N > 0$，并假设存在

$$P \in k[t_1, \ldots, t_n]$$

使得 $\deg(P) < (N/n)^{m/n}$且 $P(x) = 0$对所有 $x \in X(N)$成立。则存在一个高度为 n' 的素理想 $\mathfrak{p} \subset \mathfrak{m}$，使得

$$\mathrm{rank}(\mathrm{Stab}_X(\mathfrak{p})) = m' \quad \textit{where} \quad m'/m + n'/n > 1.$$

引理 5.9 和定理 5.10 结合起来即可得到定理 5.5。我们将证明定理 5.10 的逆否命题。对于每个 $1 \le n' \le n$，令 $m' = m'_{n'}$ 为当 $\mathfrak{p}$ 遍历包含于 $\mathfrak{m}$ 且高度等于 n' 的素理想时 $\mathrm{Stab}_X(\mathfrak{p})$ 的最大秩。若存在某个 $m' = m$，则 $m'/m + n'/n = 1 + n'/n > 1$，因此结论成立。所以设每个 $m' < m$ 都满足，并定义

$$\eta_{n'} = \frac{n'}{m - m'}.$$

注意，

$$\eta_{n'} > n/m \iff m'/m + n'/n > 1. \tag{38}$$

定理 5.10 将作为以下命题的推论得到。

定理 5.11。设 $f \in R$ 的次数为 D，并令

$$N = D^{\eta_1} + D^{\eta_2} + \cdots + D^{\eta_n}.$$

存在 $z \in X(N)$，使得 $f(z) \neq 0$。

定理 5.11 蕴含定理 5.10。事实上，如果每个 $\eta_{n'}$ 对 $1 \le n' \le n$ 都满足 $\eta_{n'} \le n/m$，那么定理 5.11 蕴含存在 $z \in X(n \deg(P)^{n/m})$，使得 $P(z) \neq 0$。但根据假设，$n \deg(P)^{n/m} < N$，这与假设 $P(z) = 0$ 对所有 $z \in X(N)$ 均成立矛盾。因此，某个 $\eta_{n'}$ 大于 n/m，由此通过（38）得到所需结果。

定理 5.11 的证明需要大量交换代数知识。我们先引入一些记号。令

$$\mathfrak{M} = \bigcup_{z \in X(N)} z \cdot \mathfrak{m}, \quad S_{\mathfrak{M}} = R - \mathfrak{M}.$$

集合 $S_{\mathfrak{M}}$ 是乘法封闭的。对于理想 $\mathfrak{a} \subset R$，定义

$$\mathfrak{a}^* = (S_{\mathfrak{M}}^{-1}\mathfrak{a}) \cap R \supset \mathfrak{a}.$$

注意，对于素理想 $\mathfrak{p} \subset R$，有 $\mathfrak{p}^* = \mathfrak{p} \Leftrightarrow \mathfrak{p} \subset z \cdot \mathfrak{m}$，其中某个 $z \in X$，否则有 $\mathfrak{p}^* = R$。事实上，若 $\mathfrak{p}^* \neq \mathfrak{p}$，则存在 $t/s \in (S_{\mathfrak{M}}^{-1}\mathfrak{p}) \cap R$，使得 $t/s \notin \mathfrak{p}$。写作 $t/s = g \in R$，其中 $g \notin \mathfrak{p}$。由于 $t = gs \in \mathfrak{p}$ 且 $\mathfrak{p}$ 是素理想，这意味着 $s \in \mathfrak{p}$。由于 $s \in S_{\mathfrak{M}}$，我们得出 $\mathfrak{p} \not\subset \mathfrak{M}$，因此对于任意 $z \in X(N)$，都有 $\mathfrak{p} \not\subset z \cdot \mathfrak{m}$。此外，在这种情况下，我们有 $s/s = 1 \in \mathfrak{p}^*$，所以 $\mathfrak{p}^* = R$。现在，以上所有步骤显然都是可逆的，唯一可能例外的是对所有 $z \in X(N)$ 成立的蕴含 $\mathfrak{p} \not\subset \mathfrak{M} \Longrightarrow \mathfrak{p} \not\subset z \cdot \mathfrak{m}$。这一陈述的逆命题是：对于某个 $z \in X(N)$，有 $\mathfrak{p} \subset \mathfrak{M} \Longrightarrow \mathfrak{p} \subset z \cdot \mathfrak{m}$。这正是素理想避开引理。至此，我们关于 $\mathfrak{p}^*$ 的论证得证。

接下来回顾一些交换代数中的定义。理想 $\mathfrak{a} \subset R$ 的伴随素理想是指满足以下条件的素理想 $\mathfrak{p}$：存在一个 R-模单射 $R/\mathfrak{p} \hookrightarrow R/\mathfrak{a}$。（在我们针对 $n = m = 2$. 的简化证明中，伴随素理想起着不可约因子的作用。）若理想 $\mathfrak{a} \subset R$ 的所有伴随素理想的高度均为 r，则称 $\mathfrak{a} \subset R$ 是高度为 r 的无混合理想。

接下来回顾 R 中理想的维数和次数的定义，以及这些函数的一些基本性质。令 $R_0 = k[t_0, \ldots, t_n]$。对于 $f \in R$，令 $f_0 \in R_0$ 表示 f 的齐次化，其定义是给 f 中的每个单项式补上适当次幂的 t_0，从而得到次数为 $\deg(f)$ 的齐次多项式。对于理想 $\mathfrak{a} \subset R$，令 $\mathfrak{a}_0$ 表示由 $f \in \mathfrak{a}$ 的 f_0 生成的齐次理想。于是，$R_0/\mathfrak{a}_0$ 是一个分次 R_0-模。

存在一个多项式

$$H_{\mathfrak{a}}(t) = a_d t^d + \cdots + a_0 \in \mathbf{Q}[x],$$

称为 $\mathfrak{a}$ 的希尔伯特多项式，使得

$$H_{\mathfrak{a}}(i) = \dim_k(i\text{th graded piece of } R_0/\mathfrak{a}_0)$$

当 i 足够大时。我们分别将 $\mathfrak{a}$ 的维数和次数定义为

$$d(\mathfrak{a}) = d, \qquad \ell(\mathfrak{a}) := \tilde{\ell}(R_0/\mathfrak{a}_0) := a_d \cdot d!.$$

这两者都是整数。它们满足以下性质：

- $\ell((f))$ 是通常意义下 f 的次数。
- 若 $\mathfrak{a} \subset \mathfrak{b}$ 且 $\operatorname{ht}(\mathfrak{a}) = \operatorname{ht}(\mathfrak{b})$，则 $\ell(\mathfrak{a}) \geq \ell(\mathfrak{b})$。
- 如果 $\mathfrak{a}$ 和 $\mathfrak{b}$ 是高度为 r的无混合理想，那么 $\mathfrak{a} \cap \mathfrak{b}$也是无混合的，并且

$$\ell(\mathfrak{a} \cap \mathfrak{b}) \leq \ell(\mathfrak{a}) + \ell(\mathfrak{b}).$$

  注意，由此可知，如果 $\mathfrak{a}$ 是无混合的，那么 $\mathfrak{a}$ 的伴随素理想数为 $\leq \ell(\mathfrak{a})$。为说明这一点，我们注意到存在一个主分解 $\mathfrak{a} = \cap_{i=1}^{r} \mathfrak{q}_i$，其中 $\{\sqrt{\mathfrak{q}_i}\}$ 是伴随素理想的集合。

我们可以开始定理 5.11 的证明。设 $f \in R$ 的次数为 D，并令

$$N_r = D^{\eta_1} + \cdots + D^{\eta_{r-1}}, \qquad \text{for } 1 \leq r \leq n+1.$$

我们将归纳地构造 f_r，它是 $X(N_r) \cdot f$中元素的一个 $\mathbf{Z}$-线性组合，使得 $\mathfrak{a}_r = (f_1, \ldots, f_r)$ 满足以下条件：$\mathfrak{a}_r^* = R$或 $\mathfrak{a}_r^*$是高度为 r 且次数至多为 D^r的无混合理想。

这将证明该定理：对于 $r = n+1$，$\mathfrak{a}_r^*$不可能具有高度 $n+1$，因此 $\mathfrak{a}_r^* = R$，这意味着 $\mathfrak{a}_r \not\subset \mathfrak{M}$。特别地，对于某个 i有 $f_i \notin \mathfrak{m}$，所以如果 $f_i = \sum d_j(z_j \cdot f)$中 $d_j \in$属于 $\mathbf{Z}$ 且 $z_j \in X(N_{n+1})$，那么对于某个 z_j，$f(z_j) \neq 0$，正如所要求的。

基例：取 $f_1 = f$, $\mathfrak{a}_1 = (f)$。于是 $\mathfrak{a}_1^* = (f^*)$，其中 f^*是 f除去不属于 $\mathfrak{M}$的任意不可约因子后所得的商。若 $f^* \neq 1$，则根据 Krull主理想定理，(f^*) 是高度1的无混合理想，其次数为 $\leq D = \deg(f)$。

归纳步骤：假设 $r \geq 2$，并且我们已经构造出 $f_1, \ldots, f_{r-1}$。若 $\mathfrak{a}_{r-1}^* = R$，则可以取 $f_r = f$。我们有 $\mathfrak{a}_r^* = R$，问题就解决了。因此，假设 $\mathfrak{a}_{r-1}^*$ 是高度为 $r-1$ 且次数至多为 D^{r-1}的无混合对象。此时 f_r 的构造稍显复杂，下面概述其步骤。

1. 对于 $\mathfrak{a}_{r-1}^*$ 的任意伴随素理想 $\mathfrak{p}$，通过计数证明存在 $a \in \mathbf{Z}^m(D^{\eta_{r-1}})$，使得 $x^{-a}\mathfrak{p}$ 不与 $\mathfrak{a}_{r-1}^*$ 伴随，即 $\mathfrak{p}$ 不与 $x^a\mathfrak{a}_{r-1}^*$ 伴随。

2。证明这意味着存在 $1 \leq i \leq r-1$，使得 $x^a f_i \notin \mathfrak{p}$。

3. 证明这意味着存在这些 $x^a f_i$ 的一个 $\mathbf{Z}$-线性组合 f_r，它不属于与 $\mathfrak{a}_{r-1}^*$ 伴随的任何 $\mathfrak{p}$。

4. 令 $\mathfrak{a}_r = (\mathfrak{a}_{r-1}, f_r)$，证明 $\mathfrak{a}_r^* = R$ 或 $\mathfrak{a}_r^*$ 是高度为 r 的无混合理想。

这里或许值得指出，上述第四点正是伴随素理想会出现在此证明中的原因——关键事实是，若元素 f_r 不属于与 $\mathfrak{a}_{r-1}^*$ 伴随的任何素理想，那么 $\mathfrak{a}_r^* = (\mathfrak{a}_{r-1}, f_r)^*$ 的高度就会增加一（或$\mathfrak{a}_r^* = R$）。现在让我们来完成上述四个步骤。

(1) 设 $\mathfrak{p}$ 与 $\mathfrak{a}_{r-1}^*$ 相关联。则 $\mathfrak{p} \subset \mathfrak{M}$，因此对某个 $z \in X$ 有 $\mathfrak{p} \subset z \cdot \mathfrak{m}$，故 $z^{-1} \cdot \mathfrak{p} \subset \mathfrak{m}$。根据定义，$\operatorname{rank}(\operatorname{Stab}_X(z^{-1} \cdot \mathfrak{p})) \leq m'_{r-1}$，由此 $\operatorname{rank}(\operatorname{Stab}_X(\mathfrak{p})) \leq m'_{r-1}$。

引理 5.12. 设 T 为正整数。令 $\mathbf{Z}^m(T)$ 表示满足对每个 i 都有 $0 \leq a_i \leq T$ 的元组 $(a_1, \ldots, a_m) \in \mathbf{Z}^m$ 的集合。若 $H \subset \mathbf{Z}^m$ 是一个秩为 h 的子群，则 $\mathbf{Z}^m(T)$ 在 $\mathbf{Z}^m/H$ 中的像的大小至少为 $(T+1)^{m-h}$。

在证明引理之前，我们先指出，它意味着 $\mathbf{Z}^m(D^{\eta_{r-1}})$ 在 $\mathbf{Z}^m/\operatorname{Stab}_X(\mathfrak{p})$ 中的像的大小至少为

$$(\lfloor D^{\eta_{r-1}} \rfloor + 1)^{m-m'_{r-1}} > (D^{\eta_{r-1}})^{m-m'_{r-1}} = D^{r-1}.$$

现在，与 $\mathfrak{a}_{r-1}^*$ 相关联的素理想数量至多为其次数 $\ell(\mathfrak{a}_{r-1}^*) \leq D^{r-1}$。因此，存在 $a \in \mathbf{Z}^m(D^{\eta_{r-1}})$，使得 $x^{-a}\mathfrak{p}$ 不是 $\mathfrak{a}_{r-1}^*$ 的伴随素理想。等价地，$\mathfrak{p}$ 不是 $x^a\mathfrak{a}_{r-1}^*$ 的伴随素理想。第一步至此完成。

引理 5.12 的证明。选取 $m-h$ 个 $\mathbf{Z}^m$ 的典范基元素，生成一个子群 B，使得 $H \cap B = \{0\}$。从 $\mathbf{Z}^m$ 到 $\mathbf{Z}^m/H$ 的典范映射限制在 B上时是单射。结论成立，因为 $B \cap \mathbf{Z}^m(T)$ 恰好包含 $(T+1)^{m-h}$ 个元素。

□

(2) 接下来进行第二步。由于 $\mathfrak{p}$ 和 $x^a\mathfrak{a}_{r-1}^*$ 是高度相同的无混合 $r-1$，但 $\mathfrak{p}$ 与 $x^a\mathfrak{a}_{r-1}^*$不相关联，因此可得 $x^a\mathfrak{a}_{r-1}^* \not\subset \mathfrak{p}$。这意味着 $x^a\mathfrak{a}_{r-1} \not\subset \mathfrak{p}$，因为 $\mathfrak{p}^* = \mathfrak{p}$。由于

$$\mathfrak{a}_{r-1} = (f_1, \ldots, f_{r-1}),$$

这意味着存在 $1 \le i \le r-1$，使得 $x^a f_i \notin \mathfrak{p}$。第二步至此完成。

(3) 第 3 步由一个一般性引理推出。

引理 5.13. 设 $\mathfrak{p}_1$ 是 R 的素理想，并且

$$f_1, \dots, f_s \in R$$

满足 $f_i \notin \mathfrak{p}_i$。则存在 f_i 的一个 Z-线性组合，使其不属于任何 $\mathfrak{p}_i$。

证明。对 s 进行归纳。在基例 $s = 1$ 中，无需证明。对于更大的 s，假设 g 是 f_1，...，f_{s-1} 的一个 Z-线性组合，且不属于 $\mathfrak{p}_1$，...，$\mathfrak{p}_{s-1}$。如果 $g \notin \mathfrak{p}_s$，那么直接取 g 即可，证明完毕。因此设 $g \in \mathfrak{p}_s$。

考虑所有满足 $a \in \mathbb{Z}$ 的线性组合 $f_s + ag$。对于每个 a，考虑集合 $S_a \subset \{\mathfrak{p}_1, \dots, \mathfrak{p}_{s-1}\}$，它由满足 $f_s + ag \in \mathfrak{p}_i$ 的 $\mathfrak{p}_i$ 组成。可能的子集 S_a 共有 2^{s-1} 个。根据鸽巢原理，如果取 $a = 0$，...，2^{s-1}，则必然存在不同的 a、a'，使得 $S_a = S_{a'}$。但是，如果对于 $1 \le i \le s-1$ 有 $f_s + ag$、$f_s + a'g \in \mathfrak{p}_i$，则 $(a - a')g \in \mathfrak{p}_i$，从而 $g \in \mathfrak{p}_i$（因为 k 具有特征零），矛盾。因此，对于 $i \le s-1$，有 $f_s + ag \notin \mathfrak{p}_i$。

此外，$f_s \notin \mathfrak{p}_s$ 但 $g \in \mathfrak{p}_s$ 意味着 $f_s + ag \notin \mathfrak{p}_s$。因此，$f_s + ag$ 就是所需的线性组合。□

现在我们可以完成步骤 3：由此可得，存在一个$x^a f_i$ 的 Z-线性组合 f_r（其中 $1 \le i \le r-1$ 且 $a \in \mathbb{Z}^m(D^{\eta_{r-1}})$），使得 f_r 不属于 $\mathfrak{a}^*_{r-1}$的任何伴随素理想。

(4) 步骤 4 可由以下引理推出。

引理 5.14。设 $\mathfrak{a} \subset R$ 是高度为 $r-1$ 的无混合理想，并假设 $f \in R$ 不包含于与 $\mathfrak{a}$相关联的任何素理想中。设 $\mathfrak{b} = \mathfrak{a} + (f)$。那么，要么 $\mathfrak{b} = R$，要么 $\mathfrak{b}$ 的高度为 r。在后一种情况下，$\ell(\mathfrak{b}) \le \ell(\mathfrak{a}) \cdot$的次数为 f。

证明。设 $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ 是一个最小主分解，并设 $\mathfrak{p}_i$ 是$\mathfrak{q}_i$的根基。若对所有 i都有 $\mathfrak{p}_i + (f) = R$，则对每个 i，都存在一个形如 $(1 - gf) \in \mathfrak{p}_i$ 的元素，因此存在一个形如 $(1 - gf)^j \in \mathfrak{q}_i$的元素。这些元素的乘积属于 $\mathfrak{a}$。该乘积模 f同余于 1，因此 $1 \in \mathfrak{b} = (\mathfrak{a}, f)$。于是，假设存在某个 $\mathfrak{p} = \mathfrak{p}_i$使得 $\mathfrak{p} + (f) \neq R$。

根据Krull主理想定理，$R/\mathfrak{p}$ 中 $\mathfrak{b}$ 的像$\overline{\mathfrak{b}}$高度为1。R中$\overline{\mathfrak{b}} \subset R/\mathfrak{p}$的任一伴随素理想的原像都是高度为（$r-1$）$+1 = r$的素理想。因此，$\mathfrak{b}$ 的高度至多为 r；由于 $\mathfrak{b} \supset \mathfrak{a}$，其高度至少为 $r-1$。

但是，如果 $\mathfrak{b}$ 的高度为 $r-1$，那么它有某个高度为 $r-1$的伴随素理想 $\mathfrak{p}'$。但是 $\mathfrak{p}' \supset \mathfrak{b} \supset \mathfrak{a}$。由于 $\mathfrak{a}$ 是高度为 $r-1$的无混合对象，这意味着 $\mathfrak{p}'$ 是.....的一个伴随素理想

$\mathfrak{a}$。但是 $f \in \mathfrak{p}'$，而我们假设 f 不包含于 $\mathfrak{a}$的任何伴随素理想中。这就产生了矛盾，因此 $\mathfrak{b}$ 的高度必为 r。

最后，我们注意到 $(\mathfrak{a} + (f))_0 \supset \mathfrak{a}_0 + (f)_0,$，因此

$$\begin{aligned}\ell(\mathfrak{b}) = \tilde{\ell}(R_0/\mathfrak{b}_0) &\leq \tilde{\ell}(R_0/(\mathfrak{a}_0 + (f)_0)) \\ &= \tilde{\ell}(R_0/\mathfrak{a}_0) \cdot \deg(f) \\ &= \ell(\mathfrak{a}) \cdot \deg(f).\end{aligned}$$

倒数第二个等式需要解释。首先，f_0 不包含在 $\mathfrak{a}_0$ 的任何伴随素理想中，因为 f 不包含在 $\mathfrak{a}$的任何伴随素理想中。这意味着乘以 f_0 在 $R_0/\mathfrak{a}_0$上是单射。此乘法映射的次数等于 $\deg(f)$，其余核等于 $R_0/(\mathfrak{a}_0 + (f_0))$，由此可得

$$H_{\mathfrak{a}_0+(f_0)}(t + \deg(f)) = H_{\mathfrak{a}_0}(t + \deg(f)) - H_{\mathfrak{a}_0}(t).$$

~ ~由此得到 $\ell(R_0/(\mathfrak{a}_0 + (f)_0)) = \ell(R_0/(\mathfrak{a}_0) \cdot \deg(f)$，正如所要求的。 □

现在我们可以完成步骤 4。我们有 $\mathfrak{a}_r = \mathfrak{a}_{r-1} + (f_r)$。令 $\mathfrak{b} = \mathfrak{a}^*_{r-1} + (f_r)$。那么 $\mathfrak{a}^*_r \supset \mathfrak{b}$，且引理 5.14 表明，要么 $\mathfrak{b} = R$ 要么 $\mathfrak{b}$ 的高度为 r，并且 $\ell(\mathfrak{b}) \leq D^{r-1} \cdot D = D^r$。

若 $\mathfrak{b} = R$，那么显然 $\mathfrak{a}^*_r = R$，因此假设后一种情况成立。令 $\mathfrak{p}$ 为 $\mathfrak{a}^*_r$的一个伴随素理想。那么 $\operatorname{ht}(\mathfrak{p}) \geq \operatorname{ht}(\mathfrak{a}^*_r) \geq r$。我们要证明等号成立。我们知道 $\mathfrak{p} \subset \mathfrak{m}'$，其中$\mathfrak{m}' = z\mathfrak{m}$，且对某个 $z \in X$（N）成立。我们可以在局部化 $R_{\mathfrak{m}'}$中进行讨论，它是一个正则局部环。理想 $\mathfrak{a}_r R_{\mathfrak{m}'}$ 由 r 个元素生成，因此根据 Krull 高度定理，其高度至多为 r，故其高度恰为 r。所以它是高度为 r 的无混合理想，因此伴随素理想 $\mathfrak{p}$也具有同样性质。

最后，$\mathfrak{a}^*_r \supset \mathfrak{b}$，且二者都是高度为 r 的无混合理想，因此 $\ell(\mathfrak{a}^*_r) \leq \ell(\mathfrak{b}) \leq D^r$。至此，步骤 4 的证明以及定理 5.11 的证明均告完成。

6 矩阵系数猜想

Waldschmidt–Masser 定理的假设和结论都相当强。例如，对于一个维数为 n、系数属于 $\mathscr{L}$或$\mathscr{L}_p$的方阵，假设该矩阵的秩小于 $n/2$，并可得出结论：经过两侧的有理基变换后，可以安排出一个大的零块；具体而言，是一个维数为 $m' \times n'$ 的零块，其中 $m' + n' > n$。

我们希望得到一个更敏锐的表述：当秩不满时，给出一个“有理”的条件。为此，我们与 Mahesh Kakde 一同提出了以下猜想。我们称之为矩阵系数猜想，因为它指出，经过左右有理基变换后，一个系数属于 $\mathscr{L}$ 且为奇异矩阵的方阵，至少可以出现一个零元素。

猜想 6.1（D–Kakde）。设 M 是一个维数为 n 、系数属于$\mathscr{L}$或 $\mathscr{L}_p$的方阵。若行列式(M) $= 0$，则存在非零向量 w、 $v \in \mathbb{Q}^n$，使得 $w^t M v = 0$。

尽管猜想 6.1 很简单，但它仍然相当深刻：在 $n = 2$ 的情形下，很容易看出它等价于四指数猜想。关于矩阵系数猜想，我们证明了以下结果：

- 猜想 6.1 可由结构秩猜想推出。
- 猜想 6.1 在 $\mathscr{L}_p$ 上的版本蕴含 Leopoldt猜想和 Gross–Kuz'min 猜想。

我们还制定了一种利用辅助多项式研究猜想 6.1 的策略，但遗憾的是，构造所需多项式的方法仍然是个谜。我们希望猜想 6.1 可能比结构秩猜想更易处理。我们将在即将开展的工作中进一步探讨猜想 6.1。

参考文献

[1] L. Alaoglu 和 P. Erd¨os. 关于高度合成数及类似数. Trans. Amer. Math. Soc. 56:448–469, 1944.[2] James Ax. 关于 Schanuel 猜想. Ann. of Math. (2) 93:252–268, 1971.[3] A. Baker. 代数数的对数的线性形式. I、II、III. Mathematika 13:204–216；同刊 14 (1967), 102–107；同刊 14 (1967), 220–228, 1966.[4] Pierre Charollois 和 Samit Dasgupta. GL$_n$ 上的整 Eisenstein 余循环，I：Sczech 上循环与全实域的p进 L函数. Camb. J. Math. 2 (1):49–90, 2014.[5]William Cherry.《非阿基米德函数论讲义》，2009. https://arxiv.org/pdf/0909.4509.pdf.[6] Pierre Colmez. $s = 1$ 上 ζ p函数的 R´留数. Invent. Math. 91 (2):371–389, 1988.[7] Samit Dasgupta、Henri Darmon 和 Robert Pollack. Hilbert 模形式与 Gross-Stark 猜想. Ann. of Math. (2) 174 (1):439–484, 2011.[8] Samit Dasgupta、Mahesh Kakde 和 Kevin Ventullo. 关于 Gross-Stark 猜想. Ann. of Math. (2) 188 (3):833–870, 2018.[9] Leslie Jane Federer 和 Benedict H. Gross. 调节子与岩泽模. Invent. Math. 62 (3):443–457, 1981. 附录由 Warren Sinnott 撰写.[10] Benedict H. Gross. $s = 0$处的 p进 L级数. J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28 (3):979–994 (1982), 1981.[11]Alan Harper. 关于对数线性形式的 Baker 定理的一个版本. https://warwick.ac.uk/fac/sci/maths/people/staff/harper/bakernotes.pdf.[12] Damien Roy. 坐标为代数数的对数的代数簇上的点. Acta Math. 175 (1):49–73, 1995.[13] Serge Lang.《超越数导论》. Addison-Wesley Publishing Co., Reading, Mass.- London-Don Mills, Ont., 1966.

[14] Michel Laurent. 关于超越性的一些近期结果. Ast ´erisque 198-200:209–230(1992), 1991. 算术日, 1989（吕米尼，1989）.[15] K. Ramachandra. 对超越数理论的贡献. I、II. Acta Arith. 14:65–72；同刊 14 (1967/1968), 73–88, 1967/68.[16] Theodor Schneider. 《超越数导论》 . Springer-Verlag, Berlin-G¨ottingen- Heidelberg, 1957.[17] Michael Spiess. Shintani 上循环与 p进 Hecke L级数在 $s = 0$处的消失阶. Math. Ann. 359 (1-2):239–265, 2014.[18] Eric Stansifer，阿贝尔和非阿贝尔情形下的 Leopoldt猜想，2012. 硕士论文，AL- GANT Erasmus Mundus.[19] Michel Waldschmidt. 代数数的对数的线性独立性. IMS 报告，第 116 卷. 数学科学研究所，马德拉斯，[1992]. 附录由 Michel Laurent 撰写.[20] . 四指数问题与 Schanuel 猜想. 预印本.[21] . 多变量中的超越性与指数函数. Invent. Math. 63 (1):97–127, 1981.[22] A. Wiles. 全实域的 Iwasawa 猜想. Ann. of Math. (2) 131 (3):493–540, 1990.