Keynote address November 2, 2018

The 11th International Conference on Mathematics and Mathematics Education in Developing Countries

The unity of mathematics : Examples from transcendental number theory

Michel Waldschmidt

Professeur Émérite, Sorbonne Université,
Institut de Mathématiques de Jussieu, Paris

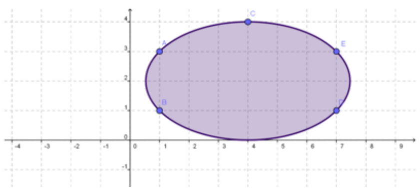
http://www.imj-prg.fr/~michel.waldschmidt/

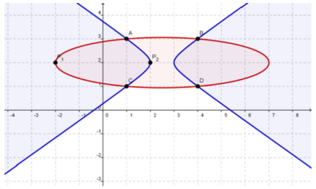
Abstract

Many different topics from mathematics are related with transcendental number theory, including Diophantine Approximation, Dynamical Systems, Algebraic Theory of Numbers, Geometry, Diophantine Geometry, Geometry of Numbers, Complex Analysis (one or several variables), Commutative Algebra, Arithmetic Complexity of Polynomials, Topology, Logic : model theory.

We select some of them to illustrate the Unity of Mathematics, namely
Geometry, Complex Analysis, Projective geometry, Commutative Algebra, Topology, Arithmetic Complexity of Polynomials.

Five points in the plane lie on a conic





Equation of a conic :

$$a_0 + a_1x + a_2y + a_3x^2 + a_4xy + a_5y^2 = 0.$$

Six coefficients, five linear homogeneous equations in the six variables : there is a non trivial solution.

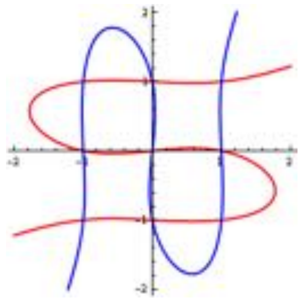
https://home.adelphi.edu/~stemkoski/EulerCramer/article06.html
Five Points Determine a Conic Section,
Wolfram interactive demonstration
http://demonstrations.wolfram.com/FivePointsDetermineAConicSection/

Nine points lie on a cubic

Equation of a cubic :

$$a_0+a_1x+a_2y+a_3x^2+a_4xy+a_5y^2+a_6x^3+a_7x^2y+a_8xy^2+a_9y^3 = 0.$$

Ten coefficients, nine linear homogeneous equations in the ten variables : there is a non trivial solution.
(May not be unique : two cubics intersect in 9 points).



Three points lie on a cubic with multiplicity ≥ 2

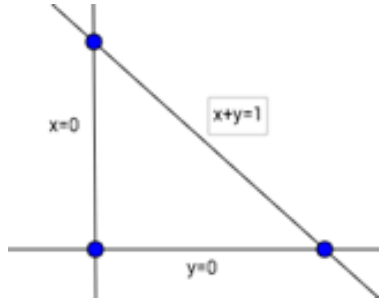
Multiplicity ≥ 2 :

$$f(x,y) = \frac{\partial}{\partial x} f(x,y) = \frac{\partial}{\partial y} f(x,y) = 0.$$

For the existence of a cubic polynomial having multiplicity ≥ 2 at three given points in the plane, we get nine linear homogeneous equations in the ten variables ; hence there is a non trivial solution.

Explicit solution : Three lines repeated twice !

Three points on a cubic with multiplicity 2



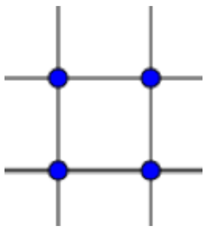
$S = \{(0,0),(0,1),(1,0)\}$
$xy(x+y-1) = 0$

$$f(x,y) = xy(x+y-1) = x^2y + xy^2 - xy,$$

$$\frac{\partial}{\partial x} f(x,y) = y(2x+y-1), \quad \frac{\partial}{\partial y} f(x,y) = x(x+2y-1).$$

Four points on a quartic with multiplicity 2

Four points in the plane lie on a quartic with multiplicity 2.



$\{(0,0),(0,1),(1,0),(1,1)\}$
$xy(x-1)(y-1) = 0$

$$f(x,y) = xy(x-1)(y-1),$$
$$\frac{\partial}{\partial x} f(x,y) = y(y-1)(2x-1),$$
$$\frac{\partial}{\partial y} f(x,y) = x(x-1)(2y-1).$$

Singularities of hypersurfaces

Zeroes of a polynomial : hypersurface.

Zero of a polynomial with multiplicity : singularity of the hypersurface.

Let n and t be two positive integers and S a finite subset of $\mathbb{C}^n$. Denote by $\omega_t(S)$ the least degree of a nonzero polynomial in n variables vanishing on S with multiplicity at least t.

One variable

In case $n = 1$, given a finite subset S of $\mathbb{C}$ and a positive integer t, the unique monic polynomial in $\mathbb{C}[z]$ of least degree vanishing at each point of S with multiplicity $\geq t$ is

$$\prod_{s \in S} (z - s)^t.$$

It has degree $t|S|$; hence, when $n = 1$,

$$\omega_t(S) = t|S|.$$

Cartesian products

More generally, for a Cartesian product $S = S_1 \times \cdots \times S_n$ in $\mathbb{C}^n$,

$$\omega_t(S) = t \min_{1 \leq i \leq n} |S_i|.$$

Proof by induction.
Fix $(s_1, \ldots, s_{n-1}) \in S_1 \times \cdots \times S_{n-1}$,
consider $f(s_1, \ldots, s_{n-1}, X) \in \mathbb{C}[X]$. $\square$

$n = 2$

Consider a finite subset S of $\mathbb{C}^2$. If S is contained in a line, then $\omega_t(S) = t$ for all t ; hence in this case $\omega_t(S)$ does not depend on $|S|$.

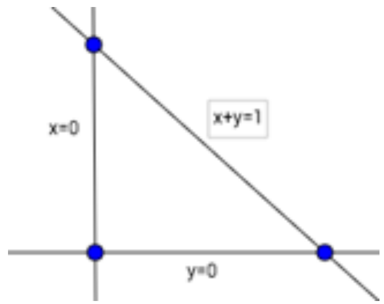
The simplest example of a set which is not contained in a line is given by three points like

$$S = \{(0,0),\ (0,1),\ (1,0)\}.$$

The polynomial $z_1 z_2$ vanishes on S, it has degree 2, hence $\omega_1(S) = 2$.
There is no polynomial of degree 2 having a zero at each point of S with multiplicity 2, but there is one of degree 3, namely

$$z_1 z_2 (z_1 + z_2 - 1).$$

$S \subset \mathbb{C}^2$ with $|S| = 3$



$$S = \{(0,0), (0,1), (1,0)\}$$

$$P_1(z_1, z_2) = z_1 z_2$$

$$P_2(z_1, z_2) = z_1 z_2 (z_1 + z_2 - 1)$$

$$\omega_1(S) = 2, \quad \omega_2(S) = 3.$$

With

$$P_{2m-1} = z_1^m z_2^m (z_1 + z_2 - 1)^{m-1},\ P_{2m} = z_1^m z_2^m (z_1 + z_2 - 1)^m,$$

we deduce

$$\omega_{2m-1}(S) = 3m - 1, \quad \omega_{2m}(S) = 3m.$$

Linear homogeneous equations : $n = 2$, $t = 1$

A polynomial in 2 variables of degree D has

$$\frac{(D+1)(D+2)}{2}$$

coefficients. Hence for $S \subset \mathbb{C}^2$ with $2|S| < (D+1)(D+2)$, we have $\omega_1(S) \leq D$.

For $|S| = 1, 2$ we have $\omega_1(S) = 1$ (two points on a line),
for $|S| = 3, 4, 5$ we have $\omega_1(S) \leq 2$ (five points on a conic),
for $|S| = 6, 7, 8, 9$ we have $\omega_1(S) \leq 3$ (nine points on a cubic).

For $S \subset \mathbb{C}^2$,

$$\omega_1(S) \leq 2|S|^{1/2}.$$

Linear homogeneous equations : $t = 1$

A polynomial in n variables of degree D has

$$\binom{D+n}{n}$$

coefficients. Hence for $S \subset \mathbb{C}^n$, if

$$|S| < \binom{D+n}{n},$$

then

$$\omega_1(S) \leq D.$$

In particular, for $S \subset \mathbb{C}^n$,

$$\omega_1(S) \leq n|S|^{1/n}.$$

Linear homogeneous equations

The number of n–tuples $(\tau_1, \ldots, \tau_n)$ of non negative integers with $\tau_1 + \cdots + \tau_n < t$ is

$$\binom{t+n-1}{n}.$$

Hence the conditions

$$\left(\frac{\partial}{\partial z_1}\right)^{\tau_1} \cdots \left(\frac{\partial}{\partial z_n}\right)^{\tau_n} P(s) = 0$$

for $s \in S$ and $\tau_1 + \cdots + \tau_n < t$ amount to $\binom{t+n-1}{n}|S|$ linear conditions in the $\binom{D+n}{n}$ coefficients of P.

Upper bound for $\omega_t(S)$

Given a finite subset S of $\mathbb{C}^n$ and a positive integer t, if D is a positive integer such that

$$|S|\binom{t+n-1}{n} < \binom{D+n}{n},$$

then

$$\omega_t(S) \leq D.$$

Consequence :

$$\omega_t(S) \leq (t+n-1)|S|^{1/n}.$$

Subadditivity of $\omega_t(S)$

$$\omega_{t_1+t_2}(S) \le \omega_{t_1}(S) + \omega_{t_2}(S).$$

Proof : if P_1 has degree $\omega_{t_1}(S)$ and vanishes on S with multiplicity $\ge t_1$, if P_2 has degree $\omega_{t_2}(S)$ and vanishes on S with multiplicity $\ge t_2$, then the product P_1P_2 has degree $\omega_{t_1}(S) + \omega_{t_2}(S)$ and vanishes on S with multiplicity $\ge t_1 + t_2$.

Therefore $\omega_t(S) \le t\omega_1(S)$, and consequently $\limsup_{t\to\infty} \omega_t(S)/t$ exists and is $\le \omega_t(S)/t$ for all $t \ge 1$.

An asymptotic invariant

Theorem. *The sequence*

$$\left(\frac{1}{t}\omega_t(S)\right)_{t\ge 1}$$

has a limit $\Omega(S)$ *as* $t \to \infty$, *and*

$$\frac{1}{n}\omega_1(S) - 2 \le \Omega(S) \le \omega_1(S).$$

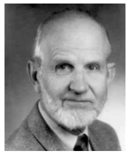
Further, for all $t \ge 1$ *we have*

$$\Omega(S) \le \frac{\omega_t(S)}{t}.$$

Remark : $\Omega(S) \le |S|^{1/n}$ by the above upper bound $\omega_t(S) \le (t+n-1)|S|^{1/n}$.

M.W. *Propriétés arithmétiques de fonctions de plusieurs variables* (II). Sém. P. Lelong (Analyse), 16è année, 1975/76 ; Lecture Notes in Math., **578** (1977), 274–292.

L^2 – estimates of Hörmander – Bombieri



Lars Hörmander

1931 – 2012

Enrico Bombieri

Existence theorems for the $\overline{\partial}$ operator.
Let φ *be a plurisubharmonic function in* $\mathbb{C}^n$ *and* $\mathbf{z}_0 \in \mathbb{C}^n$ *be such that* $e^{-\varphi}$ *is integrable near* $\mathbf{z}_0$. *Then there exists a nonzero entire function* F *such that*

$$\int_{\mathbb{C}^n} |F(\mathbf{z})|^2 e^{-\varphi(\mathbf{z})}(1+|\mathbf{z}|^2)^{-3n} \mathrm{d}\lambda(\mathbf{z}) < \infty.$$

http://www-history.mcs.st-andrews.ac.uk/history/Mathematicians/Hormander.html

Improvement of L^2 estimate by Henri Skoda

Let φ *be a plurisubharmonic function in* $\mathbb{C}^n$ *and* $\mathbf{z}_0 \in \mathbb{C}^n$ *be such that* $e^{-\varphi}$ *is integrable near* $\mathbf{z}_0$. *For any* $\epsilon > 0$ *there exists a nonzero entire function* F *such that*

$$\int_{\mathbb{C}^n} |F(\mathbf{z})|^2 e^{-\varphi(\mathbf{z})}(1+|\mathbf{z}|^2)^{-n-\epsilon} \mathrm{d}\lambda(\mathbf{z}) < \infty.$$

Corollary :

$$\frac{1}{n}\omega_1(S) \le \Omega(S) \le \omega_1(S).$$

H. Skoda. *Estimations L^2 pour l'opérateur $\overline{\partial}$ et applications arithmétiques.* Springer Lecture Notes in Math., **578** (1977), 314–323.

https://en.wikipedia.org/wiki/Henri_Skoda

Comparing $\omega_{t_1}(S)$ and $\omega_{t_2}(S)$

`Idea:` Let P be a polynomial of degree $\omega_{t_1}(S)$ vanishing on S with multiplicity $\geq t_1$. If the function P^{t_2/t_1} were an entire function, it would be a polynomial of degree $\frac{t_2}{t_1}\omega_{t_1}(S)$ vanishing on S with multiplicity $\geq t_2$, which would yield $\omega_{t_2}(S) \leq \frac{t_2}{t_1}\omega_{t_1}(S)$.

P^{t_2/t_1} is usually not an entire function but $\varphi = \frac{t_2}{t_1}\log P$ is a plurisubharmonic function. By the L^2–estimates of Hörmander – Bombieri – Skoda, e^{φ} is well approximated by a nonzero entire function. This function is a polynomial vanishing on S with multiplicity $\geq t_2$, of degree $\leq \frac{t_2+n-1}{t_1}\omega_{t_1}(S)$.

Hence
$$\omega_{t_2}(S) \leq \frac{t_2+n-1}{t_1}\omega_{t_1}(S).$$

The asymptotic invariant $\Omega(S)$

From
$$\omega_{t_2}(S) \leq \frac{t_2+n-1}{t_1}\omega_{t_1}(S),$$
one deduces :

Theorem. *For all* $t \geq 1$,
$$\frac{\omega_t(S)}{t+n-1} \leq \Omega(S) \leq \frac{\omega_t(S)}{t}.$$

M.W. *Nombres transcendants et groupes algébriques.* Astérisque, **69–70** . Société Mathématique de France, Paris, 1979.

$|S| = 1$ or 2 in $\mathbb{C}^2$

$|S| = 1 : S = \{(0,0)\}$, $P_t(X,Y) = X^t$,
$\omega_t(S) = t$, $\Omega(S) = 1$.

$|S| = 2 : S = \{(0,0),(1,0)\}$, $P_t(X,Y) = Y^t$,
$\omega_t(S) = t$, $\Omega(S) = 1$.

Generic subset in $\mathbb{C}^n$

Given two positive integers n and N, a subset S of $\mathbb{C}^n$ with N elements is generic if, for any $t \geq 1$,
$$\omega_t(S) \geq \omega_t(S')$$
for all subsets S' of $\mathbb{C}^n$ with N elements.

Almost all subsets of $\mathbb{C}^n$ (for Lebesgue's measure) are generic. The points $(s_{ij})_{1\leq i\leq n,\, 1\leq j\leq N}$ in $\mathbb{C}^{nN}$ associated to the coordinates $(s_{ij})_{1\leq i\leq n}$, $1 \leq j \leq N$, of the points $\mathbf{s}_j$ of the non–generic sets, belong to the union of countably many hypersurfaces of $\mathbb{C}^{nN}$.

Generic S with $|S| = 3$ in $\mathbb{C}^2$

Given a set S of 3 points in $\mathbb{C}^2$, not on a straight line, we have

$$\omega_t(S) = \begin{cases} \dfrac{3t+1}{2} & \text{for } t \text{ odd,} \\ \dfrac{3t}{2} & \text{for } t \text{ even,} \end{cases}$$

hence

$$\Omega(S) = \lim_{t\to\infty} \frac{\omega_t(S)}{t} = \frac{3}{2}.$$

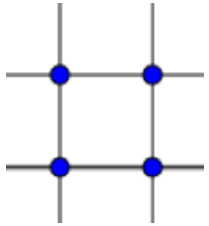
Since $\omega_1(S) = 2$ and $n = 2$, this is an example with

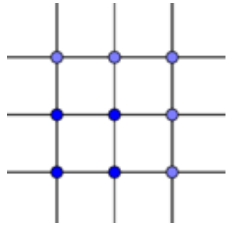
$$\frac{\omega_1(S)}{n} < \Omega(S) < \omega_1(S).$$

Generic $S \subset \mathbb{C}^2$ with $|S| = 4$

For a generic S in $\mathbb{C}^2$ with $|S| = 4$, we have $\omega_t(S) = 2t$, hence $\Omega(S) = \omega_1(S) = 2$.

Easy for a Cartesian product $S_1 \times S_2$ with $|S_1| = |S_2| = 2$, also true for a generic S with $|S| = 4$.





More generally, when S is a Cartesian product $S_1 \times S_2$ with $|S_1| = |S_2| = m$, we have $\omega_t(S) = mt$ and $\Omega(S) = m = \sqrt{|S|}$. The inequality $\Omega(S) \geq \sqrt{|S|}$ for a generic S with $|S|$ a square follows (Chudnovsky).

Generic $S \subset \mathbb{C}^2$ with $|S| = 5$

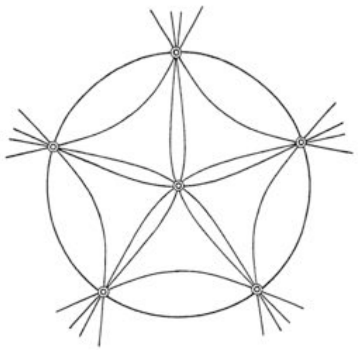
Five points in $\mathbb{C}^2$ lie on a conic.

For a generic S with $|S| = 5$ we have $\omega_t(S) = 2t$ and $\Omega(S) = \omega_1(S) = 2$.

Geogebra

https://www.geogebra.org/

Generic $S \subset \mathbb{C}^2$ with $|S| = 6$ (Nagata)



$\omega_1(S) = 3$, $\Omega(S) = 12/5$.

Given 6 generic points $s_1, \dots, s_6$ in $\mathbb{C}^2$, consider 6 conics $C_1, \dots, C_6$ where S_i passes through the 5 points s_j for $j \neq i$. This produces a polynomial of degree 12 with multiplicity ≥ 5 at each s_i. Hence $\omega_5(S) \leq 12$.

For S generic with 6 points, $\omega_{5t}(S) = 12t$, $\Omega(S) = 12/5$.

Generic $S \subset \mathbb{C}^2$ with $|S| = 7$ (Nagata)

Given 7 points in $\mathbb{C}^2$, there is a cubic passing through these 7 points with a double point at one of them.

Number of coefficients of a cubic polynomial : 10.

Number of conditions : 6 for the simple zeros, 3 for the double zero.

We get 7 cubic polynomials, their product has degree $7 \times 3 = 21$ and has the 7 assigned zeroes with multiplicities 8.

For S generic with 7 points, $\omega_{8t}(S) = 21t$, $\Omega(S) = 21/8$.

$$\omega_1(S) = 3, \quad \Omega(S) = \frac{21}{8}.$$

Generic $S \subset \mathbb{C}^2$ with $|S| = 8$ (Nagata)

Given 8 points in $\mathbb{C}^2$, there is a sextic with a double point at 7 of them and a triple point at 1 of them.

Number of coefficients of a sextic polynomial : $(6+1)(6+2)/2 = 28$.

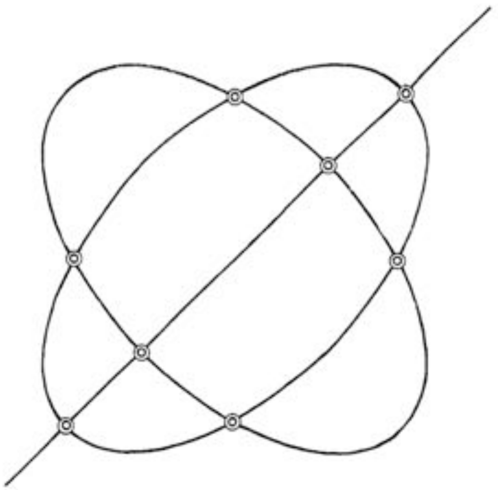
Number of conditions : $3 \times 7 = 21$ for the double zeros, 6 for the triple zero.

This gives a polynomial of degree $8 \times 6 = 48$ with the 8 assigned zeroes of multiplicities $2 \times 7 + 3 = 17$.

For S generic with 8 points, $\omega_{17t}(S) = 48t$, $\Omega(S) = 47/17$.

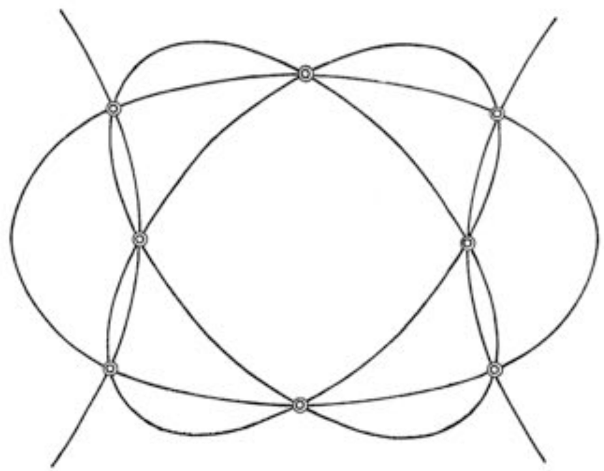
$n = 2$, $|S| = 8$, $t = 2$, $\omega_t = 5$, $\Omega = 5/2$

Not generic



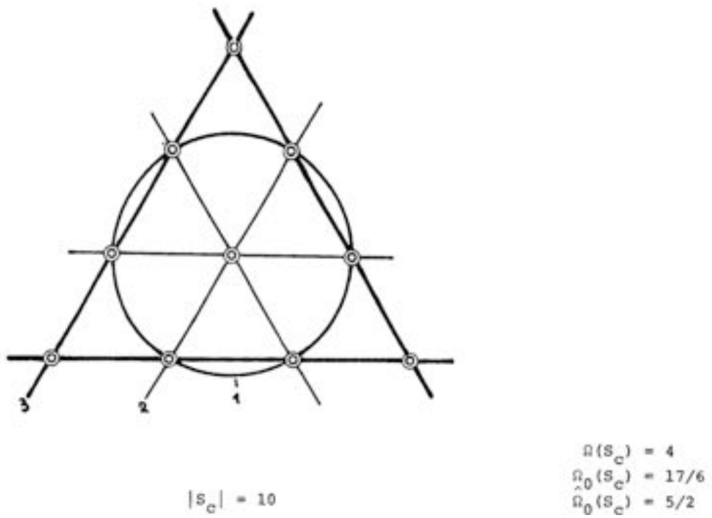
$n = 2$, $|S| = 8$, $t = 3$, $\omega_t = 8$, $\Omega = 8/3$

Not generic



$n = 2$, $|S| = 10$, $t = 6$, $\omega_t = 17$, $\Omega = 17/6$

Three sides : multiplicity 3.
Three concurrent lines : multiplicity 2.



$|S| \leq 9$ in $\mathbb{C}^2$

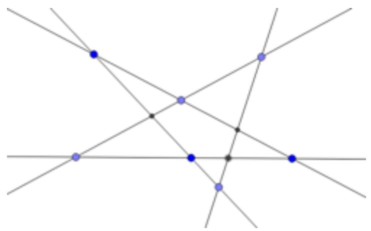
Nagata : generic S in $\mathbb{C}^2$ with $|S| \leq 9$ have $\dfrac{\omega_t(S)}{t} \leq \sqrt{|S|}$.

$\lvert S\rvert$	$=$	1	2	3	4	5	6	7	8	9
$\omega_1(S)$	$=$	1	1	2	2	2	3	3	3	3
t	$=$	1	1	2	1	1	$\mathbf{5}$	$\mathbf{8}$	$\mathbf{17}$	1
$\omega_t(S)$	$=$	1	1	3	2	2	$\mathbf{12}$	$\mathbf{21}$	$\mathbf{48}$	3
$\dfrac{\omega_t(S)}{t}$	$=$	1	1	$\dfrac{3}{2}$	2	2	$\dfrac{\mathbf{12}}{\mathbf{5}}$	$\dfrac{\mathbf{21}}{\mathbf{8}}$	$\dfrac{\mathbf{48}}{\mathbf{17}}$	3
$\sqrt{\lvert S\rvert}$	$=$	1	$\sqrt{2}$	$\sqrt{3}$	2	$\sqrt{5}$	$\sqrt{6}$	$\sqrt{7}$	$\sqrt{8}$	3

Complete intersections of hyperplanes

Let $H_1, \ldots, H_N$ be N hyperplanes in general position in $\mathbb{C}^n$ with $N \geq n$ and S the set of $\binom{N}{n}$ intersection points of any n of them. Then,

$$\omega_{nt}(S) = Nt \text{ for } t \geq 1 \text{ and } \Omega(S) = \frac{N}{n}\cdot$$



$n = 2$, $N = 5$, $|S| = 10$.

Hilbert's 14th problem

David Hilbert
1862 – 1943

Let k be a field and K a subfield of $k(X_1, \ldots, X_n)$ containing k. Is the k–algebra

$$K \cap k[X_1, \ldots, X_n]$$

finitely generated ?

Oscar Zariski (1954) : true for $n = 1$ and $n = 2$.
Counterexample by Masayoshi Nagata in 1959.

http://www-history.mcs.st-andrews.ac.uk/history/Mathematicians/Hilbert.html

http://www.clarku.edu/~djoyce/hilbert/

Hilbert's 14th problem : restricted case

Masayoshi Nagata
1927 – 2008

Original 14th problem :
Let G be a subgroup of the full linear group of the polynomial ring in indeterminate $X_1, \dots, X_n$ over a field k, and let $\mathfrak{o}$ be the set of elements of $k[X_1, \dots, X_n]$ which are invariant under G. Is $\mathfrak{o}$ finitely generated ?

M. Nagata. *On the 14-th Problem of Hilbert*. Amer. J. Math **81** (1959), 766–772.
http://www.jstor.org/stable/2372927

Fundamental Lemma of Nagata

Given 16 independent generic points of the projective plane over a prime field and a positive integer t, there is no curve of degree $4t$ which goes through each p_i with multiplicity at least t.

In other words for $|S| = 16$ generic in $\mathbb{C}^2$, we have $\omega_t(S) > 4t$.

M. Nagata. *On the fourteenth problem of Hilbert.* Proc. Internat. Congress Math. 1958, Cambridge University Press, pp. 459–462.
http://www.mathunion.org/ICM/ICM1958/Main/icm1958.0459.0462.ocr.pdf

Nagata' contribution

Masayoshi Nagata
1927 – 2008

Proposition. *Let $p_1, \dots, p_r$ be independent generic points of the projective plane over the prime field. Let C be a curve of degree d passing through the p_i's with multiplicities $\geq m_i$. Then*

$$m_1 + \cdots + m_r < d\sqrt{r}$$

for $r = s^2$, $s \geq 4$.

It is not known if $r > 9$, is sufficient to ensure the inequality of the Proposition.

M. Nagata. *Lectures on the fourteenth problem of Hilbert.* Tata Institute of Fundamental Research Lectures on Mathematics **31**, (1965), Bombay.
http://www.math.tifr.res.in/~publ/ln/tifr31.pdf

Reformulation of Nagata's Conjecture

By considering $\sum_\sigma C_\sigma$ where σ runs over the cyclic permutations of $\{1, \dots, r\}$, it is sufficient to consider the case $m_1 = \cdots = m_r$.

Conjecture. *Let S be a finite generic subset of the projective plane over the prime field with $|S| \geq 10$. Then*

$$\omega_t(S) > t\sqrt{|S|}.$$

Nagata :

- True for $|S|$ a square.
- False for $|S| \leq 9$.
- Unknown otherwise ($|S| \geq 10$ not a square).

Schwarz Lemma in one variable

Hermann Amandus Schwarz
1843 – 1921

Let f be an analytic function in a disc $|z| \leq R$ of $\mathbb{C}$, with at least M zeroes (counting multiplicities) in a disc $|z| \leq r$ with $r < R$. Then

$$|f|_r \leq \left(\frac{3r}{R}\right)^M |f|_R.$$

We use the notation

$$|f|_r = \sup_{|z|=r} |f(z)|.$$

When $R > 3r$, this improves the maximum modulus bound $|f|_r \leq |f|_R$.

http://www-history.mcs.st-andrews.ac.uk/history/Mathematicians/Schwarz.html

Schwarz Lemma in one variable : proof

Let $a_1, \ldots, a_M$ be zeroes of f in the disc $|z| \leq r$, counted with multiplicities. The function

$$g(z) = f(z) \prod_{j=1}^{M} (z - a_j)^{-1}$$

is analytic in the disc $|z| \leq R$. Using the maximum modulus principle, from $r \leq R$ we deduce $|g|_r \leq |g|_R$. Now we have

$$|f|_r \leq (2r)^M |g|_r \quad \text{and} \quad |g|_R \leq (R - r)^{-M} |f|_R.$$

Finally, assuming (wlog) $R > 3r$,

$$\frac{2r}{R - r} \leq \frac{3r}{R}.$$

$\square$

Schwarz lemma in several variables

Let S be a finite set of $\mathbb{C}^n$ and t a positive integer. There exists a real number r such that for $R > r$, if f is an analytic function in the ball $|z| \leq R$ of $\mathbb{C}^n$ which vanishes with multiplicity at least t at each point of S, then

$$|f|_r \leq \left(\frac{e^n r}{R}\right)^{\omega_t(S)} |f|_R.$$

This is a refined asymptotic version due to Jean-Charles Moreau.

The exponent $\omega_t(S)$ cannot be improved : take for f a non–zero polynomial of degree $\omega_t(S)$, $r > 0$ fixed and $R \to \infty$.

Works in 1980 – 1990

Gregory Chudnovsky

Hélène Esnault

Eckardt Viehweg
1948 – 2010

J-P. Demailly

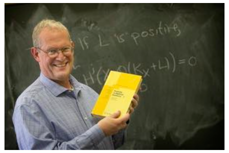
Abdelhak Azhari

André Hirschowitz

Methods of projective geometry, commutative algebra, complex analysis (Poisson–Jensen formula).

Works in 2001 – 2002


Lawrence Ein


Robert Lazarsfeld


Karen E. Smith

Ein, Lazarfeld and Smith use multiplier ideals.


Melvin Hochster


Craig Huneke

Hochster and Huneke use Frobenius powers and tight closure.

Works in 2010 –


Cristiano Bocci


Brian Harbourne


Marcin Dumnici


Thomas Bauer


SzembergThomasz


Giuliana Fatabbi

Mathematisches Forschungsinstitut Oberwolfach

October 2010 : Linear series on algebraic varieties.
February 2015 : Ideals of Linear Subspaces, Their Symbolic Powers and Waring Problem.

Cristiano Bocci, Susan Cooper, Elena Guardo, Brian Harbourne, Mike Janssen, Uwe Nagel, Alexandra Seceleanu, Adam Van Tuyl, Thanh Vu.
The Waldschmidt constant for squarefree monomial ideals.
J. Algebraic Combinatorics (2016) **44** 875–904.

Connection with transcendental number theory

Transcendence in several variables :


Theodor Schneider
1911 – 1988

Let a, b be rational numbers, not integers. Then the number

$$\mathrm{B}(a,b)=\frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$$

is transcendental.

The proof uses abelian functions and Schwarz Lemma for Cartesian products.

Schneider–Lang Theorem

One variable, or several variables for Cartesian products :

Theodor Schneider

1911 – 1988

Serge Lang

1927 – 2005

Several variables, algebraic hypersurfaces (Nagata's conjecture) :

Enrico Bombieri

Gel'fond–Schneider Theorem (special case)

Corollary of the Schneider – Lang Theorem :

$$\frac{\log 2}{\log 3} \text{ is transcendental.}$$

A.O. Gel'fond

1906 – 1968

Th. Schneider

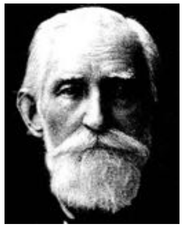
1911 – 1988

Topology

Let x be a real number. The subgroup

$$\mathbb{Z} + \mathbb{Z}x = \{a + bx \mid (a,b) \in \mathbb{Z}^2\}$$

of $\mathbb{R}$ is dense if and only if x is irrational.



Pafnouty Tchebychev

1821-1894

https://en.wikipedia.org/wiki/Pafnuty_Chebyshev
https://www.britannica.com/biography/Pafnuty-Lvovich-Chebyshev
http://www-history.mcs.st-andrews.ac.uk/Biographies/Chebyshev.ht

Multiplicative version

Given two positive real numbers α_1 and α_2, the subgroup

$$\{\alpha_1^{a_1}\alpha_2^{a_2} \mid (a_1,a_2) \in \mathbb{Z}^2\}$$

of the multiplicative group $\mathbb{R}_+^\times$ is dense if and only if α and β are multiplicatively independent : for $(a_1,a_2) \in \mathbb{Z}^2$,

$$\alpha_1^{a_1}\alpha_2^{a_2} = 1 \iff (a_1,a_2) = (0,0).$$

Proof : use $\exp : \mathbb{R} \to \mathbb{R}_+^\times$. $\square$

For instance the subgroup of $\mathbb{R}_+^\times$

$$\{2^{a_1}3^{a_2} \mid (a_1,a_2) \in \mathbb{Z}^2\}$$

generated by 2 and 3 is dense in $\mathbb{R}_+^\times$.

Dimension 2

Additive subgroups of $\mathbb{R}^2$ *:*
A subgroup

$$\mathbb{Z}^2 + \mathbb{Z}(x,y) = \{(a_1 + a_0 x, a_2 + a_0 y) \mid (a_0, a_1, a_2) \in \mathbb{Z}^3\}$$

of $\mathbb{R}^2$ is dense if and only if $1, x, y$ are $\mathbb{Q}$–linearly independent.

Multiplicative subgroups of $(\mathbb{R}_+^\times)^2$ *:*
Let $\gamma_1, \gamma_2, \gamma_3$ be three elements in $(\mathbb{R}_+^\times)^2$, say

$$\gamma_j = (\alpha_j, \beta_j) \quad (j = 1, 2, 3).$$

The subgroup of $(\mathbb{R}_+^\times)^2$ generated by $\gamma_1, \gamma_2, \gamma_3$ is

$$\{(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}, \beta_1^{a_1}\beta_2^{a_2}\beta_3^{a_3}) \mid (a_1, a_2, a_3) \in \mathbb{Z}^3\}.$$

Multiplicative subgroups of $(\mathbb{R}_+^\times)^2$

For instance the subgroup of $(\mathbb{R}_+^\times)^2$ generated by $(\alpha_1, 1)$, $(1, \beta_2)$, (α_3, β_3). is

$$\Gamma = \{(\alpha_1^{a_1}\alpha_3^{a_3}, \beta_2^{a_2}\beta_3^{a_3}) \mid (a_1, a_2, a_3) \in \mathbb{Z}^3\}.$$

When is-it dense ?

Use $\exp : \mathbb{R}^2 \to (\mathbb{R}_+^\times)^2$. Write

$$(\log \alpha_3, \log \beta_3) = x(\log \alpha_1, 0) + y(0, \log \beta_2)$$

with

$$x = \frac{\log \alpha_3}{\log \alpha_1}, \quad y = \frac{\log \beta_3}{\log \beta_2}.$$

Then Γ is dense in $(\mathbb{R}_+^\times)^2$ if and only if $1, x, y$ are $\mathbb{Q}$–linearly independent.

Multiplicative subgroups of $(\mathbb{R}_+^\times)^2$

Exemple : $\gamma_1 = (2, 1)$, $\gamma_2 = (1, 2)$, $\gamma_3 = (12, 18)$.
The subgroup Γ of $(\mathbb{R}_+^\times)^2$ generated by $\gamma_1, \gamma_2, \gamma_3$ is

$$\Gamma = \{(2^{a_1}12^{a_3}, 2^{a_2}18^{a_3}) \mid (a_1, a_2, a_3) \in \mathbb{Z}^3\}.$$

We have

$$x = 2 + \frac{\log 3}{\log 2}, \; y = 1 + 2\frac{\log 3}{\log 2},$$

with $3 - 2x + y = 0$, hence Γ is not dense.

Exemple : $\gamma_1 = (2, 1)$, $\gamma_2 = (1, 2)$, $\gamma_3 = (3, 5)$:

$$\Gamma = \{(2^{a_1}3^{a_3}, 2^{a_2}5^{a_3}) \mid (a_1, a_2, a_3) \in \mathbb{Z}^3\}.$$

The three numbers

$$1, \quad \frac{\log 3}{\log 2}, \quad \frac{\log 5}{\log 2}$$

are linearly independent over $\mathbb{Q}$, hence Γ is dense.

Multiplicative subgroups of $(\mathbb{R}_+^\times)^2$

Exemple : $\gamma_1 = (2, 1)$, $\gamma_2 = (1, 3)$, $\gamma_3 = (2, 3)$. The subgroup Γ of $(\mathbb{R}_+^\times)^2$ generated by $\gamma_1, \gamma_2, \gamma_3$ has rank 2 ($\gamma_3 = \gamma_1\gamma_2$), it is not dense.

Exemple : $\gamma_1 = (2, 1)$, $\gamma_2 = (1, 3)$, $\gamma_3 = (3, 2)$. The three numbers

$$1, \quad \frac{\log 3}{\log 2}, \quad \frac{\log 2}{\log 3}$$

are linearly independent over $\mathbb{Q}$, because $(\log 2)/(\log 3)$ is not quadratic (it is transcendental by Gel'fond–Schneider).

Exemple : $\gamma_1 = (2, 1)$, $\gamma_2 = (1, 3)$, $\gamma_3 = (5, 2)$.
Is

$$\{(2^{a_1}5^{a_3}, 3^{a_2}2^{a_3}) \mid (a_1, a_2, a_3) \in \mathbb{Z}^3\}$$

dense in $(\mathbb{R}_+^\times)^2$?

Geogebra

$$\{\gamma_1^{a_1}\gamma_2^{a_2}\gamma_3^{a_3} \mid -N \le a_i \le N \ (i=1,2,3)\} \cap \{1/2 \le x, y \le 3/2\}$$

$$\gamma_1 = (2,1), \qquad \gamma_2 = (1,3).$$

$\gamma_3 = (2,3)$
(Not dense)

$\gamma_3 = (3,2)$
(Dense)

$\gamma_3 = (5,2)$
(?)

$\gamma_1 = (2,1)$, $\gamma_2 = (1,3)$, $\gamma_3 = (5,2)$

The subgroup

$$\{(2^{a_1}5^{a_3}, 3^{a_2}2^{a_3}) \mid (a_1,a_2,a_3) \in \mathbb{Z}^3\}$$

is dense in $(\mathbb{R}_+^\times)^2$ if and only if

$$(\log 2)(\log 3), \ (\log 3)(\log 5), \ (\log 2)^2$$

are linearly independent over $\mathbb{Q}$.

Open problems

What are the algebraic relations among logarithms of algebraic numbers ?

Example : for $(a,b,c) \in \mathbb{Z}^3$,

$$a(\log 2)(\log 3) + b(\log 3)(\log 5) + c(\log 2)^2 = 0 \overset{?}{\iff} a = b = c = 0.$$

What is the rank of a matrix with entries logarithms of algebraic numbers ?

Example : for $(a,b,c) \in \mathbb{Z}^3$,

$$\det \begin{pmatrix} \log 2 & \log 3 \\ -b\log 5 & a\log 3 + c\log 2 \end{pmatrix} = 0 \overset{?}{\iff} a = b = c = 0.$$

Applications to Hasse principle

Jean–Jacques Sansuc

Damien Roy

Question of J-J. Sansuc, answer by D. Roy :
Given a number field k, the smallest positive integer m for which there exists a finitely generated subgroup of rank m of $k^\times$ having a dense image in $(k \otimes_{\mathbb{Q}} \mathbb{R})^\times$ under the canonical embedding is the number of archimedean places of k plus one.

Damien Roy. *Simultaneous approximation in number fields.* Invent. math. **109** (1992), 547–556.

Density of rational points on abelian varieties

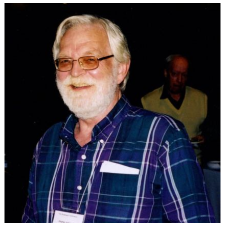
Barry Mazur

Mazur's question : given a simple abelian variety over $\mathbb{Q}$ with positive rank, is $A(\mathbb{Q})$ dense in the connected component of 0 in $A(\mathbb{R})$?

Partial answer : yes if the rank of $A(\mathbb{Q})$ is $\geq g^2 - g + 1$ where g is the dimension of A.

M.W. *Densité des points rationnels sur un groupe algébrique.* Experimental Mathematics. **3** N°4 (1994), 329–352.

Schanuel's Conjecture



Stephen Schanuel

If $x_1, \ldots, x_n$ are $\mathbb{Q}$–linearly independent complex numbers, then at least n of the $2n$ numbers $x_1, \ldots, x_n$, $e^{x_1}, \ldots, e^{x_n}$ are algebraically independent.

Special case where $e^{x_i} = \alpha_i$ are algebraic : Conjecture AIL

Conjecture AIL

Conjecture of algebraic independence of logarithms of algebraic numbers :

If $\log \alpha_1, \ldots, \log \alpha_n$ are $\mathbb{Q}$–linearly independent logarithms of algebraic numbers, then they are algebraically independent.

It is not known whether there are two algebraically independent logarithms of algebraic numbers.

Towards Schanuel's Conjecture

We want to investigate the numbers $x_1, \ldots, x_n$, $e^{x_1}, \ldots, e^{x_n}$.

We can consider the functions $z, e^{x_1 z}, \ldots, e^{x_n z}$ and their values (with derivatives) at the points in $\mathbb{Z}$.

We can also consider the functions z, e^z, and their values (with derivatives) at the points in $\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n$.

These two approaches are dual (Borel transform).

In the first case, we do not have enough points. In the second case, we do not have enough functions.

Towards Schanuel's Conjecture

We can get some results by considering functions $e^{x_1 z}, \cdots, e^{x_d z}$ and their values at points in $\mathbb{Z}y_1 + \cdots + \mathbb{Z}y_\ell$.
Assume that the numbers $\alpha_{ij} = e^{x_i y_j}$ are algebraic.
The matrix $(\log \alpha_{ij})_{\substack{1\le i\le d\\ 1\le j\le \ell}}$ is of the form $(x_i y_j)_{\substack{1\le i\le d\\ 1\le j\le \ell}}$ with x_i and y_j in $\mathbb{C}$.

Rank of matrices

A matrix $(u_{ij})_{\substack{1\le i\le d\\ 1\le j\le \ell}}$ with coefficients in a field $\mathbb{K}$ has rank ≤ 1 if and only if there exists $x_1, \dots, x_d$ and $y_1, \dots, y_\ell$ in $\mathbb{K}$ such that $u_{ij} = x_i y_j$ $(1 \le i \le d, 1 \le j \le \ell)$.

A matrix $(u_{ij})_{\substack{1\le i\le d\\ 1\le j\le \ell}}$ with coefficients in a field $\mathbb{K}$ has rank $\le r$ if and only if there exists $\mathbf{x}_1, \dots, \mathbf{x}_d$ and $\mathbf{y}_1, \dots, \mathbf{y}_\ell$ in $\mathbb{K}^r$ such that $u_{ij} = \mathbf{x}_i \mathbf{y}_j$ $(1 \le i \le d,\ 1 \le j \le \ell)$, with the standard scalar product in $\mathbb{K}^r$:

$$\mathbf{x} = (\xi_1, \dots, \xi_r), \qquad \mathbf{y} = (\eta_1, \dots, \eta_r),$$

$$\mathbf{x}\mathbf{y} = \xi_1\eta_1 + \cdots + \xi_r\eta_r.$$

Matrices of logarithms of algebraic numbers

Consider a $d \times \ell$ matrix $(\log \alpha_{ij})_{\substack{1\le i\le d\\ 1\le j\le \ell}}$ of rank r. Write $\log \alpha_{ij} = \mathbf{x}_i \mathbf{y}_j$ with $\mathbf{x}_1, \dots, \mathbf{x}_d$ and $\mathbf{y}_1, \dots, \mathbf{y}_\ell$ in $\mathbb{C}^r$. The d exponential functions in r variables $\mathbf{z} = (z_1, \dots, z_r)$

$$e^{\mathbf{x}_i \mathbf{z}}, \quad 1 \le i \le d$$

take algebraic values at $\mathbf{y}_1, \dots, \mathbf{y}_\ell$, hence at any point in $\mathbb{Z}\mathbf{y_1} + \cdots + \mathbb{Z}\mathbf{y}_\ell \subset \mathbb{C}^{\mathbf{r}}$.

Under suitable assumptions on the x's and y's, one proves

$$\ell d \le r(\ell + d).$$

Matrices of logarithms of algebraic numbers

$$r \ge \frac{\ell d}{\ell + d}.$$

For $\ell = d$, the conclusion is $r \ge d/2$, which is half the conjecture on the rank of matrices with entries logarithms of algebraic numbers :

$$r \ge \frac{1}{2} r_{\mathrm{conj}}(M).$$

M.W. *Transcendance et exponentielles en plusieurs variables.* Inventiones Mathematicae **63** (1981) N°1, 97–127.

M.W. *Diophantine Approximation on Linear Algebraic Groups.* Grundlehren der Mathematischen Wissenschaften 326. Springer-Verlag, Berlin-Heidelberg, 2000.

The conjectural rank $r_{\text{conj}}(M)$

Let M be a $d \times \ell$ matrix with coefficients $\log \alpha_{ij}$ logarithms of algebraic numbers. Let $\lambda_1, \dots, \lambda_s$ be a basis of the $\mathbb{Q}$–space spanned by the $\log \alpha_{ij}$. Write

$$\log \alpha_{ij} = \sum_{k=1}^{s} a_{ijk} \lambda_k \qquad 1 \leq i \leq d, 1 \leq j \leq \ell.$$

We denote by $r_{\text{conj}}(M)$ the rank of the matrix

$$\left(\sum_{k=1}^{s} a_{ijk} X_k \right)_{\substack{1 \leq i \leq d \\ 1 \leq j \leq \ell}}$$

viewed as a matrix with entries in the field $\mathbb{C}(X_1, \dots, X_s)$.

Two conjectures

Algebraic independence of logarithms of algebraic numbers :
Conjecture AIL : $\mathbb{Q}$–linearly independent logarithms of algebraic numbers are algebraically independent.

Rank of matrices with entries logarithms of algebraic numbers :
Conjecture RM : the rank r of M is $r_{\text{conj}}(M)$.

Clearly, Conjecture AIL implies Conjecture RM.

For Conjecture AIL, we do not know whether there are two algebraically independent logarithms of algebraic numbers.

For Conjecture RM, we know half of it : $r \geq \frac{1}{2} r_{\text{conj}}(M)$.

Equivalence between the two conjectures

D. Roy : Conjecture AIL and Conjecture RM are equivalent !

Proposition (D. Roy) : any polynomial in n variables $X_1, \dots, X_n$ over a field $\mathbb{K}$ is the determinant of a square matrix with entries in $\mathbb{K} + \mathbb{K}X_1 + \cdots + \mathbb{K}X_n$.

Damien Roy

D. Roy. *Matrices dont les coefficients sont des formes linéaires.* Séminaire de théorie des nombres Paris 1987–88, 273–281. Prog. Math.81, Birkhäuser, 1990.

Arithmetic Complexity, Theoretical Computer Science

Chap. 13 : *Projections of Determinant to Permanent*
in
Xi Chen, Neeraj Kayal and Avi Wigderson.
Partial Derivatives in Arithmetic Complexity (and beyond)
Foundations and Trends in Theoretical Computer Science
Vol. **6** 1–2, (2010), 1–138
http://www.math.ias.edu/~avi/PUBLICATIONS/ChenKaWi2011.pdf

Thanks to Anurag Pandey and Vijay M. Patankar.

Determinantal complexity of a polynomial

Given a polynomial f in n variables $X_1, \cdots, X_n$ with coefficients in a field $\mathbb{K}$ of characteristic 0, the determinantal complexity $\mathrm{dc}(f)$ of f is the smallest m such that there exists a $m \times m$ matrix with entries affine forms

$$a_0 + a_1 X_1 + \cdots + a_n X_n$$

such that the determinant of A is f.

Geometric complexity theory

L.G.Valiant.
The complexity of computing the permanent.
Theoretical Computer Science,
8 2, (1979), 189 – 201.

Leslie G. Valiant

2010 Turing Award

VNP vs VP.

Permanent of a square matrix

Augustin-Louis Cauchy
1789 – 1857

(Introduced by Cauchy in 1812 : for $A = (a_{ij})_{1 \le i,j \le n}$,

$$\mathrm{perm}(A) = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

Compare with

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

Permanent of a matrix

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \mathrm{perm} \begin{pmatrix} a & -b \\ c & d \end{pmatrix}$$

George Pólya
1887 – 1985

George Pólya asked, in 1913 : Given a square matrix A, is there a way to set the signs of the entries so that the resulting matrix A' satisfies

$$\det(A) = \mathrm{perm}(A')?$$

Negative answer : G. Szegő (1913).

Determinantal complexity of the permanent

Let perm_n be the permanent of the matrix $(X_{ij})_{1\leq i,j\leq n}$ in n^2 variables over a field of zero characteristic.
G. Szegő (1913) : $\mathsf{dc}(\mathsf{perm}_n) \geq n+1$.
Joachim von zur Gathen (1987) : $\mathsf{dc}(\mathsf{perm}_n) \geq \sqrt{8/7}\, n$.
Babai and Seress, J.Y. Cai, R. Meshulam (1989)
$\mathsf{dc}(\mathsf{perm}_n) \geq \sqrt{2}\, n$.

T. Mignon and N. Ressayre (2004) : $\mathsf{dc}(\mathsf{perm}_n) \geq \dfrac{n^2}{2}$.

Gábor Szegő
1895–1985

J. von zur Gathen

Nicolas Ressayre

Proof by D. Roy of $\mathsf{dc}(f) < \infty$

Here is a proof that any quadratic polynomial $f \in \mathbb{K}[z_1,\dots,z_n]$ is the determinant of a matrix with entries in $\mathbb{K} + \mathbb{K}z_1 + \cdots + \mathbb{K}z_n$.
Write f as $L_0 + L_1 z_1 + \cdots + L_n z_n$ where each L_i is a polynomial of degree ≤ 1, which means that each L_i lies in $\mathbb{K} + \mathbb{K}z_1 + \cdots + \mathbb{K}z_n$.
Then f is the determinant of the $(n+2)\times(n+2)$ matrix

$$\begin{pmatrix} & & & 1 \\ & & & z_1 \\ & \mathsf{I}_{n+1} & & \vdots \\ & & & z_n \\ -L_0 & \cdots & -L_n & 0 \end{pmatrix}$$

An auxiliary lemma

The determinant of a product AB of a $d\times \ell$ matrix A by a $\ell\times d$ matrix B is the determinant of the $(d+\ell)\times(d+\ell)$ matrix written as blocks

$$\begin{pmatrix} I_\ell & \mathsf{B} \\ -\mathsf{A} & 0 \end{pmatrix}.$$

Proof.
Multiply on the left the matrix $\begin{pmatrix} \mathsf{I}_\ell & \mathsf{B} \\ -\mathsf{A} & 0 \end{pmatrix}$ by the matrix $\begin{pmatrix} \mathsf{I}_\ell & 0 \\ \mathsf{A} & \mathsf{I}_d \end{pmatrix}$. This will not change the determinant, and the product is $\begin{pmatrix} \mathsf{I}_\ell & \mathsf{B} \\ 0 & \mathsf{AB} \end{pmatrix}$, the determinant of which is $\det(\mathsf{AB})$. □

A further lemma

Let M be a matrix , the entries of which are bilinear forms

$$\mathsf{M} = \left(\sum_{s=0}^{S}\sum_{t=0}^{T} m_{ijst} X_s Y_t\right)_{\substack{1\leq i\leq d\\ 1\leq j\leq \ell}}.$$

There exist a matrix A whose entries are linear forms in $X_0,\dots,X_S$ and a matrix B whose entries are linear forms in $Y_0,\dots,Y_T$ such that $\mathsf{M}=\mathsf{AB}$.
Proof.
Write $\mathsf{M} = \mathsf{M}_0 X_0 + \cdots + \mathsf{M}_S X_S$ with

$$\mathsf{M}_s = \left(\sum_{t=0}^{T} m_{ijst} Y_t\right)_{\substack{1\leq i\leq d\\ 1\leq j\leq \ell}}, \qquad (0\leq s\leq S).$$

Take

$$\mathsf{A} = (X_0 \mathsf{I}_d, \dots, X_S \mathsf{I}_d), \quad \mathsf{B} = \begin{pmatrix} \mathsf{M}_0 \\ \vdots \\ \mathsf{M}_S \end{pmatrix}. \square$$