International Journal of Algebra, Vol. 12, 2018, no. 3, 133 - 140
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2018.8413

On Cantor's Normal Form Theorem and Algebraic Number Theory

Yvon Gauthier

Faculty of Arts and Sciences, University of Montreal
Montreal, Que. Canada

Abstract

Cantor introduced his normal form theorem as an ordinal polynomial for the countable ordinals of the second class up to the first epsilon number ϵ_0. Cantor believed that the normal form was a unique representation of real algebraic numbers. The Gel'fond-Schneider theorem is a counterexample to the normal form theorem, as it exhibits a transcendental number in the power representation of algebraic numbers. The theory of p-adic numbers provides another counterexample insofar as it comprises infinite p-adic numbers not expressible in the ordinal polynomial.

Mathematics Subject Classification: 03E10, 11C08, 11D88, 11J04

Keywords: Cantor's normal form, polynomials, algebraic numbers, p-adic integers

1 Introduction

In his early set-theoretic paper of 1874 « On a property of the set of all real algebraic numbers » (*Über eine Eigenschaft des lnbegriffes aller reellen algebraischen Zahlen*) – see (Cantor [3]115-118) – Cantor introduces the irreducible polynomial

$$a_o\ \omega^n = a_o\ \omega^{n+1}\ + ... + a_n = 0 \tag{1}$$

for integers $a_0, a_1, \ldots , a_n$ and real algebraic numbers ω and comes up with his own proof for the existence of transcendental numbers : since there is a bijection between algebraic numbers and natural numbers, the set of algebraic numbers is countable and since the set of real numbers is not (by the diagonal proof), there is an uncountable infinity of non- algebraic, i.e. transcendental numbers. This theorem, which he had discussed at length with Dedekind and to whom he is indebted, is for Cantor a new proof of the existence of transcendental numbers. But Cantor is satisfied with the "negative" existence of transcendental numbers : real numbers are more numerous than natural numbers and one can say that most reals are transcendental (see Baker [1]). In his last papers on transfinite set theory (*Beiträge zur Begründung der transfiniten Mengenlehre*), Cantor (see [3], 341) defines a normal form for the ordinals of the second class of numbers for integer variables x

$$\alpha = \omega^{\alpha_0} x_0 + \omega^{\alpha_1} x_1 + ... + \omega^{\alpha_t} x_t \tag{2}$$

the ω's being this time transfinite ordinals with

$$lim\ \omega = \epsilon_0. \tag{3}$$

Cantor claims for this normal form a unique representation of transfinite ordinals up to ϵ_0 which constitute a countable set as the set of (real) algebraic numbers. One can generalize Cantor's normal form in the formula

$$pr(\gamma) = pr(\alpha)^{pr(\beta)} \tag{4}$$

for *pr* meaning polynomial power representation and α, β, γ undefined algebraic quantities (algebraic numbers, real and complex). We then have the Gel'fond-Schneider theorem as a counterexample.

2 The Gel'fond-Schneider theorem

The Gel'fond-Schneider theorem is a solution to Hilbert's 7th problem

For α and β algebraic numbers with $\alpha \neq 0, 1$ and β irrational, α^β is transcendental.

Schneider [13], [14] puts the problem in the form

Theorem 1. *For ω an algebraic number $\neq$ 0,1 and θ irrational, ω^θ is transcendental with $\theta = \frac{log\ \eta}{log\ \omega}$ for $\eta = \omega^\theta$.*

Proof. The proof proceeds by logarithmic approximations to algebraic numbers and concludes that any logarithm of an algebraic number with an algebraic base must be a transcendental or a rational number. By *reductio ad absurdum*, ω^θ is transcendental. With a similar procedure, Gel'fond [9] comes to

the conclusion that the logarithms of algebraic numbers with an algebraic base are transcendental or rational numbers. Both proofs are (partially) constructive in the sense that they extract arithmetical content (that is logarithmic approximations, minorizations and majorizations, effective bounds, etc.) from analytical methods (infinite series or power series, periodic functions, etc.); they use polynomial inequalities for the rational values of an analytic function $f(x)$ and end up by contradicting an assumption to the effect that finite values make it vanish identically $f(x) = 0$. K. Mahler [12] has applied the result in $p-$adic number theory on algebraic approximations to the exponential and logarithmic functions in the completion $\mathbf{C}_p$ of the algebraic closure of $\mathbf{Q}_p$ expressing $p-$functions in terms of polynomials. A. Baker [1] has extended and generalized those results in transcendental number theory using auxiliary functions or polynomials – which he calls fundamental polynomials –, that is linear forms and logarithms for approximations of algebraic numbers in Diophantine equations in order to establish their algebraic independence by contradiction or *reductio ad absurdum*. Take for example the power expression for the algebraic number $\sqrt{2}$

$$\sqrt{2}^{\sqrt{2}} = \gamma \; ; \tag{5}$$

it is a transcendental number γ and therefore we have a counterexample to Cantor's normal form for an algebraic number

$$pr(\gamma) \neq pr(\beta)^{pr(\beta)}. \tag{6}$$

□

It is only in 1962 that Gel'fond produced an elementary (constructive) proof for real algebraic numbers ω, $a > 0$, b for c^ω and a^b (see Gel'fond and Linnik [10], chap. 12). Gel'fond relates that he used only Rolle's theorem as an analytical tool – here a constructivist mathematician could mention that a constructive version of Rolle's theorem is to be found in Bishop [2]. Essentially, Rolle's theorem states classically that a continuous function of a real variable on $[a, b]$ with $f(a) = f(b)$ for $a < b$ has a derivative $f'(c) = 0$. Bishop's constructive version introduces $|f'(x)| \leq \epsilon \; with \; \epsilon > 0$ for moduli of continuity of f' and differentiability of f. In other words, Bishop defines more precisely the limits of the real interval $[a, b]$ much in the manner of Kronecker for Bolzano's theorem on intermediate values (see Gauthier [5] and [8]). However, Gel'fond's work is in analytic number theory and constructive number theory, not in constructive analysis. His results in transcendental number theory are algebraic in nature. The main theorem in Gel'fond and Linnik ([10] chap. 12) states that « if $\omega \neq 0$ is an algebraic real, than with e the base of natural logarithms e^ω is not algebraic » and is couched in the language of algebraic integers in finite fields. A finite field is also the arena

for an another elementary proof ([10] chap.10), Hasse's theorem on integral solutions for the equation :

$$p^2 \equiv x^3 + ax + b \pmod{p} \tag{7}$$

for integers a, b and a prime p > 3. Gel'fond formulates his solution in terms of an inequality

$$|N - p| < 2\sqrt{p} \tag{8}$$

where N is the number of integral solutions of the equation. Here, the language used is the language of polynomials and divisors with an algebro-geometric interpretation and Gel'fond quotes a major result of André Weil on Riemann's hypothesis in function fields (see Weil [13], [14]). Weil's result is a special case of the Riemann hypothesis for quadratic finite fields with a finite number of elements or points on a projective surface and Weil claims that his result is free of the transcendental theory, that is of analytic number theory. The main arithmetical tool here is the theory of forms or homogeneous polynomials. That theory has been developed first in great generality by Kronecker in his « *Allgemeine Arithmetik* » or general arithmetic (see Gauthier [7]) and Weil has repeatedly refered to Kronecker as the founding father of algebraic – arithmetic geometry on finite fields. Kronecker's theory of forms is equivalently a divisor theory (of modular systems) for which infinite descent works, since homogeneous polynomials are finite (integral and rational) functions with integer coefficients and indeterminates (variables).

3 Hensel's theory of p-adic numbers

Let us start with the well-known Hensel's lifting lemma. Hensel's lemma simply states that if the polynomial $f(x) \in \mathbf{Z}p$ has a (simple) root $r \in \mathbf{Z}p$ which satisfies

$$f(r) \equiv 0 \bmod p, f'(r) \not\equiv 0 \bmod p \tag{9}$$

where $f'(r)$ is the arithmetic derivative $(r^n)' = rn'^{n-1}$, then there is a unique $s \in Z/pZ$ such that

$$f(s) \equiv 0 \bmod p^{k+m} \text{ and } r \equiv s \tag{10}$$

for positive integers k, m with $k \leq m$. One can now lift a root r of the polynomial $f(x)$ mod p^k to the new root s mod p^{k+1} to the effect that the roots of mod p^k are lifted to mod p^{k+1}. For p-adic integers, one can write for the roots r and s the formula

$$s = r - \frac{f(r)}{f'(r)} \tag{11}$$

and the roots mod p^k or higher powers of p are better and better approximations to a p-adic root. If we look at polynomials with integer coefficients a and indeterminates x

$$f(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1} + a_n \tag{12}$$

as *finite* formal power series with decreasing powers, we can see the indeterminate x becoming smaller and smaller meaning that it is the same modular process for the composition and the decomposition of approximations.

Hensel's lifting lemma is analogous to Newton's geometric (polygon) method for locating the real root of a differentiable function, but the algebraic approach with p-adic integers has the advantage of being constructive for it allows for a simple finite nonlinear calculus. The iterative process on powers constitutes progressively finer approximations since the initial congruence at level $k = 1$ is a linear approximation (of degree 1). The nonlinear ladder, quadratic $k = 2$ and higher degree polynomials in Kronecker's paper (see [11]) of algebraic integers can be ascended for the composition of congruences as in Hensel's lemma or descended in the decomposition of powers as in Kronecker's theory of forms. In both cases, a finite process of construction steps is of the essence, in Hensel's terms « a finite number of trials » (*eine endliche Anzahl von Versuchen*), an expression he used to characterize Kronecker's finitist programme.

In his 1897 paper on a new foundation of the theory of algebraic numbers (*Über eine neue Begründung der Theorie der algebraischen Zahlen*) [4], Hensel introduces his theory of p-adic numbers by emphasizing the analogy between the theory of algebraic functions of one variable and the theory of algebraic numbers following in the footsteps Kronecker's major work [11]. Hensel puts down two formulas as the foundations of his theory

$$f(x) = a_0x^n + a_1x^{n-1} + ... + a_n = a_0(x - x_1)...(x - x_n) \tag{13}$$

and

$$f(x) = 0 \pmod{p^m} \tag{14}$$

for M the power of prime p. His idea is to associate ramification points of an algebraic function to (rational) ramification places of a prime polynomial in a locally finite field. Hensel's intention was to use infinite power series in arithmetic while Kronecker insisted that one does not need the full formal power series beyond (homogeneous) polynomials of finite degree. However p-adic number theory involves infinite degree polynomials in an algebraic number field $\mathbf{F}$, a finite extension of the rational field $\mathbf{Q}$. We denote an infinite prime p as p^∞. In that context,we can formulate the following proposition

Theorem 2. *The infinite prime p^∞ cannot be represented in the ordinal polynomial of Cantor's normal form for transfinite numbers of the second class up to ϵ_0.*

Proof. An infinite prime p^∞ is a p-adic valuation

$$v_p : \mathbf{Z} \to \mathbf{N} \tag{15}$$

defined as

$$v_p(n) = max : \{v \in \mathbf{N} : p^v/n\} \text{ if } n \neq 0, \text{ otherwise } \infty \text{ if } n = 0 \tag{16}$$

where v is the highest exponent for p^v to divide n and Hensel lemma comes in to lift p to any finite power. From a set –theoretic point of view, the set

$$\{0, p^\infty\} \tag{17}$$

is a final segment of the well-ordered set of the ω's in the second number class. Since there is a countably infinite set of infinite primes over p^∞ and although $\mathbf{Z}_p$, the ring of prime integers and $\mathbf{Q}_p$ the field of fractional prime numbers are both uncountable sets, the set $\mathbf{Z}_p/p^n\mathbf{Z}$ is countable and must be counted as belonging to Cantor's second class of ordinals up to ϵ_0, which itself contains a countably infinite set of primes in the sequence of the ω's. But the final segment $\{0, p^\infty\}$is not expressible as an isomorphism type in that sequence since its order type is incomparable or irreducible to any n in the ordinal polynomial and is therefore not representable in Cantor's normal form. □

4 Conclusion

The results of this paper show the limitations of the set-theoretic expressive power of Cantor's normal form. Kronecker, the harsh opponent to Cantor's transfinite arithmetic, seems to be vindicated here for he has a proposed a general arithmetic (*allgemeine Arithmetik*) of polynomials with integer coefficients and indeterminates in the form

$$P = b_0x^n + b_1x^{n-1} + ... + b_{n-1} + b_n \tag{18}$$

for a finite sum of finite powers

$$\Sigma\ b^n x_n \tag{19}$$

instead of the sum

$$\Sigma\ \omega^\alpha z_\alpha \tag{20}$$

for Cantor's transfinite ordinals. Kronecker's idea was to give an arithmetical foundation of algebraic quantities (*algebraische Grössen*) and his indeterminates were dummy variables to be replaced by real quantities. Kronecker had credited Gauss for the introduction of indeterminates (*indeterminatae*)

and later usage has dubbed them *transcendentals* or *infinites* (see Weil [15]). Hensel, who was a student of Kronecker like Cantor (for a little while), has extended Kronecker's ideas into p-adic number theory in the same arithmetical-algebraic spirit. Hermann Weyl in his *Algebraic Number Theory* book of 1949 (see [17]) has stressed the foundational significance of Kronecker's algorithmic approach over Dedekind's ideal theory and Hensel points out that he has laid down his new foundation of algebraic number theory independent of ideal theory. André Weil on his side has made good of Kronecker's programme in his own work in number theory and algebraic geometry (see [16]). The morale of this story, if need be of any morale, might be an indication of the preeminence of algebraic number theory over transfinite set theory in the constructivist foundations of mathematics and mathematical logic. While the set-theoretical model theory and proof theory of classical logic uses profusely (see Gauthier [6]) transfinite induction on ordinals as being part and parcel of the Cantorian tradition, the more arithmetical and algebraic constructivist approach in mathematics and logic should profit from the Kroneckerian heirdom in the logico-arithmetical foundations of mathematics.

References

[1] A. Baker, *Transcendental Number Theory*, Cambridge University Press, London, 1987.

[2] E. Bishop, *Foundations of Constructive Analysis*, McGraw-Hill, New York, 1968.

[3] E. Cantor, *Gesammelte Abhandlungen*, E. Zermelo (ed.), Georg Olms Verlag, Hildesheim, 1966.

[4] K. Hensel, Über eine neue Begründung der Theorie der algebraischen Zahlen, *Jahresbericht der Deutschen Mathematiker-Vereinigung*, **6** (1899), no. 3, 83-88.

[5] Y. Gauthier, *Internal Logic. Foundations of Mathematics from Kronecker to Hilbert*, Springer, Kluwer, Dordrecht/Boston/London, 2002. https://doi.org/10.1007/978-94-017-0083-2

[6] Y. Gauthier, Classical Function Theory and Applied Proof Theory, *International Journal of Pure and Applied Mathematics*, **56** (2011), no. 2, 223-233.

[7] Y. Gauthier, Kronecker in Contemporary Mathematics. General Arithmetic as a Foundational Programme, *Reports on Mathematical Logic*, **48** (2013), 37-65.

[8] Y. Gauthier, *Towards an Arithmetical Logic. The Arithmetical Foundations of Logic*, Birkhäuser/Springer, Basel, 2015.
https://doi.org/10.1007/978-3-319-22087-1

[9] A. O. Gel'fond, Sur le Septième Problème de Hilbert, *Comptes Rendus Acad. Sci. URSS*, Moscou **2** (1934), 1-6.

[10] A. O. Gel'fond and U. V. Linnik, *Elementary Methods in Analytic Number Theory*, Rand McNally and Co., 1965.

[11] L. Kronecker, Grundzüge einer arithmetischen Theorie der algebraischen Grössen, in *Leopold Kroneckers Werke*, K. Hensel (ed.), Vol. III, 1968, Teubner, Leipzig.

[12] K. Mahler, An interpolation series theorem for continuous functions of a p-adic variable, *J. Reine Angew. Math.*, **199** (1958), 29-34.

[13] T. Schneider, Transzendenzuntersuchungen periodischer Funktionen I. Transzendenz von Potenzen, *Journal für die Reine und Angewandte Mathematik (Crelle's Journal)*, **1935** (1935), no. 172, 65-69.
https://doi.org/10.1515/crll.1935.172.65

[14] T. Schneider, Transzendenzuntersuchungen periodischer Funktionen II. Transzendenzeigenschaften elliptischer Funktionen., *Journal für die Reine und Angewandte Mathematik (Crelle's Journal)*, **1935** (1935), no. 172, 70-74. https://doi.org/10.1515/crll.1935.172.70

[15] A. Weil, L'arithmétique sur les courbes algébriques, in *Œuvres Scientifiques Collected Papers*, Vol. I, Springer-Verlag, New York, 1979, 11-45.

[16] A. Weil, Number Theory and Algebraic Geometry, in *Œuvres Scientifiques Collected Papers*, Vol. III, Springer-Verlag, New York, 1979, 442-452.

[17] H. Weyl, *Algebraic Number Theory*, Princeton University Press, Princeton, N. J., 1940.

Received: May 2, 2018; Published: June 2, 2018