ESSENTIAL NUMBER THEORY

Ranks of matrices of logarithms of algebraic numbers, I
The theorems of Baker and Waldschmidt–Masser

Samit Dasgupta

2023

vol. 2 no. 1

msp

msp

Essential Number Theory
Vol. 2, No. 1, 2023
https://doi.org/10.2140/ent.2023.2.93

Ranks of matrices of logarithms of algebraic numbers, I
The theorems of Baker and Waldschmidt–Masser

Samit Dasgupta

Let $\mathscr{L}$ denote the $\mathbb{Q}$-vector space of logarithms of algebraic numbers. In this expository work, we provide an introduction to the study of ranks of matrices with entries in $\mathscr{L}$. We begin by considering a slightly different question; namely, we present a proof of a weak form of Baker's theorem. This states that a collection of elements of $\mathscr{L}$ that is linearly independent over $\mathbb{Q}$ is in fact linear independent over $\overline{\mathbb{Q}}$. Next we recall Schanuel's conjecture and prove Ax's analogue of it over $\mathbb{C}((t))$.

We then consider arbitrary matrices with entries in $\mathscr{L}$ and state the structural rank conjecture, concerning the rank of a general matrix with entries in $\mathscr{L}$. We prove the theorem of Waldschmidt and Masser, which provides a lower bound, giving a partial result toward the structural rank conjecture. We conclude by stating a new conjecture that we call the matrix coefficient conjecture, which gives a necessary condition for a square matrix with entries in $\mathscr{L}$ to be singular.

1. Introduction 93
2. Baker's theorem 96
3. Ax's theorem 105
4. The structural rank conjecture 111
5. The theorem of Waldschmidt and Masser 121
6. The matrix coefficient conjecture 136
Acknowledgements 137
References 137

1. Introduction

At the 1900 International Congress of Mathematicians, David Hilbert presented 23 open problems that have continued to serve as an inspiration for generations of mathematicians, including the following question:

MSC2020: 11J81.

Keywords: transcendence theory, Baker's theorem, Ax's theorem, Waldschmidt's theorem, Masser's theorem.

Hilbert's 7th problem. Let $a, b \in \overline{\mathbb{Q}}$, with $a \neq 0, 1$ and $b \notin \mathbb{Q}$. Is the value a^b necessarily transcendental?

A proof that Hilbert's question has an affirmative answer was given independently by Gelfond (1934) and Schneider (1935). The Gelfond–Schneider theorem can be stated equivalently as follows. Let

$$\mathscr{L} = \{x \in \mathbb{C} \mid e^x \in \overline{\mathbb{Q}}\}$$

denote the $\mathbb{Q}$-vector space of logarithms of algebraic numbers.

Theorem 1.1 (Gelfond–Schneider). *If two elements of $\mathscr{L}$ are linearly dependent over $\overline{\mathbb{Q}}$, then they are linearly dependent over $\mathbb{Q}$.*

A fantastic breakthrough was achieved by Alan Baker [1966; 1967a; 1967b], when he generalized from two to an arbitrary number of elements of $\mathscr{L}$.

Theorem 1.2 (Baker). *If $n \geq 1$ elements of $\mathscr{L}$ are linearly dependent over $\overline{\mathbb{Q}}$, then they are linearly dependent over $\mathbb{Q}$.*

In fact, Baker proved an effective refinement of this result giving a strong lower bound on the magnitude of any algebraic linear combination of elements of $\mathscr{L}$ that are linearly independent over $\mathbb{Q}$. Here we will present a proof of a version of Baker's theorem that is slightly weaker than Theorem 1.2.

We next shift our focus from a single linear form in logarithms to arbitrary matrices with entries in $\mathscr{L}$. Such matrices appear very naturally in number theory. For example, the regulator of a number field is the determinant of such a matrix, and this expression appears in the class number formula for the zeta function of the number field. Generalizations appear in Stark's conjectures for the leading terms of L-functions, and p-adic avatars appear in the study of p-adic L-functions. The question of the ranks of such matrices is therefore an important question, with Leopoldt's conjecture and the Gross–Kuz'min conjecture being important special cases in Iwasawa theory (these are discussed in Section 4B).

The primary conjecture about the ranks of matrices with entries in $\mathscr{L}$ is the *structural rank conjecture*. In applications, it is often useful to consider the $\mathbb{Q}$-vector space spanned by $\mathscr{L}$ and $\mathbb{Q}$, which we denote by $\mathscr{L} + \mathbb{Q}$. Given an $m \times n$ matrix M with entries in any field of characteristic 0, we define the structural rank of M as follows. Choose a $\mathbb{Q}$-basis $\{\ell_1, \ldots, \ell_r\}$ for the entries of M, and write $M = \sum_{i=1}^r \ell_i M_i$, with $M_i \in M_{m\times n}(\mathbb{Q})$. Write $M_x = \sum_{i=1}^r x_i M_i$, where the x_i are indeterminates. Then M_x is an $m \times n$ matrix with entries in the field of rational functions $F = \mathbb{Q}(x_1, \ldots, x_n)$. We define the *structural rank* of M to be the rank of M_x over F. One checks that this definition is independent of the basis $\{\ell_i\}$ chosen.

Conjecture 1.3 (structural rank conjecture). *The rank of any $M \in M_{m\times n}(\mathscr{L} + \mathbb{Q})$ is equal to the structural rank of M.*

The "über conjecture" in the transcendence theory of special values of logarithms and exponentials of algebraic numbers is the following conjecture of Schanuel. We write $\mathrm{trd}_{\mathbb{Q}}$ for the transcendence degree over $\mathbb{Q}$.

Conjecture 1.4. *Let $y_1, \dots, y_n \in \mathbb{C}$ be $\mathbb{Q}$-linearly independent. Then*

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

In particular, if $y_1, \dots, y_n \in \mathscr{L}$ are $\mathbb{Q}$-linearly independent, then

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

It is perhaps not surprising that the special case of Schanuel's conjecture given in (1) implies the structural rank conjecture; however, an elegant theorem of Roy [1995] is that the converse is also true:

Theorem 1.5 (Roy). *The structural rank conjecture is equivalent to the special case of Schanuel's conjecture given in (1).*

Theorem 1.5 is proven in Section 4. For more on the structural rank conjecture and Schanuel's conjecture, see [Waldschmidt 2023]. The strongest unconditional evidence toward the structural rank conjecture is the following theorem of Waldschmidt [1981] and Masser [1981]:

Theorem 1.6 (Waldschmidt and Masser). *Let $M \in M_{m\times n}(\mathscr{L})$. Suppose that*

$$\mathrm{rank}(M) < \frac{mn}{m+n}.$$

Then there exist $P \in \mathrm{GL}_m(\mathbb{Q})$ and $Q \in \mathrm{GL}_n(\mathbb{Q})$ such that

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

where the 0 block has dimension $m' \times n'$ with $m'/m + n'/n > 1$.

Intuitively, Theorem 1.6 states that, if the rank of $M = (\log(x_{ij}))$ is very small, then the underlying algebraic numbers x_{ij} satisfy a large number of multiplicative relations. In certain situations we can show that such relations do not exist, and hence we must have $\mathrm{rank}(M) \geq mn/(m+n)$. The six exponentials theorem (Theorem 4.2) is an example of a special case of the Waldschmidt–Masser theorem.

Transcendence results have many important applications in algebraic number theory. Especially in Iwasawa theory, it is the p-adic analogues of these statements that are most relevant. For example, Leopoldt's conjecture concerns the rank of the matrix of p-adic logarithms of a basis of units in a number field F. The p-adic analogue of the Waldschmidt–Masser theorem provides the strongest evidence for this conjecture. For instance, for a totally real field F one deduces that the rank of the Leopoldt matrix is at least half the expected one. We prove the p-adic version

of the Waldschmidt–Masser theorem in Section 5, since the archimedean case is studied more often in the literature, and discuss applications in Section 5A.

The paper is organized as follows. In Section 2, we prove Baker's theorem on the linear independence of logarithms of algebraic numbers. In Section 3, we prove Ax's theorem on the function field analogue of Schanuel's conjecture. In Section 4, we discuss the structural rank conjecture, explaining its connection to important conjectures in Iwasawa theory and proving Roy's Theorem 1.5. In Section 5, we prove the Waldschmidt–Masser theorem and give applications. In the concluding Section 6, we state a new conjecture, called the matrix coefficient conjecture, which attempts to answer the question: what can be said about a square matrix M with entries in $\mathscr{L}$ when it does not have full rank? Our conjecture is not as strong as the structural rank conjecture (and hence is perhaps more tractable), but still has important arithmetic implications.

2. Baker's theorem

Before giving an outline of the proof of Baker's theorem, let us discuss how one could hope to deduce the *conclusion* of the theorem. We are given algebraic numbers $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Q}}^*$, complex numbers x_i such that $e^{x_i} = \alpha_i$, and a linear dependence

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

with $\beta_i \in \overline{\mathbb{Q}}$. We will show that this implies the existence of integers $\lambda_1, \dots, \lambda_n$, not all zero, such that

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

This implies that the x_i, together with the complex number $2\pi i$, are linearly dependent over $\mathbb{Q}$. Therefore, the mildly weaker version of Baker's theorem that we will prove is the following:

Theorem 2.1. *If $x_1, \dots, x_n, 2\pi i \in \mathscr{L}$ are linearly independent over $\mathbb{Q}$, then $x_1, \dots, x_n$ are linearly independent over $\overline{\mathbb{Q}}$.*

It does not take much work beyond the methods that we will present to remove $2\pi i$ and prove the version of Baker's theorem stated in Theorem 1.2 above (see [Baker 1967a]). However, to simplify the exposition and highlight the main points, we have included $2\pi i$ in our proof of Theorem 2.1.

Now, how does one deduce the existence of the λ_i from the existence of the β_i? It may be enticing to try to prove that the λ_i can be taken equal to the β_i, i.e., that the β_i are rational (or, more generally, that the λ_i can somehow be extracted from the β_i in a direct way). However, in practice a more indirect approach is effective.

Theorem 2.2. *Let $\alpha_1, \dots, \alpha_n \in \mathbb{C}^*$. Suppose there exists a nonzero polynomial*

$$f(t_1, \dots, t_n) \in \mathbb{C}[t_1, \dots, t_n]$$

of degree $\leq L$ *in each variable* t_i *such that*

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

for $z = 1, 2, \ldots, (L+1)^n$. *Then there exist integers* $\lambda_1, \ldots, \lambda_n$, *not all zero, such that*

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

Proof. Consider the square matrix M whose rows are indexed by the integers

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

and whose columns are indexed by the tuples $\lambda = (\lambda_1, \ldots, \lambda_n)$ of integers with $0 \leq \lambda_i \leq L$, with corresponding matrix entry

$$\alpha^{\lambda z} := \alpha_1^{\lambda_1 z}\cdots\alpha_n^{\lambda_n z}. \tag{4}$$

The existence of the polynomial f is equivalent to the existence of a column vector v such that $Mv = 0$. Indeed, the components of v are precisely the coefficients of f.

The existence of a nonzero f therefore implies that $\det(M) = 0$. But M is the Vandermonde matrix associated to the elements $\alpha^\lambda = \alpha_1^{\lambda_1}\cdots\alpha_n^{\lambda_n}$ as the tuple λ ranges over all $(L+1)^n$ possibilities. The vanishing of the determinant therefore implies the existence of two distinct tuples λ and λ' such that $\alpha^\lambda = \alpha^{\lambda'}$. We therefore have $\alpha^{\lambda-\lambda'} = 1$, as desired. □

Baker's theorem therefore amounts to using (2) to construct an *auxiliary polynomial* f that satisfies the conditions of Theorem 2.2. We first summarize Baker's ingenious method to do this:

(1) The Dirichlet box principle is a method of using the pigeonhole principle to construct a polynomial f with certain prescribed zeroes. One can apply this to the elements α^z appearing in the statement of Theorem 2.2. Of course, the result will not produce a polynomial with enough zeroes (i.e., we may find zeroes for $z = 1, \ldots, A$ for some A, but A will be less than $(L+1)^n$). Baker's clever insight is that the condition (2) allows us to ensure that a certain number of *derivatives* of f also have zeroes corresponding to these values of z.

(2) Baker then proves a complex analytic lemma, which is a quantitative strengthening of the classical Schwarz's lemma that shows that the vanishing of f and many of its derivatives implies a strong upper bound on the size of f and half as many of its derivatives, but for B times as many integers z (for some $B > 1$ depending on parameters we will make precise later).

(3) Using the fact that the α_i and β_i are algebraic, Baker deduces that these bounded values (i.e., the values of f and many of its derivatives for $z = 1, \ldots, AB$) must actually be 0. The basic concept is that an integer of absolute value less

than 1 must vanish; a generalization of this elementary statement to algebraic numbers of bounded degree and height is applied.

(4) Armed with more vanishing, one may now go back to step (2) and once again show that half as many derivatives are small for another factor of B times as many values of z. Baker iterates this procedure N times until $AB^N > (L+1)^n$, thereby showing that the auxiliary polynomial f has enough zeroes to apply Theorem 2.2.

In the rest of this section we will describe these steps in detail.

2A. ***Construction of auxiliary polynomial.*** For each α_i, let c_i denote the leading coefficient of the integral minimal polynomial of α_i, and let d denote the maximum degree of any α_i.

Lemma 2.3. *There exist integers $a_{i,j,s}$ such that, for each integer $j \geq 0$, we have*

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

Proof. For notational simplicity, we remove the index i. So we consider $\alpha \in \overline{\mathbb{Q}}$ with degree at most d, and let c denote the leading coefficient of the integral minimal polynomial of α. Then there exist integers $b_0, \ldots, b_{d-1}$ such that

$$c\alpha^d = b_{d-1}\alpha^{d-1} + \cdots + b_1\alpha + b_0. \tag{5}$$

We prove the result by induction on j. The base cases $0 \leq j < d$ are clear. For $j \geq d$ we assume by induction that there are integers $a_{j-1,s}$ such that

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

Multiplying by $c\alpha$, we obtain

$$(c\alpha)^j = \left(\sum_{s=0}^{d-2} c \cdot a_{j-1,s}\alpha^{s+1}\right) + a_{j-1,d-1}(c\alpha^d). \tag{6}$$

Plugging in (5) for $c\alpha^d$ on the right of (6), we obtain the desired expression

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

where

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

□

Let

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

be a polynomial of degree $\le L$ in each variable t_i. Let the c_i and $a_{i,j,s}$ be as in Lemma 2.3. Writing $c = (c_1, \ldots, c_n)$ and recalling the notation (4), we calculate

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

We can therefore force $f(\alpha^z) = 0$ by imposing integer linear conditions on the coefficients p_λ, namely that, for each z, we have

$$\sum_\lambda p_\lambda c^{L-\lambda z} \prod_{i=1}^{n} a_{i,\lambda_i z,s} = 0. \tag{7}$$

This observation allows for the initial construction of an auxiliary polynomial f using the following lemma of Siegel [1929], often known as "Dirichlet's box principle":

Lemma 2.4 (Siegel). *Let $N > 2M > 0$ be integers, and let $A = (a_{i,j})$ be an $M \times N$ matrix of integers such that $|a_{i,j}| < H$ for all i and j. There is a nonzero vector $b \in \mathbb{Z}^N$ such that $Ab = 0$ and each coordinate of b has absolute value less than $2NH$.*

Proof. Consider all vectors $b \in \mathbb{Z}^N$ with coordinates of absolute value $\le NH$. There are $(2NH+1)^N > (2NH)^N$ such vectors. For each such b, each coordinate of Ab has size at most $(NH)^2$. The total number of possible vectors Ab is less than $(2(NH)^2)^M$. Since $N > 2M$, the pigeonhole principle implies that two distinct b must give the same value of Ab. Their difference gives the desired vector. □

Applying Siegel's lemma to the system of linear equations in (7) will not produce enough zeroes for Theorem 2.2. Indeed, we have not yet used the assumption (2)! A key trick noticed by Baker is that it will suffice to have f and sufficiently many of its derivatives vanish. The precise statement is given below:

Theorem 2.5. *The following holds for every sufficiently large parameter h. Let*

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

There exists a polynomial

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

of degree $\leq L$ in each variable t_i such that $|p_\lambda| < e^{h^3}$ for each λ and such that the complex analytic function of one variable $z \in \mathbb{C}$ defined by

$$\phi(z) = \sum_{\lambda} p_\lambda e^{z(\lambda_1 x_1 + \cdots + \lambda_n x_n)} \tag{8}$$

satisfies

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

Proof. Note that $\phi(z)$ has been defined so that $\phi(z) = f(\alpha^z) = f(\alpha_1^z, \dots, \alpha_n^z)$ for integers z. After dividing the linear dependence (2) by $-\beta_n$ (reordering if necessary to ensure this is nonzero) and renaming the coefficients, we can write

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

with $\beta_i \in \overline{\mathbb{Q}}$. We then have

$$\phi(z) = \sum_{\lambda} p_\lambda e^{z[(\lambda_1 + \lambda_n \beta_1)x_1 + \cdots + (\lambda_{n-1} + \lambda_n \beta_{n-1})x_{n-1}]}. \tag{9}$$

Note that $\phi^{(m)}(z)$ is the same sum as for $\phi(z)$, but with the term indexed by λ multiplied by

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

Expanding this out, it suffices to show that

$$\sum_{\lambda} p_\lambda \alpha^{\lambda z} (\lambda_1 + \lambda_n \beta_1)^{m_1} \cdots (\lambda_{n-1} + \lambda_n \beta_{n-1})^{m_{n-1}} = 0 \tag{10}$$

for all tuples of nonnegative integers satisfying

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

Let d be the degree of the number field generated by all the α_i and β_i. Let c_i denote the leading coefficient in the integral minimal polynomial of α_i. By Lemma 2.3, for every nonnegative integer j, there exist integers $a_{i,j,s}$ such that

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

Let d_i and $b_{i,j,s}$ play the same role for the β_i.

The expression (10) will vanish if

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

vanishes for all tuples $(s_1,\ldots,s_n)$ and $(t_1,\ldots,t_{n-1})$ with $0\le s_i,t_i<d$.

How many linear equations is this in the coefficients p_λ we are searching for? We want vanishing for $0\le m<h^2$ and $1\le z\le h$. Hence, the number of such equations is at most

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

Note that d and n are fixed but we are free to make h as large as we want.

The number of variables p_λ is $(L+1)^n$, so, to ensure this is bigger than $2M$ when h is large, we let $L=\lceil h^{2-1/(4n)}\rceil$, as in the statement of the theorem. Finally, we bound the size of the coefficients. An easy induction shows that there is a constant C, depending only on the α_i and β_i, such that

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

Therefore, for some constant K depending only on the α_i, β_i and n, we have

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

and, similarly,

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

By Siegel's lemma, there is a nontrivial solution in integers p_λ such that

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

2B. ***Baker's lemma.*** In this section we present a complex analytic lemma of Baker, strengthening the classical Schwarz' lemma. This will allow us to bound the sizes of f and many of its derivatives for a multiple B of the A values of z at which we ensured vanishing of our auxiliary polynomial f.

Lemma 2.6. *Let $f:\mathbb{C}\to\mathbb{C}$ be an entire function, let $\epsilon>0$, and let A, B, C, T and U be large positive integers such that*

$$\tfrac{1}{2}\epsilon C>\frac{2T+UAB}{A(\log A)^{1/2}}+\frac{UBA^{\epsilon}}{\log A}.\tag{11}$$

Suppose that:

- $|f(z)| \leq e^{T+U|z|}$ *for* $z \in \mathbb{C}$.
- $f^{(t)}(z) = 0$ *for* $t = 0, \ldots, C-1$ *and* $z = 1, 2, \ldots, A$.

Then

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

Proof. The function

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

is entire by the second assumption. By the maximum modulus principle on the circle of radius $A^{1+\epsilon}B$ around the origin, we have, for $|z| \leq AB$,

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

hence,

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

Now

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

where the inequality holds since

$$\frac{AB+i}{A^{1+\epsilon}B - i} \leq A^{-\epsilon/2}$$

for all $i = 1, \ldots, A$. Meanwhile,

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

Our goal is to show that $|f(z)| \leq e^{-(T+UAB)(\log A)^{1/2}}$, so it suffices to show that

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

It is easy to see that this is implied by the assumption of the lemma,

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

□

Let us now apply Baker's lemma to our auxiliary polynomial and its derivatives. With $\phi(z)$ as in (8) and (9), we have

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

where

$$f_{m_1,\dots,m_{n-1}}(z) = \sum_{\lambda} p_\lambda \alpha^{\lambda z} (\lambda_1 + \lambda_n \beta_1)^{m_1} \cdots (\lambda_{n-1} + \lambda_n \beta_{n-1})^{m_{n-1}}. \tag{12}$$

It is clear from this last expression that

$$|f_{m_1,\dots,m_{n-1}}(z)| < K^{h^3 + L|z|} \tag{13}$$

for a suitable constant K depending only on n, the α_i and the β_i. Indeed, the p_λ are bounded by e^{h^3}. The m_i and λ_i are bounded by h^2. We choose the constant K so that the inequality (13) holds with the α_i or β_i replaced by any of their conjugates as well.

We would like to apply Baker's lemma on each of the functions $f_{m_1,\dots,m_{n-1}}(z)$ with

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

We suppose that the constants K and h have been chosen so that the values T, U, A, B and C are integers. The first condition on $f_{m_1,\dots,m_{n-1}}(z)$ necessary to apply Baker's lemma is precisely the inequality (13). For the second condition, we note that the t-th derivative of $f_{m_1,\dots,m_{n-1}}(z)$ for $m_1 + \cdots + m_{n-1} \le \frac{1}{2}h^2$ and $t \le \frac{1}{2}h^2 - 1$ is a linear combination of $f_{m'_1,\dots,m'_{n-1}}(z)$ with $m'_1 + \cdots + m'_{n-1} \le h^2 - 1$. This gives the desired vanishing for $z = 1, \dots, h$ by the construction of the polynomial f in Theorem 2.5.

Furthermore, with our selection of parameters, the required inequality (11) reads

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

which is easily seen to hold for h large. We may therefore apply Baker's lemma to $f_{m_1,\dots,m_{n-1}}(z)$. This yields

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

for $m_1 + \cdots + m_{n-1} \le \frac{1}{2}h^2$ and $z = 1, \dots, h^{1+1/(8n)}$.

2C. ***Discreteness of algebraic integers.*** We apply the following elementary basic principle:

Lemma 2.7. *Suppose that $a \in \overline{\mathbb{Q}}$ such that da is an algebraic integer for some positive integer d. Suppose that $|a| < \epsilon$ for some positive real number ϵ and that every conjugate $\sigma(a)$ satisfies $|\sigma(a)| < M$ for some positive real number M. Finally, suppose that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \le n$ and that $\epsilon M^{n-1} d^n < 1$. Then $a = 0$.*

Proof. We bound the norm of the algebraic integer da:

$$|\mathrm{N}_{\mathbb{Q}(a)/\mathbb{Q}}(da)| = \prod_{\sigma:\mathbb{Q}(a)\hookrightarrow\mathbb{C}} |\sigma(da)| \leq d^n|a| \cdot \prod_{\sigma\neq 1} |\sigma(a)| \leq d^n \epsilon M^{n-1} < 1.$$

An integer of absolute value less than 1 must be 0. Hence, $\mathrm{N}_{\mathbb{Q}(a)/\mathbb{Q}}(da) = 0$, so $a = 0$. □

We apply Lemma 2.7 to each of the algebraic numbers $f_{m_1,\ldots,m_{n-1}}(z)$ defined in (12) for

$$m_1 + \cdots + m_{n-1} \leq \tfrac{1}{2}h^2, \quad z = 0, 1, \ldots, h^{1+1/(8n)}.$$

In (14) we showed that

$$|f_{m_1,\ldots,m_{n-1}}(z)| < \epsilon := K^{-(h^3+Lz)(\log h)^{1/2}}. \tag{15}$$

We also saw in (13) that

$$|\sigma(f_{m_1,\ldots,m_{n-1}}(z))| < M := K^{h^3+Lz} \tag{16}$$

for each σ. It is easy to see from its definition that the denominator of $f_{m_1,\ldots,m_{n-1}}(z)$ can be cleared by an integer of size at most

$$d := K^{h^2+Lz}, \tag{17}$$

after making K larger if necessary depending only on the α_i and β_i.

The inequality $\epsilon M^{n-1}d^n < 1$ is then easily seen to hold for h large because of the extra factor $(\log h)^{1/2}$ in the exponent of (15), so we conclude that

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

for $m_1 + \cdots + m_{n-1} \leq \frac{1}{2}h^2$ and $z = 0, 1, \ldots, h^{1+1/(8n)}$.

2D. ***Bootstrapping.*** We repeat the process described above, in the k-th iteration using Baker's lemma on the functions $f_{m_1,\ldots,m_{n-1}}(z)$ with $m_1+\cdots+m_{n-1} \leq h^2/2^{k+1}$ with the parameters

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

We assume that K and h had been chosen initially so that the quantities above are integers. In the k-th iteration we obtain that

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

for

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

The quantities in (16) and (17) do not change, so again Lemma 2.7 implies that the values $f_{m_1,\dots,m_{n-1}}(z)$ vanish. We may therefore move on to the next k.

Each iteration multiplies the number of zeroes by $B = h^{1/(8n)}$. After $16n^2$ iterations we will obtain more than h^{2n} zeroes. Since $L = h^{2-1/(4n)}$ and h is large, we have

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

so the polynomial $f = f_{0,0,\dots,0}$ satisfies the conditions of Theorem 2.2. Therefore, there exist integers $\lambda_1, \dots, \lambda_n$, not all zero, such that

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

This completes the proof of Baker's theorem.

3. Ax's theorem

Moving on from linear forms in elements of $\mathscr{L}$ to arbitrary polynomials, we remind the reader of Schanuel's conjecture, which was stated in the introduction:

Schanuel's conjecture. *Let $y_1, \dots, y_n \in \mathbb{C}$ be $\mathbb{Q}$-linearly independent. Then*

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

While little is known about this conjecture, we have the following function field analogue, proved by James Ax [1971]:

Theorem 3.1 (Ax). *Let $y_1, \dots, y_n \in t\mathbb{C}[\![t]\!]$ be $\mathbb{Q}$-linearly independent. Then*

$$\operatorname{trd}_{\mathbb{C}(t)} \mathbb{C}(t)(y_1, \dots, y_n, e^{y_1}, \dots, e^{y_n}) \geq n.$$

In this section we prove Ax's theorem. The section is self-contained and may be skipped by readers not interested in the function field setting. Before proceeding, we note simply the tool that is available in the function field setting that is not available in the classical setting: there is a derivative operator on $\mathbb{C}((t))$, and elements of the form e^y satisfy $(e^y)' = y'e^y$.

3A. *Derivations.*

Definition 3.2. Let A be a commutative ring and B a commutative A-algebra. An A-derivation of B into a B-module M is an A-linear map

$$D : B \to M$$

such that

$$D(ab) = aD(b) + D(a)b, \quad a, b \in B, \tag{18}$$

where we view M as both a left and right B-module since B is commutative.

There is a pair $(d = d_{B/A}, \Omega_{B/A})$ of a B-module $\Omega_{B/A}$ and an A-derivation

$$d : B \to \Omega_{B/A}$$

that is universal in the sense that any A-derivation $D : B \to M$ can be obtained by composing $d_{B/A}$ with a B-module homomorphism $\Omega_{B/A} \to M$. The module of *Kähler differentials* $\Omega_{B/A}$ is defined as the quotient of the free B-module generated by formal generators db for each $b \in B$ by the relations $da = 0$ for $a \in A$, $d(b+b') = db + db'$, and $d(bb') = b \cdot db' + b' \cdot db$. The universal derivation $d_{B/A} : B \to \Omega_{B/A}$ is defined by $d_{B/A}(b) = db$.

Lemma 3.3. *Let F/K be field extension and $x \in F$ separable algebraic over K. Then $dx = 0$ in $\Omega_{F/K}$.*

Proof. Let $f(t) \in K[t]$ be the minimal polynomial of x. Then

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

Since x is separable, $f'(x) \neq 0$, so $dx = 0$. □

Meanwhile, if $F(t)$ denotes the function field in one variable over the field F, we have that $\Omega_{F(t)/F}$ is the 1-dimensional $F(t)$-vector space generated by dt, with $d(f(t)) = f'(t)dt$.

Lemma 3.4. *Let $K \subset F \subset L$ be fields of characteristic 0. Let $D : F \to F$ be a K-derivation. Then D can be extended to a K-derivation $L \to L$.*

Proof. For $f \in F[t]$, let f^D denote the polynomial where D has been applied to the coefficients of f. We show how to extend the derivation d. Let $z \in L$ with $z \notin F$. If z is algebraic over F, let $p(x)$ be its minimal polynomial. Define

$$u = -\frac{p^D(z)}{p'(z)}, \quad \widetilde{D}(g(z)) = g^D(z) + g'(z)u. \tag{19}$$

If z is transcendental over F, we define

$$\widetilde{D}(g(z)) = g^D(z) + g'(z)u \tag{20}$$

for any $u \in L$. We leave it to the reader to check that setting $\widetilde{D}|_F = D$ and using (19) or (20) to extend to $F(z)$ yields a derivation $\widetilde{D}$. Now one uses Zorn's lemma on pairs (D', F'), where F' is a field such that $K \subset F' \subset L$ and D' is a derivation extending D, to extend D all the way to L. □

Corollary 3.5. *Let $K \subset L$ be fields of characteristic 0. Then*

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

More generally, if $K \subset F \subset L$, then

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

Proof. Let $\{f_1, \ldots, f_n\}$ be a transcendence basis for F/K. Suppose that

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

with $a_i \in L$. By the universal property of $d_{L/K}$, we have

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

for any K-derivation $D_i : L \to L$. Therefore, if we show that for each i there exists a K-derivation $D_i : L \to L$ such that $D_i(f_j) = \delta_{ij}$, then we obtain $a_i = 0$ for all i. This yields the linear independence of the $d_{L/K} f_i$ over L.

The existence of the D_i follows from the proof of Lemma 3.4. We can first extend the 0 derivation on K to $K(f_i)$ by setting $z = f_i$ and $u = 1 - f_i$ in (20), and then inductively extend to $K(f_1, \ldots, f_n)$ by setting $z = f_j$ and $u = -f_j$ for $j \neq i$. Finally, we extend D_i to L using Lemma 3.4 once more. □

3B. ***Derivation on Kähler differentials.*** Let A be a commutative ring and B an A-algebra. Let $D : B \to B$ be a derivation such that $D(A) \subset A$. There exists an A-linear map

$$D^1 : \Omega_{B/A} \to \Omega_{B/A}$$

satisfying

$$D^1(f\,dg) = (Df)dg + f\,d(Dg). \tag{21}$$

We leave the verification of this to the reader, but we note that a more general fact is true. If we consider the graded algebra of differentials

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

then the differential $D : B \to B$ extends to a graded derivation

$$D^* : \Omega^*_{B/A} \to \Omega^*_{B/A}$$

satisfying (18), where the 0th graded piece is D and the 1st graded piece is D^1. In our proof of Ax's theorem, we will only need the map D^1, but let us note that the rule (21) generalizes: for any $f \in B$ and $\omega \in \Omega_{B/A}$, we have

$$D^1(f\omega) = (Df)\omega + f D^1(\omega). \tag{22}$$

Proofs of these facts may be found in the references given in [Ax 1971, page 255].

Lemma 3.6. *Let $y \in t\mathbb{C}[\![t]\!]$, $z = e^y$, and let $D : \mathbb{C}((t)) \to \mathbb{C}((t))$ be a $\mathbb{C}$-derivation of the form $D(f(t)) = f'(t) \cdot g(t)$ for some fixed $g(t) \in \mathbb{C}((t))$. Then*

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

in $\Omega_{\mathbb{C}((t))/\mathbb{C}}$.

Proof. A direct computation with the definition (21) shows that, in general, we have

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

Yet, when $z = e^y$, the term $Dy - z^{-1}Dz$ vanishes for the derivation $D(f(t)) = f'(t) \cdot g(t)$. □

Lemma 3.7. *Let $K \subset L$ be fields and $D : L \to L$ a derivation such that* $\ker D = K$. *Then the map*

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

is injective.

Proof. Suppose there exist

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

such that

$$\sum_{i=1}^{n} f_i \otimes \omega_i \mapsto 0, \quad \text{i.e.,} \quad \sum_{i=1}^{n} f_i\omega_i = 0. \tag{23}$$

Scale so that $f_1 = 1$. If all the f_i lie in K, then

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

so we are done. Suppose this is not the case and take the minimal such vanishing linear combination. By minimality, we can assume that the ω_i are linearly independent over L. Apply D^1 to the expression (23). Using (22), we find

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

where the second equality holds since $\omega_i \in \ker D^1$. By the linear independence of the ω_i over L, we see that $Df_i = 0$ for all i and hence, by assumption, $f_i \in K$ for all i. □

The following is a technical algebraic lemma that will allow us to reduce to the setting of function fields of curves:

Lemma 3.8. *Let $K \subsetneq L$ be an extension of fields with K relatively algebraically closed in L (i.e., if $\alpha \in L$ and α is algebraic over K, then $\alpha \in K$). Let*

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

Then

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

Proof. Let $t \in L$ with $t \notin K$. We need to show there exists $F \in W$ such that $t \notin F$. Since K is relatively algebraically closed in L, the element t is transcendental over K.

Choose a transcendence basis for L/K consisting of t and a set B of elements not in $K(t)$. Let F be the relative algebraic closure of $K(B)$ in L, i.e.,

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

Then $F \in W$, since L is algebraic over $F(t)$. Since $t \notin F$, this completes the proof. □

In some sense, the following lemma is the main engine of Ax's proof:

Lemma 3.9. *Let L/K be fields of characteristic 0. Denote by dL the K-subspace of $\Omega_{L/K}$ spanned by df for $f \in L$. Denote by dL/L the $\mathbb{Z}$-submodule of $\Omega_{L/K}$ spanned by $f^{-1}df$ for $f \in L^*$. Then the canonical map of K-vector spaces*

$$K \otimes_{\mathbb{Z}} dL/L \to \Omega_{L/K}/dL, \quad k \otimes \frac{df}{f} \mapsto \frac{k}{f}df, \tag{24}$$

is injective, where $\Omega_{L/K}/dL$ denotes the quotient of $\Omega_{L/K}$ by the K-subspace spanned by df for $f \in L$.

Proof. Choose an element

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

in the kernel of the map (24), with n minimal. By minimality, the k_i are linearly independent over $\mathbb{Q}$. We will show that each f_i lies in $\overline{K}_L$, the relative algebraic closure of K in L. By Lemma 3.3, this will imply $df_i = 0$, giving the desired injectivity.

If $L = \overline{K}_L$, there is nothing to prove. Otherwise, let $F \in W$, with W as in Lemma 3.8. So $K \subset F \subset L$, $\mathrm{trd}_F\, L = 1$, and $\overline{F}_L = F$. Since the element (25) lies in the kernel of (24), we have

$$\sum_{i=1}^{n} k_i f_i^{-1} df_i = \sum_{i=1}^{m} k_i' df_i' \tag{26}$$

for some $f_i' \in L^*$ and $k_i' \in K$. Now, we would like to use properties of function fields of curves, but, unfortunately, we do not know that L is finitely generated over F. To this end, we consider a field L' generated over F by the f_i, the f_i', and by any elements used in any relations in $\Omega_{L/K}$ used to obtain (26). The field L' then still has transcendence degree 1 over F, and is finitely generated over F. We may therefore identify L' with the function field of a smooth projective algebraic curve over F. Furthermore, equation (26) still holds in $\Omega_{L'/K}$ by construction, and so it holds also in $\Omega_{L'/F}$.

Points P on this curve correspond to valuations

$$\operatorname{ord}_P : (L')^* \to \mathbb{Z}.$$

Associated to P we also have a residue map

$$\operatorname{res}_P : \Omega_{L'/F} \to F.$$

The residue and valuation maps satisfy the following well-known properties. For all $g \in (L')^*$, we have

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

Applying res_P to (26), we get

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

By $\mathbb{Q}$-linear independence of the k_i, we obtain $\operatorname{ord}_P(f_i) = 0$ for all P and i. But a function on a smooth projective curve with no zeroes or poles must be constant, and hence $f_i \in F$ for all i. Since this holds for all F, we have by Lemma 3.8 that $f_i \in \overline{K}_L$. □

We can now complete the proof of Ax's theorem.

Proof of Theorem 3.1. Let $y_1, \ldots, y_n \in t\mathbb{C}[\![t]\!]$ and write $z_i = e^{y_i} \in \mathbb{C}[\![t]\!]$. Let

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

It suffices to show that, if $\operatorname{trd}_{\mathbb{C}} L \leq n$, then $y_1, \ldots, y_n$ are $\mathbb{Q}$-linearly dependent. Suppose $\operatorname{trd}_{\mathbb{C}} L \leq n$. Then, by Corollary 3.5, the differentials

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

for $i = 1, \ldots, n$ together with dy_1 must be linearly dependent over L, so

$$\sum_{i=1}^{n} f_i\omega_i + g dy_1 = 0 \tag{27}$$

with $f_i, g \in L$ not all zero. Note that, if $y_1'(t) = 0$, then y_1 is a constant, and since $y_1 \in t\mathbb{C}[\![t]\!]$ we would get $y_1 = 0$. Then the y_i are trivially linearly dependent; so we may assume hereafter that $y_1'(t) \neq 0$. Define a $\mathbb{C}$-derivation

$$D : L \to L, \quad D(f(t)) = \frac{f'(t)}{y_1'(t)}.$$

By Lemma 3.6, we have $D^1(\omega_i) = 0$. Furthermore, a direct computation shows

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

Therefore, we have that

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

By Lemma 3.7, we may assume $f_i, g \in \mathbb{C}$.

Rewrite the equation $\sum f_i \omega_i + g dy_1 = 0$ in the form

$$\sum_{i=1}^{n} f_i \cdot (-z_i^{-1} dz_i) = -\sum_{i=1}^{n} f_i dy_i - g dy_1.$$

Lemma 3.9 implies that either all $f_i = 0$, or the $z_i^{-1} dz_i$ are $\mathbb{Q}$-linearly dependent. In the first case, from (27) and the fact that the f_i and g are not all zero, we would get $dy_1 = 0$. Hence, y_1 is a constant, and, as noted earlier, this implies that $y_1 = 0$. Therefore, we suppose we are in the second case, say

$$\sum \frac{m_i (dz_i)}{z_i} = 0$$

with $m_i \in \mathbb{Z}$ not all zero. This implies

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

so $\prod z_i^{m_i} = e^{\sum m_i y_i}$ is a constant. By considering constant terms, this constant must be 1. Therefore,

$$\sum m_i y_i = 0,$$

giving the desired linear dependence of the y_i over $\mathbb{Q}$. □

4. The structural rank conjecture

We now return to the classical setting over $\mathbb{C}$, rather than the function field setting, and move on to consider matrices of elements of $\mathscr{L}$. The simplest case of 2×2 matrices leads to the following *four exponentials conjecture*:

Conjecture 4.1. *Let $M \in M_{2\times 2}(\mathscr{L})$. Then* $\det(M) = 0$ *only if the rows or columns of M are linearly dependent over $\mathbb{Q}$.*

This conjecture was first stated in print by Schneider [1957], though versions had been considered over the previous two decades by Selberg, Siegel, Alaoglu and Erdős [1944], and others (precise statements by Selberg and Siegel do not appear in the literature, but see [Waldschmidt 2023] for a discussion of their consideration of this problem). The four exponentials conjecture remains wide open. As an example, Waldschmidt [2023] points out the following elementarily stated open question, a positive answer for which would follow from the four exponentials conjecture: let t be a real number such that 2^t and 3^t are integers; does it follow that t is a nonnegative integer?

The strongest theoretical evidence for the conjecture is the following *six exponentials theorem*:

Theorem 4.2. *Let $M \in M_{2\times 3}(\mathscr{L})$. Then* $\operatorname{rank}(M) < 2$ *only if the rows or columns of M are linearly dependent over $\mathbb{Q}$.*

The six exponentials theorem was proven independently by Lang [1966] and Ramachandra [1968a; 1968b]. See Waldschmidt's delightful personal account [2023] for details and references on the history of the four exponentials conjecture and the six exponentials theorem.

The six exponentials theorem follows as a special case of the theorem of Waldschmidt and Masser that we will discuss later (see Section 5A). A naive generalization of the four exponentials conjecture to matrices of arbitrary dimension does not hold — in general, matrices may have lower than maximal rank even if the rows and columns are linearly independent over $\mathbb{Q}$. As an example, note that

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

Therefore, if we substitute for x, y and z any elements of $\mathscr{L}$ that are linearly independent, then we obtain a matrix of rank < 3 whose rows and columns are linearly independent over $\mathbb{Q}$. Examples such as these motivate the *structural rank conjecture*, which was stated precisely in the introduction. The matrix above has structural rank equal to 2.

4A. ***The p-adic setting.*** Most statements in transcendence theory have analogues in the p-adic setting. As we will describe below, these analogues are particularly important in Iwasawa theory. Let p be a prime number, and let $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}}_p$ denote the completion of the algebraic closure of $\mathbb{Q}_p$. The statements below work equally well over $\mathbb{Q}_p$, but working with $\mathbb{C}_p$ provides extra generality. We normalize the

p-adic absolute value on $\mathbb{C}_p$ in the usual way: $|p| = p^{-1}$. There exists a p-adic logarithm and a p-adic exponential function

$$\log_p : \{x \in \mathbb{C}_p : |x-1| < 1\} \to \mathbb{C}_p, \quad \exp_p : \{x \in \mathbb{C}_p : |x| < p^{-1/(p-1)}\} \to \mathbb{C}_p \tag{28}$$

defined by the usual power series

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

The functions $\log_p$ and $\exp_p$ are injective group homomorphisms on the domains given in (28). The p-adic logarithm extends uniquely to a continuous homomorphism

$$\log_p : \{x \in \mathbb{C}_p : |x| = 1\} \to \mathbb{C}_p$$

since every $x \in \mathbb{C}_p$ with $|x| = 1$ satisfies $|x^n - 1| < 1$ for an appropriate positive integer n, and we may define $\log_p(x) = (1/n)\log_p(x^n)$. Next we extend $\log_p$ to a continuous homomorphism

$$\log_p : \mathbb{C}_p^* \to \mathbb{C}_p$$

by fixing Iwasawa's (noncanonical) choice $\log_p(p) = 0$. The kernel of $\log_p$ on $\mathbb{C}_p^*$ then consists of elements of the form $p^a \cdot u$, where $a \in \mathbb{Q}$ and u is a root of unity.

We define the $\mathbb{Q}$-vector space of p-adic logarithms of algebraic numbers,

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

The p-adic version of Baker's theorem was proved by Brumer [1967] following Baker's method.

Theorem 4.3 (Baker and Brumer). *Let $y_1, \ldots, y_n \in \mathscr{L}_p$ be linearly independent over $\mathbb{Q}$. Then $y_1, \ldots, y_n$ are linearly independent over $\overline{\mathbb{Q}}$.*

Similarly, there are natural analogues of Schanuel's conjecture and the structural rank conjecture in the p-adic setting. To be precise we state the latter of these:

Conjecture 4.4 (p-adic structural rank conjecture). *Let*

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

The rank of M is equal to the structural rank of M.

4B. ***Applications in number theory.*** Statements in transcendence theory have important applications in algebraic number theory. In this section, we describe two important conjectures in Iwasawa theory that are special cases of the p-adic structural rank conjecture. These conjectures are our personal motivation for this study.

4B1. *Leopoldt's conjecture.* Fix a prime p and an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$.

Conjecture 4.5 (Leopoldt's conjecture). *Let F be a number field of degree n over $\mathbb{Q}$ and let $\sigma_1, \dots, \sigma_n$ denote the embeddings $F \hookrightarrow \overline{\mathbb{Q}}$. Let $\{u_1, \dots, u_r\}$ be a $\mathbb{Z}$-basis for $\mathcal{O}_F^*/\mu(F)$. Let*

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

Then $\operatorname{rank}_{\mathbb{C}_p}(M) = r$.

Proposition 4.6. *The p-adic structural rank conjecture implies Leopoldt's conjecture.*

Proof. The important point here is that the archimedean analogue of the statement of Leopoldt's conjecture is known to be true; this is the classical nonvanishing of the regulator of a number field. More precisely, if we fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and let $N = \big(\log|\sigma_j(u_i)|\big)$, where the absolute value denotes the usual absolute value on $\mathbb{C}$, then we have

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

This is proved using the fact that $\log|\cdot|$ takes values in the ordered field $\mathbb{R}$ (whereas $\log_p$ does not). For this reason, the p-adic statement lies far deeper than the archimedean one.

The field $\mathbb{Q}(x_1, \dots, x_k)$ appearing in the definition of the structural rank provides a bridge between the p-adic and complex settings, with the p-adic structural rank conjecture doing most of the heavy lifting.

Let $\{c_1, \dots, c_k\} \subset \{\sigma_j(u_i)\}$ be such that $\{\log_p(c_i)\}$ is a $\mathbb{Q}$-basis for the $\mathbb{Q}$-vector space spanned by the $\log_p(\sigma_j(u_i))$. Write

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

with $M_i \in M_{r\times n}(\mathbb{Q})$. The p-adic structural rank conjecture implies that

$$\begin{aligned}
\operatorname{rank}_{\mathbb{C}_p} M &= \operatorname{rank}_{\mathbb{Q}(x_1,\dots,x_k)}\left(\sum_{i=1}^{k} M_i x_i\right) \\
&\geq \operatorname{rank}_{\mathbb{C}}\left(\sum_{i=1}^{k} M_i \log|c_i|\right) \\
&= \operatorname{rank}_{\mathbb{C}}\big(\log|\sigma_j(u_i)|\big) \qquad (29) \\
&= r.
\end{aligned}$$

Hence, $\operatorname{rank}_{\mathbb{C}_p} M \geq r$, and so we must have equality. Note that in the equality (29), we are implicitly using the fact that, if $u_i \in \overline{\mathbb{Q}}^*$ are p-adic units and $m_i \in \mathbb{Z}$ are

integers, then

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

Let us describe two applications of Leopoldt's conjecture.

Algebraic (*Iwasawa theory*). By class field theory, Leopoldt's conjecture implies that the maximal pro-p abelian extension of F unramified outside p has $\mathbb{Z}_p$-rank equal to $r_2 + 1$, where $2r_2$ is the number of embeddings $F \hookrightarrow \mathbb{C}$ with image not contained in $\mathbb{R}$. See for example the exercises in [Neukirch 1999, page 394].

Analytic (*p-adic L-functions*). Let F be a totally real field, so

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

There is a p-adic analogue of the classical Dedekind zeta function of F, denoted by $\zeta_{F,p}$. A theorem of Colmez [1988] states that

$$\lim_{s \to 1} (s-1)\zeta_{F,p}(s) = (*)R_p(F), \tag{30}$$

where

$$R_p(F) = \pm \det\bigl(\log_p(\sigma_j(u_i))_{i,j=1,\dots,r}\bigr) \tag{31}$$

and $(*)$ denotes a specific nonzero algebraic number, which we do not describe precisely here. Note that, since there are $r+1$ embeddings σ_j, the last one has been excluded in the definition of $R_p(F)$. Which embedding is excluded, as well as the ordering of the remaining embeddings, only affects the determinant in (31) up to sign; the unspecified $\pm$ in (31) includes an orientation (a sign) that makes the product independent of choices.

Colmez's formula (30) is a p-adic "class number formula". It implies that $\zeta_{F,p}(s)$ has a pole at $s = 1$ if and only if Leopoldt's conjecture for (F, p) holds.

4B2. *The Gross–Kuz'min conjecture.* There is an analogue of Leopoldt's conjecture due independently to Gross and Kuz'min concerning p-adic L-functions at $s = 0$ rather than $s = 1$. Unlike the case of classical L-functions, there is no functional equation for p-adic L-functions relating the values at 0 and 1.

We refer the reader to [Gross 1981] for details about the Gross–Kuz'min conjecture beyond what we write below. To state the conjecture, let H be a CM field and H^+ its maximal totally real subfield. Let

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

Here w ranges over all places of H that do not divide p, including the archimedean ones. Then $\operatorname{rank}(U_p^-) = r$, where r is the number of primes of H^+ above p that split completely in H.

Let X_p denote the $\mathbb{C}_p$-vector space with basis indexed by the places of H above p. Let c denote the nontrivial element of $\mathrm{Gal}(H/H^+)$, i.e., c is complex conjugation. Let X_p^- denote the largest quotient of X_p on which c acts as -1. Then X_p^- has dimension r. We define two maps

$$\ell_p, o_p : U_p^- \to X_p^-.$$

The coordinate of $o_p(u)$ at the component corresponding to a place $\mathfrak{P}$ of H is $\mathrm{ord}_{\mathfrak{P}}(u)$, and the coordinate of $\ell_p(u)$ is $\log_p(\mathrm{N}_{H_{\mathfrak{P}}/\mathbb{Q}_p}(u))$. We extend ℓ_p and o_p to $\mathbb{C}_p$-linear maps

$$U_p^- \otimes \mathbb{C}_p \to X_p^-.$$

It is not hard to show using Dirichlet's unit theorem that o_p is an isomorphism, and we define

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

Conjecture 4.7 (Gross–Kuz'min). *We have* $R_p^-(H) \neq 0$.

A proof similar to the proof of Proposition 4.6 shows that the p-adic structural rank conjecture implies the Gross–Kuz'min conjecture (one uses ord_p in place of $\log|\cdot|$). Once again there are algebraic and analytic interpretations of this conjecture.

Algebraic (*Iwasawa theory*). By class field theory, the Gross–Kuz'min conjecture implies a bound on the growth of the p-parts of class groups of fields in the cyclotomic $\mathbb{Z}_p$-extension of H. See [Federer and Gross 1981, Proposition 3.9] for details.

Analytic (*p-adic L-functions*). Let χ denote the nontrivial character of $\mathrm{Gal}(H/H^+)$. Then one knows that

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

This follows for odd p by work of Wiles [1990]; an alternative proof using the Eisenstein cocycle that works for all p was given in [Charollois and Dasgupta 2014; Spiess 2014] using an argument of Spiess. In joint work with Darmon and Pollack then with Kakde and Ventullo [Dasgupta et al. 2011; 2018], we proved that

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

where $(*)$ is a specific nonzero rational number. This is a p-adic class number formula at $s = 0$. Therefore, $L_p(\chi\omega, s)$ has a zero of order exactly r at $s = 0$ if and only if the Gross–Kuz'min conjecture is true.

4B3. *Representation-theoretic considerations.* Retaining the setting of the Gross–Kuz'min conjecture, suppose now that H contains a totally real field F such that

H/F is Galois. Let $G = \mathrm{Gal}(H/F)$. For any representation M of G over $\mathbb{C}_p$, and character χ of an irreducible representation V, let M^χ denote the χ-isotypic component of M (i.e., the span of the subrepresentations of M isomorphic to V).

Then

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

where the sums range over the characters χ of irreducible representations V of G on which c acts as -1. The maps ℓ_p and o_p also decompose as sums of maps

$$\ell_p^\chi, o_p^\chi : U_p^\chi \to X_p^\chi.$$

We define

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

We then have

$$R_p^-(H) = \prod_\chi R_p^\chi(H). \tag{32}$$

Now, for χ as above,

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

where the sum ranges over the primes of F above p, $G_\mathfrak{p} \subset G$ denotes the decomposition group of a prime of H above $\mathfrak{p}$, and $V^{G_\mathfrak{p}}$ denotes the maximal subspace of V invariant under $G_\mathfrak{p}$. When $r_p^\chi = 1$, the regulator $R_p^\chi(H)$ is a $\overline{\mathbb{Q}}$-linear combination of p-adic logarithms of algebraic numbers. As pointed out in Proposition 2.13 of Gross [1981], the nonvanishing of $R_p^\chi(H)$ follows from the theorem of Brumer and Baker (Theorem 4.3) in this case.

Theorem 4.8. *If $r_p^\chi = 1$, then $R_p^\chi(H) \neq 0$.*

There is a particular case when *every* $r_p^\chi \leq 1$. If F contains only one prime above p (for example $F = \mathbb{Q}$), and G is abelian (so every V has dimension 1), then clearly $r_p^\chi \leq 1$. Combining Theorem 4.8 with the factorization (32), we obtain:

Corollary 4.9. *Let F be a totally real field with exactly one prime above p, and let H be a CM abelian extension of F. Then the Gross–Kuz'min conjecture holds for H.*

A similar analysis holds for Leopoldt's conjecture, and one obtains:

Theorem 4.10 [Brumer 1967, Theorem 2]. *Leopoldt's conjecture holds for abelian extensions of $\mathbb{Q}$.*

4C. ***A theorem of Roy.*** Damien Roy has proven a number of beautiful results in transcendence theory. We prove one of these now.

Theorem 4.11 (Roy). *The structural rank conjecture is equivalent to the special case of Schanuel's conjecture that states that, if* $y_1, \ldots, y_n \in \mathscr{L}$ *are* $\mathbb{Q}$*-linearly independent, then*

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

Similarly, the p-adic structural rank conjecture is equivalent to the p-adic version of the special case of Schanuel's conjecture, but we will content ourselves with the archimedean setting here. Theorem 4.11 is proven in [Roy 1995].

One direction of Roy's theorem is relatively elementary.

Lemma 4.12. *The special case of Schanuel's conjecture implies the structural rank conjecture.*

Proof. We assume the special case of Schanuel's conjecture. We first consider a matrix M with entries in $\mathscr{L}$. Let $M = \sum M_i c_i$ with $M_i \in M_{m\times n}(\mathbb{Q})$ and $c_i \in \mathscr{L}$ linearly independent over $\mathbb{Q}$. Write

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

and let $r = \operatorname{rank}(M_x)$. Let J_x be an $r \times r$ submatrix of M_x such that

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

in $\mathbb{Q}[x_1, \ldots, x_n]$. The determinant of the corresponding submatrix of M is equal to $P(c_1, \ldots, c_n)$ and hence cannot vanish since the c_i are algebraically independent, by the special case of Schanuel's conjecture. Therefore, $\operatorname{rank}(M) \geq r$. Of course, it is clear that $\operatorname{rank}(M) \leq r$, so we get equality.

Now assume M has entries in $\mathscr{L} + \mathbb{Q}$, but not in $\mathscr{L}$. There are two cases.

Case 1: 1 is not in the $\mathbb{Q}$-linear span of the entries of M. The $\mathbb{Q}$-basis for this span can be taken to have the form $\{1 + c_1, c_2, \ldots, c_n\}$, where $c_i \in \mathscr{L}$. It is easy to check that the c_i must be $\mathbb{Q}$-linearly independent, and hence, by the special case of Schanuel's conjecture, they are algebraically independent. The same is therefore true of $\{1 + c_1, c_2, \ldots, c_n\}$. The previous proof then applies to this basis.

Case 2: 1 is in the $\mathbb{Q}$-linear span of the entries of M. We may take a $\mathbb{Q}$-basis of this span of the form $\{c_0 = 1, c_1, \ldots, c_n\}$, where $c_i \in \mathscr{L}$ for $i \geq 1$. We proceed as before. Write

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

Let $r = \operatorname{rank}(M_x)$ and J_x an $r \times r$ submatrix of M_x with

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

The determinant of the corresponding submatrix J of M is $P(1, c_1, \ldots, c_n)$. Since P is a nonzero homogeneous polynomial of degree r, its specialization $P(1, x_1, \ldots, x_n)$ is also nonzero, so $\det(J) = P(1, c_1, \ldots, c_n) \neq 0$ by the algebraic independence of the c_i. Therefore, $\operatorname{rank}(M) \geq r$, as desired. □

The main content of the converse is in the following lemma:

Lemma 4.13. *Let k be a commutative ring and let $P \in k[x_1, \ldots, x_n]$. There exists a square matrix N with entries in*

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

such that $\det(N) = P$.

Let us for the moment take the lemma for granted and prove Roy's theorem.

Proof of Theorem 4.11. Assume the structural rank conjecture. Suppose $c_1, \ldots, c_n \in \mathscr{L}$ are linearly independent over $\mathbb{Q}$ and that $P(c_1, \ldots, c_n) = 0$ for some nonzero $P \in \mathbb{Q}[x_1, \ldots, x_n]$. As in Lemma 4.13, let N be a square matrix with entries in $\mathbb{Q} + \mathbb{Q}x_1 + \cdots + \mathbb{Q}x_n$ such that $\det(N) = P$.

Let M be the matrix N with x_i replaced by c_i. We then have $\det(M) = 0$. Note that the matrix M_x in the structural rank conjecture is the homogenization of the matrix N, with entries in $\mathbb{Q}x_0 + \mathbb{Q}x_1 + \cdots + \mathbb{Q}x_n$. We are using here that the c_i are $\mathbb{Q}$-linearly independent from 1, since e is transcendental. The conjecture implies that $\det(M_x) = 0$, whence $\det(N) = 0$ by specializing $x_0 = 1$, a contradiction. □

It remains now to prove Lemma 4.13. We first remark that this lemma is actually the starting point of an important avenue of research in theoretical computer science, where the lemma is usually attributed to Valiant [1979]. There are well-known efficient algorithms for calculating the determinant of a matrix, so expressing a general polynomial as a determinant gives an algorithm for efficiently calculating values of a polynomial. The minimal dimension of a matrix necessary to express a given polynomial as a determinant is known as the *determinantal complexity* of the polynomial. The study of the growth of determinantal complexity in families of polynomials is a topic with an extensive literature.

We follow Roy's proof of Lemma 4.13. We will prove the more general statement that, given any matrix $N \in M_{m\times m}(P_d)$, there exists a matrix $N' \in M_{m'\times m'}(P_1)$ such that $\det(N) = \det(N')$. Lemma 4.13 is the case where we start with an element $N \in P_d$, which we view as a 1×1 matrix. The advantage of the more general statement is that it may be proven by induction on d. We need to establish two sublemmas. The first establishes that, given a matrix $N \in M_{m\times m}(P_d)$, we may write it as a product of matrices with entries in spaces $P_{d'}$ with $d' < d$. The matrices that arise in the proof are not necessarily square, and this is resolved by the second lemma.

Lemma 4.14. *For a nonnegative integer d, let $P_d \subset k[x_1, \ldots, x_n]$ denote the k-subspace of polynomials of total degree $\leq d$. Given $N \in M_{m\times m}(P_d)$ with $d \geq 1$, there exists an integer s and matrices*

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

such that $N = AB$.

Proof. Let $N = (a_{i,j})$ with $a_{i,j} \in P_d$. We can write

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

with $c_{i,j,\ell} \in P_{d-1}$ for $1 \leq \ell \leq n+1$. Let

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

Define

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

Then one calculates that $N = AB$. □

The matrices A and B in Lemma 4.14 are not square, so we cannot recursively apply the lemma. This is resolved by the following observation:

Lemma 4.15. *Let $A \in M_{m\times s}$, $B \in M_{s\times m}$. Then*

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

where the matrix on the right is square of dimension $m + s$.

Proof. We simply note that

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

and take determinants of both sides. □

We can now prove our main lemma.

Proof of Lemma 4.13. As indicated above, we will show by induction on d that, for any matrix $N \in M_{m\times m}(P_d)$, there exists a matrix $N' \in M_{m'\times m'}(P_1)$ such that $\det(N) = \det(N')$.

The base case $d = 1$ is trivial. For $d > 1$ we use Lemma 4.14 to write $N = AB$ with $A \in M_{m\times s}(P_{d-1})$ and $B \in M_{s\times m}(P_1)$. Lemma 4.15 then yields $\det(N) = \det(N')$ with $N' \in M_{(m+s)\times(m+s)}(P_{d-1})$. The induction is now complete.

The lemma is the case where we start with a 1×1 matrix in P_d. □

5. The theorem of Waldschmidt and Masser

To our knowledge, the strongest general unconditional result toward the structural rank conjecture is Theorem 1.6 of Waldschmidt and Masser, stated in the introduction. For the sake of variety, we will prove the p-adic version of the conjecture in this section, though the proof of the archimedean version is essentially the same (both versions are proven in [Waldschmidt 1981]). The statement of the p-adic version is exactly the same as the archimedean one, with $\mathscr{L}$ replaced by $\mathscr{L}_p$.

Theorem 5.1 (Waldschmidt and Masser). *Let m and n be positive integers and let $M \in M_{m\times n}(\mathscr{L}_p)$. Suppose that*

$$\operatorname{rank}(M) < \frac{mn}{m+n}.$$

Then there exist $P \in \mathrm{GL}_m(\mathbb{Q})$ and $Q \in \mathrm{GL}_n(\mathbb{Q})$ such that

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

where the 0 block has dimension $m' \times n'$ with $m'/m + n'/n > 1$.

5A. ***Applications.*** Let us first state some applications of the complex and p-adic Waldschmidt–Masser theorems. The six exponentials theorem, which had been proven earlier in the 1960s, is a corollary of the Waldschmidt–Masser theorem.

Proof of Theorem 4.2. The case where $M = 0$ is trivial. Therefore suppose $M \in M_{2\times 3}(\mathscr{L})$ has rank 1. Since $1 < \frac{6}{5}$, the Waldschmidt–Masser theorem implies that, after a rational change of basis on the left and right, the matrix M has the block matrix form

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

where the 0 block has dimension 1×2 or 2×1. In the first case, our matrix has the form

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

Such a matrix has rank 1 only if it has the form

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

In the first case, we see that PM has the same shape, which says that the rows of M are linearly dependent over $\mathbb{Q}$. In the second case, we see that MQ has the same shape, which says that the columns of M are linearly dependent over $\mathbb{Q}$. The case where the original block of zeroes has dimension 2×1 is similar. □

In the case of a square matrix, the Waldschmidt–Masser theorem simplifies to the following:

Corollary 5.2. *Let $M \in M_{n\times n}(\mathscr{L})$ or $M_{n\times n}(\mathscr{L}_p)$. Suppose that* $\operatorname{rank}(M) < \frac{1}{2}n$. *Then there exist P, $Q \in \mathrm{GL}_n(\mathbb{Q})$ such that*

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

where the 0 *block has dimension $m \times m'$ with $m + m' > n$.*

Corollary 5.3. *The Leopoldt regulator matrix and the Gross–Kuz'min regulator matrix have rank at least half their expected ranks.*

Proof. Let r be the expected rank of the Leopoldt matrix. Let

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

be an $r \times r$ submatrix of the *archimedean* regulator with $\det(M') \neq 0$. Let

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

be the corresponding submatrix of the Leopoldt matrix.

If the rank of the Leopoldt matrix is less than $\frac{1}{2}r$, the same is true for M. The Waldschmidt–Masser theorem then implies that there exist P, $Q \in \mathrm{GL}_r(\mathbb{Q})$ such that PMQ has an upper right 0 block with dimension $m \times m'$, where $m + m' > r$. But then $PM'Q$ has this same property. This implies that $\det(M') = 0$, a contradiction.

The same proof works for Gross's regulator, using ord_p instead of $\log|\cdot|$. □

5B. ***Auxiliary polynomial.*** As in the proof of Baker's theorem, the Waldschmidt–Masser theorem is proven by constructing, under the assumptions of the theorem, a suitable auxiliary polynomial whose existence implies the conclusion of the theorem. Waldschmidt's result is that the auxiliary polynomial exists, and Masser's theorem is that this polynomial gives the desired conclusion. Let us describe this in greater detail.

We have $M = (a_{i,j})$ with $a_{i,j} = \log_p(x_{i,j}) \in \mathscr{L}_p$. Here $x_{i,j} \in \overline{\mathbb{Q}}^*$. After scaling M if necessary, we may assume that $|x_{i,j} - 1|_p < 1$. For $i = 1, \dots, m$, let

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

Let $X = \langle x_1, x_2, \dots, x_m\rangle \subset (\overline{\mathbb{Q}}^*)^n$ be the subgroup generated by the x_i. For each positive integer N, define

$$X(N) = \left\{ \prod_{i=1}^{m} x_i^{a_i} \;\middle|\; a_i \in \mathbb{Z},\ 0 \le a_i \le N \right\}.$$

For a polynomial P in several variables, we write $\deg(P)$ for the total degree of P.

Theorem 5.4 [Waldschmidt 1981]. *Suppose* $r = \operatorname{rank}(M) < mn/(m+n)$. *There exists* $\epsilon > 0$ *such that, for all* N *sufficiently large, there exists a nonzero* $P \in \mathbb{Z}[t_1, \dots, t_n]$ *such that* $\deg(P) < N^{m/n-\epsilon}$ *and* $P(x) = 0$ *for all* $x \in X(N)$.

Waldschmidt's theorem is the "transcendence" part of Theorem 1.6. Masser's theorem, which is a purely algebrogeometric statement, takes the existence of an auxiliary polynomial P as above and deduces the relations necessary to give the desired result about the original matrix M. We will describe the statement of Masser's theorem precisely in a moment, but first let us comment about the numerology concerning the auxiliary polynomial in the statement of Theorem 5.4. We can view the existence of a polynomial with prescribed zeroes as a system of linear equations in the coefficients of the polynomial. Each zero gives one such linear equation. If the $x_{i,j}$ are generic, the size of $X(N)$ is $(N+1)^m$. A polynomial of degree $< d$ has fewer than d^n coefficients. Therefore, if the $x_{i,j}$ are generic, we expect that we would require $d^n \geq (N+1)^m$ for a polynomial to exist, so, in particular, $d > N^{m/n}$. For this reason, the existence of the auxiliary polynomial P in Theorem 5.4 does not hold for generic $x_{i,j}$.

Let us now state Masser's theorem precisely. Let k be a field of characteristic 0, let $(x_{i,j}) \in M_{m\times n}(k^*)$. Define X and $X(N)$ as above. Define a pairing

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

Theorem 5.5 [Masser 1981]. *Let* $N > 0$ *and suppose there exists* $P \in k[t_1, \dots, t_n]$ *such that* $\deg(P) < (N/n)^{m/n}$ *and* $P(x) = 0$ *for all* $x \in X(N)$. *Then there exist subgroups* $A \subset \mathbb{Z}^m$ *and* $B \subset \mathbb{Z}^n$ *of ranks* m' *and* n', *respectively, with* $\langle A, B \rangle = 1$ *and* $m'/m + n'/n > 1$.

Theorems 5.4 and 5.5 combine to give Theorem 5.1. In the remainder of this section, we prove these two theorems.

5C. ***Waldschmidt's theorem.*** We will give two proofs of Waldschmidt's theorem.

5C1. *Proof* 1 *of Waldschmidt's theorem.* Our first proof is similar in spirit to Waldschmidt's original proof. For simplicity, we will assume $x_{i,j} \in \mathbb{Z}$ and $x_{i,j} \equiv 1 \pmod{p}$. Standard techniques (scaling by an integer to obtain algebraic integers, and taking norms to obtain integers) allow one to handle the general case, but we would like to avoid the extra notation required.

Let r denote the rank of the matrix $M \in M_{m\times n}(\mathbb{Z}_p)$. After reordering columns if necessary, we can assume that the last $n-r$ columns of M are in the $\mathbb{Z}_p$-linear span of the first r columns. Then, for each $i > r$, there exist $\lambda_{i,1}, \dots, \lambda_{i,r} \in \mathbb{Z}_p$ such that, if $z = (z_1, \dots, z_n) \in X$, we have

$$z_i = z_1^{\lambda_{i,1}} z_2^{\lambda_{i,2}} \cdots z_r^{\lambda_{i,r}} \quad \text{for } i > r. \tag{33}$$

To make sense of the right-hand side of this equality, note that, for $\lambda \in \mathbb{Z}_p$, the function

$$t^\lambda = (1+(t-1))^\lambda = \sum_{i=0}^{\infty} \binom{\lambda}{i} (t-1)^i \tag{34}$$

is a convergent power series in $t-1$. Hence, if $t \in 1+p\mathbb{Z}_p$, then (34) converges in $\mathbb{Z}_p$.

Our goal is to find a polynomial $P \in \mathbb{Z}[t_1, \ldots, t_n]$ such that $P(z) = 0$ for $z \in X(N)$. Define $u_i = t_i - 1$ and consider the canonical map

$$\varphi : \mathbb{Z}[t_1, \ldots, t_n] \to \mathbb{Z}_p[\![u_1, \ldots, u_n]\!]/(t_i - t_1^{\lambda_{i,1}} \cdots t_r^{\lambda_{i,r}})_{i=r+1}^n \cong \mathbb{Z}_p[\![u_1, \ldots, u_r]\!]. \tag{35}$$

The elements in the quotient in (35) are interpreted as power series in the u_i via (34).

Fix a positive integer c. Define φ_c to be the composition of φ with the canonical reduction

$$\mathbb{Z}_p[\![u_1, \ldots, u_r]\!] \to (\mathbb{Z}/p^c\mathbb{Z})[\![u_1, \ldots, u_r]\!]/(u_1^c, \ldots, u_r^c). \tag{36}$$

If a polynomial $P \in \mathbb{Z}[t_1, \ldots, t_n]$ satisfies $\varphi_c(P) = 0$, then $P(z)$ will be divisible by p^c for any $z \in X$. Indeed, $\varphi(P)(z) = P(z)$ is well defined for $z \in X$, since the kernel of φ vanishes on X. Next, it is clear that $\varphi(P)(z) \pmod{p^c}$ depends only on the coefficients of $\varphi(P)$ modulo p^c. Finally, we note that

$$z_i \equiv 1 \pmod{p} \implies u_i \equiv 0 \pmod{p} \implies u_i^c \equiv 0 \pmod{p^c}.$$

Now, the ring on the right in (36) is finite. The total number of monomials in $u_1, \ldots, u_r$ modulo $(u_1^c, \ldots, u_r^c)$ is c^r, so the total number of possible values of these coefficients mod p^c is

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

Therefore, by the pigeonhole principle, if we have a subset of $\mathbb{Z}[t_1, \ldots, t_n]$ of size greater than $p^{c^{r+1}}$, then some two elements of the subset, say P_1 and P_2, will have equal image under φ_c, and the difference $P = P_1 - P_2$ will satisfy $P(z) \equiv 0 \pmod{p^c}$ for all $z \in X$.

We will take the subset of all polynomials with degree in each variable less than some constant d with coefficients that are nonnegative integers less than p^h for some constant h. The size of this subset is p^{hd^n}, and hence the condition that we want is

$$hd^n > c^{r+1}. \tag{37}$$

Now, we also want to use the principle of "discreteness of the integers" discussed in the proof of Baker's theorem to ensure that the condition $P(z) \equiv 0 \pmod{p^c}$ for $z \in X(N)$ implies that $P(z) = 0$. For this, we need a crude bound on $|P(z)|$ (the archimedean absolute value). Suppose that A is an upper bound on $|x_{i,j}|$. Then, for

each $z = (z_1, \ldots, z_n) \in X(N)$, we have $|z_i| < A^{Nm}$. Therefore, each monomial in the evaluation of $P(z)$ has absolute value at most $p^h A^{Ndmn}$, and in total we obtain

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

Therefore, if

$$d^n p^h A^{Ndmn} < p^c, \tag{38}$$

then we indeed have the implication

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

To prove the theorem, we set $d = \lfloor N^{m/n-\epsilon}/n \rfloor$, so that the constructed polynomial P will have degree less than $N^{m/n-\epsilon}$, as required. We search for parameters h and c such that both (37) and (38) hold. Not surprisingly, these inequalities are pulling in the opposite direction — the first says that h is large relative to c, and the second says that h is small relative to c. For N large, the two inequalities will be satisfied if

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

for the appropriate constants k and k'.

If we set $c = N^{(m+n)/n+\epsilon}$ and $h = cN^{-\delta}$ for a small $\delta > 0$, then it is clear that the second inequality will hold for N sufficiently large. Plugging these parameters into the first inequality yields

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

It is clear that we can choose small positive δ and ϵ satisfying this inequality if

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

This completes the proof.

5C2. *Proof 2 of Waldschmidt's theorem.* For our second proof, we will return to the completely general case, i.e., we do not assume that $x_{i,j} \in \mathbb{Z}$, only that $x_{i,j} \in \overline{\mathbb{Q}}^*$. Our motivation in giving the second proof is that it introduces an important topic in transcendence theory not discussed earlier, namely the theory of *interpolation determinants* pioneered by Michel Laurent. Laurent [1991] gave a new proof of the six exponentials theorem using his new theory. The basic idea is that we will view the existence of the desired polynomial P as the solution of a linear system of equations in the coefficients of the polynomial, and show that the associated determinant vanishes.

Again we will construct a polynomial P such that the degree in each variable is less than $d = \lfloor N^{m/n-\epsilon}/n \rfloor$ and such that $P(z) = 0$ for all $z \in X(N)$. Consider the matrix whose rows are indexed by our desired zeroes $z \in X(N)$, and columns are

indexed by the exponents

$$y \in \mathbb{Z}^n(d-1) = \{(y_1, \ldots, y_n) \mid 0 \leq y_i \leq d-1\}$$

of the monomials of our desired polynomial,

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

It suffices to show that $\operatorname{rank}(L) < N^{m-n\epsilon}/n^m < d^n$, as then any nonzero vector in its kernel will be the coefficients of our desired polynomial. Of course, by making ϵ smaller, we can ignore the constant n^m, since $N^\epsilon \gg n^m$ for N large.

We state without proof the following elementary interpretation of the rank of a matrix:

Lemma 5.6. *Let k be a field and suppose that a matrix*

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

has rank equal to r. Then there exist vectors

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

such that $a_{i,j} = \langle \beta_i, \gamma_j \rangle$.

In our situation, we have $M = \log_p(x_{i,j}) \in M_{m \times n}(\mathbb{C}_p)$ with rank r. We write

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

Without loss of generality, we can scale all the β_i and γ_j to assume all their coordinates have absolute value $< p^{-1}$. (This just scales the matrix M, which affects neither the assumptions nor conclusions of the theorem.)

If $z = \prod_{i=1}^m x_i^{\ell_i}$ for $\ell \in \mathbb{Z}^m$, then, for $y \in \mathbb{Z}^n$, we have

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

Next we will require a p-adic Schwarz' lemma. For a positive integer d and real $R > 0$, define

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

For analytic $f : B_d(R) \to \mathbb{C}_p$, define

$$|f|_R = \max_{z \in B_d(R)} |f(z)|. \tag{39}$$

Lemma 5.7. *Suppose that $f : B_1(R) \to \mathbb{C}_p$ is analytic and has a zero of order at least n at $z = 0$. Then, for any $0 < R' < R$, we have*

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

Proof. Let $g(z) = f(z)/z^n$. This is analytic on $B_1(R)$ since f has a zero of order at least n at $z = 0$. For any $z \in B_1(R')$, we have

$$|f(z)| \le (R')^n |g(z)| \le (R')^n |g|_R = \left(\frac{R'}{R}\right)^n |f|_R.$$

The last equality uses the p-adic maximal modulus principle, which states that the maximum in (39) is achieved on the boundary $|z| = R$. See [Cherry 2009, Theorem 1.4.1] or [Stansifer 2012, Theorem 7] for a proof of this analytic fact. □

Now we present Laurent's main theorem on interpolation determinants.

Theorem 5.8 (Laurent). *Let $0 < R' < R$ and let $f_1, \dots, f_d$ be analytic functions*

$$B_r(R) \to \mathbb{C}_p.$$

Let $z_1, \dots, z_d \in B_r(R')$. Then $L = \det(f_j(z_i))$ satisfies

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

where, for d sufficiently large relative to r,

$$\Theta_r(d) > \frac{r}{6e} d^{(r+1)/r}. \tag{40}$$

Proof. Define $\Delta(z) = \det(f_j(z_i z))$, which is analytic on $|z| \le R/R'$. We will show that $\Delta(z)$ has a zero of order at least $\Theta_r(d)$ at $z = 0$ for some combinatorial function Θ_r satisfying (40), which we will define in a moment. The result then follows from Schwarz' lemma:

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

using the trivial upper bound

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

(Note that, in the complex case, we would need a factor of $d!$ on the right, but, in the nonarchimedean setting, this factor is not required because of the strong triangle inequality.)

Write each f_i as a power series in the variables $u_1, \dots, u_r \in \mathbb{C}_p$. By multilinearity of the determinant, it suffices to consider the case $f_j(u) = u^{v_j} = u_1^{v_{1j}} u_2^{v_{2j}} \cdots u_r^{v_{rj}}$ for nonnegative integers v_{ij}. Then

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

where $\|v_j\| = v_{j1} + v_{j2} + \cdots + v_{jr}$. If any two tuples v_j are equal, this determinant vanishes and $\Delta(z)$ is identically 0. If not, then the order of vanishing is at least

$$\Theta_r(d) := \min\left\{ \sum_{j=1}^{d} \|v_j\| \;\middle|\; v_1, \ldots, v_d \in (\mathbb{Z}^{\geq 0})^r \text{ with } v_i \neq v_j \text{ if } i \neq j \right\}.$$

For example, $\Theta_1(d) = \frac{1}{2}d(d-1)$. For a proof of the combinatorial inequality (40), see [Waldschmidt 1992, Lemma 4.3]. □

We can now apply Laurent's theorem to complete the proof of Waldschmidt's theorem. We want to show that any square submatrix $L' = (z_i^y)$ of L of dimension $d^n \approx N^{m-n\epsilon}$ has vanishing determinant, where

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

As explained earlier, the entries of the matrix L' can be written in the form $\exp\left(\left\langle \sum \beta_i \ell_i, \sum \gamma_i y_i \right\rangle\right)$ with $\ell \in \mathbb{Z}^m(N)$ corresponding to z. For each y we have the function

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

We apply Laurent's theorem on interpolation determinants with $R = 1$ and $R' = 1/p$. We find

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

where $C > 1$ is a constant.

Now we want to put a bound on the archimedean absolute value of L'. Let

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

Then $|z^y|_\infty \leq A^{N \cdot N^{(m/n)-\epsilon} n}$. Therefore,

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

The factorial is dominated by the other term and can be ignored. Scaling to obtain integrality just scales D. The same is true for taking norm from the field generated by the $x_{i,j}$ down to $\mathbb{Q}$ in order to obtain an element of $\mathbb{Z}$.

Therefore, we will have $L' = 0$ if

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

Of course, for this inequality to hold for large N, the precise values of C and D do not matter; all that matters is that we have the corresponding inequality of exponents.

It therefore suffices to have

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

This simplifies to

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

There exists $\epsilon > 0$ satisfying this inequality if and only if

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

This gives the desired vanishing of $\det(L')$ and completes the second proof of Waldschmidt's theorem.

5D. ***Masser's theorem.*** We conclude this section by proving Masser's theorem, stated in Theorem 5.5 above. This is a purely algebrogeometric statement that does not involve the logarithm or exponential functions. In particular, we work over an arbitrary field k of characteristic 0. Recall the notation established in Section 5B. We let the group $X \subset (k^*)^n$ act on the polynomial ring $R = k[t_1, \ldots, t_n]$ by

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

Recall that the subgroup X is generated by elements $x_1, \ldots, x_m$. If $a \in \mathbb{Z}^m$, we write $x^a = \prod_{i=1}^m x_i^{a_i} \in X$. For a prime ideal $\mathfrak{p} \subset R$, let

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

Before delving into the proof, it is instructive to consider the simplest case, $n = m = 2$. We let $N > 0$ and suppose there exists $P \in k[t_1, t_2]$ such that $\deg(P) < N$ and $P(x) = 0$ for all $x \in X(2N)$. We want to show that either

(A) there is a nonzero $a \in \mathbb{Z}^2$ such that $x^a = (1, 1)$ (this corresponds to $m' = 1$ and $n' = 2$), or

(B) there exists a nonzero $b \in \mathbb{Z}^2$ such that $z^b = z_1^{b_1} z_2^{b_2} = 1$ for all $z \in X$ (this corresponds to $m' = 2$ and $n' = 1$).

We factor P into a product $\prod P_i$ of irreducibles of $k[t_1, t_2]$. We can assume that none of the P_i are monomials, since monomials have no zeroes in $(k^*)^2$. We will first show that, if any P_i satisfies $\mathrm{rank}\big(\mathrm{Stab}_X((P_i))\big) = 2$, then we are in the second case above. This follows from Lemma 5.9 below, but it is relatively easy to see in this case explicitly. Indeed, if $t_1^{a_1} t_2^{a_2}$ is a monomial occurring in P_i, then the equation $zP_i = \lambda P_i$ for $z \in X$ and $\lambda \in k^*$ yields

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

Letting $t_1^{a_1'} t_2^{a_2'}$ be some other monomial occurring in P_i (recall we may assume that P_i is not a monomial) we get a similar equation; dividing these two cancels λ, so we obtain

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

where $b_i = a_i - a_i'$ for $i = 1, 2$ are not both zero. If $\operatorname{rank}\big(\operatorname{Stab}_X((P_i))\big) = 2$, then this holds for all z in a finite-index subgroup of X, so, replacing (b_1, b_2) by an appropriate multiple, we are in case (B).

Therefore, we are left to consider the case where each irreducible factor P_i of P satisfies $\operatorname{rank}\big(\operatorname{Stab}_X((P_i))\big) \leq 1$. In this case, we will show that there is a polynomial of the form

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

where $a_i \in \mathbb{Z}$ and $z_i \in X(N)$, such that P and Q are relatively prime. Let us first explain why this completes the proof. Since P vanishes on $X(2N)$, each polynomial $z \cdot P$ with $z \in X(N)$ vanishes on $X(N)$; hence, the polynomial Q vanishes on $X(N)$. Therefore, both P and Q vanish on $X(N)$. The set $X(N)$ has size $(N+1)^2$ *unless* we are in case (A) above. But $\deg Q \leq \deg P < N$, and the polynomials are coprime, so we would obtain a contradiction to Bézout's theorem if these polynomials had $(N+1)^2$ common zeroes. We must therefore be in case (A).

To see the existence of the polynomial Q, we first show that, for each irreducible polynomial P_i, there exists z_i such that $z_i^{-1} \cdot P_i$ does not divide P, or, equivalently, P_i does not divide $z_i \cdot P$. This is established by counting. Since $\operatorname{rank}_X((P_i)) \leq 1$, there are at least $N+1$ distinct ideals among the set $(z^{-1} \cdot P_i)$ as z ranges over $X(N)$. See Lemma 5.12 below for a proof. But P has degree less than N, which is a bound on the number of irreducible factors, so some $z^{-1} \cdot P_i$ must not be a factor of P. With these z_i in hand, the existence of the linear combination Q is an easy inductive argument using the pigeonhole principle; see Lemma 5.13 below.

We now return to the general case. Recall that the *height* $\operatorname{ht}(\mathfrak{p})$ of a prime ideal $\mathfrak{p}$ is the largest integer r such that there exists a chain of distinct prime ideals

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

Lemma 5.9. *Let $\mathfrak{m} = (t_1 - 1, \ldots, t_n - 1)$. Let $\mathfrak{p} \subset \mathfrak{m}$ be a prime of height n' and let $A = \operatorname{Stab}_X(\mathfrak{p})$. There exists a subgroup $B \subset \mathbb{Z}^n$ of rank $\geq n'$ such that $\langle A, B \rangle_X = 1$.*

Proof. Let $B = \{y \in \mathbb{Z}^n \mid \langle A, y \rangle_X = 1\}$. Choose $Z \subset \mathbb{Z}^n$ such that

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

We want to show that $s := \operatorname{rank}(Z) \leq n - n'$. Let $\{z_1, \ldots, z_s\}$ be a basis for Z. Write $z_i = (z_{i,1}, \ldots, z_{i,n})$.

For $i = 1, \ldots, s$, let $u_i = \prod_{j=1}^{n} t_j^{z_{i,j}} \in R' = k[t_1^{\pm 1}, \ldots, t_n^{\pm 1}]$. Since

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

if $s > n - n'$ then there exists a nonzero polynomial Q with coefficients in k such that $Q(u_1, \ldots, u_s) \in \mathfrak{p}R'$. Suppose this is the case, and write $Q(u_1, \ldots, u_s)$ as a polynomial $Q'(t_1, \ldots, t_n) \in \mathfrak{p}R'$.

For any $a \in A$, we have $x^a \cdot Q' \in \mathfrak{p}R'$, so

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

Fix a and apply this with a replaced by da, as $d = 0, 1, \ldots$. Using the Vandermonde trick from Baker's theorem, we find that some $\mathbb{Z}$-linear combination of the z_i is orthogonal to a. More precisely, we have $\langle a, w\rangle_X = 1$ for some

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

Therefore,

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

But A is a finitely generated free abelian group and cannot be written as a finite union of proper subgroups. Therefore, there exists $w \in S$ such that $\langle A, w\rangle = 1$. But then $w \in B$, contradicting $w \in Z$. Therefore, $s \leq n - n'$, as desired. □

Given Lemma 5.9, our task now is to show the existence of a prime ideal $\mathfrak{p}$ with height n' such that $\operatorname{rank}(\operatorname{Stab}_X(\mathfrak{p})) = m'$, where $m'/m + n'/n > 1$. This is provided by the following theorem:

Theorem 5.10. *Let $N > 0$ and suppose there exists*

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

such that $\deg(P) < (N/n)^{m/n}$ and $P(x) = 0$ for all $x \in X(N)$. Then there exists a prime ideal $\mathfrak{p} \subset \mathfrak{m}$ of height n' such that

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

Lemma 5.9 and Theorem 5.10 combine to give Theorem 5.5. We will prove the contrapositive of Theorem 5.10. For each $1 \leq n' \leq n$, let $m' = m'_{n'}$ be the maximal rank of $\operatorname{Stab}_X(\mathfrak{p})$ as $\mathfrak{p}$ ranges over the primes contained in $\mathfrak{m}$ with height equal to n'. If any $m' = m$, then $m'/m + n'/n = 1 + n'/n > 1$, so we are done. Therefore, assume that every $m' < m$ and define

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

Note that

$$\eta_{n'} > \frac{n}{m} \iff \frac{m'}{m} + \frac{n'}{n} > 1. \tag{41}$$

Theorem 5.10 will arise as a corollary of the following statement:

Theorem 5.11. *Let $f \in R$ have degree D and let*

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

There exists $z \in X(N)$ such that $f(z) \neq 0$.

Theorem 5.11 implies Theorem 5.10. Indeed, if each $\eta_{n'}$ for $1 \leq n' \leq n$ satisfies $\eta_{n'} \leq n/m$, then Theorem 5.11 implies that there exists $z \in X(n \deg(P)^{n/m})$ such that $P(z) \neq 0$. But, by assumption, $n \deg(P)^{n/m} < N$, yielding a contradiction to the assumption $P(z) = 0$ for all $z \in X(N)$. Therefore, some $\eta_{n'}$ is larger than n/m, giving the desired result by (41).

The proof of Theorem 5.11 requires significant commutative algebra. We first establish some notation. Let

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

The set $S_{\mathfrak{M}}$ is multiplicatively closed. For an ideal $\mathfrak{a} \subset R$, define

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

Note that, for a prime ideal $\mathfrak{p} \subset R$, we have $\mathfrak{p}^* = \mathfrak{p}$ if and only if $\mathfrak{p} \subset z \cdot \mathfrak{m}$ for some $z \in X$, and $\mathfrak{p}^* = R$ otherwise. Indeed, if $\mathfrak{p}^* \neq \mathfrak{p}$, then there exists $t/s \in (S_{\mathfrak{M}}^{-1}\mathfrak{p}) \cap R$ such that $t/s \notin \mathfrak{p}$. Write $t/s = g \in R$ with $g \notin \mathfrak{p}$. Since $t = gs \in \mathfrak{p}$ and $\mathfrak{p}$ is prime, this implies that $s \in \mathfrak{p}$. Since $s \in S_{\mathfrak{M}}$, we conclude that $\mathfrak{p} \not\subset \mathfrak{M}$, and hence $\mathfrak{p} \not\subset z \cdot \mathfrak{m}$ for any $z \in X(N)$. Furthermore, in this case, we have $s/s = 1 \in \mathfrak{p}^*$, so $\mathfrak{p}^* = R$. Now, all of these steps are clearly reversible, except possibly "$\mathfrak{p} \not\subset \mathfrak{M}$ implies $\mathfrak{p} \not\subset z \cdot \mathfrak{m}$ for all $z \in X(N)$". The inverse (equivalently, converse) of this statement reads "$\mathfrak{p} \subset \mathfrak{M}$ implies $\mathfrak{p} \subset z \cdot \mathfrak{m}$ for some $z \in X(N)$". This is precisely the prime avoidance lemma. This completes the proof of our claim about $\mathfrak{p}^*$.

We next recall some definitions from commutative algebra. An *associated prime* of an ideal $\mathfrak{a} \subset R$ is a prime ideal $\mathfrak{p}$ such that there exists an R-module injection $R/\mathfrak{p} \hookrightarrow R/\mathfrak{a}$. (The associated primes play the role of the irreducible factors in our simplified proof for $n = m = 2$.) An ideal $\mathfrak{a} \subset R$ is called *unmixed of height r* if all its associated prime ideals have height r.

Next we recall the definitions of *dimension* and *degree* of an ideal of R and some of the basic properties of these functions. Let $R_0 = k[t_0, \ldots, t_n]$. For $f \in R$, let $f_0 \in R_0$ denote the homogenization of f, defined by padding each monomial of f with the correct power of t_0 to obtain a homogeneous polynomial of degree $\deg(f)$. For an ideal $\mathfrak{a} \subset R$, let $\mathfrak{a}_0$ denote the homogeneous ideal generated by f_0 for $f \in \mathfrak{a}$. Then $R_0/\mathfrak{a}_0$ is a graded R_0-module.

There is a polynomial

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

called the *Hilbert polynomial* of $\mathfrak{a}$, such that

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

for i sufficiently large. We define the dimension and degree of $\mathfrak{a}$, respectively, by

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

These are both integers. They satisfy the following properties:

- $\ell((f))$ is the degree of f in the usual sense.
- If $\mathfrak{a} \subset \mathfrak{b}$ and $\mathrm{ht}(\mathfrak{a}) = \mathrm{ht}(\mathfrak{b})$, then $\ell(\mathfrak{a}) \geq \ell(\mathfrak{b})$.
- If $\mathfrak{a}$ and $\mathfrak{b}$ are unmixed of height r, then so is $\mathfrak{a} \cap \mathfrak{b}$, and

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

Note that from this it follows that, if $\mathfrak{a}$ is unmixed, then the number of associated primes of $\mathfrak{a}$ is $\leq \ell(\mathfrak{a})$. To see this, we note that there is a *primary decomposition* $\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{q}_i$, where $\{\sqrt{\mathfrak{q}_i}\}$ is the set of associated primes.

We can now begin the proof of Theorem 5.11. Let $f \in R$ have degree D and let

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

We will inductively construct f_r, a $\mathbb{Z}$-linear combination of elements in $X(N_r) \cdot f$ such that $\mathfrak{a}_r = (f_1, \ldots, f_r)$ satisfies the following: either $\mathfrak{a}_r^* = R$, or $\mathfrak{a}_r^*$ is unmixed of height r and degree at most D^r.

This will give the theorem: for $r = n+1$, $\mathfrak{a}_r^*$ cannot have height $n+1$, so $\mathfrak{a}_r^* = R$, which implies $\mathfrak{a}_r \not\subset \mathfrak{M}$. In particular, $f_i \notin \mathfrak{m}$ for some i, so, if $f_i = \sum d_j(z_j \cdot f)$ with $d_j \in \mathbb{Z}$ and $z_j \in X(N_{n+1})$, then $f(z_j) \neq 0$ for some z_j, as desired.

Base case: Take $f_1 = f$ and $\mathfrak{a}_1 = (f)$. Then $\mathfrak{a}_1^* = (f^*)$, where f^* is the quotient of f by any irreducible factors not lying in $\mathfrak{M}$. If $f^* \neq 1$, then (f^*) is unmixed of height 1 by Krull's principal ideal theorem, and has degree $\leq D = \deg(f)$.

Inductive step: Suppose $r \geq 2$ and that we have constructed $f_1, \ldots, f_{r-1}$. If $\mathfrak{a}_{r-1}^* = R$, then we can take $f_r = f$. We have $\mathfrak{a}_r^* = R$, and we are done. Therefore, we suppose that $\mathfrak{a}_{r-1}^*$ is unmixed of height $r-1$ and degree at most D^{r-1}. The construction of f_r is slightly elaborate in this case, so let us outline the steps:

(1) For any associated prime $\mathfrak{p}$ of $\mathfrak{a}_{r-1}^*$, show by counting that there exists $a \in \mathbb{Z}^m(D^{\eta_{r-1}})$ such that $x^{-a}\mathfrak{p}$ is not associated to $\mathfrak{a}_{r-1}^*$, i.e., that $\mathfrak{p}$ is not associated to $x^a\mathfrak{a}_{r-1}^*$.

(2) Show that this implies there exists $1 \leq i \leq r-1$ such that $x^a f_i \notin \mathfrak{p}$.

(3) Show that this implies there exists a $\mathbb{Z}$-linear combination f_r of these $x^a f_i$ that does not lie in any $\mathfrak{p}$ associated to $\mathfrak{a}_{r-1}^*$.

(4) Letting $\mathfrak{a}_r = (\mathfrak{a}_{r-1}, f_r)$, show that $\mathfrak{a}_r^* = R$ or $\mathfrak{a}_r^*$ is unmixed of height r.

It is perhaps worth pointing out here that the fourth point above is precisely the reason that associated primes appear in this proof — the key fact is that, if an element f_r does not lie in any prime associated to $\mathfrak{a}_{r-1}^*$, then the height of $\mathfrak{a}_r^* = (\mathfrak{a}_{r-1}, f_r)^*$ goes up by one (or $\mathfrak{a}_r^* = R$). Let us now carry out the four steps above:

(1) Let $\mathfrak{p}$ be associated to $\mathfrak{a}_{r-1}^*$. Then $\mathfrak{p} \subset \mathfrak{M}$, so $\mathfrak{p} \subset z \cdot \mathfrak{m}$ for some $z \in X$, so $z^{-1} \cdot \mathfrak{p} \subset \mathfrak{m}$. By definition, $\operatorname{rank}(\operatorname{Stab}_X(z^{-1} \cdot \mathfrak{p})) \leq m'_{r-1}$, whence $\operatorname{rank}(\operatorname{Stab}_X(\mathfrak{p})) \leq m'_{r-1}$.

Lemma 5.12. *Let T be a positive integer. Let $\mathbb{Z}^m(T)$ denote the set of tuples $(a_1, \ldots, a_m) \in \mathbb{Z}^m$ with $0 \leq a_i \leq T$ for each i. If $H \subset \mathbb{Z}^m$ is a subgroup of rank h, then the image of $\mathbb{Z}^m(T)$ in $\mathbb{Z}^m/H$ has size at least $(T+1)^{m-h}$.*

Before proving the lemma, we first note that it implies that the image of $\mathbb{Z}^m(D^{\eta_{r-1}})$ in $\mathbb{Z}^m/\operatorname{Stab}_X(\mathfrak{p})$ has size at least

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

Now, the number of primes associated to $\mathfrak{a}_{r-1}^*$ is at most its degree $\ell(\mathfrak{a}_{r-1}^*) \leq D^{r-1}$. Therefore, there exists $a \in \mathbb{Z}^m(D^{\eta_{r-1}})$ such that $x^{-a}\mathfrak{p}$ is not an associated prime of $\mathfrak{a}_{r-1}^*$. Equivalently, $\mathfrak{p}$ is not an associated prime of $x^a\mathfrak{a}_{r-1}^*$. This completes the first step.

Proof of Lemma 5.12. Choose $m-h$ elements of the canonical basis of $\mathbb{Z}^m$ that generate a subgroup B such that $H \cap B = \{0\}$. Then the canonical map from $\mathbb{Z}^m$ to $\mathbb{Z}^m/H$ is injective when restricted to B. The result follows since $B \cap \mathbb{Z}^m(T)$ contains exactly $(T+1)^{m-h}$ elements. □

(2) Since $\mathfrak{p}$ and $x^a\mathfrak{a}_{r-1}^*$ are unmixed of the same height $r-1$, but $\mathfrak{p}$ is not associated to $x^a\mathfrak{a}_{r-1}^*$, it follows that $x^a\mathfrak{a}_{r-1}^* \not\subset \mathfrak{p}$. This implies $x^a\mathfrak{a}_{r-1} \not\subset \mathfrak{p}$ since $\mathfrak{p}^* = \mathfrak{p}$. Since

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

this implies there exists $1 \leq i \leq r-1$ such that $x^a f_i \notin \mathfrak{p}$.

(3) The third step follows from a general lemma:

Lemma 5.13. *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be prime ideals of R and let*

$$f_1, \ldots, f_s \in R$$

such that $f_i \notin \mathfrak{p}_i$. Then there exists a $\mathbb{Z}$-linear combination of the f_i that does not lie in any $\mathfrak{p}_i$.

Proof. Induction on s. In the base case $s = 1$, there is nothing to prove. For $s > 1$, suppose that g is a $\mathbb{Z}$-linear combination of $f_1, \ldots, f_{s-1}$ that does not lie in $\mathfrak{p}_1, \ldots, \mathfrak{p}_{s-1}$. If $g \notin \mathfrak{p}_s$, then we can simply take g and we are done. So suppose $g \in \mathfrak{p}_s$.

Consider all linear combinations $f_s + ag$ with $a \in \mathbb{Z}$. For each a, consider the set $S_a \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{s-1}\}$ consisting of the $\mathfrak{p}_i$ such that $f_s + ag \in \mathfrak{p}_i$. There are 2^{s-1} possible subsets S_a. By the pigeonhole principle, if we take $a = 0, \ldots, 2^{s-1}$, then there must exist distinct a and $'$ such that $S_a = S_{a'}$. But, if $f_s + ag$ and $f_s + a'g \in \mathfrak{p}_i$ for $1 \leq i \leq s-1$, then $(a - a')g \in \mathfrak{p}_i$, whence $g \in \mathfrak{p}_i$ (since k has characteristic 0), a contradiction. Therefore, $f_s + ag \notin \mathfrak{p}_i$ for $i \leq s-1$.

Also, $f_s \notin \mathfrak{p}_s$ but $g \in \mathfrak{p}_s$ implies $f_s + ag \notin \mathfrak{p}_s$. Therefore, $f_s + ag$ is the desired linear combination. □

We can now complete step (3): We conclude that there is a $\mathbb{Z}$-linear combination f_r of the $x^a f_i$ (where $1 \leq i \leq r-1$ and $a \in \mathbb{Z}^m(D^{\eta_{r-1}})$) such that f_r does not lie in any associated prime of $\mathfrak{a}^*_{r-1}$.

(4) The fourth step will follow from the following lemma:

Lemma 5.14. *Let $\mathfrak{a} \subset R$ be unmixed of height $r-1$ and suppose $f \in R$ is not contained in any of the primes associated to $\mathfrak{a}$. Let $\mathfrak{b} = \mathfrak{a} + (f)$. Then either $\mathfrak{b} = R$ or $\mathfrak{b}$ has height r. In the latter case, $\ell(\mathfrak{b}) \leq \ell(\mathfrak{a}) \cdot \deg f$.*

Proof. Let $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ be a minimal primary decomposition and let $\mathfrak{p}_i$ be the radical of $\mathfrak{q}_i$. If $\mathfrak{p}_i + (f) = R$ for all i, then, for each i, there exists an element of the form $1 - gf \in \mathfrak{p}_i$, and hence an element of the form $(1-gf)^j \in \mathfrak{q}_i$. The product of these lies in $\mathfrak{a}$. This product is congruent to 1 modulo f, so $1 \in \mathfrak{b} = (\mathfrak{a}, f)$. Therefore, assume that there exists some $\mathfrak{p} = \mathfrak{p}_i$ such that $\mathfrak{p} + (f) \neq R$.

By Krull's principal ideal theorem, the image $\bar{\mathfrak{b}}$ of $\mathfrak{b}$ in $R/\mathfrak{p}$ has height 1. The inverse image of any associated prime of $\bar{\mathfrak{b}} \subset R/\mathfrak{p}$ in R is a prime of height $(r-1)+1 = r$. Therefore, the height of $\mathfrak{b}$ is at most r and, since $\mathfrak{b} \supset \mathfrak{a}$, the height is at least $r-1$.

But, if the height of $\mathfrak{b}$ is $r-1$, then it has some associated prime $\mathfrak{p}'$ of height $r-1$. But $\mathfrak{p}' \supset \mathfrak{b} \supset \mathfrak{a}$. As $\mathfrak{a}$ is unmixed of height $r-1$, this implies that $\mathfrak{p}'$ is an associated prime of $\mathfrak{a}$. But $f \in \mathfrak{p}'$ and we assumed f was not contained in any associated primes of $\mathfrak{a}$. This is a contradiction, so we must have that the height of $\mathfrak{b}$ is r.

To conclude, we note that $(\mathfrak{a} + (f))_0 \supset \mathfrak{a}_0 + (f)_0$; hence,

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

The second-to-last equality requires explanation. Firstly, f_0 is not contained in any of the associated primes of $\mathfrak{a}_0$ since f is not contained in any of the associated primes of $\mathfrak{a}$. This implies that multiplication by f_0 is injective on $R_0/\mathfrak{a}_0$. This multiplication map has degree equal to $\deg(f)$ and cokernel equal to $R_0/(\mathfrak{a}_0 + (f_0))$, whence

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

This yields $\tilde{\ell}\big(R_0/(\mathfrak{a}_0 + (f)_0)\big) = \tilde{\ell}(R_0/\mathfrak{a}_0) \cdot \deg(f)$, as desired. □

We can now complete step (4). We have $\mathfrak{a}_r = \mathfrak{a}_{r-1} + (f_r)$. Let $\mathfrak{b} = \mathfrak{a}_{r-1}^* + (f_r)$. Then $\mathfrak{a}_r^* \supset \mathfrak{b}$, and Lemma 5.14 implies that either $\mathfrak{b} = R$ or $\mathfrak{b}$ has height r and $\ell(\mathfrak{b}) \leq D^{r-1} \cdot D = D^r$.

If $\mathfrak{b} = R$ then of course $\mathfrak{a}_r^* = R$, so assume the latter case holds. Let $\mathfrak{p}$ be an associated prime of $\mathfrak{a}_r^*$. Then $\mathrm{ht}(\mathfrak{p}) \geq \mathrm{ht}(\mathfrak{a}_r^*) \geq r$. We want to show equality. We know $\mathfrak{p} \subset \mathfrak{m}'$, where $\mathfrak{m}' = z\mathfrak{m}$ for some $z \in X(N)$. We can work in the localization $R_{\mathfrak{m}'}$, which is a regular local ring. The ideal $\mathfrak{a}_r R_{\mathfrak{m}'}$ is generated by r elements, so Krull's height theorem implies it has height at most r; hence, it has height exactly r. Therefore it is unmixed of height r and hence the same is true of the associated prime $\mathfrak{p}$.

Finally, $\mathfrak{a}_r^* \supset \mathfrak{b}$ and both are unmixed of height r so $\ell(\mathfrak{a}_r^*) \leq \ell(\mathfrak{b}) \leq D^r$. This completes the proof of step (4), and of Theorem 5.11.

6. The matrix coefficient conjecture

Both the assumption and the conclusion of the Waldschmidt–Masser theorem are quite strong. For instance, in the case of a square matrix of dimension n with entries in $\mathscr{L}$ or $\mathscr{L}_p$, one assumes that the rank of the matrix is less than $\frac{1}{2}n$ and one concludes that, after a rational change of basis on both sides, one can arrange a large block of zeroes, precisely a block of dimension $m' \times n'$, where $m' + n' > n$.

We would like a statement that is more sensitive, and gives a "rational" condition whenever the rank is not full. Such a statement is necessary if one wants to prove Leopoldt's conjecture, rather than the partial result given in Corollary 5.3.

To this end, we have formulated with Mahesh Kakde the following conjecture. The name *matrix coefficient conjecture* is inspired by the theory of automorphic representations, where expressions of the form $w^t M v$ are called matrix coefficients.

Conjecture 6.1 (Dasgupta and Kakde). *Let M be a square matrix of dimension n with entries in $\mathscr{L}$ or $\mathscr{L}_p$. If $\det(M) = 0$, then there exist nonzero vectors $w, v \in \mathbb{Q}^n$ such that $w^t M v = 0$.*

Despite its simplicity, Conjecture 6.1 remains quite deep: in the case $n = 2$, it is easily seen to be equivalent to the four exponentials conjecture. We have proven the following about the matrix coefficient conjecture:

- Conjecture 6.1 is implied by the structural rank conjecture.
- The version of Conjecture 6.1 over $\mathscr{L}_p$ implies both Leopoldt's conjecture and the Gross–Kuz'min conjecture.

We have also developed a strategy to study Conjecture 6.1 using auxiliary polynomials, but unfortunately the construction of the necessary polynomials remains a mystery. Our hope is that Conjecture 6.1 may be more tractable than the structural

rank conjecture. We will prove the results stated above and explore Conjecture 6.1 further in forthcoming work.

Acknowledgements

I would like to extend a great thanks to Damien Roy, who provided a detailed reading of an earlier draft of this paper and made many helpful suggestions that greatly improved the exposition. I would also like to thank Mahesh Kakde, my collaborator with whom I learned this material, as well as Michel Waldschmidt for helpful discussions. We are very grateful to Adam Harper [2010], whose exposition we follow for Baker's theorem, and to Eric Stansifer [2012], whose exposition was very influential for our discussion of the Waldschmidt–Masser theorem. Finally, we thank the referees for very helpful comments.

This note arose out of a topics course that I taught online at Duke University during Spring 2020, and I thank those attending the course for lively discussions.

References

[Alaoglu and Erdős 1944] L. Alaoglu and P. Erdős, "On highly composite and similar numbers", *Trans. Amer. Math. Soc.* **56** (1944), 448–469. MR Zbl

[Ax 1971] J. Ax, "On Schanuel's conjectures", *Ann. of Math.* (2) **93** (1971), 252–268. MR Zbl

[Baker 1966] A. Baker, "Linear forms in the logarithms of algebraic numbers", *Mathematika* **13** (1966), 204–216. MR Zbl

[Baker 1967a] A. Baker, "Linear forms in the logarithms of algebraic numbers, II", *Mathematika* **13** (1967), 102–107. MR Zbl

[Baker 1967b] A. Baker, "Linear forms in the logarithms of algebraic numbers, III", *Mathematika* **13** (1967), 220–228. MR Zbl

[Brumer 1967] A. Brumer, "On the units of algebraic number fields", *Mathematika* **14** (1967), 121–124. MR Zbl

[Charollois and Dasgupta 2014] P. Charollois and S. Dasgupta, "Integral Eisenstein cocycles on $\mathbf{GL}_n$, I: Sczech's cocycle and p-adic L-functions of totally real fields", *Camb. J. Math.* **2**:1 (2014), 49–90. MR Zbl

[Cherry 2009] W. Cherry, "Lectures on non-Archimedean function theory", lecture notes, *Advanced school on p-adic analysis and applications*, Abdus Salam International Centre for Theoretical Physics, 2009. arXiv 0909.4509

[Colmez 1988] P. Colmez, "Résidu en $s = 1$ des fonctions zêta p-adiques", *Invent. Math.* **91**:2 (1988), 371–389. MR Zbl

[Dasgupta et al. 2011] S. Dasgupta, H. Darmon, and R. Pollack, "Hilbert modular forms and the Gross–Stark conjecture", *Ann. of Math.* (2) **174**:1 (2011), 439–484. MR Zbl

[Dasgupta et al. 2018] S. Dasgupta, M. Kakde, and K. Ventullo, "On the Gross–Stark conjecture", *Ann. of Math.* (2) **188**:3 (2018), 833–870. MR Zbl

[Federer and Gross 1981] L. J. Federer and B. H. Gross, "Regulators and Iwasawa modules", *Invent. Math.* **62**:3 (1981), 443–457. MR Zbl

[Gross 1981] B. H. Gross, "p-adic L-series at $s = 0$", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28**:3 (1981), 979–994. MR Zbl

[Harper 2010] A. Harper, "A version of Baker's theorem on linear forms in logarithms", preprint, 2010, available at https://warwick.ac.uk/fac/sci/maths/people/staff/harper/bakernotes.pdf.

[Lang 1966] S. Lang, *Introduction to transcendental numbers*, Addison-Wesley, Reading, MA, 1966. MR Zbl

[Laurent 1991] M. Laurent, "Sur quelques résultats récents de transcendance", pp. 209–230 in *Journées arithmétiques* (Luminy, 1989), edited by G. Lachaud, Astérisque **198–200**, Soc. Math. France, Paris, 1991. MR Zbl

[Masser 1981] D. W. Masser, "On polynomials and exponential polynomials in several complex variables", *Invent. Math.* **63**:1 (1981), 81–95. MR Zbl

[Neukirch 1999] J. Neukirch, *Algebraic number theory*, Grundl. Math. Wissen. **322**, Springer, 1999. MR Zbl

[Ramachandra 1968a] K. Ramachandra, "Contributions to the theory of transcendental numbers, I", *Acta Arith.* **14** (1968), 65–72. MR Zbl

[Ramachandra 1968b] K. Ramachandra, "Contributions to the theory of transcendental numbers, II", *Acta Arith.* **14** (1968), 73–88. MR Zbl

[Roy 1995] D. Roy, "Points whose coordinates are logarithms of algebraic numbers on algebraic varieties", *Acta Math.* **175**:1 (1995), 49–73. MR Zbl

[Schneider 1957] T. Schneider, *Einführung in die transzendenten Zahlen*, Springer, 1957. MR Zbl

[Siegel 1929] C. L. Siegel, "Über einige Anwendungen diophantischer Approximationen", *Abh. Preuß. Akad. Wisse.. Phys.-Math. Kl.* **1** (1929), 1–70. Reprinted as pp. 81–138 in *On some applications of Diophantine approximations*, edited by U. Zannier, Quad./Monogr. **2**, Ed. Norm., Pisa, 2014. MR Zbl

[Spiess 2014] M. Spiess, "Shintani cocycles and the order of vanishing of p-adic Hecke L-series at $s = 0$", *Math. Ann.* **359**:1-2 (2014), 239–265. MR Zbl

[Stansifer 2012] E. Stansifer, *Leopoldt's conjecture for abelian and non-abelian cases*, Master's thesis, ALGANT Erasmus Mundus, Universitá degli Studi di Milano, 2012, available at https://algant.eu/documents/theses/stansifer.pdf.

[Valiant 1979] L. G. Valiant, "Completeness classes in algebra", pp. 249–261 in *Conference record of the eleventh annual ACM symposium on theory of computing* (Atlanta, GA, 1979), edited by M. J. Fischer et al., ACM, New York, 1979. MR

[Waldschmidt 1981] M. Waldschmidt, "Transcendance et exponentielles en plusieurs variables", *Invent. Math.* **63**:1 (1981), 97–127. MR Zbl

[Waldschmidt 1992] M. Waldschmidt, *Linear independence of logarithms of algebraic numbers*, IMS Report **116**, Institute of Mathematical Sciences, Madras, 1992. MR Zbl

[Waldschmidt 2023] M. Waldschmidt, "The four exponentials problem and Schanuel's conjecture", pp. 579–592 in *Mathematics going forward*: *collected mathematical brushstrokes*, edited by J.-M. Morel and B. Teissier, Lecture Notes in Math. **2313**, Springer, 2023. MR Zbl

[Wiles 1990] A. Wiles, "The Iwasawa conjecture for totally real fields", *Ann. of Math.* (2) **131**:3 (1990), 493–540. MR Zbl

Received 2 Mar 2023. Revised 12 Dec 2023.

SAMIT DASGUPTA:

dasgupta@math.duke.edu

Department of Mathematics, Duke University, Durham, NC, United States

ESSENTIAL NUMBER THEORY

msp.org/ent

See inside back cover or msp.org/ent for submission instructions.

Essential Number Theory (ISSN 2834-4634 electronic, 2834-4626 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ENT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

https://msp.org/

ESSENTIAL NUMBER THEORY

2023 vol. 2 no. 1

On the Northcott property for infinite extensions 1
MARTIN WIDMER

The Kelley–Meka bounds for sets free of three-term arithmetic progressions 15
THOMAS F. BLOOM and OLOF SISASK

On gamma factors for representations of finite general linear groups 45
DAVID SOUDRY and ELAD ZELINGHER

Sur la conjecture de Tate pour les diviseurs 83
BRUNO KAHN

Ranks of matrices of logarithms of algebraic numbers, I: The theorems of Baker and Waldschmidt–Masser 93
SAMIT DASGUPTA