Siegel, Carl Ludwig | Encyclopedia.com

Complete Dictionary of Scientific Biography COPYRIGHT 2008 Charles Scribner's Sons 23-29 minutes

(b. Berlin, Germany, 31 December 1896; d. Göttingen, Federal Republic of Germany, 4 April 1981)

mathematics.

The son of a postal worker, Siegel studied at the University of Berlin from 1915 to 1917, attending lectures by Georg Frobenius that introduced him to the theory of numbers. Called into military service in 1917, he could not adapt to army life and was discharged. He then went to the University of Göttingen (1919-1920), where he worked on his inaugural dissertation and *Habilitationsschrift* under the guidance of Edmund Landau, a specialist in analytic <u>number theory</u>. Siegel was a professor at the University of Frankfurt from 1922 to 1937 and at the University of Göttingen from 1938 to 1940.

Siegel despised the Nazi regime. After lecturing in Denmark and Norway in 1940, he left Norway for the <u>United States</u> just a few days before the Nazi invasion. From 1940 to 1951 he worked at the <u>Institute for Advanced Study</u> at Princeton, where he had spent the year 1935. In 1946 he was appointed to a permanent professorship at the institute. Five years later he returned to Göttingen, where he spent the rest of his life.

Siegel was one of the leaders in the development of the theory of numbers, but he also proved important theorems in the theory of analytic functions of several complex variables and in <u>celestial mechanics</u>.

Siegel's inaugurual dissertation (1920) was a landmark in the history of Diophantine approximations. Joseph Liouville had been the first to observe that algebraic numbers of degree n > 1 are "badly" approximated by rational numbers: for any such number ξ there is a constant *C* (ξ) such that, for every rational number p/q with greatest common divisor (p, q) = 1, one has

The proof is almost trivial, but the improved result obtained by Axel Thue in 1908 was more difficult to prove: the inequality

(where $\varepsilon > 0$ is arbitrary) is possible only for a finite number of values of p/q. Siegel obtained a still better result, which was crucial for his work of 1929 on Diophantine equations: there are only a finite number of rational numbers p/q such that

The proof was very ingenious. In fact, Siegel did not directly prove that (3) has only a finite number of solutions p/q, but he showed that this is true for the inequality

where being any integer such that $0 \le s \le n-1$; from that (3) is easily deduced by a suitable choice of *s*. The proof was by contradiction. If it is assumed that (4) has infinitely many solutions, it is possible to choose two of them. p_1/q_1 and p_2/q_2 , such that q_1 and $r = [\log q_2/\log q_1]$ are arbitrarily large.

Siegel introduced two integers:

and m, which is the integral part of

He considered the two numbers

and showed that there is a constant *C*, depending only on ξ , such that $E_1 < 1$ and $E_2 < 1$. On the other hand, using the fact that ξ is an algebraic number of degree *n*, he constructed, by very intricate arguments, for each value of *p* satisfying (5) a polynomial $R_p(x, y)$ of degree m + r - p in *x*, and degree *s* in *y*, with integral coefficients $\leq C^n$ (with a constant C^n depending only on ξ). Then, using Gustav Dirichlet's pigeonhole principle, he could show that there is a degree *p* satisfying (5) for which $\neq 0$, and hence an integer ≥ 1 ; and that number, compared with the sum $E_1 + E_2$, implies that one of these two numbers must be ≥ 1 , yielding the required contradiction.

In 1955 Siegel's result (3) was drastically improved by K. F. Roth: there are only a finite number of rational numbers p/q such that

where ε is any number > 0; this result is the best possible because there is an infinity of rational numbers p/q such that

In 1929 Siegel published a long paper in two parts that is probably his deepest and most original. The first part (contemporary with Aleksandr Gelfond's proof of the transcendence of e^{π}) contains an entirely new result on transcendental numbers: he

proved that if J_0 is the Bessel function of index 0, then $J_0(\xi)$ is transcendent for any algebraic value of $\xi \neq 0$. More precisely, let g(y, z) be a polynomial of total degree p > O whose coefficients are integers of <u>absolute value</u> $\leq G$; if ξ is an algebraic number of degree *m* and $\neq 0$, then

where c depends only on p and ξ .

Siegel's method differed from those used earlier in the theory of transcendental numbers. He starts with an analytic study, in the manner of Liouville, of the algebraic relations between x, $J_0(x)$ and . The main result was the following: let

where the $f_{\alpha\beta}$ are polynomials in x with real coefficients, which are $\neq 0$ for q values of the pair $(\alpha, \beta - \alpha)$; then ϕ and its derivatives up to order q - 1 are q linear forms in the whose determinant is a polynomial in x that is not 0.

Let l > p be an integer, and $k = \frac{1}{2}(l+1)(l+2)$; let $n \ge 2k^2$ be an arbitrary integer and $\varepsilon > 0$ an arbitrary real number. The center of the proof consisted in constructing a function (8) with the following properties: (1) the *k* polynomials $f_{\alpha\beta}$ for $\beta \le l$ have a degree $\le 2n - 1$, with integer coefficients at most $(n!)^{2+\varepsilon}$ (2) the Maclaurin series of ϕ begins with a term in $x^{(2k-1)n}$ and its coefficients are majorized in <u>absolute value</u> by those of the series

Let $T_j(x)$ for $1 \le j \le k$ be the functions for $\beta \le l$ and $\alpha \le \beta$, with $T_1 = 1$. As J_0 satisfies the second-order Bessel differential equation, the function ϕ and its derivatives can be written in the form

where $\sigma_{ab}(x)$ is a polynomial of degree 2n + a - 1, with coefficients that are integers $O((n!)^{3+2\epsilon})$ for a lt; $n + k^2$. The essential part of the proof involved showing that for $a \le n + k^2 - 1$ and for every real number $\xi \ne 0$, the matrix $(\sigma_{aj}(\xi))$ has rank equal to k.

It is then possible to choose k integers

 $h_v \le n + k^2 - 1$

such that the k functions

are linearly independent. Let r = l - p, v = (r + l)(r + 2)/2, and consider the functions

for $p + \sigma \le r$; they can be written

for $1 \le \mu \le v$, where the cµj are integers whose absolute value is $\le G$; the *v* functions ψ_{μ} are linearly independent and can be completed by w = k - v functions ϕ_v in order to have *k* linearly independent linear combinations of the T_j . It can then be shown that the determinant Δ of the coefficients of these *k* linear forms is a polynomial in ξ of degree w ($3_n + k^2 - 2$) with integer coefficients all $0((n!)^{3w+2\varepsilon Gv})$. This finally proves that $|\Delta|$ is majorized by

where $K \ge 1$ is independent of *n*.

All this is true for any real number $\xi \neq 0$. But now suppose $\xi \neq 0$ is an algebraic number of degree *m*; if *c* is an integer such that $c\xi$ is an algebraic integer, then $c^{w(3n+k^2-2)}\Delta$ is an algebraic integer $\neq 0$. It is then enough to write that the norm of that algebraic integer is ≥ 1 to obtain (7) after having chosen conveniently *n* as a function of *G*.

Shidlovskii later generalized Siegel's transcendence theorem to what Siegel had called *E*-functions (he had introduced them as auxiliaries in his proof). They are series defined by arithmetic conditions on their coefficients.

The second part of Siegel's 1929 paper was even more startling, since it contained the first general result on Diophantine equations

where *f* is a polynomial with integer coefficients. Until then the best result had been Thue's theorem for the special type of equations (14), written g(x, y) - a = 0, where $a \neq 0$ and *g* is a homogeneous polynomial of degree ≥ 3 . Thue had shown that such equations have only a finite number of solutions (x, y) consisting of integers. What Siegel showed is that the same thing may be said of all equations (14) except those for which the curve Γ having (14) for equation possesses a parametric representation by rational functions with denominators of degree 1 or 2 (this implies that Γ has genus 0 and at most two points at infinity).

The least difficult part of the proof concerned the case when Γ has genus 1. Let *L* be the field of rational functions on Γ and *F* a function in *L* of order *m*, and suppose there are infinitely many pairs (x/z, y/z) with *x*, *y*, *z* integers having no common factor, such that (1) F(x/z, y/z) = 0; (2) F(x/z, y/z) is an integer. Then one can extract from that set of pairs (x/z, y/z) a sequence that converges to a point of Γ that is a pole of *F*; if *r* is the order of that pole, then for every function $\phi \in L$ that vanishes at that pole and every $\varepsilon > 0$ there is a constant $C(\phi, \varepsilon)$ such that

(Where h is the degree of f) for every point in the convergent sequence.

Since Γ has genus 1, there is a parameterizing of Γ by elliptic functions x = w(s), y - v(s). Let *r* be the number of roots of the equation w(s) = a in a parallelogram of periods. Siegel made essential use of a theorem proved by Louis J. Mordell in 1922: If *M* is the *Z*-module of complex numbers *s* such that both w(s) and v(s) are rational numbers, then *M* has a finite basis s_1, \ldots, s_q . Let *n* be an arbitrary integer (later allowed to be arbitrarily large); using the euclidean algorithm, one can write every element of *M* in the form

where $\sigma \in M$ and $c \in M$ takes only a finite number of values. The proof used contradiction (as in Thue's theorem). Suppose equation (14) has infinitely many solutions in integers. There is therefore an infinity of these solutions for which, in the expression of the parameter *s*, the number $c \in M$ is the same. Apply inequality (15) to F(x/z, y/z) = x. From the addition theorem of elliptic functions, it follows that $s \mapsto w(ns + c)$ belongs to the field *L* and has order n^2m , and its n^2m poles have coordinates that are algebraic numbers of degree $\leq n^2m$.

From (14) it follows that one of these poles is the limit of a sequence of points $(\xi/\zeta, \eta/\zeta)$ of Γ , where ξ, η , and ζ are integers with no common factor. If the sequence of the numbers ξ/ζ has a finite limit *p*, it is an algebraic number of degree $\leq n^2 m$, and the inequality (15) shows that

where k > 0 does not depend on *n*. On the other hand, the inequality (3) proved by Siegel in his dissertation showed that, except for a finite number of numbers ξ/ζ of the sequence, one has

where C'(n) depends only on *n*. Comparing (17) and (18) yields

But it is clear that, when , the relation (19) can be verified only for finitely many pairs of integers (ξ, ζ) , which yields the desired contradiction. The argument is similar and simpler when the sequence of the $|\xi/\zeta|$ tends to $+\infty$.

Siegel was able to construct a similar but much more intricate proof when r has genus ≥ 2 , by making use of Andr Weil's generalization of Mordells theorem. But instead of the curve I' the Jacobian of I' must be used, which causes complications. Until very recently Siegel's theorem remained the most powerful of its kind. In 1983, however, G. Faltings obtained a more profound result: for curves (14) of genus ≥ 2 , there are only finitely many points of the curve that have rational coordinates, a theorem that had been conjectured by Mordell.

In 1934, H. Heilbronn had proved a conjecture of <u>Carl Friedrich Gauss</u>: if h(-d) is the number of ideal classes in an imaginary quadratic field of discriminant -d, then h(-d) tends to $+\infty$ with d. In 1935 Siegel, using the relation between the zeta functions of two quadratic fields and the zeta function of their "compositum," was able significantly to improve Heilbronn's theorem: when d tends to $+\infty$,

 $\log h (-d) \sim \frac{1}{2} \log d.$

From 1935 on, most of Siegel's papers in the theory of numbers were concerned with the arithmetic theory of quadratic forms in an arbitrary number n of variables, with integer coefficients. The theory had been stated by Joseph Lagrange and Gauss for n = 2 and n = 3, and developed during the nineteenth century for arbitrary dimension n by Adrien-Marie Legendre, Ferdinand Eisenstein, <u>Charles Hermite</u>, Henry J. S. Smith, and <u>Hermann Minkowski</u>. The work of Siegel in this domain may be considered the crowning achievement of the theory; but at the same time, he broadened it considerably and prepared its modern versions by connecting it with the theory of Lie groups and automorphic functions.

In three long papers published between 1935 and 1937, Siegel tackled the general problem of using linear transformations with integer coefficients to transform a quadratic form Q in m variables with integer coefficients into a quadratic form R in $n \le m$ variables with integer coefficients. It is easier to express the problem in terms of matrices with integer coefficients: Given two symmetric matrices, an $m \times m$ matrix S and an $n \times n$ matrix T, one must study the $m \times n$ matrices X such that

The first paper deals with the case in which *S* and *T* are positive definite, which had been most studied by Siegel's predecessors. The number A(S, T) of matrices *X* satisfying (20) is then finite. The number E(S) = A(S, S) is the order of the subgroup of GL(m, Z) leaving *S* invariant (called the group of "units" of *S*). Gauss had defined the concepts of class and of genus for binary quadratic forms. They can be extended to any number of variables. Two $n \times n$ matrices *S*, *S*₁ with integer coefficients belong to the same class if there exists an invertible $n \times n$ matrix *Y* with integer coefficients, such that

when A(S, T) is finite, it depends only on the classes of S and T. The definition of genus was simplified by Henri Poincaré and Minkowski: S and S_1 are in the same genus if, on the one hand, there is an $n \times n$ invertible matrix Y with real terms satisfying equation (21) and, on the other hand, for every integer q, there is an $n \times n$ matrix Y_q with integer coefficients and a determinant invertible mod. q, such that Hermite's reduction process showed that, for positive definite matrices, a genus contains only a finite number of classes. Suppose a genus contains *h* classes, and let S_j be matrices chosen in these classes $(1 \le j \le h)$. Eisenstein and Smith had associated to the genus its "mass"

and Smith (and independently Minkowski) had expressed (23) with the help of the "characters" of the genus.

Siegel's first paper on quadratic forms was concerned, more generally, with the expression

where S and T are positive definite, and S_1, \ldots, S_h are representatives of the classes in the genus of S. The main result was the value of M(S, T) as an infinite product

In (25) p varies in the set of all prime numbers. Let $A_q(S, T)$ be the number of solutions mod. q of the congruence in matrices with integer coefficients

 $d_p(S, T)$ is the limit of $A_q(S, T)/q^{nn-\forall n(n+1)}$ when, for $q = p^N$, N tends to $+ \infty$ [a "p-adic mean value" of A(S, T)]. Finally, $A_{\infty}(S, T)$ is also a kind of "mean value": when m > n and $m \neq 2$, consider a neighborhood V of T in the space of $n \times n$ symmetric real matrices (an open set in $R^{\forall n(n+1)}$); $A_{\infty}(S, T)$ is the limit, when V tends to T, of the ratio of the volume of the inverse image of V by $X \mapsto 'X.S.X$ in R^{nm} , to the volume of V. The proof is by induction on m and a very subtle adaptation of the methods used by Gauss, Dirichlet, and Minkowski.

Siegel's second paper on quadratic forms dealt with "indefinite" quadratic forms of arbitrary signature. He first proved that the right-hand side of (25) is still meaningful except in two particular cases (when m = 2 and –det S is a square, and when m - n = 2 and –det S.det T is a square). However, (23) and (24) are meaningless because the subgroup of GL(m, Z) leaving S invariant is infinite. Finding what should replace the left-hand side of (25) was a problem that had been tackled by Georges Humbert only in a very particular case, the ternary forms.

Siegel was able to solve it in general: in the space of symmetric $m \ge m$ matrices of given signature, let B be a neighborhood of S, and let B_1 , be its inverse image in the space R^{mm} by the map $X \mapsto X.S.X.B_1$ is invariant by the group of "units" of S acting by left multiplication. There is a fundamental domain D for that action on B_1 . v(B) is finite, then the volume v(D) is also finite and the limit

 $p(S) = \lim v (D / v (B))$

exists when *B* tends to *S*. In a genus containing *S* there are again only a finite number of classes. Let S_t, \ldots, S_h be representatives of those classes. The number

replaces the "mass" of the genus of *S*. There is a similar, more complicated definition of a number $\mu(S, T)$ that replaces the numerator of (24). Finally. Siegel's formula (25) is valid when the left-hand side is replaced by $\mu(S, T)/\mu(S)$. Siegel improved that formula in 1944, showing that in some cases the terms in the expression of $\mu(S, T)$ are the same for all classes of a genus.

In the third paper (1937) on quadratic forms, Siegel considered quadratic forms in which the coefficients belong to a field of algebraic numbers, which nobody had studied before him. There are new difficulties in the theory, but he is able to overcome them.

Siegel's results on positive definite quadratic forms warrant further discussion. When a genus contains only one class, the lefthand side of (25) is A(S, T); this is true for $m \le 8$ when S is the unit matrix: if, in addition, n = 1, then (25) gives back the formulas of Carl C. J. Jacobi. Eisenstein, Smith, and Minkowski for the number of representations of an integer as a sum of m squares for $4 \le m \le 8$. Jacobi's proof relied on his study of theta functions and their relations with the modular group SL(2, Z), which proceed from the formula (found independently by Gauss, <u>Augustin-Louis Cauchy</u>, and Siméon-Denis Poisson)

for the simplest of theta functions

In his first paper on positive definite quadratic forms, Siegel observed that (25) is equivalent to a remarkable identity between functions that generalize modular forms. The space of the variables is what is now called "Siegel's half-space," a generalization of "Poincaré's half-plane." It consists of the symmetric complex $n \ge n$ matrices Z, whose imaginary part is positive definite. For any symmetric $m \ge m$ matrix S with integer coefficients, Siegel considered the following function of Z that is a generalization of theta functions—

where C takes all values in the space Z^{mm} of m x n matrices with integer coefficients; this series is absolutely convergent when Z is in the Siegel half-space. It is easy to see that

where T takes all values in the space of $n \ge n$ symmetrical matrices with integer coefficients. Now, if

then (25) is equivalent (for large enough m) to an expression for F(S, Z) as a convergent series

where *K* and *L* are *n* x *n* matrices with integer coefficients satisfying additional arithmetic conditions. The series (33) is clearly similar to the Eisenstein series (for n = 1); this led Siegel, in several later papers, to make a systematic study of what he called modular forms of degree *n*. They are holomorphic functions defined in the Siegel half-space *D*; the symplectic group Sp(2*n*, *R*), consisting of such that 'U.J.U = *J* for acts on D by

 $Z \mapsto (AZ+B)(CZ+D)^{-1}$

In a 1939 paper Siegel considered the subgroup Sp(2n, Z) of Sp(2n, R), which is the group of transformations of the systems of 2*n* periods of a linearly independent system of abelian integrals of the first kind on a Riemann surface of genus *n*. That subgroup acts on *D* in a properly discontinuous way. Siegel described a fundamental domain for that action, using Minkowski's reduction of quadratic forms. The modular forms of degree *n* and weight *r* are the holomorphic functions defined in *D* that transform under Sp(2n, Z) according to the relation

(for even r). Siegel could express these forms by series generalizing Eisenstein's series. He next considered modular functions, which are meromorphic in D and invariant under the action of Sp(2n. Z). A quotient of two modular forms of the same weight is such a function, and in 1960 Siegel proved that all modular functions can be obtained in that way. He also showed that the set of all modular functions is a field having transcendence degree n (n + 1) / 2 over C.

Siegel thus inaugurated the general theory of automorphic functions in any number of variables, which since Poincaré had not gone beyond the consideration of some very particular cases. In a paper of 1943, Siegel studied other subgroups of Sp(2n, R) also acting in a properly discontinuous way on the Siegel half-space D. He linked this question to the theory of Lie groups, showing that D is isomorphic to a bounded domain in C^n that is a symmetric space in the sense of Élie Cartan (who had determined all bounded domains in C^n that are symmetric spaces). Since then the study of automorphic functions has been developed for groups acting in a properly discontinuous way in these domains.

In 1903 Paul Epstein had defined "zeta functions" for a positive definite quadratic form $Q(x_1, x_2, ..., x_n)$ with integer coefficients, the simplest of which is

where the summation is over $Z^n - \{0\}$. The series converges for Re s > n/2, and Epstein had shown that it can be continued to a meromorphic function in the whole complex plane, satisfying a functional equation similar to those satisfied by zeta functions of number fields. Definitions such as (35) were of course meaningless for indefinite quadratic forms.

In two papers of 1938 and 1939, Siegel showed what to do in that case. Let *S* be the symmetric matrix of a quadratic form of signature (n, m - n), and let $\Gamma(S)$ be its group of "units." It acts properly on the open subset *U* of the Grassmannian $G_{m,n}$ consisting of the *n*-dimensional subspaces of \mathbb{R}^m in which the quadratic form is positive definite; there is in *U* a fundamental domain of finite volume $\mu(S)$ for that action. For a vector $\mathbf{a} \in \mathbb{Z}^m$, let $\Gamma(S, a)$ be the subgroup of $\Gamma(S)$ leaving a fixed; for $m \ge 3$, $\Gamma(S, a)$ has in *U* a fundamental domain of finite volume $\mu(S, a)$. For every integer t > 0 such that the equation ${}^ta.S.a = t$ has at least a solution $a \in \mathbb{Z}^m$, Siegel wrote

where the sum is extended to a set of representatives of the orbits of $\Gamma(S)$ in the set of solutions of 'a.S.a = t. Siegel's zeta function is then

He showed that the series converges for Re s > m/2 and is continued in the whole complex plane as a meromorphic function satisfying a functional equation. His proof is a generalization of Riemann's proof of the functional equation for the usual zeta function, using a theta function, which depends on a parameter varying in a fundamental domain in U of the group $\Gamma(S)$.

In the year 1951–1952 Siegel returned to the theta function and its transformations by the modular group, and gave an expression for its "mean value" in a fundamental domain of $\Gamma(5)$. From that he deduced another proof for his fundamental result of 1936 on indefinite quadratic forms. He also stated without proof that his mean value formula could be extended to quadratic forms in which both coefficients and variables belong to a simple algebra over the rational field Q, equipped with an involution.

A central theme in all these works is the computation of "volumes" of fundamental domains or, equivalently, of quotients of Lie groups by discrete subgroups. These computations have led to general views on "measures" on Lie groups or on *p*-adic groups, the outcome of which was the discovery by Tamagawa of a privileged measure on a group of "adeles" of an algebraic group defined on a number field. Tamagawa showed that the properties of that measure implied Siegel's theorems on quadratic forms; Weil similarly interpreted the mean value formula Siegel had proved in 1951 on such groups of "adeles."

In another area, in 1935 Siegel had deduced from his formula (25) the remarkable fact that the zeta function of a number field takes rational values at integers <0. Later he improved that result, using the theory of modular forms. These results form the basis of numerous papers on that subject published in recent years.

The papers we have analyzed are those which have given Siegel his eminent position in the theory of numbers. But they are far from exhausting his scientific production, which includes many results of lesser scope although none of them is trivial. They cover a wide range of topics: geometry of numbers, Pisot numbers, mean values of arithmetic functions, sums of squares and

Waring's problem in number fields, zeros of Dirichlet's *L*-functions, iteration of holomorphic functions, meromorphic functions on a compact kählerian manifold, groups of isometries in non-euclidean geometries, abelian functions, differential equations on the torus, and calculus of variations. After the theory of numbers, Siegel's favorite subjects were <u>celestial</u> <u>mechanics</u> and analytic differential equations, particularly hamiltonian systems.

Siegel had few students working under his guidance; the perfection and thoroughness of his papers, which did not leave much room for improvement with the same technique, discouraged many research students because to do better than he required new methods. Siegel enjoying teaching, however, even elementary courses, and he published textbooks on the theory of numbers, celestial mechanics, and the theory of functions of several complex variables.

Siegel, who never married, devoted his life to research. He traveled and lectured in many countries, particularly at the Tata Institute in Bombay. His mental powers remained unabated in his old age, and he published important papers when he was in his seventies. He was the recipient of many honorary doctorates, and a member of the most renowned academies. In 1978, when the Wolf Prize for mathematics was awarded for the first time, he and Izrail Moiseevich Gelfand were selected for this honor.

BIBLIOGRAPHY

Siegel's writings are collected in *Gesammelte Abhandlungen*, K. Chandrasekharan and H. Maass, eds., 4 vols. (Berlin and <u>New</u> York, 1966).

Jean Dieudonné