Studies in Universal Logic

Yvon Gauthier

Towards an Arithmetical Logic

The Arithmetical Foundations of Logic

Birkhäuser

Birkhäuser

Studies in Universal Logic

This series is devoted to the universal approach to logic and the development of a general theory of logics. It covers topics such as global set-ups for fundamental theorems of logic and frameworks for the study of logics, in particular logical matrices, Kripke structures, combination of logics, categorical logic, abstract proof theory, consequence operators, and algebraic logic. It includes also books with historical and philosophical discussions about the nature and scope of logic. Three types of books will appear in the series: graduate textbooks, research monographs, and volumes with contributed papers.

More information about this series at http://www.springer.com/series/7391

Yvon Gauthier

Towards an Arithmetical Logic

The Arithmetical Foundations of Logic

Birkhäuser

Yvon Gauthier
University of Montreal
Montreal
Québec, Canada

ISSN 2297-0282 ISSN 2297-0290 (electronic)
Studies in Universal Logic
ISBN 978-3-319-22086-4 ISBN 978-3-319-22087-1 (eBook)
DOI 10.1007/978-3-319-22087-1

Library of Congress Control Number: 2015949819

Mathematics Subject Classification (2010): 01-02, 03-02, 03-A05, 13F-20, 14-02

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media
(www.birkhauser-science.com)

Dedicated to the memory of the great
arithmetician André Weil

Foreword

The project of an arithmetical logic has been in the making for many years and the present work is the continuation of my 2002 book *Internal Logic. Foundations of Mathematics from Kronecker to Hilbert* (Kluwer, Dordrecht). In the intervening years, I have pursued the programme and I have published many scientific papers and a book in French on the subject. The progress made towards an arithmetical logic is here recorded, but the idea of an internal logic of arithmetic has not been altered. It is still the inner structure of classical arithmetic or number theory, which is the objective of the foundational enterprise. I have baptized that arithmetic the Fermat-Kronecker (FK) arithmetic and I have constantly opposed it to Peano arithmetic. What I have been trying to show is that there is no set-theoretic element in pure arithmetic, while Peano or Dedekind-Peano formalized arithmetic is embedded in a transfinite set-theoretic framework. Kronecker's finitist stand in mathematics extends from Hilbert to contemporary constructive mathematics, e.g. Bishop's constructive analysis and Nelson's predicative arithmetic. Gödel's ‹extended finitism› of the *Dialectica Interpretation* could be counted as a mitigated reappropriation of Kronecker's radical constructivism via Hilbert's introduction of functionals inherited from Kronecker's higher-order forms (polynomials). This is one of the main themes I have proposed in the recent years.

The central thesis of this book has been expanded to cover the constructivist insights in physics and mathematical physics, from relativity theory to quantum physics and cosmology where I have attempted to explore the ramifications of the constructivist-finitist motives. My objective here has been to elaborate on the foundational aspects of arithmetical logic—the proper name of which I have dubbed modular polynomial logic—with incursions in probability theory and theoretical and mathematical physics. At the same time, I have been trying to see what is conceptually (and technically) going on in contemporary ‹real› mathematics from the constructivist viewpoint of arithmetical foundations, without too much prejudice as to what constitutes mathematical practice with or without foundational concerns. Still, needless to say that constructivist foundations are inherently critical of mathematical (and logical) practice in classical logic and classical mathematics, but the critique comes from within, that is without invoking principles that are alien to mathematical activity in its historical, epistemological and rational pursuits.

In that endeavour, the main source of my inspiration remains André Weil with whom I discovered both Fermat and Kronecker in the 1980s. Early on, André Weil had encouraged me in correspondence to explore further the mathematical virtues of Fermat's method of infinite descent and I discovered at the same time the importance of Kronecker's general arithmetic in Weil's original writings on algebraic geometry (see his *Œuvres scientifiques. Collected Works*, Springer-Verlag, 3 vols, 1980)—see my review Gauthier (1994b) of Weil (1992). Weil has put Kronecker's theory of forms or homogeneous polynomials and his divisor theory (moduli systems) at the very beginning of algebraic-arithmetic geometry with the emphasis on finite fields where Fermat's infinite descent is at work. I must also acknowledge the beneficial exchanges I have had over a period of years, either in personal contacts or in correspondence with Henri Margenau, A. Wheeler, E.P. Wigner, I.M. Segal, G. Chew, René Thom, N.A. Shanin, H.M. Edwards, Ed Nelson, G. Kreisel, Y. Gurevich, U. Kohlenbach, H. Putnam, D. van Dalen, A. Urquhart, A. Joyal, Bas van Fraassen either for scientific counsels, critical assessments or friendly approvals. All have contributed to my understanding of the many facets of foundations, may they be logical, mathematical, physical or philosophical.

In the writing of this opus, I have drawn freely from previous work, my two books on the subject *Internal Logic* mentioned above and *Logique arithmétique. L'arithmétisation de la logique* (PUL, Québec, 2010) and numerous papers that have appeared in recent years in a variety of scientific journals, *Synthese*, *Logique et Analyse*, *Revue internationale de philosophie*, *Foundations of Science*, *International Studies in the Philosophy of Science*, *Reports on Mathematical Logic*, *International Journal of Theoretical Physics*, *Journal of Physical Mathematics*, *International Journal of Pure and Applied Mathematics* and *Reports on Mathematical Physics*. Some of the ideas that are still on the forefront here have appeared in earlier publications in *Modern Logic*, *Zeitschrift für mathematische Logik und Grundlagen der Mathematik* and *Archiv für mathematische Logik und Grundlagenforschung*, *Zeitschrift für allgemeine Wissenschaftstheorie*, *Notre-Dame Journal of Formal Logic*, *Dialectica* and *Philosophy of Science*, but those ideas have taken on new clothes in my up-to-date synthesis. I have completed the writing of this work in the summer and fall of 2014, not without the assistance of my two LaTeX men, David Montminy and Benoit Potvin. Benoit Potvin has made it possible for me to be up to the requirements of scientific journals by diligently latexizing my papers in the last five years. He is here thanked for his expertise as a computer scientist. I also wish to thank the Canadian Research Council (SSHRC) for funding my research in the last four years (and many years before!). Finally, I am grateful to Jean-Yves Béziau who has had a sympathetic ear and a friendly reception to my work over the years.

Montreal
August 2015

Yvon Gauthier

Contents

Chapter 1
Introduction: The Internal Logic of Arithmetic

The idea of an internal logic of arithmetic or arithmetical logic is inspired by a variety of motives in the foundations of mathematics. The development of mathematical logic in the twentieth century, from Hilbert to the contemporary scene, could be interpreted as a continuous tread leading to arithmetical logic. Arithmetization of analysis with Cauchy, Weierstrass and Dedekind and arithmetization of algebra with Kronecker have lead to the foundational inquiries initiated by Hilbert. Frege's logical foundations of mathematics, mainly arithmetic, have contributed to clarify philosophical motives and although Frege's logicism has not achieved its goals, it has given birth to Russell's theory of types and to some extent to Zermelo's set-theoretic cumulative hierarchy while launching philosophical logic and philosophy of language. But the "arithmetism" I have in mind here is mostly anti-Fregean in that in turns logicism upside down and asks the question: "how far can we go into logic with arithmetic alone" rather than the Fregean question: "how far can we go into arithmetic with deductive logic alone?" It is Kronecker's polynomial arithmetic that guides here and the purpose of this book is to see how far a Kroneckian constructivist program can go in the arithmetization (and algebraization) of logic in the twenty-first century. The present work has been conceived has a sequel to my 2002 book *Internal Logic, Foundations of Mathematics from Kronecker to Hilbert* (Kluwer) and as a continuation of my efforts towards an arithmetical logic.

Hilbert is the starting point in the arithmetization process of logic; he is the one who introduced logic into mathematics and if he wanted to provide foundations for logic and arithmetic at the same time, he realized later on that logic should be arithmetized in order to provide a consistency proof for arithmetic and he adopted finally a finitist foundational stance reminiscent of his former teacher, Kronecker. Skolem wanted also a finitist arithmetic and Brouwer's theory of choice sequences with his assignment of natural numbers to members of a species (set) and sequences was a predecessor to Gödel's arithmetization of syntax (formal system). The birth certificate of model theory, Tarski's method of quantifier elimination, can be traced to Kronecker's theory of substitution-elimination of indeterminates. The proof theory of first-order arithmetic and its subsystems is another witness to the arithmetization program and finally the idea of algorithm and

Y. Gauthier, *Towards an Arithmetical Logic*, Studies in Universal Logic,
DOI 10.1007/978-3-319-22087-1_1

ramifications in complexity theory, in computer algebra and in theoretical computer science counts certainly as one of the major achievements of such a programme. Cantor's transfinite arithmetic is also part of the arithmetization of analysis and we could pinpoint the reasons why the Cantorian enterprise has ended in transarithmetical transfinite set theory. And can analysis be constructivized? Brouwer said yes, to a certain extent. Bishop thought that it could be arithmetized, that is, have numerical content. Non-standard analysis with Robinson's hyperreals goes even further in trying to give some content to infinitesimals. Cantorian set theory has nevertheless become the standard semantics of classical logic and Peano arithmetic and it is not easy to disentangle the arithmetical syntax from the set-theoretical semantics of contemporary logical theories, may they be Martin-Löf's constructive or intuitionistic type theory and other alternatives like reverse mathematics and Feferman's predicative mathematics. Only Nelson's predicative arithmetic stands out as a radical program, but it is considered too restrictive to serve as a foundational guideline.

From a more philosophical viewpoint, Yessenin-Volpin's ultrafinitism is out of touch with actual practice and Wittgenstein's finitist views do not seem to have grasped the full extent of mathematical logic in the twentieth century. What is at stake is not the existence of mathematical or logical entities, the ideal elements Hilbert had introduced to eliminate them afterwards as a mere detour, nor the objectivity of public mathematical construction, but the arithmetical, ultimately computational, content of logical or mathematical theory. The objectual reality of mathematics can be summarized as the different ways it counts physical objects and non-physical entities and how it accounts for the uncountable, if at all. Kronecker's attitude in that matter has been largely misinterpreted and it must be emphasized that Kronecker's polynomial arithmetic, which he called general arithmetic "*allgemeine Arithmetik*", has been a central theme in the advent of abstract algebra. One must keep in mind that contemporary algebraic or arithmetic geometry has originated in Kronecker's work on elliptic functions, as has been pointed out by André Weil, and Kronecker's arithmetical ideal could be tracked in present-day grandiose programmes of Langlands and Grothendieck. Algebraic number theory has also benefited immensely from Kronecker's arithmetic theory of algebraic quantities—that is the subject matter of his 1882 seminal paper dedicated to Kummer—and Hermann Weyl has stressed the advantages of the Kroneckerian theory of domains of rationality over Dedekind's ideal theory.

Elementary or ordinary number theory was the arena of the first axiomatisations by Dedekind and Peano. Recursive functions and the idea of recurrence made an early appearance. Dedekind is supposed to have introduced that mode of thought in his "*What are and what should be numbers*"—"*Was sind und was sollen die Zahlen*" but the procedure is implicit in Kronecker's theory of forms (homogeneous polynomials). Dedekind's and Peano's axiomatisations are based on Cantorian set theory and they are impregnated in a set-theoretic semantics which obnubilate the arithmetical motivations. Hilbert will be more aware of that arithmetical background in his metamathematics devoted to formalized mathematics in a finite system of arithmetical operators and polynomials equations (and inequations).

Kronecker's work has been ignored, except by mathematicians. Logicians and philosophers know only his "*On the concept of number*" (*Über den Zahlbegriff*), not his most important work by far. Frege mentioned Kronecker only once and characterized him as an empiricist, in the like of Helmholz—which Kronecker quotes at the end of his "*On the concept of number*"—then discrediting him as a non-logician. Most people associated Kronecker with his dictum stating that "Integers are the creation of God, the rest is the creation of man", which is not to be found in Kronecker's writings, but is probably attributed to him by association! Hilbert, maybe with some resentment towards his former professor, depicted him as a "*Verbotsdiktator*" or dictator of interdiction.

Arithmetization of logic took place without the contribution of the algebra of logic before Tarski. De Morgan, Boole, Peirce, Schröder and Löwenheim were not part and parcel of the process, except that Boole was influential in the algebrization of classical elementary logic, which he linked to the theory of probability in his 1854 *An Investigation of the Laws of Thought*. But what should be emphasized at this point is the separation of arithmetic from number theory. The tradition of number theory from Fermat, Euler, Gauss, Legendre, Lagrange, Dirichlet up to Kummer, Kronecker's cherished professor, has developed autonomously, as the queen of sciences, as Gauss would name it. Classical number theory is not on the same footage as Dedekind-Peano arithmetic and one should make it clear that there is no historical connection between number theory and formal arithmetic of logical descent. However arithmetical logic is aimed at bridging the gap between logic and arithmetic (the "true" arithmetic of number theory) and this is why I shall be using extensively Fermat's method of infinite descent still prominent in the work of contemporary number-theorists from Mordell to Weyl. Infinite descent combined with Kronecker's polynomial arithmetic will reveal an essential ingredient of the program of an arithmetical logic that I want to confront here with alternative programs in the foundations of mathematics. In so doing, I hope to connect historical, philosophical, logical, mathematical and foundational questions—foundations being the synthesis of all—into a unified treatment and propose a new framework for the philosophical question and the mathematical problem of the consistency of arithmetic. The programme of arithmetical logic finds its final justification in the internal logic of arithmetic, an internal logic that shows that arithmetic has to be self-consistent if it is to be the building stone of logic and mathematics.[1]

[1] In the following, all translations from French, German, Russian, Italian and Latin are mine.

Chapter 2
Arithmetization of Analysis and Algebra

Arithmetization of analysis evokes at once the names of Cauchy, Weierstrass, Cantor and Dedekind and to a lesser degree those of Dirichlet, Abel or Bolzano; the process of arithmetization illustrates the need to instill rigour in analysis through what Cauchy called algebraic analysis in order to overcome the intuitive limitations of the geometer's method of proof. The story of arithmetization needs not to be retold here (see Grattan-Guinness 1970); it is not a one-sided history, for rigour had a different meaning then and the tools used for rigorization (e.g. quadratic forms or homogeneous polynomials) were partly available in the nineteenth century. The algebraic symbolism (Descartes, Fermat and Leibniz) was already invading geometry and number theory (Diophantine equations) from Fermat on was to become the queen of arithmetical sciences.

2.1 Cauchy and Weierstrass

In the introduction of his 1821 *Cours d'analyse*, Cauchy warns that: "It would be a serious error to think that certainty can be found only in geometrical demonstration or in the testimony of the senses", but he begins with an algebraic analysis of real functions and their limits, polynomials as continuous functions and of convergent and divergent series. Cauchy still talks of infinitively small quantities or infinitesimals, but he equals them with limits approached by real-valued functions. He introduces there the convolution product—also named Cauchy product—for convergent series and recursive series ("*séries récurrentes*") or polynomials in the increasing or decreasing order of their powers. Cauchy achievement resides in his precise definitions of limits 0 and ∞ for an infinite quantity.

> When the successive values given to the same variable approach indefinitely a fixed value in such a way as to differ from it as little as one wishes, this fixed value is called the limit of all the other values (Cauchy 1847, p. 14)

Weierstrass has not been satisfied with Cauchy's notion of a variable approaching a limit. In his text "*Theorie der Maxima und Minima von Functionnen einer und mehrerer*

Y. Gauthier, *Towards an Arithmetical Logic*, Studies in Universal Logic,
DOI 10.1007/978-3-319-22087-1_2

Veränderlichen" or *Theory of maxima and minima of functions of one and many variables*, Weierstrass innovates with his idea of the $\epsilon - \delta$ method.

> For a function $f(x)$, one says that its value at $x = a$ is a minimum when it is smaller for $x = a$ than all the neighboring values of x, that is when a positive quantity δ can be determined such that
>
> $$f(a + h) - f(a) > 0$$
>
> with $|h| < \delta$. And the values of a function $f(x)$ for $x = a$ is called a maximum, when for all values under the restriction $h < \delta$, one has
>
> $$f(a + h) - f(a) < 0$$
>
> (Weierstrass 1894–1927, p. 7)

Weierstrass then shows that for the derivative

$$f(a + h) - f(a) = hf'(a + \epsilon h)$$

a quantity is needed with the sufficient condition

$$0 < \epsilon < 1$$

and the first necessary condition for the existence of a minimum or a minimum for $f(x)$ at $x = a$ is that $F'(a) = 0$; the second necessary condition is that in the sequence of derivatives the first non-vanishing derivative for $x = a$ must be of even order. Weierstrass goes on and generalizes easily these conditions to many-variable functions (Weierstrass 1894–1927, p. 7).

The interesting fact here is that Weierstrass couches his ideas in the language of quadratic forms (homogeneous polynomials): these are the arithmetical foundations by excellence in the number-theoretic tradition since Gauss. Of course Bolzano has already proven that polynomials are continuous and Weierstrass had only to define a vanishing positive definitive form as one whose variable have all the value 0 (Weierstrass 1894–1927, p. 20). Further considerations have to do with Sturm's theorem on changed signs in the real roots of an algebraic equation; Kronecker had also dealt with refinements of Sturm's theorem as he has criticized Bolzano's intermediate value theorem for being imprecise, since the interval for the values was not defined, although Bolzano had believed to arithmetize the geometrical intuitive proofs for continuous functions. But Cantor and Dedekind will give a new twist of the history of arithmetization in extending the more or less constructive methods of their predecessors into a new array of non-constructive techniques.

2.2 Dedekind and Cantor

From Dedekind's side, arithmetization is a logical enterprise to the extent that proof and provable are interwoven in mathematical constructions, and the logic he has in mind is internal to arithmetic or the science of number ("*Wissenschaft der Zahlen*"). Irrational numbers, Dedekind insists, must be grounded arithmetically, but foundations have to be general or abstract, for the science of number is *a priori*, independent of space and time; this is why Dedekind speaks of things and systems of things as the building blocks of arithmetic (Dedekind 1965). Soon enough, those concrete building blocks will be assembled by abstract concepts like mappings (*Abbildungen*) and images (*Bilder*). Chains (*Kette*) remain the concrete links for the assembly-line of things and systems. In Dedekind chain of thought however, the highest point is his unification of an infinite system as a system which is in bijection with a proper part of itself, that is excluding itself; otherwise, a system is finite. The proof of the statement has been diversely appreciated—some have downgraded it as a metaphysical or psychological proof—it involves "the world of my thoughts" ("*meine Gendankenwelt*") as an actual infinite system, while Dedekind expressly says that the world of my thoughts, that is the totality of things that can be objects of my thought, is infinite, which points out to a potential infinite at most (Dedekind 1965, p. 14). It is not without reason that Dedekind notes that there is a similar consideration in the Platonist Bolzano. One could say there is a clash here between the arithmetical potentialities and the set-theoretical actuality of the transarithmetical or transcendental world.

In Dedekind's hands, the construction of the natural number system with complete induction as a simply infinite bijection system $N \rightarrow N$ is straightforward. In a sharp contrast, the construction of the rational and irrational numbers in his "*Stetigkeit und irrational Zahlen*" (Continuity and irrational numbers) is completed in a purely arithmetical style, as if we are entering the real mathematical world with rational and irrational numbers. Dedekind's writes:

> I see the whole arithmetic as a necessary or at least as a natural consequence of the simplest arithmetical act of counting, and counting itself as nothing more than the successive creation of the unending sequence of positive whole numbers (integers)... (Dedekind 1965, II, p. 5)

The idea of a chain is born out of the step by step unfolding of numbers in their natural succession, rational numbers when compared to a point or straight line, are situated on the right or on the left of a given point and on the continuous line there is an infinity of points which do not correspond to any rational number. The essence of continuity lies in the principle:

> If we cut the straight line in two segments (or classes) in such a manner as to put all the points of the first segment to the left of any point of the second segment, then there is only one point that divides all the points in two segments of the straight line. (Dedekind 1965, II, p. 10)

A cut ("*Schnitt*") (A_1, A_2) has the meaning that every rational number in A_1 is smaller than any number in A_2 and also that there is either a largest number in A_1 or a smallest number in A_2. It follows immediately that there is an infinity of cuts in the straight line that are not generated by rational numbers which therefore do not exhaust the whole continuous line. So an irrational number like $\sqrt{2}$ is represented by an irrational cut. Total order and Dedekind-completeness of the real line are properties directly following from the cut construction, since supremum and infimum are consequences of the theorem that there is only one number that cuts the system of all real numbers in two. Dedekind also saw his theory of cuts as applying easily to differential calculus or infinitesimal analysis because of the centrality of the concept of continuity.

Of greater importance to us is Dedekind emphasis on the arithmetic construction of the real continuum; for him, the main guiding principle, despite the set-theoretic overtones, is the arithmetic process that extends in a natural way ordinary arithmetic into higher arithmetic (number theory and algebra) and analysis. In the same arithmetical spirit, Cantor went even further into a transfinite arithmetic that would exhaust not only the real line, but also the real arithmetic spirit itself by immersion in the set-theoretic universe!

At the beginning, Cantor was interested in number theory and algebra, as his first writing reveals. Indeed, his 1867 dissertation deals with quadratic forms (homogeneous polynomials) and one of his thesis is that purely arithmetical methods prevail over analytical ones. These writings seem to be mere exercises on problems raised by number-theorists from Gauss to Kronecker (his professor in Berlin) until he reaches the rich terrain of trigonometric functions where his mathematical talent finds its start. Cantor inherits from Riemann and Heine the problem of how to represent a real-valued function $f(x)$ by a convergent trigonometric series for all the values of x and show that there is no other series of the same form which is convergent and uniquely represent the said function $f(x)$. In other words, it is the problem of the canonical representation of a real-valued function by a trigonometric series. In the course of his work on the canonical representation, Cantor came to benefit from Kronecker's comments for a simplification of his proof; the simplification amounted to evince infinitesimals by using two arithmetical expressions $y + x$ and $y - x$ where y is a constant in order to cancel or make vanish the infinitesimal coefficients

$$\lim(c_n nx) = 0 \quad \mathit{for} \;\; n = \infty$$

It is interesting to note that Cantor's rejection of infinitesimals originates in Kronecker's arithmetization program. But Cantor was quick to find another use for his finite limits in his theory of derived sets of points. As I said, Cantor did not rest content with the arithmetical simplifications (or restrictions) suggested by Kronecker and went on extending his results on trigonometric series in 1872. Here Cantor develops a theory of limit points ("*Grenzpunkte*") or accumulation points ("*Häufungspunkte*"), which is of geometric inspiration (with Cartesian coordinates) even if it looks like Weierstrass' arithmetical theory from the outside. Cantor's infinitary inclination is apparent in his propension to include the infinite as well as the finite in his mathematical research.

The limit point of a set of points P is a point on the straight line such that every neighborhood of that point contains an infinity of points, but in the interior ("*in seinem Innern*") of the (real) interval. We have here the first lineaments of point-set topology. Cantor denotes P' the set of limit points as the first derived set of points of P, if that derived set of points contains an infinite number of points, P has a second derived set of points denoted by P'' and so on till $P^{(v)}$ for the vth derived set of points. The construction of an unending series of derived sets of points opens the way for a theory of fundamental sequences, defined by

$$\lim_{v \to \infty} (\alpha_{v+\mu} - \alpha_v) = 0$$

and in general

$$\lim_{v \to \infty} \beta_v = \beta.$$

Those sequences remind us of Cauchy sequences, but where Cauchy and his followers saw a limit, Cantor took that limit symbol as a radical departure from traditional views. He wrote:

> One should pay attention to this cardinal point, the significance of which could easily be misunderstood in the third definition of the real number—with the help of fundamental sequences as in
>
> $$\lim_{v \to \infty} \alpha_v = b$$
>
> number b is not defined as the bound ("*Grenze*") of the parts of a fundamental sequence (α_v), it would be a logical mistake similar to our discussion of the first definition—of a limit as a sum—where the existence of the bound
>
> $$\lim_{v \to \infty} \alpha_v$$
>
> would only be presumed; it is much more the other way around, since from our former definitions of the concept with its properties and relations in the rational number system we can conclude with certainty that the limit exists and is equal to b. Forgive my insistence on this apparent trifle ("*Kleinigkeit*")... (Cantor 1966, p. 187)

Cantor goes on and declares that the irrational numbers derive the same status of determinate reality in our mind ("*bestimmte Realität*") as do the rational numbers. Then

$$\lim b_v = b$$

also exists and arbitrary high orders of fundamental sequences exist as well. I see in this passage the birth certificate of transfinite set theory with the unlimited generation of orders of fundamental sequences becoming infinite ordinals of the second number class

$$\omega, \omega + 1, \ldots, \omega^2, \ldots, \omega^\omega, \omega^{\omega^{\cdot^{\cdot^{\cdot^{\omega}}}}}, \epsilon_0$$

defined by

$$\lim_{n \to \omega} \omega^{\omega^{\cdot^{\cdot^{\cdot^{\omega}}}}} \}^n = \epsilon_0$$

and more explicitly

$$\begin{aligned} \omega &= \lim < 0, 1, 2, \ldots n > \\ \omega \cdot 2 &= \lim < \omega n > \\ \omega^2 &= \lim < \omega \cdot n > \\ \omega^\omega &= \lim < \omega^n > \\ \omega^{\omega^\omega} &= \lim < \omega^{\omega^n} > \\ \epsilon_0 &= \lim < \omega^{\omega^{\cdot^{\cdot^{\cdot^{\omega}}}}} \} \, n > \end{aligned}$$

Cantor even imagined a third number class

$$\epsilon_0, \epsilon_v, \ldots \epsilon_\omega, \epsilon_{\omega+1}, \ldots$$

in a transfinite hierarchy of ordinals, but the totality Ω of all ordinals like the totality (ת, taw) of all cardinals would not be a set, but an absolute inconsistent plurality ("*eine absolut inkonsistent Vielheit*").

There is no doubt however that Cantor conceived his theory of transfinite numbers as an extension of the arithmetic continuum. He explained that in the past there has not been a satisfactory logico-mathematical treatment of the continuum (Cantor 1966, p. 190 and ss). The first generation principle ("*Erzeugungsprinzip*"), he explained, was the addition of unity to a given number—the first number class of finite ordinals,—the second generation principle simply applies the same procedure to limit ordinals ω up to ϵ. In the same 1882 paper "On infinite linear sets of (multiplicities) of points" ("*Über unendliche lineare Punktmannigfaltigkeiten*") Cantor formulated his continuum hypothesis

$$\aleph_0 < 2^{\aleph_0} = \aleph_1$$

still unproven. Cantor was probably devising his own "*Mannigfaltigkeitslehre*" or theory of multiplicities in the footsteps of Riemann who had introduced his n-dimensional multiplicities (manifolds) in differential geometry. The analogy is certainly in Cantor's mind when he mentioned n-dimensional continuum, but to his great surprise he found out that n-dimensional continua have the same cardinality ("*Mächtigkeit*") as the linear continuum, that is $c = 2^{\aleph_0}$. Brouwer has shown afterwards that beyond that set-theoretic characterization, there is no homeomorphism between continua of different dimensions.

My intention is not to draw a complete picture of Cantor's set-theoretic landscape, but only delineate the essential elements that will be kept alive in the following tradition of arithmetization.

We know that Hilbert wanted to keep the Cantorian paradise open to ideal elements and he hoped to solve the continuum hypothesis (the first problem of his famous 1900 list), but he returned at the end to the safe haven of Kroneckerian finitism. Peano himself inherited the set-theoretic model for his axiomatic number theory, but he left to others the business of arithmetical logic. Gödel employed Cantor's diagonal method in his incompleteness proof for Peano arithmetic, but he renounced transfinite ordinal arithmetic in his later attempts to prove the consistency of arithmetic.

I give a sketch of the diagonal method in the following. Cantor introduced the diagonal method in his 1890 paper ("*Über eine elementare Frage der Mannigfaltigkeitslehre*") (On an elementary question of the theory of multiplicities), in order to prove that the power set $P(X)$ of an infinite set X is strictly greater than X or card $X <$ card $P(X)$. Already in 1874 (Cantor 1966, pp. 115–118), he had shown that the set $\mathbb{R}$ of real numbers is not denumerable by an argument involving algebraic numbers of the form

$$a_0\omega^n + a_1\omega^{n-1} + \ldots + a_n = 0;$$

here the ω's are simply reals—and the described polynomials have finite degree n and therefore algebraic numbers have a denumerable cardinality. The totality ω of such numbers can be arranged in a sequence

$$\omega_1, \omega_2, \dots, \omega_n, \dots$$

Using Liouville proof in 1844 on the existence of irrational transcendental (non-algebraic) numbers that can only be approximated by rationals, Cantor concludes that if there are more numbers in the real interval than the algebraic irrationals, then they are not denumerable. The diagonal appears at first less as an existence proof and more as a constructive method, but there is less than meets the eye. Cantor starts here with an infinite coordinate system $\mathbb{M}$ of elements with two "characters" m and w and dresses up an infinite array of sequences E of those elements

$$\begin{aligned} E^1 &= (m, m, m, m, \dots) \\ E^2 &= (w, w, w, w, \dots) \\ E^3 &= (m, w, m, w, \dots) \end{aligned}$$

He then supposes that the totality of those sequences is not in bijection with the sequence of natural numbers, is not denumerably infinite with cardinality $\aleph_0$.

One has only to show that the denumerable array of sequences representing real numbers

$$\begin{aligned} E_1 &= (a_{1,1}, a_{1,2}, \dots, a_{1,\nu}, \dots) \\ E_2 &= (a_{2,1}, a_{2,2}, \dots, a_{2,\nu}, \dots) \\ &\dots\dots\dots\dots\dots\dots\dots\dots \\ E_\mu &= (a_{\mu,1}, a_{\mu,2}, \dots, a_{\mu,\nu}, \dots) \end{aligned}$$

does not exhaust $\mathbb{M}$, the set of real numbers in the interval (m, w) or $(0, 1)$ since the sequence

$$E_\nu = (b_1, b_2, b_3, \dots)$$

defined by $b_\nu \neq a_{\nu,\nu}$ is not there, because the elements b_ν are taken to be different from any element a_ν in the diagonal of E_1 to E_μ. The elements b_i are taken on the antidiagonal or on the codiagonal, as I prefer to say, since they are drawn from the complement $\mathbb{R} - \mathbb{N}$ of the presumed list of all natural numbers. Instead of Liouville expression

$$|x - \frac{p}{q}| > \frac{M}{q^n}$$

where x is an algebraic irrational of degree n, p, q and M are integers, we have in Cantor

$$\text{card } \mathbb{N} < \text{card } \mathbb{M}$$

for $\mathbb{N}$ the natural numbers and $\mathbb{M}$ the totality ("*Inbegriff*") of real numbers. Cantor's method is nonetheless existential or non-constructive in the sense that it picks up freely in the complement $\mathbb{M} - \mathbb{N}$ diagonal elements different from all elements in a denumerable diagonal list. Real numbers are more numerous than natural numbers and transcendental numbers are the most numerous among the reals; since the element b_ν is picked up randomly in the complement $\mathbb{M} - \mathbb{N}$, it is most probably a transcendental element. At the end of the 1880 paper, Cantor felt free to embark on his continuing search for larger actually infinite powers ("*Mächtigkeiten*") $\mathbb{M}_0 < \mathbb{M}_1 < \ldots < \mathbb{M}_n$ and believed that their succession constitute a well-ordered set, thus building up on an extension of finite number theory by other means (Cantor 1966, p. 280). But Cantor was now to discover that the totality of all powers did not amount to a consistent set, but to an absolutely inconsistent plurality.

Cantor's diagonal method gave rise to paradoxes, one of them, Richard's antinomy goes like this: suppose that I want to enumerate all sentences in the French language which denote a real number, for instance, the ratio between the circumference and the diameter of the circle, that is π; I then put these sentences in a lexicographical order and call the nth real number of the enumeration the nth Richard number

$$r_n = 0, a_{n1}a_{n2}\ldots a_{nn}$$

in a decimal expansion. Define a diagonal real number; the real number whose nth decimal is 1, if the nth decimal of the Richard number is not 1 and whose nth decimal is 2, if the nth decimal of the Richard number is 1, that sentence defines a Richard number, say the rth Richard number, but it differs from the Richard number previously defined by the rth decimal. What we have is $r_{nn} = 1$, if $a_{nn} \neq 1$ and $r_{nn} = 2$, iff $a_{nn} = 1$; we have a Richard number b_n which is different from all the r_n and consequently it does not belong in the enumeration whilst it is defined by a finite number of letters in the lexicographical order. Gödel was inspired by the paradox, as well as by the liar's paradox, his logical use of Cantor's diagonal method leading him to an undecidable sentence stating of itself that it was not provable. Another logical use of Cantor's theorem—which stipulates that for set x, the cardinality of the set is smaller than its power set—is Skolem paradox which goes like this: in a first-order logical theory, there is no bijection between the set ω of natural numbers and $P(\omega]$ its power set, for a first-order language can only entertain ω being of cardinality $\aleph_0$, but a first-order theory may have a model of arbitrary high cardinality, like $2^{\aleph_0}$, by the Löwenheim-Skolem theorem. The question is : how could a first-order theory say anything about a non-denumerable model? In fact, the set $P(\omega)$ is denumerable in the model of first-order theory as seen from the outside and there is a bijection between ω and $P(\omega)$, but that bijection is not the model as seen from the inside. Such a paradoxical situation is derivable simply because the notion of cardinality and other set-theoretic notions are semantically relative—to a model—or that set-theoretic semantics cannot be absolute or invariant, as Skolem had remarked.

In conclusion, could Cantor's transfinite number theory be counted as a legitimate extension of the arithmetization program like number theory or p-adic analysis? And Conway's surreal numbers, are they an extension of Dedekind's notion of cut? Extensions of number theory and completions (of number fields) are not on the same footing.

One thing is sure, many mathematicians have renounced the Cantorian paradise (among those the so-called French semi-intuitionists or pre-intuitionists, notably Poincaré). André Weil, one of the major number theorists of the twentieth century did not admit Cantor's diagonal method as a valid method of proof in number theory. Weil had constructivist leanings and one of his privileged methods was Fermat's infinite descent which he characterized as a "method of finite descent in finite number fields". For the arithmetician, the denumerable means "denumerable at infinity" and this involves only the unlimited sequence of natural numbers, not a completed actual infinity.

2.3 Frege

Neo-logicism has been milling Hume's principle to rejuvenate Frege's logicism, but the lurking problem is the logical status of the principle (see Burgess 2005). On the face of it, Hume's principle is an abstraction principle that cannot count as being arithmetical in Frege's hands, although in his *Treatise of Human Nature*, Hume was only concerned with numerical equality that we can express

$$\forall R \forall S[(Num\ (R) = Num\ S)) \leftrightarrow R \equiv S]$$

for R and S numerical relations: it says that numerical relations e.g. in algebra, are equal if the numbers they relate are also equal in arithmetic. Hume thought that it is only in arithmetic and algebra and not in geometry, that we can have a perfect exactness of equality (Hume 1978, i, p. 3, 1). Hume's idea accords quite well with the counting process "*Zahlen*" omnipresent in the arithmetization program, whereas Frege deals with concepts and general undetermined objets ("*allgemeine unbestimmte Gegenstände*") and his basic law V in the *Grundgesetze der Arithmetic* (§36) states

$$\forall F \forall G[Ext(F) = Ext(G) \leftrightarrow \forall x(Fx \equiv Gx)]$$

that is, two concepts have the same extension, iff they have the same "general" objects. Law V gives rise immediately to the unlimited comprehension principle

$$\exists x \forall y(y \in x \leftrightarrow P(y))$$

and Russell's contradictory instance when one substitutes general object x for y.

The truth is that new logicism, from C. Wright to G. Boolos, does not so much rehabilitate Frege's logicism as it tries to adopt it to second-order arithmetical theories, for instance Peano's arithmetic, by having recourse to Hume's principle which was arithmetical as a numerical equality. Frege's initial idea of an internal logic of arithmetic was to see how far one could go in arithmetic by deduction alone:

> Wie weit man in der Arithmetik durch Schlüsse allein gelangen könnte, (Frege 1983, X.)

Logical consequence, as Frege says, must mimick the sequential or serial order of arithmetic (addition as a paradigm) insuring thus the uniformity of a process totally independent of intuition. This was also the idea behind his 1874 Jena habilitation work on the methods of calculation “based on the extension of the concept of quantity”. Addition represents then the primary operation or for the foundation of arithmetic or as a conceptualization of arithmetic in the sense that arithmetic remains the archetype of a theory of concepts. This would explain the intention or motivation of Frege’s later work on the notions of concept, object and function or on sense and reference; the resulting philosophy of concept or philosophy of language could then fit into the grand scheme of a general philosophy based on an arithmetical model. My interpretation is not orthodox here for it evacuates the essence of logicism understood as a full-fledged foundation of arithmetic and mathematics on logic. But what if logic is not the formalization of arithmetic, as Frege seems to have taught us? If Frege takes refuge in geometry after his attempt of conceptualization of arithmetic away from intuition and experience, it is because he believed that geometry is the sole source of (experiential) mathematical knowledge and that the spatio-temporal continuum (as in Kant) is the origin of the idea of the infinite; he also acknowledged that his notion of number as the extension of a concept was a failure. One is tempted to say here that concepts play the role of Kronecker’s indeterminates while numbers take the place of integral coefficients in a polynomial expression, the difference being that indeterminates as dummy variables do not have a conceptual or Platonic existence conferred to Frege’s general indeterminate objects: only numbers as counting symbols subsist in the flatland of arithmetic.

The fate of logic in Frege’s project is certainly dependent upon the formalization of the function concept. Function and argument are derived from polynomial functions in arithmetic and Frege is quite explicit on this in his Preface to the *Begriffsschrifft*: his formalization of a “formula language for pure thought” is modeled upon the formula language of arithmetic. In a nutshell, then, Frege’s intent was at first the arithmetization of ordinary (Aristotelian) logic, a project that finally ended in a logicization of arithmetic which could build on the whole of arithmetic up to function theory, i.e. summation and integration. The arithmetical ideal is echoed in the 1877 *Begriffsschrift* where a formalized language is designed to the sole purpose of translating the informal language of arithmetic. There is no sign of “logicization” here, nor in the 1884 *Grundlagen der Arithmetik* in which Frege is satisfied with a logico-mathematical research on the concept of number. All this is still compatible with the arithmetization program and even with the non-logicist mode of speech that one finds in Dedekind and Cantor.

Thus it seems that the logicist program of a logical conceptualization of arithmetic is merely philosophical and is not meant as an alternative to the current arithmetical foundations of mathematics, at least up to the *Grundgezetze* where the philosophical program emerges. But one could interpret Frege’s anti-Kantian or non-aprioristic proposal, not so much as a logicist imperative but as a philosophical motive akin to Leibniz’s *calculus philosophicus* or *ratiocinator*. But the idea of a rational formalism or ideography is purely an extension of arithmetic for the representation of classical logical judgments in the first two parts of the *Begriffsschrift*, whereas the third part deals with a notational representation of sequences that could extend to calculus and even to *analysis situs* (topology) and physics. Frege’s philosophical dream is driven by an arithmetical spirit; it is a pity that

Frege had not taken into account another extension of arithmetic, Kronecker's polynomial or general arithmetic ("*allgemeine Arithmetik*"), a purely mathematical development, in his conceptual enterprise. One could conclude that Frege's formal logic is nothing more than a general arithmetic for the needs of philosophical conceptualization. The fact that Frege's formalization (without its notational system) has facilitated Russell's theory of definite descriptions is a sign of its philosophical fertility, not of its mathematical richness. My interpretation of logicism attempts at showing that Frege's so-called logicist program is born in arithmetic and is not destined to provide foundations for arithmetic and the whole of mathematics, but rather to continue arithmetic by other means.

Formal logic was initiated by Aristotle, it was arithmetized by Frege and made into a fully arithmetized theory by Hilbert and his school. Philosophical logic was made possible by Frege. Mathematical logic was realized by Hilbert. In between stands Russell whose type theory is a hybrid creature which was the incentive for the conception and demise of logicism as traditionally understood. After the dismissal of Frege's attempted arithmetical theory of concepts, Russell's enterprise as well as Hilbert's and Zermelo's axiomatizations could be seen as polynomializations of logic. Notwithstanding Quine's precept that second-order logic is no more logic, but mathematics, the proposal that second-order logic with Hume's equinumerical principle is equivalent to second-order Peano arithmetic should not impress the mathematical logician who does not care much about the philosophical underpinnings of his field. This is why my arithmetization of Frege's logicism should not surprise him no more that my following characterization of Russell's logicism as a polynomial calculus of degrees (orders) of propositional functions that look alike polynomial functions. Moreover the problems encountered in Russell's theory of types (simple or ramified) could have been solved by reverting to a theory of polynomials of finite degree as the finite support of infinite power series. That Russell was partly aware of such a solution is the theme of the next section.

2.4 Russell, Peano and Zermelo

The incentive of Russell's invention of the different theories of classes, the zigzag theory, the limitation of size theory, and the no-classes theory is certainly his formulation of the paradox for Frege's unlimited comprehension axiom V of the *Grundgezetze*: the invention of type theory was more in accordance with a simple arithmetical solution to the paradox. It is not difficult to see that the hierarchy of the simple theory of types with the first type 0 assigned to objects or individuals, the second to predicates, the third to predicates of predicates and so on is on a natural number scale. Transfinite type theory is a later extension; it was not considered by Russell. In that respect, it resembles closely Peano's axiomatization of arithmetic and the vicious-circle principle

> Whatever contains an apparent (bound) variable must not be a possible value of that variable. (Russell 1966, p. 163)

is there to prevent contradiction from arising. The ramified theory of types is a theory of types for propositional functions, whose type depends on the types of their arguments but also on the types on bound variables they contain (which can be of a higher type than the argument of the function). This forced Russell to introduce the notion of order and the ensuing axiom of reducibility which states that any function of arbitrary order n is coextensive with a predicative function of order $n-1$, that is one of order equal to the type of its bound variables. Had Russell thought of propositional functions as polynomials—the translation from the one to the other is simple—he would have seen no need to introduce the notion of order, for the notion of degree would have sufficed: the degree (or order) of a polynomial is the maximum of the degrees of all the terms in the polynomial. The same applies to Weyl's predicative theory of levels: Weyl was however well aware of the analogy of his hierarchy of levels with the hierarchy of polynomials of finite order—their extensions of infinite order are (formal) power series. In any event, the ramified type theory was designed to tackle paradoxes—Russell called them reflexive fallacies—outside of mathematics and Ramsey advised Russell that he should simply drop it in favor of the simple theory of types. But Russell had added an axiom of infinity, not having power series of infinite order. In this type theory, $\aleph_0$ must exist as the class of finite cardinals, i.e. in Russell's words, $\aleph_0$ exists as the cardinal of the class of classes of classes of individuals and $2^{\aleph_0}$ exists as the class of classes of classes of classes of individuals! The enterprise of *Principa Mathematica* co-authored with A.N. Whitehead was conducted on the firm basis of a finite type theory. The remains of Russell's endeavor are found however in his logic and his philosophy of language (the theory of descriptions) e.g. the actual king of France is bald

$$\exists x[((\varphi x) \wedge \forall y(\varphi y \rightarrow x = y)) \wedge \psi x]$$

Russell used ιx as the definite descriptor.

As far as logic is concerned, Russell defends Frege's alleged thesis that mathematics should be based on logic, as exemplified in *Principia Mathematica*. But the exemplification as it is easily observed, is mainly notational and in many cases superfluous. If the definitional logic of classes is set-theoretic, type theory could be recast in polynomial arithmetic. As for Frege, the formal language of logic is entirely comprised in propositional connectives and first-order logic and if one follows Quine's dogma, it means the whole of logic. Later, Lindström will characterize (first-order) logic as the language with the properties of compactness and Löwenheim-Skolem. First-order logic consists in the employment of quantifiers $\exists x$ (introduced by Russell) for "exists" and $\forall x$ (introduced by Gentzen) *Alle*, for "all", 0-order logic being the employment of connectives. The propositional content in both cases is first of all ordinary language and afterwards only specialized languages, e.g. elementary mathematics. Formal logic separates sentences (closed expressions) from formulas (open expressions) with constants and variables (bound and free), well-formed formulas are generated by rules of formation in a vocabulary and rules of transformation—in Carnap's parlance—or inference allow for the passage from axioms to theorems, e.g. *modus ponens*. Peano's *Formulaire* seems to be plagued with an absence of logical content despite his use of the notion of indeterminates for variable signs. Peano arithmetic is still the basic system for arithmetic for logical purposes: his axiom of induction (in the *Formulaire* reads) :

> If a set F of natural numbers contains one and if, containing an arbitrary number a it contains also its successor, then S contains all natural numbers. (Peano 1959, p. 35)

This is a second-order formulation and it corresponds to the axiom of infinity in Zermelo-Fraenkel axiomatic set theory

$$\exists x\{\emptyset \in x \wedge \forall y(y \in x \rightarrow y \cup \{y\} \in x)\}$$

for {y} as the singleton (or the one-element set). This formulation links clearly Peano arithmetic to Cantor's naive set theory, whence our notion of set-theoretic arithmetic.

Zermelo's axiomatization of set-theory had also the goal of eliminating the paradoxical consequence of the axiom of unlimited comprehension of Frege's law V in the *Grundgesteze* and limited comprehension is expressed by axiom of separation (*Aussonderungsaxiom*), in Zermelo (1908a)

$$\forall x \exists x \forall z(z \in y \leftrightarrow z \in x \wedge A(z)).$$

Zermelo is also prompted to attack Peano's *Formulaire* and its tentative reduction of mathematics to syllogisms in the Aristotelian-Scholastic sense (Zermelo 1908a,b). It behooves to admit that Zermelo resumed with the arithmetical spirit of Cantor's endeavor, if only to introduce, as he said, some restrictions to Cantor's theory; in his work on finite sets which he identified with elementary arithmetic (Zermelo 1909), Zermelo did not hope to restrict himself to finite sets and believed that the well-ordering principle for natural numbers could be extended into the transfinite. But the axiomatic set theory he initiated was to be reworked by others, Skolem, Fraenkel, von Neumann among them. Von Neumann who introduced the axiom of foundation or regularity

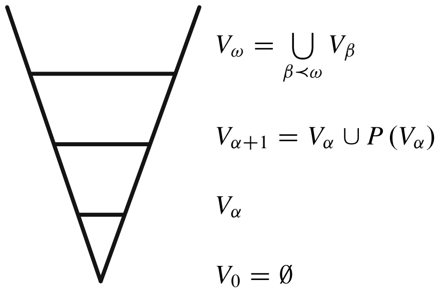
$$\forall x(x \neq \emptyset \rightarrow \exists y(y \in x \wedge y \cap x = 0)$$

or in a second-order formulation

$$\forall X \forall x[X(x) \rightarrow \exists y \forall z\{X(y) \wedge [X(z) \rightarrow z \in y]\}]$$

quotes Mirimanoff (1917) who did define "ordinary sets" as those which generate only finite descent—there is no infinite descending sequence of elements $e_1 \ni e_2 \ni e_3 \ldots$ for it must stop at an indecomposable element $\emptyset$, called also core ("*noyau*") by Mirimanoff. Mirimanoff who was familiar with Fermat's method of infinite descent in number theory was followed also by Skolem who spoke of descending ϵ-sequences in his 1922 paper "*Some remarks on the axiomatic foundation of set theory*"; such sequences have also to terminate in the finite. In the same paper, Skolem stresses the fact that set-theoretic notion are relative, result that would prompt Gödel to define absolute formulas in a minimal inner model of Z-F.

The cumulative structure for set theory resulting from the efforts of Zermelo, Mirimanoff, Skolem and von Neumann


$V_\omega = \bigcup_{\beta \prec \omega} V_\beta$
$V_{\alpha+1} = V_\alpha \cup P\,(V_\alpha)$
V_α
$V_0 = \emptyset$

extending into the transfinite with the iteration of addition and the power set operations and their closure for inaccessible and higher cardinals is seen as built upon the axiom of foundation. A reflection principle equivalent to the axiom of replacement

$$Func(F) \to F''x \in V$$

plus the axiom of infinity gives a full-blown image of an ever expanding set-theoretic universe V reflecting itself in the transfinite levels of the ordinals hierarchy.

Does the transfinite extension of the arithmetical world, its transarithmatical completion in completed infinite totalities have an absolute meaning or is it only relative to finite arithmetic, as Skolem would have put it?

A number-theoretician or a constructivist logician in the lineage of Kronecker—as was Skolem—cannot but deny absolute existence or validity to the full set-theoretic universe. But many want to retrieve the arithmetical content of set theory, as Cauchy, Weierstrass and Dedekind and Hilbert hoped to achieve for analysis where the notion of limit was put to test by arithmetical methods, e.g. when it was not simply removed. What happened with Cantor goes the other way around: the limit concept was actualized and ordinalized, meaning that limit ordinals are not to be approached, they exist *de facto* and *de jure* by the sanction of a transcendent decree—Kronecker would have added that actual existence of these entities was a matter of philosophy or theology, not of mathematics.

A more tolerant attitude would simply define transfinite arithmetic as transarithmatic extension of arithmetic to the benefit of a few customers. What happened after Cantor is that free creation attracted more people than the rigid Kronecker would have dreamed of. There is no question of binding or bending mathematical imagination, but the Kroneckerian heritage in pure mathematics, number theory and algebraic or arithmetic geometry seems to have been more fruitful that the Cantorian influence, which however, has spread rapidly in elementary mathematics, in the language of mathematics and in foundational issues. Algebra as the proper extension of arithmetic is the right place to look for the development of general arithmetic in the Kroneckerian sense.

2.5 Kronecker and the Arithmetization of Algebra

It could seem paradoxical that Kronecker entitled his program "the arithmetization of algebra" since algebra is another name for general arithmetic or "*allgemeine Arithmetic*". Hankel in his 1867 "*Prinzip der Permanenz der formalen Gesetze*" (Principle of the permanence of formal laws) after Peacock's "principle of the permanence of equivalent forms", hoped to extend the laws of ordinary arithmetic to different number systems (e.g. complex numbers). Kronecker's ambition is different. In a letter to Lipschitz (1896), he writes :

> On that occasion [the publication of his 1882 paper], I have found the long-sought foundations of my entire theory of forms which somehow bring to completion "the arithmetization of algebra" which has been the goal of my entire mathematical life. It is entirely clear to me that at the same time arithmetic cannot dispense with the "association of forms" and that without them, it only goes astray in meandering thoughts "*Gendankenspinste*" as in the case with Dedekind, when the true nature of the matter is obscured rather than illuminated.
>
> Lipschitz 1896 (Gauthier 2002, pp. 181–182)

The 1882 paper in question is of course the major publication "Fundamental features of an arithmetical theory of algebraic quantities" ("*Grundzüge einer arithmetishen Theorie der algebraishen Grössen*") where he lays the foundations of his theory of forms (homogeneous polynomials). Beyond the polemical tone, one sees the central rôle of his 1882 formulation.

> In the Kroneckerian approach, the transfinite construction of algebraically closed fields is avoided by the simple expedient of adjoining new algebraic numbers to Q as needed.
>
> (Edwards 1987a,b, p. 97)

Here adjoining new algebraic numbers constitutes a numerical extension, whereas an algebraically closed field is obtained by a universal (transfinite) quantification on all natural numbers. What this means is that the adjunction in the Kroneckerian approach proceeds "step by step", in extending the field, not in the Dedekind's transcendental set-theoretic way of completing the field Q in *one stroke*. As for the general setting of Kronecker's theory of forms, it is that very generality—independent of the ambient field, as one says—that is responsible for its foundational import. Kronecker's arithmetization programme can be summarized in the title "General Arithmetic" which contains, in Kronecker's words, the complete development of the theory of entire (rational and algebraic) functions of a variable together with the system of divisors. In this complete theory, the association of forms allows for the conservation of the laws of factorization, so that the passage from natural and rational domains to the more general algebraic domains (of algebraic integers) is perfectly uniform (Kronecker 1968a,b, III, pp. 350–351). The conservative extension of arithmetic up to the highest reaches of algebra—the theory of entire rational and algebraic functions—is the ultimate goal of general arithmetic defined as the theory of all forms with an arbitrary number of indeterminates.

It has been noticed why Kronecker has preferred the term "domain of rationality" "*Rationalitätsbereich*" to the term "*Körper*", "field" in English. While "field" is rather innocuous, "*Körper*", "*corps*" in French, was too "material" for Kronecker. Whether there is an idealistic overtone implied here is open to question—what about ideals and ideal numbers? In any case, the notion of integral domains and unique factorization domains are well known today and are part of contemporary algebra.

What does Kronecker understand by the foundation of the arithmetical existence of algebraic quantities, as W. Hodges asks in his treatise on model theory (Hodges 1993). Kronecker's answer is in the title of chapter 13 of the first part of his paper, but the real answer is in chapter XII on "The general theory of rational functions of several indeterminate quantities". Starting with Galois's and Abel's theory of algebraic equations, Kronecker wants to develop a theory of all equations of a given class for a given domain of rationality, a problem which has escaped Galois, but has preoccupied Abel, as Kronecker says. The problem is of the same kind as Diophantine equations, except that here coefficients are algebraic quantities (integers) belonging to an extended domain of rationality. We have an entire function with integer coefficients in the following equation

$$\Phi(g, f_1, f_2, \ldots, f_n) = 0$$

in which the f's are symmetric functions and g a genus. On substitutes for those $n + 1$ quantities rational functions $\varphi_0, \varphi_1, \varphi_2, \ldots, \varphi_n$ in the equation

$$\Phi(\varphi_0, \varphi_1, \varphi_2, \ldots, \varphi_n) = 0$$

and thereby obtains an arithmetical formulation of the problem. Of course, the question is the solubility of Diophantine equations of arbitrary degree, Kronecker hastens to explain, but it is the general setting in arithmetical terms which is relevant. Diophantine equations are also called indeterminate equations and involve unknowns which Gauss names "*indeterminatae*", whence the Gaussian heritage which Kronecker revendicates. For Galois, it is the Galois field, the smallest factorization field (domain) for polynomials—which is fundamental in the Kroneckerian context. As a polynomial can be factored into linear factors by the group of permutations of the coefficients, in the same manner one can order the entire functions of a given genus according to the permutation group of generating functions, so that one can arrive at a formulation like

$$rg^{(k)} = m'\varphi_k^{'}g' + m''\varphi_k^{''}g'' + m'''\varphi_k^{'''}g'''$$

where the m_i's are integers, divisors of r, the φ_i's are entire functions with integer coefficients and g a genus function, that is a general function of the whole domain of rationality. Such a formulation shows, after Kronecker, that all functions g_i are reducible to linear functions of the generic elements "*Gattungselemente*" of the fundamental domain of rationality and the coefficients of those linear functions are entire functions with rational numbers as coefficients.

Kronecker links his work on general arithmetic with his generalization of Sturm's theorem using the Jacobi-Hermite interpolation method for Sturm's series where he introduces entire functions of successive domains of rationality R, R', R'' (Kronecker 1968a,b, I, pp. 305–348). Again, in this case, the goal is a general arithmetic or the arithmetization of algebra, as he puts it his letter to Lipschitz mentioned above and

Kronecker adds that it was a goal that he had wished to reach from the beginning. His true "*Jugendtraum*" may be the arithmetization of algebra.

The second part of Kronecker's main paper deals with the divisor theory of algebraic quantities and also presents the general formulation of his programme in a sequence of fundamental propositions. The theory of polynomial equations and their discriminants finds here its fullest expression. The central concept is the concept of association of quantitive formations "*Grössengebilde*" for the construction of general algebraic divisors or moduli systems. Kronecker makes use of Kummer's equivalence principle for classes of ideal numbers and extends the principle to algebraic quantities without having to change the theory of divisibility :

> The conservation of these conceptual determinations in the transition from the rational to the algebraic case was the incentive which has served me as the guiding principle in the treatment of algebraic quantities.
>
> (Kronecker 1968a,b, II, p. 327)

The general theory of elimination for polynomial equations proceeds along the lines of a general arithmetic of rational functions with integer coefficients and indeterminates. Forms (polynomials) can contain "*enthalten*" other forms or be contained in other forms and two forms are said to be "absolutely equivalent" when they contain each other. Definitions of primitive, prime, irreducible forms follow. It is useful to quote in full proposition IX (Kronecker 1886, p. 345):

> When a homogeneous linear form F is contained in another form F_0, the latter can be transformed in the former provided that forms of the domain (of rationality) are substituted for the indeterminates of F; those forms are linear if F_0 is itself a linear form. In such a case the contained linear form F is transformed into the containing form through a linear substitution with integral coefficients and this is a sufficient condition for the containment "*Enthalten-Sein*" of F in F_0.

Kronecker explains that the linear substitution refers to the indeterminates and the integer coefficients are the entire rational functions or integral quantities of the domain of rationality R, R', R''. Proposition X then ensues:

> Equivalent homogeneous linear forms can be transformed one into the other through substitution with integral coefficients (ibid.).

Divisibility properties are easily deducible e.g. absolutely equivalent forms have the same divisors and the final conclusion is reached with the statement XIII (and XIII°) on the unique factorization of integral algebraic forms as products of irreducible (prime) forms. What this shows, Kronecker maintains, is that the fundamental laws of ordinary arithmetic are preserved in the encompassing sphere of algebraic quantities by the process of association of algebraic forms.

The association of integral algebraic forms, Kronecker continues, is shown by the result on unique factorization to conserve the conceptual determinations and the laws (of arithmetic) in the extension of the rational to the algebraic; still further, it provides the simplest apparatus, which is also necessary and sufficient, capable to fully exhibit the arithmetical properties of the most general algebraic quantities (Kronecker 1886, p. 353). The association of forms is comparable to the association of imaginary numbers in analysis, Kronecker contends, and shares the same necessity and the indeterminates involved in the process are totally in line with Gauss's "*indeterminatae*" introduced in his theory of quadratic forms. At the end, one could dispense with "irrational" algebraic numbers, if it could be shown that they are algebraic after all, that is rational approximations of a non-rational algebraic indeterminate number.

The programme of a general arithmetic has numerous ramifications, especially in the theory of moduli systems where Kronecker constantly goes back to Gauss and Galois as sources of his combinatorial ideas—in another tradition, of Dedekindian heritage, modular systems are called polynomial ideals. It is Gauss's congruence concept which is at the origin of the general theory of modular systems and Galois's permutation group in the theory of polynomial equations—see the papers "*Über einige Anwendungen der Modulsystem auf elementare algebraische Fragen*" and "*Ein Fundamentalsatz der allgemeinen Arithmetik*" (Kronecker 1968a,b, II and III).

These results consolidate general arithmetic as an algorithmic theory of divisibility. This is one of the major tasks that Kronecker has left to posterity from Hensel, Hurwitz and Molk (1885) or König to Vandiver (1936), Weyl and Edwards. Hurwitz, for example, shows how the Euclidean algorithm works in Kronecker's theory of moduli systems while Molk's analysis offers a lengthy summary of Kronecker's divisor theory. An interesting example is Vandiver's work on a "Constructive derivation of the decomposition-field of a polynomial" (Vandiver 1936). Building on Kronecker's work and van der Waerden's reworking, Vandiver obtains the decomposition field by a finite algorithm for the extraction of irreducible factors without the assumption of the beforehand existence of the decomposition field (or domain of rationality). Vandiver clearly confesses his adhesion to Kronecker's programme when he says that the method of moduli systems with indeterminates is essential for the foundations of commutative algebra. Vandiver uses induction, in fact the descent method, on a polynomial $\varphi(\beta, z)$ to obtain the decomposition of a field $F(\beta)$. Edwards, another adherent to Kronecker's programme, proceeds along the same lines with his emphasis on natural rings of integers where there is a finite descent method for the factorization of polynomials. Edwards (1989, p. 21) shows how one obtains irreducible polynomials by assuming that if a polynomial h (an integral algebraic form, "*ganze algebraische Form*" in Kronecker's terminology) is not irreducible, then one can suppose that there are polynomials of smaller degree than h *ad infinitum* and with the same properties as s, which is impossible, so that by a *reductio ad absurdum* we arrive in a "finite number of steps" at an irreducible polynomial

$$h(x) = b_0x^n + b_1n^{n+1} + \ldots + b_n$$

in which the decreasing order of powers exhibit the finite descent from an arbitrary integer n, the degree of the polynomial. This is, obviously, the essence of Kronecker's method. However, I think that Edward's exposition is not entirely faithful to Kronecker's programme when he criticizes Weyl for having put the emphasis in his "*Algebraic Theory of Numbers*" (1940) on unique factorization which was also the objective of Dedekind's theory of ideals. Edward's argument rests on the fact that factorization depends on the ambient field, but one should add that one of Kronecker's main results, on his own admission as we have seen, is unique factorization of forms in the largest of ambient fields or domains of rationality. Kronecker's theory of general arithmetic encompasses the theory of forms, their composition in terms of the association of forms and their decomposition in terms of the theory of algebraic divisors or modular systems; it was undoubtedly part and parcel of Kronecker's programme to reach the most general result on unique factorization for algebraic number fields—in Kronecker's terminology again, in integral algebraic forms. We have seen that Kronecker repeatedly insisted on the "generality" of his general arithmetic.

Edwards (1989) also discusses Dedekind's Prague theorem which generalizes Gauss's lemma to algebraic integers in relation to Kronecker's earlier result on the theory of forms of higher level (Kronecker 1968a,b, II, pp. 419–424). Gauss's lemma says essentially in one of its versions that two primitive polynomials have a product that is also primitive. Kronecker's generalization uses the Cauchy (convolution) product for polynomials

$$\sum_h M_h U_k \cdot \sum_i M_{m+i} U^{i+1} = \sum_k M'_k U^k$$

where the M's are integral forms and the U's indeterminates so that the product

$$\prod_h \sum_k M'_k U_{hk}$$

is "contained" in the resulting (primitive) form and the product can be expressed as

$$\sum_k M'_k U^k = (M_k M_{m+1})^k + (M_k M_{m+1})^{k-1} + (M_k M_{m+1})^{k-2} + \ldots + (M_k M_{m+1})$$

in the decreasing order of the degree k of the polynomial. This linear combination obtained by the convolution product and the finite descent on powers shows simply that integral algebraic forms "produce" integral algebraic forms, i.e. algebraic integers. What Edwards finds so difficult in Kronecker's "terse style" is simply a generalization of Kronecker's 1882 theory of forms which encompasses both the theory of moduli systems and the theory of polynomials. The equivalence principle for forms stated in 1882 is extended to divisors. The notion of content "*Enthaltensein*" is expressed thus : F_r is a form with indeterminates U_{hi} which contains the product of forms where f_i's are entire functions of indeterminates U_{hi}

$$\prod_h (f_0 U_{h0} + f_1 U_{h2} + \ldots = f_n U_{hn}).$$

Kronecker refers explicitly to the content of primitive polynomials in his text, a remark which leads immediately to Gauss's lemma in its modern version "The product of two primitive polynomials is primitive" (polynomials having the g.c.d. of their coefficients). As a matter of fact, Hurwitz (1895) obtained a proof of Kronecker's theorem by using Lagrange's interpolation rather than Cauchy's convolution and the Euclidean algorithm which is also a form of the descent method—Hurwitz speaks of the elimination of composite powers. Dedekind's Prague Theorem which uses a form of descent is a consequence of Kronecker's more general theorem on the product of forms. Again the ring of polynomials is the proper arena (with the largest area!) for Kronecker's general arithmetic of forms and their divisors. Dedekind's Prague theorem (1892) paradoxically can be counted in Kronecker's posterity—Kronecker died in 1891. I say paradoxically since Kronecker has vividly polemicized with Dedekind and their methods were known at the time to be divergent.

The immediate and long-term posterity of Kronecker's programme includes a vast number of people from Aldolf Hurwitz and Kurt Hensel to André Weil and Robert Langlands. One should include in the list Brouwer, Poincaré and the French semi-intuitionists like Borel and Lebesgue to a certain extent and even Hadamard, who like Brouwer borrowed from Kronecker's arithmetical theory of functions for the particular purposes of topology—the winding number (which is an integer) or index giving the number of times a closed curve C passes around a designated point P in the plane. Russian constructivists like Markov, Shanin, Kolmogorov up to Essenine-Volpin have also some share of Kronecker's finitism. But it is certainly in algebraic geometry that Kronecker's heritage is most strongly felt. Weil (1976) considers Kronecker as the originator of modern algebraic (arithmetic) geometry in the sense that Kronecker has initiated the work on the arithmetic of elliptic functions—they have become the elliptic curves or the modular forms of the contemporary scene. Elliptic curves even play a rôle in recent cryptography, for they have an arithmetical content hidden under their surface of intersection!

On that count, Langland's programme (1976) is consciously inspired by Kronecker "*Jugendtraum*" which can be seen as an arithmetic theory at the interface of algebra and analysis. It is still the arithmetical core which imports in that connection of the fields of arithmetic, algebra and analysis, as Kronecker points out in his analysis of Dirichlet's theorem on the infinity of primes in any arithmetic progression. Dirichlet was well aware, Kronecker notes (1901, p. 482), of "the need for appropriate principle formulations of the conditions under which transcendental connections involving indeterminate integers can vanish". Dirichlet was unable to further his investigations simply because he was blinded by the overemployment of infinite series for which there is no need beyond the formal power series considered as a finite expression or a finite series, that is as a polynomial of finite degree (Kronecker 1968a,b, III, p. 156). See also Lejeune-Dirichlet (1969) edited by Kronecker.

It is decidedly the motto of the "finite number of steps" which is found in Hensel's introduction to Kronecker's *Vorlesungen über Zahlentheorie* (1901) that defines the algorithmic or finitist stance in the foundations of mathematics. A number of logicians, like many mathematicians, have adopted the motto, from Skolem and Goodstein to Nelson, not to mention philosophers like Kaufmann or more importantly Wittgenstein (see Marion 1998). I contend that Hilbert was the first to apply Kronecker's programme, in a more or less conscious fashion, to logic and that his own programme is the continuation of Kronecker's by other means. These other means are called "metamathematics".

Chapter 3
Arithmetization of Logic

3.1 Hilbert after Kronecker

Hilbert is not the originator of the expression “metamathematics”, but he is the first to define it as the theory of formal systems designed to capture the internal logic (“*inhaltliche Logik*”) of mathematics and it is the internal logic of arithmetic, what I call arithmetical logic, that was to be his primary concern.

It is common knowledge that metamathematics—theory of formal systems or proof theory—is concerned with finitary methods and requires a finitist approach in the sense of Kronecker, as some early manuscripts of Hilbert seem to attest (see Hallett 1998).

The rather sketchy attempt at the simultaneous foundation of logic and arithmetic (Hilbert 1905) puts forward the concept of homogeneous equations in a manner reminiscent of Kronecker’s combinatorial theory of (homogeneous) polynomial equations. Consistency, following Hilbert (1905) boils down to the homogeneous equation $a = a$ or inequation $a \neq a$. At the time, according to the testimony of Bernays, Hilbert was tempted to lay down his arms to the finitist Kronecker, whom he accused of dogmatism; but under the threat of the paradoxes, he momentarily abandoned his foundational query, and submitted to Kronecker in perpetuating the Kroneckerian tradition in number theory and in algebra. It is only in 1918 that Hilbert resumed his foundational research and returned to finitism, not without polemizing with Kronecker (posthumously!), Brouwer and Weyl whom he considered as Kronecker’s direct heirs. The simultaneous foundation of logic and arithmetic still dominates his preoccupations and the recourse to the notion of formal system is meant as a mechanism (a finite algorithm) for the introduction of ideal elements. My hypothesis is that this process mimicks Kronecker’s association of forms in his general arithmetic and the consistency which is required for the association of ideal elements can only be achieved by a formalism which is the exact counterpart of an arithmetic (polynomial) algorithm, e.g. the method of descent as a generalized Euclidean algorithm.

The propositions of general arithmetic that are found in Kronecker’s “*Grundzüge einer arithmetischen Theorie der algebraischen Grössen*” can be considered as so many axioms from which Kronecker derived his results with arithmetical means alone. In

Y. Gauthier, *Towards an Arithmetical Logic*, Studies in Universal Logic,
DOI 10.1007/978-3-319-22087-1_3

his “*Axiomatisches Denken*” (1918), Hilbert pinpoints the properties of independence and consistency as the main features of the axiomatic method. Relative consistency of geometry and other scientific disciplines, Hilbert suggests, is based on the consistency of arithmetic, but there is no further foundation for arithmetic and, Hilbert adds, set theory. Logic is the ultimate foundation and it must also be axiomatized and in the final analysis there only remains for the axiomatic method the question of decidability which must be settled “in a finite number of operations” (Hilbert 1935, III, p. 154). Here Hilbert gives the example of the theory of algebraic invariants for which he had provided a finiteness proof inspired by the very method he had used in his major result (see Hilbert 1890 and Hilbert 1893): Hilbert’s finite basis theorem depends heavily on Kronecker’s own methods in general arithmetic and becomes the paradigm case for the decidability property of a logical system! But there is no logic involved in Hilbert’s result and his paradigmatic case is drawn from polynomial arithmetic (Kronecker’s general arithmetic of forms). Decidability implies, of course, that we have an algorithm or a finite procedure to decide of a given question in a “finite number of steps”. We then come back to our point of departure and it is not surprising to see that foremost decidable theories are elementary (first-order) algebraic theories and have ended as the subject-matter of model theory, not proof theory. The method of quantifier elimination, for instance, is a test for decidability and has been employed by Tarski in his well-known model-theoretic results; van den Dries (1988) has stressed the influence of Kronecker’s methods in that context. But then what is the logical point of the decision method? A decidable theory when consistent is finitely so. In the specific case of the elementary theories, logic does not play any special rôle since the equational calculus of polynomials does not need other operations than the purely arithmetical (combinatorial) laws.

The case for logic rests solely on the alleged conservative extensions of arithmetic into the transfinite domain of ideal elements. It remains though that even if Hilbert had hoped for a logical introduction of ideal elements, he has constantly stressed that a finite process (or procedure) is the inference engine of internal “*innere*” consistency.

Internal consistency is obtained by internal means in the case of general arithmetic as in the case mentioned above of the theory of algebraic invariants. Hilbert was not mistaken there and he saw consistency as internal to the polynomial equation calculus when he defined consistency as the equation $a = a$ and inconsistency as $a \neq a$. We have observed that one of the essential tools of internal consistency is the convolution product which generates linear polynomial expressions from linear polynomial expressions as in Kronecker’s result, Dedekind’s Prague theorem or Hilbert’s work in invariant theory. The convolution or Cauchy product can be called Cauchy diagonal. A serious blow to Hilbert’s programme was given from the outside, the “external” Cantor diagonal in Gödel’s results. The set-theoretic diagonalization does not belong to number theory or algebra, but to set-theoretic arithmetic, as Hilbert himself has named it, but it is also set theory that he wanted to secure in his proof theory. It is another paradoxical situation for the logician Hilbert to see his full-blown programme for consistency of set theory and analysis put in jeopardy by a set-theoretic device!

Kreisel has put the emphasis on modifications of Hilbert’s original programme; others, Sieg, Feferman (1960) and Simpson among others have insisted on partial realizations of Hilbert’s programme. Whatever the merits of the programme of Reverse Mathematics

(Friedman-Simpson), it is *a posteriori* and may serve only the limited goal of *regressive* justification. The Weyl-Feferman programme on the other side, or predicative mathematics as an alternative to Hilbert's programme, does not seem to recover as much mathematics as Reverse Mathematics while sweeping too large for constructivist mathematics. The objective of constructive foundations is not negative, it does not have to reject major trends of mathematical practice, but only to enclose the safe haven of real mathematics, in Kronecker's words. A *forward* or progressive programme for logic and mathematics is an attempt at extending the conservative domain without relinquishing the basic principles of a foundational stance that need not be a philosophical refuge, nor a negativist attitude against non-constructivist credos. And an incitation to revisionism is meant primarily as an incentive to creative foundational work. Despite the moralizing overtones of many pronouncements by Kronecker, one is reminded that he has been the target of numerous vindictive attacks. Hilbert was not himself immune to polemics (nor Brouwer, for that matter).

A more balanced view would call for a reconciliation of Kronecker's and Hilbert's programmes. New foundations for Hilbert's programme invite to dig deeper in Hilbert's programme and to lay bare the roots of Hilbert's metamathematical idea. Consistency and decidability constitute the main avenues we have followed—independence being a minor logical track for our purpose—and they appear already in Kronecker's work in another disguise. I have put these ideas together (with some others) in a consistency proof for arithmetic which I claim to be Kroneckerian in spirit and at the same time compatible with (a revised) Hilbert's programme.

Hilbert hoped for a logic of arithmetic that would transgress finite arithmetic into transfinite arithmetic; the logic of arithmetic would thus be transformed into an "external" set-theoretic logic. The internalization of the logic of arithmetic goes the other way around for it is the logical continuation of the arithmetization of analysis.

The nineteenth century was the century of arithmetization from Gauss and Cauchy to Kronecker, Weierstrass and Dedekind, who conceived his theory of cuts as an arithmetization of the real numbers. Even Cantor is interpreted in the arithmetic framework, since some pretend that transfinite arithmetic belongs to an "extended" finitist programme, forgetting that Cantor saw things "from the inside", for example in his interpretation of the concept of limit. Cauchy and Weierstrass introduced the concept of (finite) limit, the $\epsilon - \delta$ formalism, in order to approach "infinitely" the finite; that is certainly the idea behind Cauchy sequences (of rational numbers). For Cantor, it is not the process of approaching the limit that counts, it is possession of the limit "beforehand", as some sort of Platonic *a priori*. Cantor's normal form theorem, seldom discussed in that context, is only apparently a finite descent for the second number class (the ω-hierarchy) for ordinals that are all limit-ordinals supposed to subsist independently of any approaching or approximation process. Such a Jacob's ladder never touches the ground!

The ground in question is arithmetic and its internal logic. But what is that logic, beyond and above what Kronecker called the conceptual determinations "*Begriffsbestimmungen*" or what Dedekind and Hilbert called "the laws of thought" inherent in arithmetic itself? Frege asked the question "How far can one go in arithmetic by using only inferences?" and his answer was that the inferential link consisted in transforming the concept of succession in a series "*Anordnung in einer Reihe*" into the concept of logical consequence "*logische Folge*" (Frege 1983). Sequences or consequences, one is tempted to say. Frege's logic overpasses arithmetic in a theory of concepts that reaches for a Platonic world of subsistent entities also inaccessible to mathematical practice, if not to philosophical and theological—in Cantor's case—speculation.

The internal logic of arithmetic consists simply of the arithmetical operations and the laws that can be extracted from their combinations. The logic of the content emerges from the content and is not superimposed on it. Formal logic, in the sense that Hilbert has initiated, after Frege and Russell, is external to a logic of contents, but for Hilbert the finitist conception of mathematics or proof theory (or the theory of formal systems) had to stay close to the proper inferential structures of arithmetic while retaining classical (Aristotelian, traditional or ordinary) logic, in particular its law of excluded middle. Excluded middle is of course part of finitary reasoning, but is not an *a priori* principle, it must be derived from the internal logic of arithmetic, for example, as the conclusion of a descent procedure after a finite number of steps in a reductive process of infinitely proceeding sequences, where the principle does not apply following Brouwer.

Formal logic or a formal system with its axiomatic apparatus would then be nothing else than the projection in the external world—the world "out there" of realists, platonists and some structuralists—of the internal structure of arithmetic. I have named that internal logic of arithmetic, arithmetical logic and its extension to Kronecker's general arithmetic of forms, polynomial logic. More recently, the name "modular logic" has seemed also appropriate for a logic built on the model of modular arithmetic or the arithmetical theory of modular systems in which congruence represents an equivalence relation in a polynomial equational calculus. Herbrand and Gödel, among many others (e.g. Goodstein) after Hilbert, have grounded logic on an equational calculus. All of these logical developments take their source, in my opinion, in the ramifications of Kronecker's original programme. I say ramification, for I do not want to give the impression that everything was already in Kronecker. There are more things in "general arithmetic" than Kronecker could ever dream of, but not as many as Dedekind or Cantor have wanted. Dedekind hoped to go further in arithmetic with unrestricted inductive definitions and Cantor still further with his normal form theorem for the second number class. But, as Brouwer has objected, the second number class does not exist, it is only replete with "indeterminate ordinals". What we have called arithmetic continuation can go as far as Kronecker's general arithmetic and not into any transcendental realm where association of forms becomes formless, as one is tempted to say after Kronecker. Arithmetic continuation means rather arithmetization of algebra and it may be the notion of algebraic extension which could best serve Kronecker's original purpose. Extensions with a finite number of indeterminates are isomorphic with polynomials in the field (domain of rationality) of algebraic integers, so that the notion of modular systems affords a "reductive" algebraic theory, Kronecker's general arithmetic.

3.2 Hilbert's Arithmetization of Logic and the Epsilon Calculus

Hilbert introduced the epsilon calculus in 1920 to translate the quantifier ∃ and ∀ and replace the axiom of choice, according to Bourbaki in his *Théorie des ensembles* (Bourbaki 1970). But Hilbert's deeper motive was a finitary reduction of the consistency problem for arithmetic, Hilbert was prompted by the failure of the logicist programme to provide a finitist foundation of arithmetic and eventually for analysis and set theory.

Hilbert's intent in introducing the ϵ-symbol was to insure the passage from arithmetic to the ideal elements of set theory (including analysis), that is to insure consistency of infinitary mathematics with the help of finitary arithmetic, the theory of (primitive recursive) classical arithmetic. Hilbert devised the transfinite choice function to bridge the gap between finite arithmetic and Cantor's transfinite arithmetic (see Hilbert 1926). But once the higher level of existence has been reached, one as to return or climb back to the finite basis: this is the descent method "*Methode der Zurückführung*" (Hilbert and Bernays 1968–1970, p. 190) which consists of a construction "*Aufbau*" and its decomposition "*Abbau*" in arithmetical terms. The whole problem of consistency is thus a matter of recovering finite arithmetic through a process of elimination of the ϵ-symbol and the critical formulas attached to it. To the question often asked "Why introduce the ϵ-symbol if it is only to eliminate it afterwards?" the answer is simply: "To build up the ideal realm and redescend to the (arithmetical) foundations in order to secure the whole edifice of mathematics". Logic (and the axiomatic method) remains only a tool, insofar at it warrants elementary arithmetical inferences and the truth of elementary arithmetical statements.

The first axiom for the ϵ-symbol is

$$A(a) \rightarrow A(\epsilon_x A(x))$$

where $\epsilon(A)$ is a transfinite logical choice function (Hilbert 1926). The existential quantifier is defined by

$$\exists x Ax \equiv A(\epsilon_x A(x))$$

and the universal quantifier by

$$\forall x Ax \equiv A(\epsilon_x \neg A(x))$$

meaning that universal quantification can be asserted if no counterexample can be found—after a finite search, that is a finite iteration of the transfinite choice function.

Together with the Aristotelian axiom

$$\forall x Ax \rightarrow A(a)$$

and the excluded middle principle

$$\neg \forall x Ax \rightarrow \exists x \neg A(x)$$

these axioms constitute the axiomatic framework for the symbol and its minimal character could provide a passage from arithmetic to analysis and set theory with the rules of logic being only an auxiliary means "*Hilfsmittel*" or even a deviation "*Umweg*".

The introduction of the ϵ-symbol requires two theorems on critical formulas and their elimination: the first ϵ-theorem eliminates critical formulas attached to a term t

$$A(t) \to A(\epsilon_r A(r))$$

by a method of symbolic resolution

$$(R) = \begin{cases} A(t_1) \to A(\epsilon_r A(r)) \\ \qquad\qquad \vdots \\ A(t_n) \to A(\epsilon_r A(r)) \end{cases}$$

which reproduces the decomposition of polynomials since terms and expressions are ordered according to degree and rank; the degree here is the maximal (finite) number of terms in a sequence of ϵ-terms and the rank of an ϵ-expression is the maximal (finite) number of expressions in a sequence of ϵ-expressions. As for polynomials, one obtains a reduction to a disjunctive form of terms without the ϵ-symbol, that is a linear expression. The second ϵ-theorem applies the same method to existential formulas and the identity axiom. It is the induction schema which creates problems here and requires a new critical formula

$$A(t) \to \epsilon_r A(r) \neq t^{'}.$$

Substitution in this case is effected by means of number-names “Ziffer” or numerals for the ϵ-terms and the method will induce a formulation of the principle of induction with the help of the ϵ-symbol. The formulas

$$A(a) \to \epsilon_x A(x) \neq a^{'}$$

and

$$a \neq 0 \to \delta(a)' = a$$

for the existence of successors and their recursion give way to a new induction principle which is stated:

> For every numerical predicate P which applies to at least one number, there is a number corresponding to P but for whose predecessor, if it exists at all, P is not applicable (1970 II, 87).

The principle is a direct consequence of the least number principle with the general recursive function μ

$$A(a) \to (\mu_x A(x)),$$

and

$$A(x) \to \exists y(A(y) \wedge \forall z(z < y \neg A(z))),$$

but the general procedure is reminiscent of polynomial decomposition in irreducible factors, i.e. the Euclidean algorithm of the greatest common divisor and its generalization by infinite descent for polynomials of degree n or by the chain condition for polynomial rings.

The substitution principle takes the form of global or partial substitutions and the effective substitutions for terms will consist in finding the resolvent or the solution polynomial in reducing substitutions of term instances to substitutions in fundamental types of terms, i.e. terms that are not part of an other term. The process mimicks Kronecker's general theory of elimination and the consistency proof will lead to the "*irreducible*" reduced formulas, as can be shown on the example of Ackermann's consistency proof for arithmetic—reproduced in the second edition of Hilbert and Bernays (1968–1970, Supplement V, pp. 535–555). Ackermann's proof relies essentially on the reduction number of global substitutions "*Gesamtersetzungen*" for numerals and functions using the machinery of recursive function theory: one ends up with a "normal sequence" in a polynomial expression

$$n_0 \cdot 2^h + n_1 \cdot 2^{h-1} + \ldots + n_{h-1} \cdot 2 + n_h$$

for the numbers n substituting for terms. The reduction number has the value 1 or 0, depending upon the global substitution being reduced to 0 or $j \neq 0$. The total number of global substitutions is 2^n when the number of ϵ-terms (of rank) occurring in the series of formulas is n, as is the case for the number of coefficients in the binomial, for example. For higher ranks, primitive recursive equations suffice

$$\psi(1,n) = 2^n$$

$$\psi(m+1,n) = 2^{n \cdot \varphi(m,n)} \cdot \psi(m,n).$$

The second ϵ-theorem has to do with the critical formulas of the second kind and the symbolic resolution of existential formulas. The main idea is to eliminate the existential quantifier from formulas like

$$\exists r_1 \ldots \exists r_r \forall n_1 \ldots \forall n_s A(r_1, \ldots, n_s)$$

to obtain a disjunction

$$A(t_1^{(1)}, \ldots, t_r^{(1)}, f_1(t_1^{(1)}, \ldots, t_r^{(1)}), \ldots, f_s(t_1^{(1)}, \ldots, t_r^{(1)})) \vee \ldots \vee$$

$$A(t_1^{(m)}, \ldots, t_r^{(m)}, f_1(t_1^{(m)}, \ldots, t_r^{(m)}), \ldots, f_s(t_1^{(m)}, \ldots, t_r^{(m)}))$$

where the terms $t_j^{(1)}$ do not contain the ϵ-symbol and the f_i's are function symbols with r-arguments

$$f_1(c_1, \ldots, c_r), \ldots, f_s(c_1, \ldots, c_r).$$

If an equality axiom is added, a pure predicate calculus without the ϵ-symbol can be formulated and opens the way to an Herbrand-type consistency proof.

3.3 Herbrand's Theorem

The elimination theory can be seen as a forerunner to Herbrand's consistency theorem for the predicate calculus. We give a brief treatment of Herbrand's formulation. Let A be a formula in prenex form, for instance

$$A \equiv \exists x \forall y \exists z \forall t B(x, y, z, t)$$

with B quantifier-free. Introduce two new function letters with f unary and g binary with terms $U_1 \ldots U_n, W_1 \ldots W_n$, then A is provable in predicate calculus in the form

$$A \equiv B(U_1, f(U_1), W_1, g(U_1, W_1)) \vee \ldots \vee B(U_n, f(U_n), W_n, g(U_n, W_n)).$$

This disjunction, as the former one, is derivable in propositional calculus and may be used as a criterion of refutability in a *negative* interpretation (see Hilbert and Bernays 1968–1970, II, p. 170 ss).

The negation of A is

$$\neg A \equiv \forall x \exists y \forall x \exists t \neg B(x, y, z, t)$$

or

$$\neg A \equiv \neg B(x, f(x), z, g(x, z))$$

and while Herbrand thought of propositional formulas as refutable in an infinite or indefinite recursive domain "*champ infini*", Kreisel has introduced the no counterexample interpretation as a functional interpretation of higher type: the type recursive functionals are simply defined by

$$B_{x_1 \ldots x_n}[F_1(f_1, \ldots f_n), \ldots F_m(F_1, \ldots F_n)]$$

with B open. For a true formula A, we have

$$B[F(f, g), f(F(f, g)), G(F, g), g(F(f, g)), G(f, g))]$$

where the F's and the G's are obviously our new type recursive functionals (on this see Cook and Urquhart 1993).

This last formula A is true if there is no counterexample of the form

$$\neg B[x, f(x), z, g(x, z)]$$

with f and g being arguments of the higher-type recursive functionals F and $G \cdot H$; F and G are continuous and may thus be linked with polynomials of arbitrary degree; we can define the composition of F and G as

$$F \cdot G = \Big(\sum_i F_i x^i\Big)\Big(\sum_j G_i x^i\Big) = \sum_i \sum_j = \big(F_i G_j x^{i+j}\big).$$

Since we cannot quantify over all such functionals—by diagonalization there is a recursive functional which is distinct from all recursive functionals—we must restrict ourselves to polynomials of finite degree and use descent on degrees and heights of polynomials to recover a finitist version.

Let us remark that primitive recursive functions can be easily translated as polynomial functions. It is obvious for initial constant functions; composition and recursion are treated as the convolution product of functions $G \cdot H$ for G and H such as

$$F(x)_{\vec{n}} = G_n(H_1(a_n), \ldots, H_p(a_n))$$

with

$$H \cdot G = \sum_i \sum_j (F_i G_j x^{i+j})$$

The μ-operator as the equivalent of the least number principle is replaced by infinite (finite) descent on decreasing powers of a polynomial of finite degree

$$F(x)_{\overleftarrow{n}} = f_0 x^n + f_1 x^{n-1} + \ldots + f_{n-1} x + f_n.$$

Along with Hilbert's idea of a terminating sequence of predecessors for a give n, Fermatian descent allows for a finite reduction process in the guise of a decreasing linear order of powers of a given polynomial.

3.4 Tarski's Quantifier Elimination

Another line of attack in Hilbert's metamathematical programme was pursued by Tarski and gave birth to model theory. Elimination of quantifiers led Tarski to the positive solution of the decision problem for elementary algebra and geometry with the use of Sturm's Theorem (Tarski 1951). Artin and Schreier also used Sturm's theorem in their 1927 construction of real fields, but it can be dispensed with and replaced by quadratic forms (polynomials), as is shown by later proofs for the closure of real fields, the end result of which is a disjunctive normal form (disjunction of conjunctions of atomic formulas), a close relative to the Hilbert-Ackermann theorem (1928) for open theories, that is theories whose non-logical axioms are formulas without quantifiers. Obviously, here is a meeting ground for proof theory and model theory—which evolved quite independently afterwards under the auspices of the compactness theorem and Skolem's functions. But to arrive at the syntactic result, Tarski followed a route quite similar to Hilbert's elimination theory. The point of departure is a system of polynomials (see Tarski 1951, p. 31)

$$\begin{aligned}
\alpha &\equiv \alpha_0 + \alpha_1\xi + \ldots + \alpha_m\xi^m \\
\beta &\equiv \beta_0 + \beta_1\xi + \ldots + \beta_n\xi^n \\
\gamma_1 &\equiv \gamma_{1,0} + \gamma_{1,1}\xi + \ldots + \gamma_{1,n_1}\xi^{n_1} \\
&\vdots \\
\gamma_r &\equiv \gamma_{r,0} + \gamma_{r,1}\xi + \ldots + \gamma_{r,n_r}\xi^{n_r}
\end{aligned}$$

over which a function T is defined for formulas Φ of the form

$$\binom{E\xi}{k}[a = 0]$$

where $\underset{k}{E}\,\xi$ means "there exist exactly k values of ξ''" such that $T(\Phi)$ is an equivalent quantifier-free formula. The elimination procedure relies essentially on Sturm's theorem on the number of real roots of a polynomial between two arbitrary values $F_0(x)$ and $F_1(x)$ of the variable and reduces to an Euclidean algorithm for finding the greatest common divisor of $F_0(x)$ and $F_1(x)$ in the counting of variations of sign in the given polynomial (equation or inequality). Although Tarski mentions Kronecker and despite van den Dries' suggestion that elimination theory has evolved in the wake of Kronecker (1988), Tarski does not draw directly from Kronecker's theory of forms (polynomials). Kronecker's general arithmetic of "algebraic quantities" is a theory of content of polynomials, but Tarski will use a notion of content only in his theory of implication and logical consequence. In that context, Sturm's theorem appears as a special case of Kronecker's divisor theory. I shall outline in the next section a treatment of polynomials in the more general setting of Kronecker together with Fermat's infinite descent, which is in fact a generalization of Euclid's algorithm. If Tarski concludes (1951, p. 53) that the decision method amounts to a proof of consistency and completeness (for real closed fields, for example), my aim is self-consistency of arithmetic and I review now Gödel's idea of an internal consistency proof as an extension of the finitist point of view.

3.5 Gödel's Functional Interpretation

Gödel (1958) introduced functionals (recursive functions of higher types) over all finite types as abstract objects beyond the (concrete) natural numbers. The *Dialectica* interpretation has been extended by Spector, Howard and Kreisel and others in the intuitionistic spirit of bar-induction and bar-recursion of finite type. Although Gödel was animated by intuitionistic motives, his proof for Heyting arithmetic can be translated for Peano arithmetic where its constructive content can be carried over. I propose a different approach to the consistency problem. Arithmetic here is not Peano arithmetic, but Fermat (or Fermat-Kronecker) arithmetic with Fermat's infinite descent replacing Peano's induction and we have Kronecker's indeterminates instead of functional variables. The "general arithmetic" of polynomials (or forms, in Kronecker's terminology) is built upon "effinite" (infinitely proceeding, in Brouwerian terminology) sequences. Finite sequences are sets and the Cauchy (convolution) product for polynomials is used as a mapping from sequences to sequences in while the degree of a polynomial replaces the type of a formula, the motive here being a formulas-as-polynomials interpretation.

Gödel states in a phrase reminiscent of Gentzen that the notion of accessibility "*Erreichbarkeit*" is an abstract concept which requires a kind of reflection on finite constructions. Such a notion is the notion of a computable functional of finite type over the integers, which Gödel substitutes for the abstract notions of assertion and proof in intuitionistic mathematics. Formulas like

$$F = \forall x \exists y A[x.y.z]$$

and

$$G' = \forall w \exists v B[w, v, u]$$

will be used to obtain a consistent interpretation of Heyting's arithmetic: for example, we have

$$(F \supset G)' = \forall y, w \exists VZ[A(y, Z(yw), x) \supset B(V(y), w, u)]$$

and

$$\neg(F)' = \exists y \exists \bar{Z} \neg A(y, \bar{Z}(y), x)$$

where x, y, z and w are finite sequences of variables of arbitrary type, u is a sequence of number variables while Y, V, Z and $\bar{Z}$ are second-order variables—A and B are quantifier-free. Those generalized formulas (see Schoenfield 1967, p. 218) constitute the functional interpretation. Gödel defines the finite types inductively with the following three clauses:

1. 0 is a finite type (the type of integers)
2. if s and t are finite types, then $s \times t$ (their Cartesian product) is a finite type
3. if s and t are finite types, then $s \rightarrow t$ is also a finite type.

Remark: the third clause means that there is a mapping from functionals of type s to functionals of type t.

The last transformation raises questions of interpretation and the literature on the subject is abundant, but I observe only that I translate this mapping as a convolution product for polynomials. By the Curry-Howard isomorphism we can identify types and formulas, in particular a product of types is identified to a conjunction of formulas. I extend the isomorphism by having implication identified to a power representation. Formulas can be rendered in the following manner:

$$\exists x \forall x \supset \exists y B y = \sum_{0}^{n} \left(\sum \bar{a}_0 x + \sum b_0 x \right)^n$$

and

$$\forall x A x \supset \forall y B y = \prod_{o}^{n} \left(\prod \bar{a}_0 x + \prod b_0 x \right)^n$$

where $\bar{a}_0$ stands for $1 - a$ with integral coefficients a and b and indeterminate x. Combinatory logic is of no help in that context, since it fulfils only an abstract goal which seems superfluous in arithmetic.

Such a rendering of formulas is in line with Hilbert's arithmetization programme as we shall presently see.

Hilbert had introduced the notion of a "disparate (mixed) system of functions" with the explicit aim of producing a consistency proof for the pure predicate calculus (i.e. without identity). The functions in question are simple arithmetic functions which associate a numeral with a numerical expression in such a manner that for a given numerical symbol "*Ziffer*" p and a disparate function system

$$\varphi_1, \ldots, \varphi_s,$$

the disjunction $S_p^{(\varphi)}$ is derivable in the propositional calculus. A disparate or mixed function system is, for example (see Hilbert 1968–1970, II, p. 175)

$$\varphi_i(n_i, \ldots, n_r) = \psi_0^i \cdot \psi_1^{n_i} \ldots \psi_r^{n_r} \qquad (i = 1, \ldots, s)$$

where the ψ_i's are the first $r + 1$ primes. The idea is to associate, *disparately*, to each r-tuple of numerical symbols a different numerical symbol. The procedure looks like Brouwer's choice sequences, as Hilbert remarks, and can be extended to infinitely proceeding sequences. This first step in the arithmetization process must be completed by an arithmetical imitation of the grammatical structure of logical formulas (1968–1970 II, 217) through a translation with the help of recursive functions and predicates. Gödel achieved that kind of translation for the syntax of Peano arithmetic. We know that in this case the arithmetization could not be completed, mainly because the induction over an infinite set of numbers lends itself to Cantor's diagonalization procedure in contrast to Cauchy's diagonalization (the convolution product) which we can apply to Fermat-Kronecker arithmetic.

It might be worthwhile to note that the potential infinity of Brouwer's choice sequences, which Hilbert alludes to, allows for a treatment of the consistency problem compatible with Hilbert's programme. It is apparently in his attack on Cantor's continuum problem (see Hilbert and Bernays 1968–1970, II, p. 216) that Hilbert had the idea of arithmetization. The fact that the translation of transfinite arithmetic into finite arithmetic has not succeeded in Hilbert's hands is certainly one of the reasons for the success of the incompleteness results. Hilbert's programme however is not confined to set-theoretic arithmetic in Hilbert's own terminology and I am tempted to say that the ideal of arithmetization survives for the very reason that, as Hilbert confessed, the programme itself antedates Hilbert's efforts and can be traced back to Kronecker's idea of arithmetization of algebra. Arithmetization of logic is but a consequence of that original programme which was taken anew by E. Nelson's predicative arithmetic.

Robinson's theory of arithmetic Q is consistent and essentially undecidable. But E. Nelson's proof for the self-consistency of Q in (Nelson 1987a,b) rests on a notion of genetic, as opposed to formal, number which allows for a computable or polynomially bounded exponentiation in the form

$$\sigma_0(\ell, n) = \exists f \; Exp \; Comp \; (\ell, n, f)$$

$$\sigma_n = \sigma_0(n, n).$$

The theorem on logical consistency says for a theory T:

$$T \text{ is tautologically consistent} \rightarrow T \text{ is } \sigma - \text{consistent}$$

and the inference

$$\sigma(b) \rightarrow \sigma(Sb)$$

is genetic while exponentiation $e(n)$ does not imply $\forall n \; e(n)$; exponentiation is not total

$$\exists n \neg \varphi(n) \qquad \text{for } \varphi = e^y.$$

This is reminiscent of Herbrand's arithmetic with induction on formulas without free variables (quantifier-free induction). Nelson's proof is based upon the Hilbert-Ackermann consistency proof for open theories (without quantifiers) which reduce to disjunctive propositional formulas—as in Herbrand's theorem—and they can be considered as *de facto* or intrinsic polynomials. In Nelson's genetic self-consistency proof for predicative arithmetic, the numbers denoted by terms of the arithmetized theory are bounded by the terms themselves (see Nelson 1987a,b, p. 176), while in the case of polynomialized arithmetic, the numbers (the terms) are bounded by the degree (and the height) of the translation polynomial. Bounded polynomial arithmetic would be an appropriate name for such an arithmetic. If we look at primitive recursive arithmetic and add as in Hilbert or Herbrand some restricted form of the least number principle (also found in Nelson), we are coming close to an arithmetic which I call Fermat arithmetic, where the Peano's induction postulate is replaced by the method of infinite descent, which is not equivalent to (formal) infinite induction from a constructive point of view: the equivalence requires a double negation over an infinite set of natural numbers, a procedure which is obviously disallowed on constructivist (intuitionistic) grounds. Poincaré—who calls infinite descent "*récurrence*"—and Peirce are two authors who have forcefully emphasized the distinction for different reasons. The main reason to me is that infinite descent embodies a central method of proof in number theory. The method is employed negatively as *reductio ad absurdum*, but also positively. Fermat, Euler, Lagrange, Legendre and Kummer all used the method to prove important theorems in number theory. Nowadays, Mordell, Weil and others use it in arithmetic (algebraic) geometry.

Hilbert acknowledges that Kronecker has succeeded in constructing a finitary theory of algebraic numbers and of the field of algebraic numbers, but he says that this theory was to be found only in Kronecker's lectures without mentioning that the major paper of 1889 "*Grundzüge einer arithmetischen Theorie der algebraischen Grössen*" contains certainly the main ingredients of the theory. Nevertheless, Hilbert does not misrepresent Kronecker's achievements and one can suppose that it is the same process of association he has in mind when he wants to adjoin ideal elements to finite arithmetic, although he seems to give credit to Kummer rather than to Kronecker (Hilbert 1926).

The finitist "stand", "*die finite Einstellung*", is certainly the heir of Kronecker's arithmetical constructivism, but the introduction of the ϵ-symbol and formal logic that one eliminates to come back to the internal "*inhaltliche*" logic of arithmetic means that finite arithmetic is self-consistent by construction: logical formulas are true by granting them numerical content through numeral substitution in the method of return and polynomial decomposition or descent reverses the process of construction into a process of reduction. If the notion of predecessor is more structural or less internal than the notion of "smaller than", as Hilbert suggests, it is to preserve the axiomatic character of the least number principle, but its true arithmetical nature is revealed in the finite process of the Fermatian method of descent.

Formal logic for Hilbert has only an ancillary rôle, it only guarantees the passage from arithmetic to its algebraic extensions through the adjunction of ideal elements (indeterminates). But these ideal elements are algebraic in essence and Kronecker did not need formal logic for his general arithmetic. From Kronecker, the negative transcendence of non-algebraic extensions cannot be redeemed by indeterminate quantities (Kronecker 1882, p. 253). At this point, one is reminded of Steinitz who in his 1910 "*Algebraische Theorie der Körper*" has "completed" the Kroneckerian theory of domains of rationality integrating infinite transcendent extensions (with an infinite number of indeterminates also called "transcendents"), but only by resorting to set-theoretic notions of well-order (the axiom of choice and transfinite induction on ordinals). The continuation is no more of Kronecker's intent and Kronecker had warned (Kronecker 1882, p. 156) against infinitary procedures and had emphasized the fact that infinite power series have an arithmetical construction of their coefficients and also that finite polynomial expressions dispense with any extension of the concept of finite series.

The way back from extensions in the ideal realm meant for Hilbert that consistency of analysis and set theory could be attained by finite means. But the reduction has also another meaning for Kronecker: the theory of divisors or congruences in modular systems affords a reductive theory of algebraic extensions under the isomorphism between extensions with a finite number of indeterminates and polynomials in the field (or rather domain of rationality) of algebraic numbers. It is that lesson which Hilbert seems to have remembered, at least partially, in his ultimate finitist programme of the *Grundlagen der Mathematik*. But it is the algebraic closure of the theory of indeterminates (beneath the theory of real fields) which limits upstream Hilbert's programme whilst Gödel's incompleteness results are only a downstream obstacle that is not fatal to finitist foundations understood in Kroneckerian terms.

3.6 Skolem and Brouwer

Skolem, like Herbrand, was an arithmetician and has conceived arithmetic as a recursive procedure in terms of elementary operations indefinitely iterated and he has defended a finitist constructivist standpoint in the line of Kronecker (see Skolem 1970). He is the first to define primitive recursive functions without having recourse to quantifiers or infinite domains with quantification over variables in the infinite set of natural numbers. Again, like Herbrand, he was inspired by intuitionistic or rather constructivist motives and rejected the excluded middle principle beyond primitive recursive functions and into general recursive functions admitting the least number principle with the μ operator. The functions of addition, multiplication and the relation of divisibility defined as

$$D(a, b) = \sum\nolimits_x (a = bx)$$

are limited to a finite domain of application, as in the case of the Euclidean algorithm for the greatest common divisor and the least common multiple. Here Skolem devotes a long development to the notion of prime number and to the definition of a least number for which a certain proposition P is true without binding it to a universal quantification on an infinite domain; such a proposition is always decidable for an arbitrary x in a finite domain. This discussion reminds of Hilbert's idea of the least number principle in his elimination procedure of the epsilon symbol, but with Fermatian and Kroneckerian overtones on this occasion, if one may say.

What Skolem calls a descriptive function is a function that does run on a finite set or sequence of positive integers with the constructive definition (or description) of a given integer n; the same goes for the concept of cardinality when one uses a finite function or mapping to define a cardinal number of a finite class of elements and then generalize the notion to an arbitrary class of objects. Skolem concludes by saying that he doubts of the possibility of a justification for the actual infinite or the transfinite and he reiterates his adhesion to a finitist standpoint in agreement with the Kroneckerian idea of determination "*Bestimmung*" of mathematical concepts: such a determination, which one can identify with an algorithm, is a process completed in a finite number of steps according to Hensel's characterization of Kronecker's finitism.

Although Brouwer did not deal with arithmetic or number theory, his main interest being analysis, he did contribute to the arithmetization of logic with his critique of the excluded middle principle for infinite sequences and non-constructive proofs in classical analysis. He introduced the notion of choice sequences which constituted the foundations of constructive analysis for which Bishop (1967) claimed numerical content (see below). Intuitionistic logic summarized in the BHK interpretation was defined as the canonical interpretation of a constructivist logic which consists in refuting certain principles of classical logic like the following for sequences α:

1. $\neg\forall\alpha \vee \exists x(\alpha x = 0)$
2. $\forall\alpha\neg\neg\exists x(\alpha x = 0)$
3. $\neg\forall\alpha(\exists x(\alpha x = 0) \vee \neg\exists x(\alpha x = 0))$
4. $\neg(\exists\alpha\neg\neg\exists x(\alpha = 0) \rightarrow \neg\neg\forall\alpha\exists x(\alpha x = 0))$
5. $\neg\exists\alpha(\neg\neg x(\alpha x = 0) \rightarrow \exists x(\alpha x = 0))$

where 2 refutes the excluded middle principle and 5 refutes Markov's principle which supposes that

$$\neg\neg\exists xA(x, y) \rightarrow \exists xA(x, y).$$

These are "negative" counter-principles or counter-examples, but they should not be counted as improductive. The positive side has been used by Kolmogorov to distinguish "true" mathematics from the (classical) mathematics of pseudo-truth, while Gödel introduced his 1933 "negative" one-way translation of intuitionistic logic into classical logic in order to insure its consistency:

1. $P^- = \neg\neg P$
2. $(P \rightarrow Q)^- = P^- \rightarrow Q^-$
3. $(P \wedge Q)^- = P^- \wedge Q^-$
4. $(\neg P)^- = \neg P^-$
5. $(P \vee Q)^- = \neg(\neg P^- \wedge \neg Q^-$
6. $(\forall xPx)^- = \forall xP^-x$
7. $(\exists xPx)^- = \neg\exists x\neg Px)$.

Gödel also recognized that Brouwer's critique of classical logic and mathematics was an incentive for his own *Dialectica* functional interpretation as an extension of the finitist point of view. However it is certainly the Brouwerian procedure of associating natural numbers as integral values to species (sets) and choice sequences as in the fan theorem for finite sequences or the bar theorem—a constructive analogue of the Peano's induction postulate which has been an important moment in the arithmetization process. Notwithstanding the real constructive content of those principles, il is clear that they are important steps in the arithmetization of logic. Brouwer's attempts at the constructivization of analysis can certainly be seen as preparing Gödel's arithmetization of syntax, even though Gödel's incompleteness results for Peano arithmetic cannot be deemed as thoroughly constructive.

3.7 Gödel and Turing

Gödel has achieved the arithmetization of syntax following the steps of Hilbert and Russell in the axiomatization of arithmetic. The arithmetic in question is Peano's arithmetic—the S_2 formal system as we label it—and it involves the infinite set of natural numbers with the cardinality $\aleph_0$ (see Gödel 1931 and Gödel 1967). His completeness result for first-order predicate logic was already couched in the model-theoretic language of set-theoretical semantics with a denumerable universe. The representation of recursive functions (primitive and general) and relations in Peano's arithmetic led him to arithmetize the logical syntax of the formal system with the help of a numbering (Gödel numbering) which associates formulas to natural numbers. Using a diagonal argument *à la* Cantor, Gödel could now construct an undecidable sentence in S_2. The relation $Pr_A((u),y)$ is primitive recursive; Pr is represented in S_2 by the wff $\underline{Pr}(\underline{x}_1,\underline{x}_2)$ in the object language. Take now the formula $\forall\underline{x}_2\neg\underline{Pr}(\underline{x}_1,\underline{x}_2)$ and k as r the Gödel number of that formula; by substituting $\bar{k}$ to x_1 in the formula, one obtains the closed formula or the sentence

$$\forall\underline{x}_2\neg\underline{Pr}(\bar{k},\underline{x}_2) \qquad (*)$$

which corresponds to the relation $Pr((u),y)$. That formula says in reality that there is no proof represented by the variable x_2, of $\forall\underline{x}_2\neg\underline{Pr}(\bar{k},\underline{x}_2)$ and such a formula supposes the fixed-point theorem for the sentence k

$$\vdash_{S_2} k \leftrightarrow A(\bar{k});$$

the formula $A(k)$ is obtained by substituting in $A(x_1)$—which has x_1 as its only variable—the Gödel number of the sentence k to x_1. The sentence k then says indirectly about itself that it is true by the equivalence between the sentence and the formula expressing its Gödel number. This leads to Gödel's theorem (1931) which states that:

1. If S_1 is consistent, then the wff $(*)$ is not provable in S_2.

The proof is simple: suppose that S_2 is consistent and that $\forall\underline{x}_2\neg\underline{Pr}(\bar{k},\underline{x}_2)$. Take t as the Gödel number of a proof of that wff in S_2; we have then $Pr(k,t)$, hence $\vdash_{S_2} \underline{Pr}(\bar{k},\bar{t})$. But from $\forall\underline{x}_2\neg\underline{Pr}(\bar{k},\underline{x}_2)$, one gets $E\forall$(by elimination of the universal quantifier) $\neg\underline{Pr}(\bar{k},\bar{t})$. $\underline{Pr}(\bar{k},\bar{t})$ et $\neg\underline{Pr}(\bar{k},\bar{t})$ are both provable, therefore contradiction (since we have supposed S_2 to be consistent).

2. S_2 is ω-consistent, then the negation of $(*)$ is not provable in S_2.

Proof: ω-consistency means that for any $A(x)$ and for all natural numbers n

$$\vdash_{S_2} A(\bar{n}) \rightarrow \bar{n}_{S_2}\exists x\neg A(x).$$

Let us suppose first that $\neg\ (*)$, that is

$$\vdash_{S_2} \neg\forall x_2\neg Pr(\bar{k},x_2),$$

we have then

$$\vdash_{S_2}\ \exists x_2\, Pr(\bar{k},x_2), \qquad (**)$$

but by the consistency of S_2, we have

$$\nvdash_{S_2} \neg\forall x_2 \neg Pr(\bar{k}, x_2)$$

thus

$$\forall n(\vdash_{S_2} \neg Pr(\bar{k}, \bar{n}))$$

and by ω-consistency of S_2, this means that for all natural numbers n, n is not the Gödel number of $(*)$, consequently

$$\nvdash_{S_2} \exists x_2 Pr(\bar{k}, x_2) \qquad (**)$$

which contradicts $(**)$.

The second incompleteness theorem or theorem on the consistency proofs asserts that if S_2 is consistent, the wff formula Cons_{S_2} is not provable in S_2, then $\nvdash_{S_2} \mathrm{Cons}_{S_2}$. As a matter of fact, Gödel's second incompleteness theorem supposes that

$$\vdash_{S_2} \mathrm{Cons}_{S_2} \rightarrow \text{the wff } (*)$$

but is not provable as shown above, thus

$$\vdash_{S_2} \mathrm{Cons}_{S_2} \rightarrow \text{the wff } (*)$$

is a false sentence. Otherwise, if S_2 is inconsistent

$$\vdash_{S_2} \mathrm{Cons}_{S_2} \rightarrow \text{the wff } (*)$$

is a true sentence, then

$$\nvdash_{S_2} \mathrm{Cons}_{S_2}.$$

Other results like Tarski's theorem on the undefinability of truth in S_2 characterize Peano's theory as a set-theoretic arithmetic. But Turing gave a new turn to arithmetization of formal systems by introducing the notion of computation as a mechanical process.

With Turing, arithmetization of logic entered the era of theoretical computer science which has become in the words of Yuri Gurevich a challenge for logic itself (Gurevitch 1988). Gödel had praised Turing already in 1937 for the correct definition of computability (as a mechanical procedure), but later on deplored that Turing's machines put a limitation on the transcendent powers of the human mind! In any case, Turing computability has to do with finite procedures or algorithms and could certainly be considered as a natural (or artificial!) extension of Kronecker's finitism. Turing himself has attempted to overcome the limitations of the incompleteness theorems by investigating ordinal logics which were intended to pull back the transfinite ordinal machinery into the finite. Gurevich's abstract machines as finite state machines are an instance of drawing on bounded resources to produce dynamic structures capable of surmounting the limitations of classical logic. In the same vein, Gurevich's search for a logic of infons or information units indicates that classical logic, or even intuitionistic logic, do not capture the internal structure of information from a computer-theoretical point of view. From a different perspective, finite model theory does not house the metalogical properties (completeness, Löwenheim-Skolem, etc.) of classical first-order logic since Trakhtenbrot's theorem (1950) has shown that the set of all finite structures or classes—due to the lack of a definite cardinality—is not recursively enumerable, i.e. is not decidable.

The problem of computational complexity for decision problems has come to the forefront and complexity classes range from polynomial time to exponential space inside deterministic and non-deterministic Turing machines with the culmination in the $P = NP$ problem; is the non-polynomial reducible to the polynomial? The question is still undecided, but it shows that the theory of algorithms and complexity theory have taken up arithmetization beyond the field of logic. Applied proof theory, programming languages and proof verifiers (Coq, Agda) exhibit constructive features that tend to demonstrate that finitism is gaining ground in the arithmetical foundations of mathematics. Meanwhile, work on formal arithmetic, Peano arithmetic and its fragments or subtheories and subsystems, has been going on.

3.8 Arithmetic

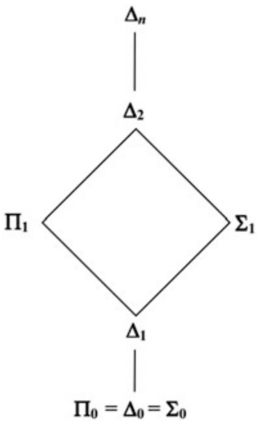
The study of fragments of Peano arithmetic (see Hájek and Pudlák 1993; Kaye 1991) is relatively recent; for all practical purposes, it has taken over the study of subsystems of analysis which has not given the expected fruits. Reductive proof theory for subsystems of classical analysis aimed at reducing the consistency problem of classical analysis. Reductive model theory may be the appropriate name for the consistency problem of fragments of arithmetic. But here also consistency is a genetic problem, since the consistency of a fragment depends on the consistency of the whole, i.e. Peano arithmetic. The hierarchy $\varDelta_n$ of fragments is infinite

$$I\sum_0 \subseteq I\sum_0 +\varOmega_1 \subseteq I\sum_0 +\varOmega_2 \subseteq \ldots \subseteq I\sum_0 +Exp \subseteq I\sum_0 +Superexp$$

where I is induction and $\varOmega_1$ is

$$\forall x \exists y (x^{\log_2 x} = y)$$

and none of the fragments is finitely axiomatizable. The fragments $I\varDelta_0$ and $I\varDelta_0 + \varOmega_1$ in the hierarchy



(for Δ_0 the class of bound formulas with quantifiers and terms $\forall x < t$ and $\exists x < t$) are not consistent, that is not interpretable in Robinson's system Q (or R) for sequences of polynomial length. But exponentiation cannot be total

$$I\Delta_0 \vdash \forall x \forall y \exists x\ \eta(x, y, z)$$

for $\eta = \exp : x^y = z$ and in $I\Delta_0 + \Omega_1$, 2^x exists iff 2^{2^x} exists in such a way that for a bound formula $\varphi(x)$, we have

$$I \sum_{o} + \Omega_1 + \forall x(|x|^{k+1}) \qquad \forall k$$

where $|x|^k$ denotes the function $x \to |x|$ reiterated x times for $|x|$ the length of the binary representation of x. Then

$$\vdash \neg\big(I \sum_{o} + \Omega_1 + \forall x(|x|^{k+1})\big)$$

implies the consistency of φ—by Gödel's second incompleteness result; 2^x exists iff 2^{2^x} exists means that there is an infinite hierarchy of applications of bounded exponentiation.

Hilbert-Ackermann theorem and Herbrand theorem on consistency have a rôle to play in complexity theory and Gentzen's Hauptsatz or the elimination of cuts, i.e.

$$\frac{A \vdash C \quad C \vdash B}{A \vdash B}$$

is evoked in bounded arithmetic to contravene the superexponentiation involved in cut elimination or in the elimination of transitivity for implication

$$\frac{A \supset D \quad D \supset B}{A \supset B}.$$

Consistency in that context puts constraints on the length of proofs, their incompressibility rate, if one is willing to speak the language of Kolmogorov-Chaitin algorithmic complexity theory. In that connexion, logics without *modus ponens* (without the need of cut elimination) are conceivable that would reduce maximally the length of proofs in the spirit of complexity theory (see Carbone and Semmes 1997). In the same direction, probabilistic proof systems, interactive proof systems or zero-knowledge proofs (see Goldreich 1995), all define effective computation in terms of effective bounds on the complexity of proofs taking into account a randomization process that delivers pure validity of a proof without further ado. Classical proof theory is then reduced to its bare essentials in the form of a finite system, over and above the geometry of proofs which displays proof figures as spatial (graphical) configurations with or without interaction. Geometry is still another possibility, this time maybe without any player of the game, unlike current game theory.

In that context, Robinson arithmetic Q is an open theory with a finite set of axioms and without Peano's induction postulate, but it has the infinite set of natural numbers as its intended interpretation and is thus essentially undecidable. E. Nelson's proof for the consistency of Q rests on a notion of a genetic number, that is a non-formal number which allows for a computable or polynomially bounded exponentiation in the form

$$\sigma_0(I,n) = \exists f Exp\ Comp\ (1,n,f)$$

$$\sigma_n = \sigma_n(n,n).$$

The theorem on (logical) consistency says for a theory T

$$T \text{ is tautologically consistent} \rightarrow T \text{ is } \sigma\text{-consistent}$$

and the inference

$$\sigma(b) \rightarrow \sigma(Sb)$$

is genetic while exponentiation $e(n)$ does not imply $\forall n\ e\ (n)$; exponentiation is not total

$$\exists n \neg \varphi(n) \quad \text{for } \varphi = e^y$$

and one goes back to Parikh's theorem (1971) which states that total exponentiation cannot be proven in bounded arithmetic. However, as Nelson notes, Parikh's proof is not constructive, since it is cast in a non-standard model (of Peano arithmetic) in which a non-standard integer is called upon

$$\forall x \exists k (x < \alpha^k) \qquad \text{for a standard } k$$

generating a submodel where bounded arithmetic is valid. The non-standard model hosts also a non-standard y such that for $B = \alpha - k$, one gets

$$\exists y(x \cdot B) \geq 1 \cdot \alpha^k) \text{ for } y \neq 0$$

which is impossible. By way of consequence, Parikh's theorem states for bounded exponentiation $r = x^k$ that

$$\forall x \exists y \varphi(x, y) \rightarrow \forall x \exists y \leq r(x) \varphi(x, y)$$

and for Herbrand's theorem, that we have a term $t(x)$ such that

$$\forall x \exists y \varphi(x, y) \rightarrow \forall x \exists t(x) \varphi(x, t(x)).$$

In the framework of feasible arithmetic introduced by Parikh, there is no proof of

$$P^k(A) \vee P^k(\neg A)$$

for $P(A)$ the smallest number of symbols corresponding to a (reasonable) feasible proof of A for a sufficient large k in Zermelo-Fraenkel axiomatic set theory. It is certainly appropriate to recall here Poincaré's critique of induction in the footsteps of Parikh's feasible arithmetic. The critique addresses the justification of (formal) complete induction grounded on another formal induction, that is by ω-induction on all n

$$P[A(\bar{0})] \vee P[A(\bar{n})] \rightarrow P[A(S\bar{n})] \rightarrow P[A(\bar{n} + 1)].$$

By *MP*, it follows that

$$\forall x A x \equiv \forall n P[A(\bar{n})].$$

Bars mean that we have to do with numerals and formal equivalence is obtained in a Gödelian fashion when one supposes that ω-induction is a logical inference on $\forall x A x$; we are back to Nelson's critique of unbounded induction, since inductive exponentiation $e(n)$ is subjected to Gödel's second incompleteness result, but the self-consistency of Robinson's arithmetic does not fall a prey to the predicament for the reason that the consistency proof is bounded by the very terms of predicative arithmetic. Poincaré's criticism is further evidence for the link between the impredicativity of formal induction (or complete induction) and *MP* inference for unbounded arithmetic. Poincaré, as a semi-intuitionist, seems to have anticipated to some extent the rise of bounded predicative arithmetic.

3.9 Constructive Arithmetic and Analysis

From a full intuitionistic point of view, a constructive function is defined as

$$\forall x \exists y \; \varphi(x, y) \rightarrow \exists f \; \forall x \varphi(x, f(x))$$

that is, for a formula $\varphi(x, y)$ there is a function f of x which computes the value $y, f(x) = y$

$$\forall x \exists f \varphi(x, f(x))$$

for

$$\forall x \exists !\, y \varphi(x, y).$$

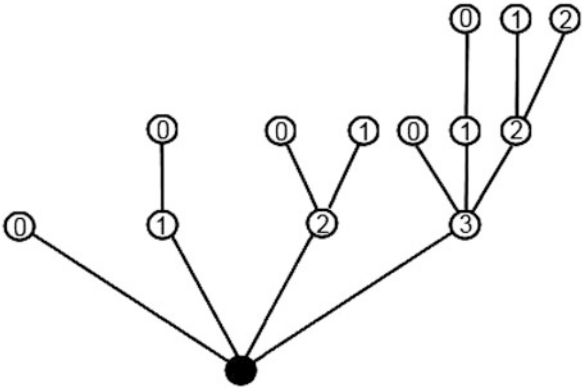
In the general framework, one can draw on the system $I \sum_1$, a formal system for recursive functions or $I \sum_1^1$, a formal system for recursive functionals. The Brouwer-König theorem may be seen in that context as a finiteness theorem in one direction

$$\forall x \exists F \varphi(\vec{x}), F(\vec{x}) \rightarrow \forall n \exists F \forall x \leq n \varphi(\vec{x}, F(\vec{x}))$$

for $\vec{x} = (x_0, \ldots x_n)$ and as a theorem on infinity in the other direction

$$\forall n \exists F \forall x \leq n \varphi(\vec{x}, F(\vec{x})) \rightarrow \forall x \exists F \varphi(\vec{x}), F(\vec{x}).$$

König's lemma is a statement of induction on well-founded trees



$$\forall b \in A \exists n \forall m (m > n \rightarrow b^* < n >= 0) \rightarrow \exists N \forall b (b \leq N)$$

for all branches b (lengths of initial segments) of a well-founded A, $*$ the concatenation operation and N the top of the tree (its height). The strong König's lemma stipulates that if A is an infinite tree with finite branching, there is a path $S \leq A$. Notice that a well-order is a well-founded order which is linear for a linear polynomial x such that $x \rightarrow y^x$. Obviously, König's lemma is infinitary when we have quantification over all finite sequences of natural numbers; here an ordinal is the number of a transitive well-order which is a well-founded linear order. To any initial segment corresponds an ordinal and Zermelo's theorem states that the class of all ordinals is well-ordered by $\in$ $(\leq)$ while the axiom of foundation in $Z - F$ postulates that all sets are well-founded. Continuing along that line, transfinite induction rests on Cantor's normal form theorem for recursive ordinals up to ω_1; this iterated exponentiation of linear order cannot be predicative and might be inconsistent. But let us regress to our point of departure.

König's lemma is akin to Brouwer's bar-induction principle for lawless sequences (well-founded species of finite sequences)

$$\forall\alpha\exists x X(\bar{\alpha}x) \wedge \forall n(X(n) \to Y(n)) \wedge \forall n\forall m(X(n) \to Y(n * m))\wedge$$

$$\forall n(\forall x Y(n * \hat{x} \to Y(n)))\forall n Y(n)$$

for any property of an inhabited sequence $\hat{x} =< x >$. Bar induction, as a matter of fact, has been compared to transfinite induction on ordinals

$$\forall\sigma[\forall t(t < \sigma \to A(t,x) \to A(\sigma,x))]\forall\sigma(\sigma,x),$$

but it has more import in association with Brouwer's principle for numbers

$$\forall\alpha\forall x X(\bar{a},x) \to \forall\alpha\exists x\exists y\forall\beta(\bar{\alpha}x = \bar{\beta}x \to X(\beta,y))$$

which means that if we have a procedure which allows for the determination of a natural number x for any choice sequence α, then the same procedure allows for the determination of a natural number y for any other choice sequence having the same initial segments; in other words, the existence of a definite numerical value for an arbitrary choice sequence implies that there is a continuous regular functional which can determine that value

$$X\bar{\alpha}x = X\bar{\beta}y.$$

The fan theorem looks more like a finiteness theorem for choice sequences

$$\forall\alpha\exists x X(\mathit{\Gamma}_\alpha\alpha, x, \alpha_0, K) \to \exists y\forall\alpha\exists x\forall\beta(\mathit{\Gamma}_\alpha ay = \mathit{\Gamma}_\alpha a\beta y \to X(\mathit{\Gamma}_\alpha\beta, x, \alpha_0, k))$$

where X is a species (of properties), $\mathit{\Gamma}$ a continuous functional, α a choice sequence, x a natural number and a a fan (or spread) law defined by the following four clauses

1. $\alpha 0 \neq 0$
2. $\forall n\forall m(a(n * m) \neq 0$
3. $\exists n\exists x(an \neq 0 \to an * \hat{x} \neq 0)$
4. $\forall n\exists z\forall x(an * \hat{x} \neq 0 \to x \leq z)$

The fourth clause is a finiteness stipulation. The fan theorem is instrumental in Brouwer's proof of his fundamental theorem "any real-valued function defined on the interval $[-1, 1]$ is uniformly continuous"—for all these notions, see Gauthier (2000).

It would be excessive to consider the various principles of intuitionistic arithmetic as a formal bounded arithmetic, but its finitary inspiration is quite evident. It is not an easy matter to trace a boundary line between the constructive and the non-constructive and the extensions of the finitary viewpoint open up often with infinite vistas on the non-constructible.

Let us take, for example, induction on Δ_0 bounded formulas (for fragments of arithmetic) together with the following collection or replacement axiom

$$I\sum_1 \vdash \forall x \leq u \exists y\, \varphi(x,y) \rightarrow \exists v \forall x \leq u \exists y \leq v \varphi(x,y)$$

or the following comprehension axiom

$$I\sum_1 \vdash \forall x \exists y, z \forall u \leq x (u \in (x,y) \equiv \varphi(u)),$$

then we have full Peano arithmetic

$$Pa = I\Delta_0 + \ Collection.$$

Strictly bounded arithmetic can afford those principles only by restricting terms t in

$$\exists \omega \leq t(s,t)$$

and defining

$$t(s,t) = bound(s, s^{|t|+1})$$

where $2^{|t|+1}$ is a finite polynomial bound. Fragments of arithmetic must be bounded themselves in order to cope with the notion of finite computability central to bounded arithmetic (see Buss 1986). Recursive function theory or classical recursion theory are unable to capture elementary calculable functions without the concept of bounded recursion. If Nelson's predicative arithmetic is self-consistent, it is because the numbers denoted by the terms of the arithmetic theory are bounded by the terms of the original theory Q. Buss' bounded arithmetic entertains two special functions

$$|x| = [\log_2(x+1)]$$

for the length of the binary representation of x and the diesis function

$$x\#y = 2^{\log x \cdot \log y}$$

for logarithmic bounds.

3.10 Complexity

Bounded arithmetic hoists also logarithmic and polynomial bounds for induction $\sum_1^b LIND$, $\sum_1^b \Pi IND$ or even $\sum_1^b LMIN$ for the least number principle which is dual to $\sum_1^b \Pi IND$. The idea of a logarithmic induction enables the verification of an inductive property taking only polynomial time and this leads us again to (algorithmic) complexity theory where the principal question is $P = NP$? i.e., is polynomial time (of a computation) the same as non-deterministic polynomial time in which many actions take place in a given state (of a Turing machine, for example)? Another problem is

$$NP = CO - NP?$$

for the complement of NP. But here in analogy with the Δ_n hierarchy of fragments of arithmetic, the hierarchy of polynomial time P, $\sum_1^p$, Π_1^p (between linear and exponential time) does not collapse on a finite level, it is infinite. Induction is once again the target and it seems that in order to deal with infinity, one has to bind down induction to finite descent, the bound of infinite or indefinite descent.

Bishop (1967) has baptized "principle of logical omniscience" the generalized excluded middle principle

$$\forall x P(x) \vee \exists x \neg P(x)$$

which Brouwer was the first to reject (only for infinitely proceeding sequences, of course). But the principle is clothed in different forms. For example, the relation of total accessibility in a Kripkean semantics induces a principle of transit over all possible worlds. At the other extreme, the concept of feasible number confines to a limited accessibility and Sazonov's (1995) principal axiom imposes the limit

$$\forall y(\log_2 \log_2 < 10)$$

and makes it impossible to transgress

$$2^{2^{10}} = 2^{1024} = \infty.$$

Compare this bound to the bound of superexponentiation in Nelson's predicative arithmetic (1986)

$$2 \Uparrow 5 = 2^{65,536}$$

or to J. Mycielski's theory of finite sets (Mycielski 1981) with the bound

$$c < \omega_p$$

for constant c and a rational number p. In the last case, the notion of potential infinity plays an important rôle in set-theoretic semantics, but it doesn't have any impact on complexity theory where *untractable* problems concern computational feasibility rather than decidability in a logical classical sense. Bounded linear logic (see Buss and Scott 1990) enjoys resource polynomials to take care of perishable goods (temporary data)! Although not on a par with classical logic, theoretical computer science can display its riches, but they are of limited applicability and negation by default lurks at the corner. Greater danger lies in the deep: infinitary classical logic and Peano arithmetic are but superficial symptoms of a science of the infinite which Leibniz had dreamed of, but would be actualized only in a model theory of finitely generated infinitesimals (with compactness and ultrapowers!).

The theory of series is the true arena of the infinite and before Cauchy and Weierstrass introduced the limiting $\epsilon - \delta$ concepts, infinitesimal calculus had a light rein over the theory of series. Here could be found the very foundations of the theoretical (or ideological) clash between Cantor and Kronecker. Either one supposes that the limit of an infinite series (e.g. trigonometric series) actually exists, this is the case of Cantor who would say that it is because we already possess the notion of limit as an irrational number that the limit of a fundamental sequence

$$\lim_{v \to \infty} a_v = b$$

exists while the limit process confers only potential existence; or someone like Kronecker who would extract the arithmetical core, the polynomial support of the series (e.g. power series) or someone like Brouwer after Kronecker who would insist that an infinite sequence is a process "*ein Fortgangsprozess*" in Kronecker's words or "a process in becoming" "*ein Prozess im Werden*" in Brouwer's phrase. Cantor also believed that points at infinity of projective geometry really exist; nowadays, arithmetic geometry tends to eliminate them without too much ado, i.e. Hermitian metrics. The gulf between the two attitudes is still sensible in the distinction between Peano arithmetic (with infinite induction) and Fermat arithmetic (with infinite descent).

The great American philosopher-mathematician C. S. Peirce who considered Fermat's method of infinite descent as "the greatest feat of pure intellect ever performed" made use of infinite descent to distinguish between what he termed a numerable collection and an innumerable collection in a way analogous to the distinction he had drawn using De Morgan's syllogism of transposed quantity between a finite and an infinite collection. However, Peirce would write to Cantor that Fermatian inference, as he called it, was not equivalent to what was very improperly called "*vollständige Induktion*" in German.

We have observed that induction was the main target of a constructivist critique. Infinite descent can do the job of complete induction, even though it cannot be identified with it, unless double negation is performed on an infinite set as we indicate in Chap. 4. Infinite descent finds a natural berth in the theory of forms (polynomials) and arithmetical or polynomial logic aims at a radical reduction of logic to arithmetic. Formulas become polynomials in the polynomial translation (see Gauthier 1998), but it is not a functional (combinatorial or lambda) interpretation which is at stake here. Proof theory and abstract languages of programmation tend to be oblivious of the concrete advantages of effective computation, a resource readily available in a polynomial calculus. A finite degree polynomial is more easily subjected to a calculus than a theory of arbitrary types. Finite recursiveness is steadily insured by the sum and product operations; composition (substitution and recursion) is embodied in the convolution Cauchy product for polynomials and the μ-operator is replaced by infinite descent. We see then that elementary recursive function theory is absorbed by the theory of polynomials. So goes arithmetic.

Logical constants loose their "logicality" when translated into polynomial operations, they do not loose their inferential power which a sequent calculus (or intelim rules) can adequately reproduce. The very idea of a "*Sequenzenkalkül*" derives from the sequential character of series and polynomials and the generalized arithmetic of polynomials is apt to encompass the conceptual or logical ramifications of the notion of sequence and, by the same token, of the notion of a *consequence*. The notion of logical consistency with its propositional disjunctive expression (Herbrand and Hilbert-Ackermann theorems) lends itself to arithmetical consistency. Molecular formulas are made up of monomials and their evaluation is effected on atomic components (coefficients), i.e. polynomial compositionality is guaranteed by the evaluation map

1. $\hat{\varphi}\,(\mathrm{A}) = 1 \qquad \forall \mathrm{A} \in \mathrm{D}_M$
2. $\hat{\varphi}\,(\neg\, \mathrm{A}) = 0 \qquad \neg\forall \mathrm{A} \in \mathrm{D}_M \qquad \forall \mathrm{A} \notin \mathrm{D}_M$

where D_M is an arithmetical domain which can be seen as a domain of rationality in Kroneckerian terms. The valuation map is unique and is defined for addition and multiplication such that

$$\hat{\varphi}(\neg(A \wedge A))[n] = (1 - a_0 x)$$

since $(1 - a_0x) + (1 - a_0x) = 0$ for $A = 1$ and the negation of an atomic formula A gives

$$\hat{\varphi}(\neg A)[n] = (1 - a_0 x)$$

where $[n]$ is obtained by the assignment of a natural number to the formula A in the arithmetical universe D. Logical validity is therefore reduced by the polynomial valuation map to arithmetical existence and arithmetical consistency to $\neg(0 = 1)$ or $0 \neq 1$, which we have shown to be the case for polynomial arithmetic. Classical validity in terms of truth and falsity becomes superfluous in that context. Propositional disjunctions are transposed into constant polynomials or, if one wishes, positive formulas are transformed into constant polynomials and their negations into zero polynomials; all this amounts either to $0 \neq 1$ or $-\infty \neq 0$, where $-\infty$ is the degree of the zero polynomial, 0 the degree of constant polynomials and 1 the degree of linear polynomials.

The total absorption of logic by polynomial arithmetic has an anti-Fregean or anti-logicist flavor. However, the fundamental motive of Frege's entreprise was to translate the notion of ordered series "*Anordnung in einer Reihe*" into the concept of logical consequence "*logische Folge*" and we have seen that the missing link or the middle term here is the notion of polynomial form. Frege's original idea is not responsible for his ill-fated logicism, it is the conceptual foundation of his formal system of arithmetic which is at stake and the comprehension axiom is faulty only because it has unlimited extent and intent, as a critic could say. Internal logic stands in closer relationship to the mathematical practice and does not allow for conceptual (metaphysical) foundations that divorce a mathematical theory from its constructive content. Platonism does not inform us on our practice, it is only an ideal account of intelligible structures. Structuralism itself need not be the mundane version of a Platonic realm withdrawn from the actual construction of mathematical objects whose objectivity cannot be detached from the creative subject, as Brouwer would certainly claim.

Intuitionistic arithmetic has a privileged access to internal logic, for it is a theory of content. The same could be said of polynomial arithmetic in Kronecker's formulation of the theory of forms. Tarski initially thought that logic was a theory of the content of implication or logical consequence. Hilbert, Brouwer and Weyl have all emphasized content over form. From the vantage viewpoint of internal logic, the whole of formal logic appears as a surface phenomenon, a photographic developer which, despite its ancillary function, plays an instrumental rôle in the foundations of mathematics. The concrete combinatorial content of the arithmetic of polynomial logic singles out its internal logic as a minimal logic for formalized logic. Pure predicate logic is the logical core Hilbert wanted to retain, but for the needs of arithmetic it is easily translatable in the arithmetic of polynomials and one could finally ask what, if any, is the place of logic in arithmetic? Once again, formal logic occupies the same place as the "ideal elements" which would only serve as a detour "*Umweg*" to be dispensed with when there is or could be a direct route. The polynomial translation is that direct route in the internal logic of arithmetic and infinite or rather effinite descent, in our terminology, together with the indeterminates of the Kroneckerian theory of forms leads us back to our point of departure. It remains to be seen if Kronecker's and Hilbert's legacy can testify for our "effinitism".

Chapter 4
Kronecker's Foundational Programme in Contemporary Mathematics

4.1 Introduction

A few important mathematicians have emphasized Kronecker's influence on contemporary mathematics, among them, first and foremost Weil (1976, 1979a) has stressed the fact that Kronecker is the founder of modern algebraic geometry and Edwards (1987a,b, 1992) after Weyl (1940) has insisted on Kronecker's pioneering work in algebraic number theory (divisor theory). Bishop (1970) has admitted in his work on the computational (or numerical) content of classical analysis that his enterprise was more in line with Kronecker than with Brouwer. Brouwer himself paid tribute to Kronecker—as did Poincaré and Hadamard—for his contribution to the fixed point theorems (see Gauthier 2009a). Poincaré for one among many others like Skolem or van der Waerden repeated Hensel's catch phrase in the Preface of Kronecker (1901) "a finite number of trials" (*eine endliche Anzahl von Versuchen*) to characterize Kronecker's finitist stand; Poincaré used the phrase "finite number of hypotheses" (*nombre fini d'hypothèses*) in his work on the arithmetical properties of algebraic curves (Poincaré 1951) which was the starting point of contemporary algebraic geometry, from Mordell to Weil and Faltings. I want to concentrate in the following on contemporary algebraic-arithmetic geometry and the two main programmes in the field, Langlands' programme and Grothendieck's programme as they are motivated to a large extent by Weil's own work in algebraic geometry (see Weil 1979a,b,c). Both programmes invoke Kronecker's dream of youth, his theory of forms (homogeneous polynomials) and modular systems which consist in sums and products of polynomials in a general divisor theory that was to become a theory of moduli spaces by successive generalisations and enlargements. In my view, these programmes share some measure of Kronecker's arithmetical philosophy which sees arithmetic as the building block of mathematics.

The content of this chapter has originally appeared partially in *Reports on Mathematical Logic* **48** (2013), 37–65.

Y. Gauthier, *Towards an Arithmetical Logic*, Studies in Universal Logic,
DOI 10.1007/978-3-319-22087-1_4

The Kroneckerian point of view, as Grothendieck will emphasize, implies that function fields are the analogue of number fields in the sense that an algebraic function field in one variable over the field of rational numbers $\mathbb{Q}$ is an extension of finite degree of the ring of polynomials in one indeterminate $\mathbb{Q}[x]$; function fields behave in $\mathbb{Q}[x]$ as algebraic number fields in $\mathbb{Z}$, the ring of integers, while the field of rational functions is the field of quotients $\mathbb{Q}[x]$ of $\mathbb{Q}[x]$. Kronecker (1883) had sketched in his paper "On the Theory of Higher-Level Forms" (*Zur Theorie der Formen höherer Stufen*) a notion of content or inclusion (*Enthalten-Sein*) for forms or homogeneous polynomials with sums and products of rational functions in a domain of rationality—*Rationalitätsbereich* is the term used by Kronecker instead of Dedekind's term *Körper*, *corps* in French and field in English (see Gauthier 2002). The notion of *Enthalten-Sein* or "being contained in" is not perfectly clear in Kronecker (1882). Molk (1885) and Vandiver (1936) have shown how to give a meaning to Kronecker's construction. Molk had insisted on the divisibility theory of polynomials and Vandiver has exhibited an explicit construction of decomposition or devolution (as opposed to convolution) for polynomial ideals. I give here a brief description (or reconstruction) of Kronecker's construction of these higher-level forms—Kronecker's terminology is in various contexts *Stufe*, *Rang*, *Ordnung* or even *Dimension*. Kronecker had outlined (1882) the most general setting for the decomposition (*Zerlegung*) of polynomial content. I propose here my own interpretation in terms of the convolution (Cauchy) product for polynomials. The general form of the convolution product of two polynomials (forms) encloses (includes) or contains higher-order forms and the substitution-elimination method enables one to remain within the confines of integral forms. Let us start with the convolution or Cauchy product of two polynomials

$$f \cdot g = (\sum_m f_m x^m) \cdot (\sum_n g_n x^n) = (\sum_m \sum_n f_m g_n x^{m+n})$$

with addition of their coefficients m and n. In his major work, Kronecker (1882, p. 343) states that a form M is contained in another form M' when the coefficients of the one are contained in the second. He then goes on to formulate propositions on the equivalence of forms like:

> Linear homogeneous forms that are equivalent can be transformed into one another through substitution with integer coefficients.
>
> (Proposition *X* in Kronecker 1882, p. 345.)

and

> Two forms are absolutely equivalent, when they contain each other.
>
> (Proposition X^0 in Kronecker 1882, p. 351.)

Kronecker states then what he calls a principal result (*Hauptresultat*),

> Every entire algebraic form in the sense of the absolute equivalence of Proposition X^0 is representable as a product of irreducible (prime) forms in a unique way.
>
> (Proposition $XIII^0$ in Kronecker 1882, p. 352.)

Here Kronecker declares that this result shows that the association of entire algebraic forms by the method of indeterminate coefficients conserves the conceptual determinations of the elementary laws (of arithmetic) in the passage from the rational domain or the domain of entire rational functions to the domain of algebraic functions. But Kronecker is not satisfied and comes back the following year (Kronecker 1883, p. 422) to the question and introduces the product

$$\sum_{h=0}^{m} M_h U^h \cdot \sum_{i=1}^{m+1} M_{m+2} U_{m+1}$$

(where $M = M_0, M_1, M_2, \ldots, M_{n+1}$ are integral quantities of successive domains of rationality R and the U's are indeterminates) which defines a form of power r containing the product of forms

$$\prod_{h}^{r} \sum_{k} M'_k V_{hk}$$

which he maintains is still more general than the 1882 formulation. "To be contained" here means only that the polynomials in the domains of rationality are included or contained in a higher rank (order) of their coefficients. A moduli system will then decompose this construction into irreducible polynomials. Hence, the notions of inclusion and of equivalence (reciprocal inclusion) of forms are valid generally, i.e. for both forms and divisors and factor decomposition is a descending technique perfectly similar to the division algorithm for integers or the Euclidean algorithm for polynomials. Dedekind's Prague Theorem is in the continuity of Kronecker's construction; it says[1] that if all coefficients of the product fg of two polynomials f and g (in one indeterminate) are algebraic, then the product of any coefficient of f and any coefficient of g is an algebraic integer.

For this unique decomposition of polynomials, descent is used to arrive at irreducible polynomials, much in the same way as in Euclid's proof of the divisibility of composite numbers by primes. Now the fact (Gauss lemma) that the product of two primitive polynomials (with the g.c.d. of their respective coefficients = 1) is primitive can also be had with infinite descent and *reductio ad absurdum*. From this fact combined with the fact that there is unique decomposition into irreducible (prime) polynomials, we obtain unique prime factorization. Kronecker's version of unique decomposition rests on the formula quoted above

$$\prod_{h=1}^{r} M_k U_{hk}$$

[1] See Kronecker (1883, p. 421). Edwards (1990, p. 2) rightly suggests that Dedekind's Prague Theorem—a generalization of Gauss Lemma to the algebraic case—is but a consequence of Kronecker's result.

and

$$\prod_{i=j+k} c_i = \sum_{j+k=i} a_j b_k$$

with $j = (0, \ldots, m)$ and $k = (0, \ldots, n)$. We shall read it in the form—remembering that $a^{p-1} \equiv 1(mod\, p)$ from a divisibility point of view:

$$\prod_{i=1}^{m+n}(1 + c_i x_i) = \sum_{i=0}^{m+n}(c_i x^{m+n-1}) = \sum_{m+n=1} (a_m b_n).$$

Kronecker's generalization uses the convolution product for polynomials

$$\sum_h M_h U^h \cdot \sum_i M_{m+i} U^{i-1} = \sum_k M'_k U^k$$

where $k = 0, 1, \ldots, n$ and the equation defines an $n + 1$ order system containing n order forms. I would call those forms *polynomial functionals*; they are the entire integer-valued functions that fill up the sphere of forms (Kronecker 1883, p. 423). Here the M's are integral forms and the U's indeterminates so that the product mentioned above

$$\prod_h \sum_k M_{k'} U_{hk}$$

is "contained" in the resulting form and the product can then be expressed as

$$\sum_k M'_k U^k = (M_k M_{m+1})^k + (M_k M_{m+1})^{k-1} + (M_k M_{m+1})^{k-2} + \ldots + (M_k M_{m+1})$$

in the decreasing order of the rank k of the polynomial sum. This linear combination obtained by the convolution product and the finite descent on powers shows simply that integral rational forms generate integral algebraic forms, i.e. algebraic integers. What we find in the 1883 text is simply a generalisation of Kronecker's 1882 theory of forms which encompasses both the theory of modular systems and the theory of polynomials. The equivalence principle for forms stated in 1882 is valid in full generality and the generalised notion of content or being contained in (*Enthalten-sein*) shows that in the construction (*Bildung*) of entire or integral functions the sphere of forms finds its fullest expression (Kronecker 1883, p. 423). This is not to say that Kronecker has fully realized his dream, only that he has conceived of an ambitious project that could possibly be fulfilled by a long list of successors.

Kronecker (1883, p. 422) refers explicitly to his 1882 text for the narrower concept of content in his text. As a matter of fact, Hurwitz (see 1932–1933, vol. 2, pp. 198–207) obtained a proof of Kronecker's theorem by using Lagrange's interpolation (rather than Cauchy's convolution product) and the Euclidean algorithm which is also the original form of the descent method—Hurwitz speaks of the elimination of composite powers.

Here again the ring of polynomials is the proper arena (with the largest area!) for Kronecker's general arithmetic of forms and their divisors. It is at this point that Dieudonné (1974, vol. 1, p. 200) speaks of Kronecker's old dream (*vieux rêve*) as being realized by Grothendieck's notion of scheme (*schéma*). It is of course Kronecker's *Jugendtraum* that Dieudonné evokes here and he describes Kronecker's ambitious project as encompassing both number theory and algebraic geometry in the polynomial theory of moduli systems (see Dieudonné 1974, vol. 1, pp. 59–61). Kronecker's forms or homogeneous polynomials become algebraic varieties and his notion of level (*Stufe*) means dimension or codimension in algebraic geometry—Kronecker's dream of youth in that context is translated into Hilbert's 12th problem on the extension of Kronecker's proposition on Abelian fields in an arbitrary algebraic domain of rationality.

The decomposition process or division algorithm is thus a descent to irreducible (linear) polynomials and Kronecker (1884, p. 336) in a later paper "On Some Uses of Modular Systems in Elementary Algebraic Questions" (*Über einige Anwendungen der Modulsysteme auf elementare algebraische Fragen*) makes it clear that his theory of higher forms or moduli systems makes it unnecessary to have recourse to infinite series as in formal power series and that finite series, that is polynomials, suffice or are up to the task of extracting the arithmetic-algebraic content of general arithmetic, as Kronecker says. The content in question amounts to substructures and extensions in model-theoretic terms and the function field appears then naturally as an extension of the number field, but Kronecker's way was algorithmic in the combinatorial build-up of the hierarchy of forms. As Edwards points out in his *Divisor Theory* (1987a), such extensions of finite degree are not couched in an algebraic closed field in modern usage and Kronecker avoids the transfinite setting by simply introducing new algebraic numbers to $\mathbb{Q}$ in a finite process of adjunction (see Gauthier 2002, Chap. 4 for details). Weil has insisted on the deep connection between function fields and number fields without avoiding entirely the transfinite construction and Grothendieck in his pursuit of Weil's conjectures has enlarged the geometric landscape with his notion of scheme.

4.2 Grothendieck's Programme

In *SGA 1*, that is *Séminaire de Géométrie algébrique du Bois-Marie* of 1961, Grothendieck and Raynaud (1971) starts his inquiry into what will be called Grothendieck's programme of the new foundation of algebraic geometry by taking a Kroneckerian point of view:

> The present volume introduces the foundations of a theory of the fundamental group in algebraic geometry from a "Kroneckerian" point of view which allows to deal on the same footing with an algebraic variety (of current usage) and with the ring of integers over a number field, for example. This point of view is best expressed in the language of schemes [. . .].
>
> (my translation)

What we call today an algebraic variety (with a finite number of polynomials in a field K) was essentially a divisor system or a moduli system (*Modulsystem*) for the polynomial ring in the hands of Kronecker; when it changes hands it becomes a locally ringed space in the functorial category-theoretic style of Grothendieck. Here functors transport arrows (functions) and their objects by making room for the larger topological or toposical (topos-theoretic) structures. I would call this approach structuralist as it is in line with the Bourbaki School to contrast it with the constructivist approach of Kroneckerian ascent and one could consider algebraic geometry *à la* Grothendieck as a tension between two mother-structures, algebraic structures and topological structures, as defined by Bourbaki. Grothendieck (1960) in any case refers indifferently to descent techniques or construction techniques in his 1958–1961 exposés in the Bourbaki Seminar. Algebraic geometry could be seen more accurately as pulled between a purely arithmetical internal logic and an external geometrical logic. I would put Langlands' programme more on the side of arithmetic geometry with Grothendieck's programme on the other, geometric side of algebraic geometry. In Langlands' case as we shall see, the "principle of functoriality" puts the emphasis on the correspondence between arithmetic objects and analytic data or a deep relationship between algebra (groups) and analysis over the complex numbers, while for Grothendieck the question is, is algebraic geometry more algebraic than geometric? For example in Grothendieck's theory of motives (*motifs*), correspondences are sought between arithmetic objects and algebraic-geometric structures. One answer could be found, I believe, in the massive work of Jacob Lurie (2009) on *Higher Topos Theory*. Lurie's work is certainly of Grothendieck's lineage and I would like to concentrate my short analysis of the matter in the chapter "Descent versus Hyperdescent" of Lurie's treatise.

4.3 Descent

Descent is a central topic in algebraic geometry. It is of course of arithmetic inspiration having its origin in Fermat's notion of infinite or indefinite descent. It has been practised in number theory by Fermat, Euler, Gauss, Lagrange, Legendre, Dirichlet, Kummer and Kronecker (see Kronecker 1901) and in modern times by Hilbert, Poincaré, Mordell, Weil, Faltings, Serre and many others. Since I have explored infinite descent extensively elsewhere (see Gauthier 2002, 2010), I shall simply again quote André Weil's version:

> Infinite descent *à la* Fermat depends ordinarily upon no more than the following simple observation, if the product $\alpha\beta$ of two ordinary integers (resp. two integers in an algebraic number-field) is equal to an m-th power, and if the g.c.d. of α and β can take its values only in a given finite set of integers (resp. of ideals), then both α and β are m-th powers, up to factors which take their values only in some assignable finite set. For ordinary integers this is obvious; it is so for algebraic number-fields provided one takes for granted the finiteness of the number of ideal-classes and Dirichlet's theorem about units. In the case of a quadratic number-field $\mathbb{Q}(\sqrt{N})$, this can be replaced by equivalent statements about binary quadratic forms of discriminant N.
>
> (see Weil 1984, pp. 335–336)

For algebraic number theory, descent in Weil's sense boils down via a height function on integers $m \geq 2$ to the finite quotient group A/mA of rational points of an Abelian group A, which is then said to be finitely generated: this is the starting point of Galois cohomology inaugurated by Weil. I would designate this form of infinite descent as a general Euclidean algorithm for divisor theory and Kronecker (1889) has used it accordingly in his theory of modular systems where we have an extensive treatment of the elimination or decomposition of forms into irreducible factors. For model theory, Tarski's theory of quantifier elimination has its source in Kronecker's elimination theory following van den Dries (1988). For algebraic geometry (and Galois cohomology), it should be noted that Kronecker had defined a generalized Galois principle which consists essentially to move from the group of substitutions for algebraic equations to the permutation group of a higher invariant theory, that is for entire functions with integer coefficients and n indeterminates (see Kronecker 1968b, Chap. 11, pp. 284–285), these are the forms for which Kronecker claims that it is the most complete arithmetical theory of algebraic quantities (*ibid*, p. 377). His principal result quoted above, as Kronecker emphasizes, is the analogue of the fundamental theorem of arithmetic for algebraic forms:

> Any entire algebraic form is representable as a product of irreducible (prime) forms in a canonical way.
>
> (my translation of Kronecker 1968b, p. 352)

This amounts in contemporary elementary algebra to the fact that the domain $F[\mathrm{x}]$ of polynomials is a principal ideal domain, a major ingredient of divisor theory. The Noetherian chain condition on ideals is ascending and descending on the field of $F(\mathrm{x})$ of rational functions. The direct method of calculating the g.c.d. here is the Euclidean algorithm or in the more general algebraic-geometric situations, the descent method *à la* Fermat described by Weil above and which I have characterized as a generalized Euclidean algorithm. This is one of the junction points between number theory and algebraic geometry that Weil (1979b) has stressed and it is here that Weil and Grothendieck would agree, despite Weil's reluctance to admit the category-theoretical language. Even the recalcitrant Dieudonné who didn't have much taste for constructive mathematics had recognized that Grothendieck's notion of scheme was genetically linked to the *Modulsysteme* or moduli systems of Kronecker.

If classical infinite descent relied on the well-ordering of the natural numbers to prove impossibility results by *reductio ad absurdum* for example, it consisted also in reduction procedures for Diophantine equations of finite degree with possibly infinite solutions, a kind of *positive* descent. It is also a kind of positive descent that Weil defines and Serre as well as Grothendieck have named that descent "descending induction" or "recurrent induction"—Poincaré preferred the term "*récurrence*" to "induction". It is Weil again who has introduced the practice of infinite descent for field extensions in the theory of Galois cohomology. Cohomology as the computational dual of homology harbours various devices and descent appears under many disguises such as spectral sequences, exact sequences, descending sequences, recurrence hypothesis, finiteness conditions, etc. Noetherian rings and spaces have an intrinsic descent (chain) condition. Grothendieck has even invented the term "*dévissage*" to express the unscrewing of the sequence of integers inherent to the descent method. But in his categorical idiom, descent consists in representing the algebraic structures—on a Noetherian frame most of the time—in the geometric universe or universes by arrows pointing to the objects of the ground level (the discrete topology), thus collecting the descent data from above and glueing them below. This is more or less a pictorial or intuitive approach, as Giraud (1964) admits in his treatise on Grothendieck's theory of descent. For a recent example of the use of descending induction in a somewhat more constructive style, one should consult Serre's paper (2009) "How to use finite fields for problems concerning infinite fields", a most elegant illustration of a simple descent technique. For an another illustration, Faltings had built his proof of the Mordell conjecture—on the finite number of rational points of a rational algebraic curve (of genus greater than one)—on moduli spaces which are geometric spaces endowed with a Noetherian algebraic structure and finite coverings (see Faltings and Wüstholz 1984). The method of descent still works by climbing down the ladder of natural numbers from a given n or the sparser rungs of the prime numbers from a given p or l (for l-cohomology). The same is true for the ring of integers and the ring of polynomials which are Noetherian, as are finite fields. Geometric descent with functors and morphisms must count on the algebraic-arithmetic descent to recover the ground field or the polynomial ring which is the fundamental arena of algebraic geometry. A nice illustration of this fact can be found in Jacob Lurie's voluminous *Higher Topos Theory*.

Infinite categories or infinity-categories (∞-categories or ω-categories) along with n-categories are new objects of higher category theory and topos theory. For brevity's sake, let us say that n-categories for n finite become infinite when $n = \infty$. The same holds for topoi and Grothendieck descent applies to n-topoi, where it is the usual descent *à la* Fermat as introduced by Weil. Recall that Serre defines "descending induction" as acting on two (positive) integers m and N with $m > N$ descending to $m = N$ (see Serre 2009, p. 10). What happens in the case of infinite topoi above and beyond cohomology and cobordism for infinite categories? The notion of cobordism was introduced by René Thom in differential topology and was a starting point of cohomology and homotopy theories. The situation becomes more complicated with hyperdescent, as Lurie admits (2009, p. 67) and one has to introduce the set-theoretic machinery of transfinite iteration (induction) on limit ordinals that reside in the universe of a regular uncountable cardinal; descent consists then in a transfinite sequence of downward-closed subsets (*ibid*., p. 800) in order to decompose them into pieces before glueing them in a suitable topological space. Lurie does not refrain again from using higher set-theory with regular (infinite) cardinals and an uncountable cardinal in his 2012 treatise *Higher Algebra* for infinity-categories (or quasi-categories) and their descent machinery—see also André Joyal's 2008 *Notes on quasi-categories*. Even M. Makkai's scheme of FOLDS, that is first-order logic with dependent choices has to use a descent (via the axiom of regularity) from the ω-categories it entertains in his type-theoretic categorical treatment of abstract sets—see his 2013 paper "The theory of abstract sets based on first-order logic with dependent choices". In the same Grothendieck's lineage or line of thought, Voevodsky (2010) is proposing geometric (non set-theoretic) univalent foundations for homotopy types—with equivalence classes of continuous maps for paths between topological spaces—for an axiomatization in a dependent type system *à la* Martin-Löf (intuitionnistic type theory). But he needs, as he says "at least one unreacheable cardinal α" (*ibid*., 5), which means that one has to climb the cumulative hierarchy of axiomatic set theory ZFC up to an inaccessible cardinal before redescending to a topological space or to its fundamental groupoid–groupoids are a generalization of the notion of group and they construct all morphisms as isomorphisms in category theory by having a partial function instead of a binary operation between group elements or objects. Here univalent logico-geometrical foundations might be seen as multivalent transfinite arithmetical foundations! It is true that Grothendieck didn't care much about the cardinality of the universes of his *U-topoi*, the totality of which could be called *U-topia* from a finitist point of view! But here we are a far cry from the Kroneckerian point of departure of *SGA 1*, to say the least. The set-theoretic background (the category of sets)—as a matter of fact the category of sets is *reducible* to a point in topoi theory and *contractible* to a point in homotopy type theory—is the starting point of category theory and topos theory, but the algebraic side of algebraic geometry finds its basic objects in simplicial sets, that is finite series of ordinals. Here, I would put Quillen's original work in homotopical algebra with the Quillen-Sullivan rational homotopy theory in the algebraic trend, while the geometric side exploits the ground territory of (homogeneous) topological spaces with the full resources of higher set theory. Of course, one could accept the logical, classical equivalence of arithmetic descent with transfinite induction, but from a constructivist point of view, it can be shown that the equivalence does not hold since it involves the excluded middle principle via a double negation over an infinite set of natural numbers (see Appendix 1 "La descente infinie, l'induction transfinie et le tiers exclu" of Gauthier 2010, pp. 133–151, and also Gauthier 2002, p. 51). Let us note that higher topoi theory, not unlike ordinary (lower) topoi theory, makes room for Heyting topoi where a second-order intuitionistic logic leaves no place for the classical excluded middle principle. The arithmetic scope of arithmetic-algebraic geometry appears to be more faithful to its Kroneckerian inspiration and I want to look briefly at Langlands programme in that perspective.

4.4 Langlands' Programme

In his paper on contemporary problems with origins in Kronecker's *Jugendtraum* Langlands (1976) evokes Hibert's 12^{th} problem in the 1900 list which reads "Extension of Kronecker's proposition on Abelian fields over an arbitrary algebraic domain of rationality". Hilbert declares that it is one of the deepest and far-reaching problems of number theory and function theory to generalize Kronecker's proposition on the generation of every commutative (Abelian) rational field through the decomposition of fields for the roots of unity; the idea here is to extend the rational field to any algebraic number field—what is called today the Kronecker-Weber theorem asserts that any Abelian extension of $\mathbb{Q}$ belongs to the cyclotomic field $\mathbb{Q}(\zeta_m)$. Hilbert holds the problem to be at the internal junction of number theory, algebra and the theory of functions (analysis). Such a language recalls Kronecker's statement in his inaugural speech at the Berlin Academy of Science in the year 1861 (see Kronecker 1968a, vol. V, p. 388):

> [...] the study of complex multiplication of elliptic functions leading to works the object of which can be characterized as being drawn from analysis, motivated by algebra and driven by number theory.
>
> (my translation)

Kronecker was perfectly aware of the centrality of his programme which he sees in the continuity of Gauss and Dirichlet and there is no doubt that he hoped for a full arithmetization of analysis. The dream of his youth (*Jugendtraum*) was that vision of an arithmetical theory of elliptic functions, an arithmetic of *ellipotomy* or divison of the ellipse, as I venture to say in analogy with the notion of cyclotomy. In a letter to Dedekind, Kronecker goes even as far as to say that the fundamental relation he has found between arithmetic and analysis originates in a philosophical intuition (see Kronecker 1899, vol. V, p. 453). Kronecker's foundational insight is given its fullest expression in his main paper on the arithmetical theory of algebraic quantities of 1882 where he gives the final formulation of his *Allgemeine Arithmetik* or General Arithmetic. It contains, in Kronecker's words, the complete development of the theory of entire (rational and algebraic) functions of a variable together with the systems of divisors. In such a complete theory, the association of forms allows for the conservation of the laws of factorization, so that the passage from natural and rational domains to the more general algebraic domains (of algebraic integers) is perfectly uniform. The conservative extension of arithmetic up to the highest reaches of algebra—the theory of entire rational and algebraic functions—is the ultimate goal of general arithmetic defined as the theory of all forms, homogeneous polynomials with integer coefficients and an arbitrary number of indeterminates.

Langlands insists also on number theory in connection with algebraic geometry, as Weil has taught. Here Langlands points to the continuation of Kronecker's work on Abelian extensions by the generalization to Abelian varieties in the hands of a long offspring of number theorists from Hilbert to Shimura and Deligne. For example, Shimura varieties embody some ideas of Kronecker who sought arithmetic objects within the analytic core of elliptic curves which are supported by polynomials of degree 3 over $\mathbb{Q}$ and extended to $\mathbb{R}$ and $\mathbb{C}$. Abelian varieties are nowadays spread out over algebraic number fields, finite fields, local fields and extend to contemporary arithmetic algebraic geometry in the work of Faltings and Wiles—by the way, descent is still present in the proof of Fermat's last theorem, if it is only by the Noetherian ring on the sequence of primes, modular and automorphic forms being on their side generalizations of Kronecker's moduli systems; moreover Wiles' (and Tailor's) proof rests on an Euler system of primes, the arithmetic bone structure of Riemann zeta function.

Langlands' programme or Langlands' philosophy, as it has come to be known, could be seen as a contemporary revival of Kronecker's idea of the deep analogy or correspondence between number fields and function fields. Evidently, as I mentioned above, the contemporary mathematician will not refrain from transcendental methods, but when he comes down to the arithmetic level, he sticks as the typical arithmetician would say, to the motto "denumerable at infinity", which means that denumerable infinity is seen as a limit or that the non-denumerable is unknown territory (*terra incognita*). Langlands' philosophy has met with success in two recent instances, Lafforgue's and Ngô's contributions to Langlands' programme. I want to deal briefly with Laurent Lafforgue's result.

Lafforgue (2002) has succeeded in showing the exact Langlands' correspondence between pieces of the modular space (or algebraic variety) and its (denumerable) rational points with the help of an iteration technique on Drinfel'd chtoukas—chtoukas comes from the Russian < штука > and is drawn from the German *Stücke*, meaning pieces. The ground field of Langlands' correspondence is a finite field F with a Galois group

G and we come back to the priviledged arena of applications for Fermat's descent on Weil's conception. I'll not pursue that theme, but only recall that Drinfel'd himself has drawn on some motives from Kronecker, his chtoukas are elliptic moduli and have an ancestral relationship to Kronecker's search for arithmetic objects or "discrete pieces" in the complex multiplication of elliptic functions.

Kronecker's dream and programme of a general arithmetic have provided a fertile soil for large-scale foundational projects, if only as deep-seated motivations or inspirational ideas. The immediate and long-term posterity of Kronecker's programme includes a vast number of people from Hurwitz and Hensel to Weil and Langlands. One should include in the list Brouwer, Poincaré and the French semi-intuitionists like Borel and Lebesgue to a certain extent and even Hadamard, who did borrow from Kronecker's arithmetical theory of functions for the particular purposes of topology e.g. the winding number (*Windungszahl*) which is an integer or index giving the number of times a closed curve c passes around a designated point P in the plane or in contemporary idiom the topological degree for a continuous function to itself on the closed unit ball D^n. Russian constructivists like Markov, Shanin, Kolmogorov up to Essenine-Volpin have also some share of Kronecker's finitism. But it is certainly in algebraic geometry that Kronecker's heritage is most strongly felt. Weil (1976) considers Kronecker as the originator of modern algebraic (arithmetic) geometry in the sense that Kronecker has initiated the work on the arithmetic of elliptic functions—they have become the elliptic curves or the modular forms of the contemporary scene. Arithmetic elliptic curves are the central target of the Shimura-Taniyama-Weil conjecture that led to the proof of Fermat's last theorem. Wiles and Taylor solved the semi-stable case and Breuil, Conrad, Diamond and Taylor finally proved the full conjecture. The calculations needed for the proof along with Faltings' result on the finiteness of rational points on an elliptic curve (the Mordell conjecture) are a testimony to the finiteness results in the rational number field $\mathbb{Q}$ in the tradition of Fermat-Kronecker-Weil arithmetic, the F-K-W arithmetical tradition, as I may encapsulate it.

4.5 Kronecker's and Hilbert's Programmes in Contemporary Mathematical Logic

I see Hilbert's metamathematical programme as the continuation of Kronecker's arithmetical programme with other means, that is the means of logic. In turn, I consider Hilbert's theory of formal systems and axiomatization as the initiation of the arithmetization of logic after Kronecker's arithmetization programme. Such an arithmetization of logic is manifest in contemporary theoretical computer science and in applied proof theory. I want to emphasize the new developments in Hilbert's proof-theoretical programme.

It is common knowledge that metamathematics or proof theory is concerned with finitary methods, as in Hilbert's conception of the theory of formal systems. I contend (see Gauthier 1989, 1991, 1994, 2002) that the consistency question is the crux of the matter and that it requires a finistist approach in the sense of Kronecker, as some Hilbert's early manuscripts seem to attest—see Sieg (1999) for Hilbert's later papers. The rather sketchy attempt on the simultaneous foundation of logic and arithmetic (Hilbert 1905) puts forward the concept of homogeneous equations in a manner reminiscent of Kronecker's combinatorial theory of homogeneous polynomials. Consistency, following Hilbert boils down to the homogeneous equation $a = a$ or inequation $a \neq a$. In his report on Hilbert's research on the foundations of arithmetic, Bernays says that Hilbert, in spite of his durable opposition to Kronecker whom he accused of dogmatism, has wanted a reconciliation with Kronecker's finitist stand:

> Kronecker has elaborated a clear conception which he has put to use in many cases and his conception accords essentially with our finitist position
>
> (see Hilbert 1935, vol. III, p. 203, my translation).

The quotation refers to Hilbert (1930) on the foundations of elementary number theory and is a sequel to Hilbert's paper "*Über das Unendliche*" (1926). The finitist position in question is the metamathematical idea of proof theory which I would formulate in the following way, To use finite logical rules with transfinite axioms in order to extend the finite into the infinite. The metamathematical conception is modeled after Kronecker's extension of elementary arithmetic into general arithmetic, an extension which should preserve the conceptual determinations of elementary arithmetic, following Kronecker; for Hilbert, the objective was to preserve the laws of finite logic with the excluded middle principle in the transfinite (set-theoretic) realm of ideal elements (*ideale Elemente*) for which classical (Aristotelian) logic could not make place because it did not distinguish between the finite and the transfinite—Kronecker could respond to Hilbert here by saying that there was no actual infinite in Aristotelian logic either, but only a potential infinite for Aristotle and Euclid. Logic will provide the passage from the finite to the infinite, since there is no place for the infinite (Hilbert 1930, p. 487) as it was also proclaimed in the lecture "On the Infinite". From my point of view, Hilbert's metamathematical programme is but the continuation or the consequence of Kronecker's arithmetization programme.

A further proof of Kronecker's inspiration, if not direct influence, on Hilbert's proof theory is the introduction by Hilbert of the finite-type functionals in his (unsuccessful) attempt to prove Cantor's continuum hypothesis in his 1926 paper "On the Infinite" (see Hilbert 1926)). As Kohlenbach notes (2008a,b) those finite-type functionals were used by Gödel (1958) in his *Dialectica* interpretation for the consistency of intuitionistic arithmetic and it is an essential tool (with Herbrand's theorem) for applied proof theory (see Gauthier 2009a); it must be added here that Gödel had already referred to Hilbert's construction in his 1931 paper on completeness and consistency (cf. *Über Vollständigkeit und Widerspruchsfreiheit*. *Ergebnisse eines mathematischen Kolloquiums* 3 (1932, p. 13)) where he imagines a transfinite sequence of formal systems of higher type. Let us remark though that in his proof for the consistency of intuitionnistic arithmetic (the *Dialectica* interpretation), Gödel limits his (impredicative) construction to all finite types up to ω. Hilbert's idea was to introduce number-theoretic functions "as those functions of an integral argument whose values are also integers" and then add up functions of functions, functions of functions of functions in a finite procedure for the iteration of types of functional variables over primitive integral types. Those higher-type functionals according to their height are associated with propositions that are supposed to come into a one-to-one correspondence with the transfinite ordinals up to the ϵ_0 of Cantor's second number class.

Hilbert needed transfinite induction here, but since only a finite iteration was necessary for the build-up of the functional hierarchy, the methods of substitution and recursion would suffice to produce a finitary proof, because substitution and recursion are counted as finitary procedures according to Hilbert. Hilbert's course, I forcibly suggest, follows up or reproduces Kronecker's construction of higher-level (*Stufe*) or (*Rang*) forms or homogeneous polynomials in his 1883 paper (Kronecker 1883) where substitution and decomposition—or descent for recursion—were used in a radical finitist setting, as I have shown above. Kronecker's idea was to build a finite hierarchy of (polynomial) functions to encompass the content of general arithmetic, what he calls the multilevel extension domain of arithmetic (*stufenweise Gebietserweiterung der Arithmetik*) in the footsteps of Gauss (Kronecker 1889, p. 356). Beyond and above this—and despite his repeated finitist commitment (*finite Einstellung*)—Hilbert wanted to include Cantor's transfinite arithmetic (up to ϵ_0).

$$\lim_{n\to\omega} \left.\omega^{\omega^{\cdot^{\cdot^{\omega}}}}\right\}^{n} = \epsilon_0.$$

One step further and the ordinal rank structure of von Neumann or the cumulative rank structure of Zermelo-Fraenkel set theory would look like transcendental extensions of Kronecker's finite arithmetical rank construction! In this line of thought, one could follow the thread of the classical identification of infinite descent with transfinite induction and go a long way with the axiom of foundation into von Neumanns universe of classes having transitive sets playing the rôle of inner models in Gödel's constructible universe (with the axiom $V = L$). And still going into Cohen's generic extensions of the forcing method as analogues of Kronecker's finite field extensions with indeterminates, one ends up in an idealized—or realized in a Platonic or Cantorian paradise—version of Fermat-Kronecker arithmetic. It is no wonder that Gödel's and Cohen's results for the axiom of choice and the continuum hypothesis could not be contained within Z-F axiomatic set theory, realizing their independence in the free spirit of transfinite ideal arithmetic, which could be called *transcendental arithmetic*, not to be confused with transcendental number theory.

Hilbert took a more direct course by following faithfully the Kroneckerian construction I have outlined above in using the two fundamental procedures of substitution (for new variables) and recursion (*Rekursion*) where the values of a function of height $n + 1$ are derived from the values of a function of height n (Hilbert 1926, p. 184). Kronecker had instead polynomials of order n generating a system of order $n + 1$ by the product operation (Kronecker 1883, p. 419).

Hilbert's attempt failed, but the construction was pursued by Hilbert's followers like Gentzen, Ackermann (1940), Kalmár—with the infinite descent idea—and Gödel in allegedly extended finitist ways—see my critique in Gauthier (2002, pp. 57–58) where I insist that transfinite induction with an (excluding third) double negation on the infinite set of natural numbers cannot be identified with infinite descent from a constructive finitist point of view. Gödel did not use transfinite induction in his *Dialectica* interpretation, but induction on all finite types and I contend that the functional interpretation has a natural translation in the polynomial arithmetic of Kronecker's theory of higher-level forms (see Gauthier 2002, pp. 74–76).

Herbrand (see 1968, p. 152), a follower of Hilbert, wanted also a consistency proof for arithmetic and he had formulated what I call Herbrand conjecture (see Gauthier 1983a),

> Transcendental methods cannot demonstrate theorems in arithmetic that could not be demonstrated by arithmetical means alone.
>
> (my tranlation)

Herbrand stated his conjecture for a suitable formal system which he does not describe. Herbrand was also a practitioner of (algebraic) number theory and he expressed himself in Kroneckerian terms when he used what he called "intuitionistic" arguments where one supposes that an object, logical or mathematical, does not exist without the means to construct it. In the same line of thought, he defends the potential infinite for his notion of infinite domain (*champ infini*) by saying that it is built iteratively (*pas-à-pas*) or (*Schritt zu Schritt*) in Kroneckerian terms, an expression also used by Skolem. Herbrand worked for instance on extensions (finite and infinite) of finite fields in the tradition of Hilbert and Kronecker, foreshadowing to some extent the contemporary work of Weil and Serre.

4.6 Conclusion: Finitism and Arithmetism

<Arithmetism> is the name I give to a foundational option in radical opposition to logicism and to Frege's question (1983, X), "How far can one go in arithmetic solely by deductive (logical) means?" (*Wie weit man in der Arithmetik durch Schlüsse allein gelangen könnte?*), the arithmetician Kronecker would respond, "How far can one go in mathematics with arithmetic alone?" and Hilbert following suit as a logician would ask, "How far can we go into the transfinite using only finite logical means?". One must admit that after the demise of the logicist programme (Frege and Russell) and despite the efforts of philosophers and logicians to recover Frege's logicist foundations of arithmetic with the second-order Hume principle, it is Kronecker's arithmetics programme which is still alive in the farthest reaches of contemporary mathematics, arithmetic-algebraic geometry. That does not mean however that mathematicians inspired by Kronecker from Hilbert to Weil adhere wholly to the Kroneckerian doctrine of finitism. On the contrary, most would allow for methods that leave Kronecker's arithmetical safe haven and venture into transarithmetical (set-theoretic), geometrical or analytical (trancendental) extended universes. A good pilot here is certainly Hilbert himself.

Hilbert introduced ideal elements (*ideale Elemente*) in order to have a clear-cut divide between the finite and the non-finite, a divide that Aristotelian logic did oversee, because it could not survey—(*Unübersichtlichkeit*) in Hilbert's text (1926)—the extent of its applications. The idea of the epsilon-calculus for the ϵ-symbol was to enable the extension of the simple laws of Aristotelian logic, excluded middle and universal instantiation with existential import, to the transfinite universe of ideal statements. Once this is achieved, one could redescend in the finite by elimination of the ideal elements or the epsilon formulas by a finite process in polynomial arithmetic, that is Hilbert's use of infinite descent (*die Methode der Zurückführung*) (see Gauthier 2002, 2011) which reduces transfinite expressions to arithmetical statements. In recent lectures on Hilbert's programme, Saul

Kripke has seemed to rediscover the same argument (see Kripke 2009). Although Kripke does not mention infinite descent as in previous lectures, he refers to a minimilazation argument which amounts to the same for Mirimanoff's "*ensembles ordinaires*" obtained from descent or transitive sets in ZF via the axiom of foundation or regularity—on this compare (Gauthier 1989, 1997a, 2007).

Intuitionistic logic, after the work of Brouwer, Kolmogorov, Heyting and Gödel, fares better in discriminating between the finite and the infinite, simply by rejecting the extension of classical logical laws beyond the finite domain and by exploring the potential infinite. This explains why it is the starting point of the functional interpretation privileged by applied proof-theorists; in their hands, intuitionistic logic is extended by various non-constructive principles or one-way translations from intuitionistic logic to classical logic. There is the foundational shift from Hilbert's programme and it has proven successful in recent proof-theoretic research with Kohlenbach (2008a) and others.

If applied proof theory and the proof mining enterprise represent a shift of emphasis in original (pure!) proof theory as Kohlenbach repeats after Kreisel (Kreisel 1981), it remains that the idea of extracting more constructive information (with an enrichment of data) from a given classical proof concurs with the idea of certainty (*Sicherheit*) or of certification (*Sicherung*) that Hilbert defined as the ideal goal of his proof theory and the motto of applied proof theory could very well be "More information, more certainty". Detracting from that ideal would mean fruitless prospection for proof-theorists, either in the abstract realm of constructivist principles or in the mining field of promising applications. Of course, the motto has to be substantiated by further foundational research into the historical, logico-mathematical and philosophical motives of proof theory. Hilbert was certainly the first mathematician to think of mathematical proofs in terms of a systematic study of the internal logic of deductive reasoning "*das inhaltliche logische Schliessen*" in line with Kronecker's constructive stance in his general arithmetic "*allgemeine Arithmetik*" for which he claimed "*innere Wahrheit und Folgerichtigkeit*", that is internal truth and consistency; these objectives could very well be shared by applied proof theory in the search for effective proofs in classical analysis where proofs were made available by the (constructive and non-constructive) means at hand. Proof theory puts the emphasis on proofs with the aim of making manifest their constructive hidden content and I would count such an enterprise as a revival of the Kroneckerian spirit with the logical means that Hilbert introduced in the programme of the arithmetization of logic after the arithmetization of analysis by Cauchy and Weirstrass along the arithmetization of algebra by Kronecker. It is maybe in contemporary theoretical computer science, for example in computational algebraic geometry with the Gröbner basis technique as well as in a variety of computational disciplines, that arithmetization can be pursued with a finite number of procedures as I would translate Hensel's phrase (*eine endliche Anzahl von Versuchen*). Finitist arithmetism may sound redundant, but it renders the idea of the arithmetical foundations of mathematics as a finitist programme quite different from Weierstrass' programme claimed by Felix Klein as the epitome of the arithmetization of mathematics. Arithmetization of analysis in the Cauchy-Weierstrass file is not really on par with Kronecker's foundational entreprise of general arithmetic (*allgemeine Arithmetik*).

Finally, if Klein's Erlanger Program as a unification of classical geometry based on the notion of group could be compared according to the category theorist André Joyal to the Grothendieck program of unification of modern algebraic geometry based on the notion of topos, both programs belong to algebraic foundations. And if Kronecker program of the arithmetization of algebra were to succeed, for example in Grothendieck's idea of an arithmetic (motivic geometry), it would still be in the Kroneckerian spirit that Grothendieck himself announced in *SGA1* when he introduced the notion of scheme (*schéma*) as a generalization of Kronecker's concept of moduli system (*Modulsystem*). In that case, the intent and the goal is to obtain concrete arithmetical results on the integers from abstract algebraic, category-theoretic methods and the like and this is the spirit of arithmetical logic.

Chapter 5
Arithmetical Foundations for Physical Theories

5.1 Introduction: The Notion of Analytical Apparatus

The notion of analytical apparatus was introduced in the paper by Hilbert, Nordheim and von Neumann (1928) ≪ Über die Grundlagen der Quantenmechanik ≫: The analytical apparatus <*der analytische Apparat*> is simply the mathematical formalism or the set of logico-mathematical structures of a physical theory. Von Neumann used the notion extensively in his 1932 seminal work on the mathematical foundations of Quantum Mechanics and he stressed particularly the auxiliary notion of conditions of reality <*Realitätsbedingungen*>. I want to show that this last notion corresponds grosso modo to our notion of model in contemporary philosophy of physics. Hermann Weyl, who has initiated group theory in Quantum Mechanics (1928), also exploited the idea in his conception of the parallelism between a mathematical formalism and its physical models. We know that Weyl defended a constructivist interpretation of physics and the exact sciences in general (see Weyl 1918, 1960). But one can even go further and argue that Minkowski, a close friend of Hilbert, shared the same idea of the prevalence of the analytical apparatus over its physical interpretation and it can be shown that in his papers on physics, particularly his 1908 paper ≪ Raum und Zeit ≫, Minkowski proposed a derivation of physical geometry from the geometry of numbers in the Leibnizian spirit of the harmony between pure mathematics and the physical world.

I am drawing here parts from various recent papers of mine, especially from three different sources "Hilbert's idea of physical axiomatics: the analytical apparatus of quantum mechanics" in *Journal of Physical Mathematics*, Vol. 2 (2010), 1–14, "Hermann Minkowski:From Geometry of Numbers to Physical Geometry", Chapter 10 in Minkowski Spacetime: A Hundred Years Later, ed. by Vesselin Petkov, Springer, 2010, 247–257 and "A General No-Cloning Theorem for an Infinite Multiverse", in *Reports on Mathematical Physics*, Vol. 2 (2013), no. 2, 191–199.

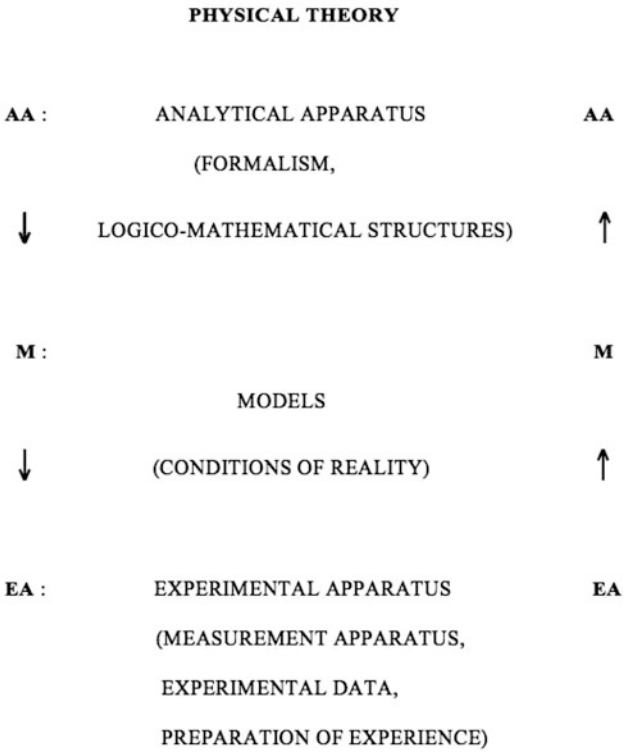
Y. Gauthier, *Towards an Arithmetical Logic*, Studies in Universal Logic,
DOI 10.1007/978-3-319-22087-1_5

5.2 Analytical and Empirical Apparatuses

In order to show the relevance of the concept of analytical apparatus, one needs to contrast it with the usual notion of the experimental apparatus. The experimental apparatus is the set of the observation experiments and measurement procedures of experimental data together with their preparations recorded in a physical instrument or a laboratory equipment while the analytical apparatus consists solely of the theoretical data, that is, those data collected from logical and mathematical structures in pure mathematics or in mathematical physics. The distinction here is finer than the distinction between theoretical physics and experimental physics, since any physical theory, may it be in applied physics, needs an analytical apparatus. The laser as an applied measurement device is a good example of an experimental instrument that would not have been possible without the quantum theory of Bose-Einstein statistics for symmetric amplitudes. The philosophical problem of the applicability of mathematics to the physical world is not addressed in that context as a mystery in E.P. Wigner's terms, but rather as the relationship between two apparatuses which process information from two different sources in order to give a full picture of physical reality. In that picture, experimental data are at first overdetermined by the analytical apparatus through the mediation of models, our new conditions of reality <*Realitätsbedingungen*> for a given formalism. The idea of theory-ladenness takes a new turn in such a perspective and the schema below is meant to illustrate the rôle of models in the construction of physical theories to the extent that they are supposed to combine a theoretical framework with the physical universe as interpreted in our theories:

5.3 Models

Arrows (or homomorphisms) on the left show the direction of overdetermination while arrows on the right indicate that in turn the analytical apparatus can be modified according to new conditions of reality reflected in the models of the theory. Those models are multifarious since the analytical apparatus in not canonical—the formalism cannot be categorical (or univocal) and from a logical point of view there cannot be a standard model of a physical theory, when it is couched in a first-order logical language as shown by Putnam and others. In the most interesting cases, for example General Relativity or Quantum Mechanics (with a Hilbert space formalism), physical theories cannot be reduced to first-order languages and theorems like the Löwenheim-Skolem theorem cannot be applied to generate non-standard models. But even in the case of higher-order theories, non-principal models coexist with the principal model of a physical theory. A physical theory has a standard model only from a sociological point of view in the sense that a standard model in physics or in the sciences in general is the model accepted by a majority in a given field, e.g. the standard model in elementary particle physics. The multiplicity of models points also to the flexibility of the physical interpretation in view of the rigidity of



PHYSICAL THEORY

AA : ANALYTICAL APPARATUS **AA**

(FORMALISM,

↓ LOGICO-MATHEMATICAL STRUCTURES) ↑

M : **M**

MODELS

↓ (CONDITIONS OF REALITY) ↑

EA : EXPERIMENTAL APPARATUS **EA**

(MEASUREMENT APPARATUS,

EXPERIMENTAL DATA,

PREPARATION OF EXPERIENCE)

the axiomatic or formal part of a physical theory, as Hilbert emphasized. But Hilbert also insisted that it is only through axiomatization that a concept like probability could loose its mystical character.

A nice illustration of the complex relationships that are entertained between the analytical apparatus and the experimental apparatus is the interaction of the observed system and the observing system in Quantum Mechanics: The observer disposes of an analytical apparatus which imposes an instrumentalist meaning to the measurement process, since the probabilistic account of measurement is given in terms of the square $|\psi|^2$ of the absolute value of the wave function ψ—a state of affairs derived from the analytical apparatus related to Hilbert's work on L^2 (square integrable functions).

Of course, Hilbert did not have our notion of model and could not appreciate the richness of non-standard models either in logic or in physical axiomatics, a field he has invented for a foundational purpose. The logical empiricists (Carnap, Reichenbach et *alii*) who conceived of physical theories as semi-interpreted axiomatics systems could not imagine that the syntactical view of theories could be supplemented or even superseded by a semantical (one is tempted to say semi-model theoretic) view of physical theories. Notice that the above schema only depicts the interdependence of analytical and experimental apparatuses via the double rôle of models as mediators and stresses the dynamical structure or the constructive content of a physical theory. There is no provision for ontological commitments or metaphysical options in our view, except for an overt constructivist foundational posture in the foundations of physics (and mathematics).

5.4 The Consistency of Physical Theories

Hilbert's idea of a physical axiomatics is introduced in his 6th problem in his 1900 list. It is the axiomatization of probability and mechanics, he says, that should concern the mathematician who wishes to secure the foundations of physics as rigorously as it is achieved in arithmetic and geometry. In his major work (1968, III, pp. 245–387), Kronecker, who had inspired Hilbert in more ways than one, referred to Kirchhoff's mechanics as a model of a scientific theory for its simplicity and completeness, attributes he claimed for his own general arithmetic. The same Kirchhoff furnished to Hilbert a radiation theory for his early work on foundations of physics (1932, III, pp. 217–257). What we call now Kirchhoff's law on the equality between rates of emission and absorption of energy in thermal equilibrium is indeed a good example of a physical domain that should be investigated in view of the consistency of its axioms. One is reminded here that Hilbert had made of this question already in 1900 the sixth problem of his list "The mathematical treatment of the axioms of physics". Hilbert names probability theory and mechanics as the two privileged domains of such interpretations. The central problem in physical theories is still the consistency problem, because a fundamental physical theory proceeds like geometry from general axioms to more specific ones and the extension from the first principles to the secondary ones must preserve consistency. Consistency is not a matter of feeling or experimentation, but of logic, Hilbert insists, and the extension of the theory of thermal radiation to elementary optics is possible only on the grounds of consistency. For Hilbert, there is a clear distinction between classical mechanics and quantum mechanics: on the one hand, you have a deterministic treatment, on the other, you must employ probabilistic methods to deal with classical and quantum-mechanical theories. But the differential treatment has to obey the internal logic of a physical theory which turns out to be of arithmetical nature.

The problem area under discussion is of no particular interest for our purposes, nor are Hilbert's contributions to relativity theory (1932, III, pp. 257–289) since they are mathematical elaborations and only partly foundationally illuminating—Hilbert had also worked on the foundations of the kinetic theory of gases and other occasional physical subjects. The work on (general) relativity theory in particular seems to have been inspired by the groundbreaking inquiries of Weyl, more than by Einstein's original work (see also von Neumann 1932). Of greater interest to us is the paper written in collaboration with von Neumann and Nordheim "On the Foundations of Quantum Mechanics" (1928).

In that paper we find the clear exhortation to make explicit the concept of probability in order to extract the mathematical content from its mystical (philosophical) gangue. But the main themes are, in my view, associated with the notions of "analytical apparatus" (*analytischer Apparat*) and "conditions of reality" (*Realitätsbedingungen*). Which comes first, the analytical apparatus or conditions of reality, is a matter of foundational outlook and we shall see how Hilbert conceived a so-called "physical axiomatics".

Probabilities and their relationships constitute the material we start from. The physical requirements a probability theory of physical phenomena has to fulfil represent the basis on which a “simple” analytical apparatus is defined; then follows a physical interpretation of the analytical structure and if the basis is fully determined, the analytical structure should be canonical. This is the axiomatic formulation already present in the Hilbertian foundations of geometry and the general argument leaves no doubt as to the permanence of the axiomatic ideal in Hilbert’s work on the foundations of physics. What Hilbert seems to strive to is the conception of a categorical mathematical theory with a multiplicity of models; however, not all models would be isomorphic. Non-standard models point rather to a complete first-order theory that generates a variety of interpretations. But the mathematical structure is generally not first-order. The dilemma of a physical axiomatics or of a “physical logic” opens up numerous avenues of research.

The analytical apparatus or the mathematical formalism is first conjectured and then tested through an interpretation in order to check its adequacy. The two components, analytical apparatus and its physical interpretation, must be sharply distinguished and that separation has the effect that the formalism is stable throughout the variations of its (physical) interpretations where some degree of freedom and arbitrariness cannot be eliminated. However, this is the price to pay for the axiomatization and vague concepts like probability will finally loose their fuzzy character. The conditions of reality in general call for the complex Hilbert space to have models in the reals, but the specific conditions of reality for probability will prove to be intrinsically linked with the calculus of Hermitian operators and Hilbert’s early theory of integral equations. Thus the fact that a probability measure is real positive depends on the finiteness of the sum

$$a_1x_1 + a_2x_2 + \dots$$

for a linear function. Hilbert’s result, which is a building-block of the Hilbert space formalism, was inspired by a similar result of Kronecker on linear forms. Kronecker’s influence on Hilbert has also a conservative extension in the foundations of quantum mechanics (see Kronecker 1889, Chap. 12 and Hilbert 1932, pp. 56–72).

Hilbert’s ideas of the foundations of *QM* have been made to work by von Neumann (1932, 1961) in the Hilbert space formulation of quantum mechanics, which is the standard formulation of *QM*. We shall explore in the following the continuation of Hilbert’s programme in the hands of his followers. I start with a notion which is not found in Hilbert, but can be traced back to von Neumann’s foundational work in *QM*.

5.5 Quantum Mechanics

5.5.1 Hilbert Space

The usual presentation of *QM* requires the analytical apparatus of Hilbert space as a linear vector space with complex coefficients; among all linear manifolds that constitute a Hilbert space, the closed ones or the subspaces are of special interest for physics (i.e. *QM* here), since notions like orthogonal vectors, orthogonal complements, projections, etc., can be defined on them. It is a well-known fact that not all linear manifolds are closed (see Halmos 1957) and that the set of all linear subsets of the infinite-dimensional Hilbert space is not orthocomplementable (see Jauch 1968, p. 122): it is this possibility which I want to exploit, keeping in mind that a Hilbert space is a metric and topological space. The interesting fact about Hilbert space from a physical point of view is that it permits the definition of orthogonality

$$(f, g) = 0$$

written $f \perp g$; the orthogonal complement of f, $f^{\perp\perp}$ obeys the Boolean rule $f^{\perp\perp} = f$ and $f^{\perp}$ forms a subspace of $\mathcal{H}$. For *QM*, it is important to notice that there is a bijection between subspaces and projections, i.e. the linear operators E such that $EE^{\perp} = E$ for $E^{\perp}$ the adjoint of E defined by $\left(E^{\perp}\right)^{\perp} = E$ (if $E^{\perp} = E$, then E is a self-adjoint or Hermitian operator). The spectral theorem states that there is a bijection between self-adjoint operators and spectral measures on (the Borel set of) the real line R^1 and the von Neumann *dogma* states that there is a bijection between self-adjoint operators and the observables of *QM*.[1] Let us look at the orthogonal complement: we have seen that $f^{\perp\perp} = f$; consequently, the orthogonal complement corresponds to the orthocomplement $(a^-)^- = a$ of a Boolean lattice, where $\leq$ correspond to $\rightarrow$, a^- to $\neg a$, $a \cap b$ to $a \wedge b$ and $a \cup b$ to $a \vee b$. Orthocomplementation induces an involutive antiautomorphism $\left(a^{\perp}\right)^{\perp}$ on the field vector space. It is such an antiautomorphism which yields Gleason's important theorem stipulating that any probability measure $\mu\,(A)$ on the subspaces of $\mathcal{H}$ has the following form

$$\mu\,(A) = Tr\,(WP_A)$$

where Tr means $TrX = \sum_r (\varphi_r, X\varphi_r)$ for any complete system of normalized orthogonal vectors, P_A denotes the orthogonal projection of A and W is a Hermitian operator which satisfies

$$W > 0,\ sTrW = 1 \text{ and } W^2 \leq W.$$

Other spaces, like Banach spaces, which lack the restriction of orthogonality, do not seem to be suited to the needs of *QM*.

[1] Von Neumann's dogma has been challenged in 1952 by Wick, Wightman and Wigner who introduced superselection rules showing that there exist Hermitian operators that do not correspond to observables; on the other side, Park and Margenau argue that there are observables, for example, the non-commuting x and z—components of spin which are not represented by Hermitian operators.

The usual formulation of QM requires the analytical apparatus of the Hilbert space $\mathcal{H}$ as a complex vector space (see Jauch 1968) with

$$\forall f, g \in \mathcal{H}\,((f+g) \in \mathcal{H})$$
$$\forall f \in \mathcal{H}\,\forall \lambda \in C\,(\lambda f \in \mathcal{H})$$

for f and g and a complex coefficient λ with

$$1 \cdot f, \theta + f = f \text{ and } \theta \cdot f = 0$$

for the null vector θ. The Hilbert space has also a scalar or interior product which is strictly positive. In particular, we have

$$(f, g+h) = (f, g) + (f, h)$$
$$(f, \lambda g) = \lambda\,(f, g)$$

and

$$(f, g) = (g,f)^*$$

the complex conjugate with the norm

$$\|f\|^2 \equiv (f,f) > 0 \text{ for } f \neq \theta.$$

The space $\mathcal{H}$ is separable (dense)

$$\forall f \in \mathcal{H}\ \forall \varepsilon > 0\ \exists f_n\ \|f - f_n\| < \varepsilon \text{ for } n = 1, 2, \ldots$$

and complete, i.e. any Cauchy sequence

$$\forall \varepsilon > 0 \exists N < i,j\left(\rho\left(x_1, x_j\right)\right) < \varepsilon_0$$

converges

$$\lim_{n \to \infty} \|f - f_n\| = 0 \text{ in } \mathcal{H}.$$

The analytical apparatus consists also of the following physical postulates or axioms

1. physical states are represented by state vectors (in $\mathcal{H}$),
2. there is a bijection between observables and Hermitian operators—von Neumann's *dogma*,
3. the evolution of the physical system is described by Schrödinger's equation,
4. the probability to find a particle in a particular position is given by

$$pr\,(\underline{r}, t) = \psi^*\,(\underline{r}, t)\,\psi\,(\underline{r}, t) = |\psi\,(\underline{r}, t)|^2$$

where $\underline{r}$ is the position vector and ψ^* the complex conjugate of ψ (the so-called Born rule)

$$\left(\psi^*\psi = |\psi|^2\right).$$

5. the projection postulate which states that immediately after a measurement (that is, an interaction), the superposition $\sum c_j\sigma_j\alpha_j$ is transformed or reduced to $\sigma_n\alpha_n$.

The fifth postulate for the wave packet reduction characterizes von Neumann's theory of measurement. For instance, the superposition of states $\sum \sigma_j\alpha_j$ is made up of the combined system—the observer and the observed system—and for von Neumann a measurement projects the system Σ in a state $\sigma_n\alpha_n$ (we neglect the terms of the expansion here). Vectors $\sigma_n\alpha_n$ have a well-defined value since projections are in bijection with the subspaces of the Hilbert space, but the system is no more in a pure state, but in a mixture. Everett's multiverse theory (or relative state theory) supposes that the superposition is not reduced or projected in a determinate state, but ramifies after an interaction in a multitude of branches each corresponding to a component of the superposition: there would be as many worlds as there are components and the result of measurement would be valid on only one world among a (non-denumerable) infinity of universes. Here is the rub, more irritating than von Neumann's cut (*Schnitt*) between the observed system and the observer: the set of all values of the wave function ψ is C, the set of complex numbers, which has the cardinality $2^{\aleph_0}$; thus, the ramified ψ cannot be measured, for the set of all possible measurements certainly does not exceed $\aleph_0$ and there is no bijection between $\aleph_0$ and $2^{\aleph_0}$. The inconsistency is fatal in view of Everett's idea that the formalism generates its own interpretation. If the ramification of ψ must have a probabilistic objective content, one is obliged to admit that it cannot emerge from the divergent ramification of non-denumerable probability values, a probability theory being at most σ-additive, that is denumerably convergent. Another example of an inconsistent probability theory of *QM* is the theory of consistent histories, first formulated by Griffiths (1984) and adopted since by some important physicists, Gell-Mann and Hartle, among others. The theory can be considered as a variant of Everett's many-universe or multiverse interpretation with a historical component, since parallel universes can have different histories, that is temporal sequences of quantum events. In order for a given history to be consistent, it is granted a weakened logical status which forbids, for instance, joining two incompatible events (e.g. spin states a and b of an electron) in a classical conjunction $a \wedge b$. These singular histories must preserve probability measures or σ-additivity for denumerable measures with the help of elementary logical notions such as *modus ponens*, conditional probabilities and counterfactuals, truth and liability. But the main question is the consistency of consistent histories. Recent work by Goldstein and Page (1995), Dowker and Kent (1996) tends to show that Griffith's theory is inconsistent in its probabilistic assumptions about consistent histories. From a combinatorial point of view, denumerable or σ-additivity supposes that the decomposition of probability measures covers up inconsistent history subsequences (subsets) as well as consistent but irreconcilable subsequences in the density matrix of consistent histories; in other words, there is no bijection between the $\aleph_0$ sequences and the $2^{\aleph_0}$ subsequences (the power set of all histories) and standard probabilities are lost in the multiplicity of divergent histories (and subhistories). The lesson to be drawn here is perhaps that a paraconsistent logic that accommodates contradictions as well as tautologies can take care of a "quasi-consistency" for the "quasi-classicality" in a mixture of coherent histories in quantum systems and decoherent histories in classical (macroscopic) systems, as quantum decoherence theory seems to indicate. But the term "consistency histories" would nonetheless sound like a misnomer for a theory which makes room for too many divergent histories, as the universal ramification of the wave function would have it in Everett's multiverse interpretation.

5.5.2 Probabilities

Hilbert (followed in this by von Neumann) introduced the notion of analytical apparatus (*analytischer Apparat*) drawn from the general structure of an axiomatic system in physics and he made no mystery of his intention to provide physics with the same kind of axiomatic foundations as geometry. Physical situations must be mirrored in an analytical apparatus, physical quantities are represented by mathematical constructs which are translated back into the language of physics in order to give real meaning to empirical statements. The analytical apparatus is not subjected to change while its physical interpretation has a variable degree of freedom or arbitrariness. What this means is that the mathematical formalism of a physical theory is a syntactical structure which does not possess a canonical interpretation, the analytical apparatus does not generate a unique model. At the same time, axiomatization helps in clarifying a concept like probability which is thus rescued from its mystical state. It is noteworthy that another pair of renowned mathematicians, Hardy and Littlewood, expressed the same opinion at about the same time: "Probability is not a notion of pure mathematics, but of philosophy or physics."

Probabilities had, long before Quantum Mechanics, been knocking at the door of physics, but Laplace had entitled his work *Essai philosophique sur les probabilités* (1814) after having called it *Théorie analytique des probabilités* (1812). Statistical mechanics can certainly count as a forerunner of *QM* as far as the statistical behaviour of a large number of particles is an essential ingredient in the probability theory of quantum-mechanical systems. But even in the work of pioneers like Born and Pauli, probability has entered *QM* somehow through the backdoor and it seems that it is only reluctantly that Born, for example, has admitted the idea of probability. Later work by Kolmogorov on the axiomatic foundations of elementary probability theory or von Mises and Reichenbach on the frequentist interpretation of probability will achieve some measure of success, but it is the historical advent of a rigorous formalization of the notion of probability as it occurs in quantum physics which has not been sufficiently stressed.

If probability has evidently a multiple application in *QM*, it remains that it is mainly a mathematical notion. Von Neumann's work in 1927–1932 focuses on what is called the finiteness of the eigenvalue problem. The point here is that any calculation is finite and since we have only finite results, those must be the products of a finite calculation which is itself made possible only if the analytical apparatus contains the mathematical structures which enable such calculations. Such a formalism is the complex Hilbert space with

$$|\psi|^2 \in L^2(\mu)$$

where μ is a real positive measure on the functional space L^2 (i.e. the equivalence class of square-integrable functions). The integral

$$\int |\psi|^2 \, d\mu$$

is finite, which is equivalent to the fact that, in the theory of bounded quadratic forms, the sum

$$K(x,x) = \sum_{p,q=1}^{\infty} k_{pq} x_p x_q$$

of all sequences $x_1, x_2, \ldots$ (of complex numbers) is finite in an orthonormal system of vectors. That mathematical fact, which Hilbert derived in the theory of integral equations in 1907, states that a linear expression

$$k_1 x_1 + k_2 x_2 + \ldots$$

is a linear function, if and only if the sum of the squares of the coefficients in the linear expression $k_1, k_2, \ldots$ is *finite*. The theorem, inspired by Kronecker's result on linear forms (homogeneous polynomials), is the very basis of the Hilbert space formulation of *QM*. Notice that on the probabilistic or statistical interpretation, the "acausal" interaction between an observed system and an observing system takes place in a given experimental situation and produces a univocal result of finite statistics for real or realized measurements.

In order for real measurements to have real positive probability values, the analytical apparatus must satisfy certain realizability conditions, (*Realitätsbedingungen*) as Hilbert and von Neumann put it. For example, orthogonality for vectors, linearity and hermiticity for functional operators and the finiteness of the eigenvalue problem for Hermitian operators, as in von Neumann's further work *Mathematische Grundlagen der Quantenmechanik*, are such constraints of realizability.

5.5.3 Logics

The requirements for realizability are not limited to additivity for Hermitian operators—Grete Hermann seems to have been the first one to criticize the requirement on philosophical grounds—but are strictures imposed by the analytical apparatus or the deductive structure of the theory in von Neumann's terminology. In their joint paper of 1936, Birkhoff and von Neumann, attempt to define the "logical calculus" of quantum-mechanical propositions associated with projection operators alluded to in von Neumann

(1932, p. 134). They are led to denote the orthogonal complement ($\perp$) as the "negative" of an experimental proposition in an orthocomplemented lattice satisfying

1. $\left(a^{\perp}\right)^{\perp} = a$
2. $a \leq b,\ \mathit{iff}\ b^{\perp} \leq a^{\perp}$
3. $a \wedge a^{\perp} = 0$
4. $a \vee a^{\perp} = 1.$

The dual antiautomorphism of period two (or the involuntary antiautomorphism of projective geometry) does not however uniquely determine complements in a continuous geometry and von Neumann came back to quantum logic in his paper "Quantum Logics" (1961) with the discussion of a continuous geometry without points and whose elements are all the linear subspaces of a given space (more general than a Hilbert space); von Neumann thought that the logic of quantum probabilities (frequencies) could be built upon such a geometry. But here the probability measures must be infinite in order to be convergent and the probability statements that express those measures are required to have a finite meaning, as Reichenbach claimed for the verifiability theory of his probability theory. Von Neumann was dissatisfied with Hilbert space vector formalism—but was unable to define a finite probability theory for his abstract projective geometry framework—the type *II* factor of a modular non-atomic lattice.

In that context, Birkhoff and von Neumann deny the distributive law of logic in favour of a weaker modular identity or orthomodularity

$$a \leq b \rightarrow a \vee b\,(b \wedge c) = (a \vee b) \wedge c$$

weakened by Jauch and Piron to

$$a \leq b \text{ iff } a \text{ and } b \text{ are compatible}$$

(compatibility is an equivalence relation which is symmetric, but not transitive). The underlying logic here is the non-commutativity of operators P_1 et P_2

$$P_1 P_2 \neq P_2 P_1$$

of which the uncertainty relations are "a direct intuitive explanation," as Heisenberg said. But the denial of the distributive law did not prove to be sufficient basis for a quantum logic, that is an internal logic of quantum mechanics.

The quantum logic of Jauch and Piron is another example of an impossibility proof for hidden variables as compatible propositions in the framework of essentially non-compatible quantum-mechanical propositions. Kochen and Specker devised rather a quantum logic for a partial Boolean algebra of commuting (or "commeasurable," as they say, (1967, p. 64)) quantum-mechanical observables (or propositions) which is not embeddable in a commutative Boolean algebra—there is no 2-valued homomorphism h from the partial algebra A to the Boolean algebra B with the properties

1. $h\,(a)\,h\,(a)\,h\,(b)$

2. $h(\mu a + b) = \mu(h(a))\lambda(h(b))$
3. $h(ab) = h(a)h(b)$
4. $h(1) = 1$

where is the relation of commensurability, a, b are elements of A and μ, λ belong to a field of sets K (compare with the relation of compatibility defined in 2.4 above).

The fact that the 2-valued propositions form a commutative algebra which does not imbed commeasurable quantum-mechanical propositions can be seen as a far-reaching consequence of Gleason's theorem on the measure of the closed subspaces of a Hilbert space (Gleason 1957). See Hrukovski and Pitkowsky (2004) for contructive proofs.

5.5.4 Local Complementation

Even in the case of set complementation (as in the theory of Hilbert spaces), we can have local complementation. Consider Hilbert space as a metric and a topological space; D is in this case the set of subspaces of the Hilbert space and E is obtained by local complementation; E is the "location" of the local observer. We shall see that the Hilbert space can make room for a notion of local observer: the observer becomes the (local) complement of the observable, i.e. the closed linear manifolds of the Hilbert space—of course the whole Hilbert space contains all bounded linear transformations (defined on open subsets) and is therefore not orthocomplementable. But here we obtain non-orthocomplementability in a different way. (Remember that in a finite-dimensional space, every linear manifold is closed).

Theorem. Hilbert space admits the observer through local negation (or complementation)—that is, we do not have orthocomplentation on the whole Hilbert space even in the finite-dimensional case (For the notion of local negation, see Gauthier 1985).

Proof. Let $\mathcal{H}$ be an n-dimensional Hilbert space and let $F^{\perp}$ be the set of closed linear manifolds $f^{\perp}$, $F^{\perp} = F^{-}$, the closure of all f. One can now define the relative complement F^{+} of F^{-} such that $\mathcal{H} - F^{-} = F^{+}$; F^{+} is then an open subset. From the topology, we pass to the metric of $\mathcal{H}$; for the metric of $\mathcal{H}$, a subset A of $\mathcal{H}$ is located (this notion of located subset has been introduced by Brouwer. E. Bishop has put it to use in his *Foundations of Constructive Analysis* (1967), if the distance

$$\forall x \in \mathcal{H}\,[\rho(x, A) \equiv \inf\{\rho(x, y) : y \in A\}]$$

from x to A exists. The metric complement $-A$ of a located subset A is the set

$$-A \equiv \{x : x \in \mathcal{H}, \rho(x, A) > 0\}$$

which is open, since

$$\forall x, y \in \mathcal{H}\left[\rho(x, A) \leq \rho(x, y) + \rho(y, A)\right].$$

Here the observer has a topological and metrical place as the local complement of the closed set of subspaces of $\mathcal{H}$. In order to further constructivize this result, I introduce the topological boundary operator b which is to be interpreted as the boundary between the observable (or observed) and the observer : we have the relations

$$E = \neg D - b(E)$$

and

$$D = \neg E \cup b(D)$$

thus

$$\neg D(\mathcal{H}) = E(\mathcal{H}) - b(E(\mathcal{H})).$$

The interior of E, i.e. E°, is the complement of the closure of the complement of E and is thus open; we have also

$$E = E^{\circ}.$$

For any x, $D(\neg x)$ means that $x \in E$. So for some a, we have

$$E(a) = D(\neg\, a) - b(D(\neg\, a));$$

On the other hand, the closure of D, i.e. D^{-} implies that

$$B(D(\neg\, a)) = a^{-} \cap (D - a)^{-}.$$

Hence

$$A^{-} = a \cup b(D(\neg\, a))$$

and

$$a^{-} \in E(\mathcal{H}) = a \in D(\mathcal{H}) \cup b(a \in D(\mathcal{H}))$$

and

$$a \in D(\mathcal{H}) = a^{-} \in E(\mathcal{H}) - b(E(\mathcal{H}))$$

which shows that E is disjoint from its boundary, that is, it is open and consequently the whole Hilbert space $D(\mathcal{H}) \cup E(\mathcal{H})$ is not orthocomplementable, since local complementation excludes $(a^{-})^{-} = a$.[2]
Remark: the effect of abandoning orthocomplementation amounts to adopting an indefinite metric which may, in fact, be more convenient for some physical theories (e.g. quantum field theory).

5.5.5 The Total Hilbert Space

Gleason's theorem says that in a separable Hilbert space of dim ≥ 3, every measure on the closed subspaces has the form

$$\mu(A) = Tr(WP_A)$$

where the trace Tr means $TrX = \sum_R (\varphi_R, X_{\varphi_R})$ for any complete system of normalized orthogonal vectors φ_R; P_A denotes the orthogonal projection of A and W is a Hermitian operator which satisfies

$$W > 0, TrW = 1 \text{ and } W^2 \leq W.$$

Since the sum for the linear span B over a countable set of orthogonal subspaces A_i

$$\mu(B) = \sum \mu(A_i)$$

is finite, μ can be regarded as a real positive measure on the functional space L^2 as we saw above. Gleason's result states that "frame functions" defined on the unit sphere are regular, that is, there exists a self-adjoint operator T defined on the Hilbert space $\mathcal{H}$ such that the frame function f is

$$f(x) \equiv (Tx, x).$$

When the (real) Hilbert space is finite-dimensional, the frame functions are regular, iff they are the restriction to the unit sphere of quadratic forms (homogeneous polynomials of degree 2)—again in accordance with the Hilbert-Kronecker theorem on the finite sum of the squares of coefficients in a linear expression. But the total Hilbert space containing not only the subspaces (closed varieties), but all the linear varieties is infinite-dimensional and is not orthocomplementable. In view of the fact that complements in the total Hilbert space cannot be uniquely determined, a fact that von Neumann and Birkhoff had noticed, one can introduce a local or relative complement in the lattice of open subsets of $\mathcal{H}$ beyond the

[2] Orthocomplementation requires that $(a^{-})^{-} = a, a^{-} \cap a = \emptyset$ and $a \leq b \leftrightarrow b^{-} \leq a^{-}$.

closed sequence of subspaces of$\mathcal{H}$. Topologically then, the local complement is an open subset of $\mathcal{H}$ and the topological boundary operator separates the space of the observed system from the space of the observing system, since points on the boundary are neither in A nor in $X - A$ for a given set and its complement in a topological space X. All linear varieties are closed in a finite-dimensional space $\mathcal{H}$, and we have to "open up" that space; we need to locate finitely the relative complement and a metric to that effect can be defined on the topology. Brouwer has introduced the notion of located subset for subsequences: a subsequence A of B, i.e. $A \subset B$, is localised, if there exists a distance ρ (for points x and y) such that

$$\forall x \in \mathcal{H}\,[\rho\,(x, A) \equiv \inf\{\mathrm{p}\,(\mathrm{x}, \mathrm{y}) : y \in A\}]\,.$$

The metric local complement $-A$ of the subsequence A is

$$-A \equiv \{x : x \in \mathcal{H}, \rho\,(x, A) > 0\}$$

and is open, since

$$\forall x, y \in \mathcal{H}\,[\rho\,(x, A) \leq \rho\,(x, y) + \rho\,(y, A)]\,.$$

The notion of local complement with its distance function constitutes the basis of a probability calculus which differs from the classical notions.

5.5.6 Finite Derivation of the Local Complement

In accordance with Hilbert's result on finite sums for linear expressions, the local complement of our probability calculus is also embedded in a finite form. Instead of Kolmogorov's infinite probability space, we have a finite probability space as in Nelson (1987a,b): a finite probability space is a finite set Ω and a (strictly positive) function pr on Ω such that for $\omega \in \Omega$

$$\sum pr\,(\omega) = 1$$

and expectation is defined

$$Ex = \sum x\,(\omega)\,pr\,(\omega)$$

for a random variable x; the probability of an event $A \subseteq \Omega$ is

$$\mathrm{Pr}A = \sum_{\omega \in A} pr\,(\omega)\,.$$

Nelson also defines the complementary event as $A^c = \Omega \backslash A$ for all $\omega \in \Omega - A$. This is the Boolean complement which we replace by our local complement $(\Omega - a) + b$ or

$(1 - a) + b$. Putting $\bar{a}$ for $1 - a$, we introduce polynomials in the following (binomial) form with decreasing powers

$$(\bar{a}_o x + b_0 x)^n = \bar{a}_0^n x + n\bar{a}_0^{n-1} x b_0 x + [n(n-1)/2!]\, \bar{a}_0^{n-2} x b_0^2 x + \ldots + b_0^n x$$

where the companion indeterminate x shares the same power expansion. By some calculation (on homogeneous polynomials that are symmetric i.e. with a symmetric function $f(x, y) = f(y, x)$ of the coefficients—see Chap. 7 for a complete derivation or descent of that binomial form.)

$$\begin{aligned}
(\bar{a}_0 x + b_0 x)^n &= \bar{a}_0^n x + \sum_{k=1}^{n-1} (n - 1/k - 1)\, \bar{a}_0^{k-1} x + (n - 1/k)\, \bar{a}_0^k x b_0^{n-k} x + b_0^n x \\
&= \sum_{k=1}^{n} (n/k - 1)\, \bar{a}_0^k x b_0^{n-k} x + \sum_{k=0}^{n-1} (n - 1/k)\, \bar{a}_0^k x b_0^{n-k} x \\
&= \sum_{k=0}^{n-1} (n - 1/k)\, \bar{a}_0^{k+1} x b_0^{n-1-k} x + \sum_{k=0}^{n-1} (n - 1/k)\, \bar{a}_0^k x b_0^{n-k} x \\
&= \bar{a}_0 \sum_{k=0}^{n-1} (n - 1/k)\, (\bar{a}_0 - 1)^k\, b_0^{n-1-k} x + \sum_{k=0}^{n-1} (n - 1/k)\, \bar{a}_0^k x\, (b_0 - 1)^{n-1-k}\, c \\
&= (\bar{a}_1 x + b_1 x)\, (\bar{a}_1 x + b_1 x - 1)^{n-1}
\end{aligned}$$

and continuing by descent and omitting the x's, we have

$$\begin{aligned}
&(\bar{\mathrm{a}}_2 + b_2)\, (\bar{\mathrm{a}}_2 + b_2 - 2)^{n-2} \\
&\cdots\cdots\cdots\cdots \\
&(\bar{\mathrm{a}}_{\mathrm{n}-2} + b_{n-2} + \bar{\mathrm{a}}_{\mathrm{n}-2} + b_{n-2} - (n-2))^{n-(n-2)} \\
&(\bar{\mathrm{a}}_{\mathrm{n}-1} + b_{n-1} + \bar{\mathrm{a}}_{\mathrm{n}-1} + b_{n-1} - (n-1))^{n-(n-1)} \\
&(\bar{\mathrm{a}}_{\mathrm{n}} + b_n)\, (\bar{\mathrm{a}}_{\mathrm{n}} + b_n)^{n-n}
\end{aligned}$$

Applying descent again on $(\bar{a}_n + b_n)$, we obtain

$$(\bar{a}_0 + b_0)$$

or, reinstating the x's

$$(\bar{\mathrm{a}}_0 x + b_0 x)\,.$$

Remembering that

$$(\bar{a}x + bx)^n_{k<n} = \sum_{k+m=n} (k + m/k)\, \bar{a}^k b^m x^n$$

we have

$$(\bar{a}x + bx)_{k<n}^{n+m=n} = \prod_{k+m=n} (k, m) = 2^n$$

or more explicitly

$$\sum_{i=0}^{m+n} c_1 x^{m+n-1} = \bar{a}_0 x \cdot b_0 x \prod_{i=1}^{m+n} (1 + c_i x) = 2^n$$

where the product is over the coefficients (with indeterminates) of convolution of the two polynomials (monomials) a_0 and b_0. The descent that we have applied here is the arithmetic finite descent from a given n to the first ordinal (0, or 1). The finite descent (or derivation) is applied to a probability calculus, but it could be applied also to a propositional calculus as in Kochen and Specker (1967). The interesting difference is that the calculus is no more classical nor Boolean, but intuitionistic, since the local complement corresponds to intuitionistic implication

$$a \to b = In\,((X - a) \cup b)$$

and the algebra of propositions (or events) is not even a partial Boolean algebra, but a Brouwerian lattice, that is a partially ordered set with two binary operations (meet and join) and a relative "pseudo-complement"

$$a \to b = a \cap c \leq b$$

for c the greatest element different from a. The Brouwerian lattice is isomorphic to a Heyting algebra, which is the algebraic structure corresponding to the intuitionistic logic of propositions. The open subsets of a topological space also determine a Brouwerian lattice.

Kolmogorov's axiomatization of the probability calculus is based on a triple $< \Omega, \Sigma, \mu >$ for μ a probability measure on the σ-algebra Σ of subsets or events A of a probability space Ω

1. $A \in \Omega$
2. $\forall A \in \Omega \to \bigcup_{j=1}^{x} A_i \in \Omega$
3. $A' = \Omega - A$ for A' the complement of A

with $0 \leq \mu\,(A) \leq 1$ for $A \in \Omega$ and $\mu\,(0) = 0$, $\mu\,(\Omega) = 1$; countable or σ-additivity means

$$\mu\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} \mu\,(A_i)$$

for $A_i \cap A_j = \emptyset$, if $i \neq j$. Properties of the Boolean complementation of probabilities are summarized as follows

$$\left(A'\right)' = A, A \cup A' = \Omega, A \cap A' = \emptyset$$

and

$$(A \cup B)' = A' \cap B' \text{ and } (A \cap B)^{-} = \left(A' \cup B'\right).$$

For local complementation, we have $(A')' \neq A$ for

$$C = A \Rightarrow B = In\,((X - a) \cup B)$$

where In is the set of interior points and A, B, C are open subsets of a topological space X (C is here the largest open subset distinct from A). This relative "pseudo-complement" is the main distinctive feature of a Brouwerian lattice. We see that probabilities according to the local complement do not satisfy the Boolean equality or duality and make it possible to adjoin an intermediary or included third, that is the open subset B here. The expectation value

$$Exp\ \ (A) \int\ Ad\mu$$

for a dispersion ΔA is given by

$$Var\,(A) = Exp\,[A - Exp\,(A)]^2$$

and it is easy to see that in order to take into account the local complement, we must have

$$\Delta A^2 = Exp\,[A - Exp\,(A) + Exp\,(\neg A)]^2$$

where $\neg A$ is the local complement of the space of events. For non-interactive systems and dispersion-free states, the local complement has a negligible effect on the statistics. But in quantum interactive systems (where a measurement is *some kind* of interaction between an observed system and an observing system), the statistical *weight* of the local complement cannot be ignored, although it is confined and *indeterminate*. The indeterminacy has something to do with the Indeterminacy or Uncertainty relations, but only indirectly in that the local complement acquires a determinate value upon measurement and only within actual measurement results as a relative complementation of probabilities. It might be the place here to put some emphasis on the indeterminacy relations "*Unbetimmtheitsrelationen*". As one knows, quantum mechanics can be derived entirely from those determinate relations, for instance between the position x and the momentum p_x

$$pq - qp = i\hbar \qquad \text{where } \hbar = h/2\pi$$

of a particle as expressed in quantum statistics by

$$\Delta x \cdot \Delta p_x \geq \hbar/2$$

for Planck quantum h or even

$$\Delta x \cdot \Delta p_x = \hbar/2$$

from a classical-mechanical point of view. One may want here to have an entropic information measurement with a probability wave equation like Schrödinger's ψ

$$i\hbar \, \frac{\partial}{\partial t} \, \psi(\boldsymbol{r}, t) = H\psi(\boldsymbol{r}, t) \qquad \text{for the point } \boldsymbol{r} \text{ at time } t$$

through its Fourier transform that pins down the wave frequency spectrum to a pointlike signal particle, as one may say; we have seen above that the probability to find a particle in a particular position is given by

$$Pr(\boldsymbol{r}, t) = \psi^*(\boldsymbol{r}, t) \cdot \psi(\boldsymbol{r}, t) = |\psi(\boldsymbol{r}, t)|^2 \text{ for the complex conjugate } \psi^* \text{ of } \psi$$

which makes it clear that probability is ingrained in the analytical apparatus of *QM*, since it coincides with the mathematical structure of *QM* and its measurement theory. Again, refinements of measurements reveal that the interaction between the observed system and the *external* observing system is the essence of the Copenhagen (Bohr-Heisenberg) interpretation of *QM* and as far as the entropic (Shannon) information is involved $H = -K \log p$, the local observer is one more time the (entropic or anthropic?) informant, since in statististical mechanics, entropy is a measure of uncertainty or, better said, of indeterminacy as in quantum mechanics. And it should not be a surprise to observe that the formalisms of quantum mechanics and statististical mechanics are intertranslatable for the simple fact that the Markov stochastic processes active in the latter are memoryless when it comes to measurement. There is no mystery in probability, as Hardy and Hilbert had deplored, when it becomes measured in an *actual* measurement—with or without von Neumann entropy for the wave function collapse—and the same demystification applies to Everett's *internal* observer who gets caught in the collapse and is then split or ramified in as many universes as there are in the uncountable cardinality of the wave function where measurements, according to Everett's relative state theory, could be (ideally) perfectly accurate and not only approximate as they are in the actual world. Such an ideal universe or multiverse is not really different from an unstable or false metastable vacuum of quantum field theory in which someone might find some true nothingness (L. M. Krauss) turning into something! More seriously, unified theories which look for stringy or granular ultimate constituents of the ground stuff (*Urstoff* in German), String Theory with supersymmetry and supergravity or Loop Quantum Gravity, are trying to find a common ground between Quantum Mechanics and General Relativity. Quantum fluctuations of the *true* vacuum are defined as Heisenberg indeterminacy relations between energy and time

$$\Delta E \cdot \Delta T \approx h/4\pi$$

where the metric of the Einstein field equations for gravitation with the metric tensor $g_{\mu\nu}$ and the Ricci curvature tensor $R_{\mu\nu}$

$$G_{\mu\nu} = R_{\mu\nu} - 1/2 g_{\mu\nu} R$$

has zero curvature

$$R_{\mu\nu} = 0.$$

What this means is that the quantum vacuum is full of energy—potentially beyond the Higgs mass at 125 GeV and even Planck length at 10¯33 cm—the nothing universe, to mock Krauss' popular title "*A Universe from Nothing*", is impatient to rush into being and become *something* real before a Big Bang in the standard model or after a (Bojowald's) Big Bounce or forever in a Penrose's ekpyrotic cyclic universe (or whatever in a non-standard alternative cosmological scenario, inflationary or not). In any case, the old adage still stands "*Ex nihilo, nihil fit*" which could be translated or paraphrased as "From nothing, nothing fits"!

It is possible to reconstruct the EPR argument for "elements-of-reality" without Bell's inequalities by appealing to indirect measurements or *reductio ad absurdum* arguments. The contextuality and nonlocality appear as features of a realist interpretation incompatible with *QM* to the extent that undefined values for observables of *QM* become definite for "elements-of-reality" in the EPR reconstruction. The simple case of the spin angular momentum will suffice for our argument.

The fundamental relationship for the x, y, z components of spin along the $x-, y-, z-$ axes is (S being the spin observable and squaring)

$$S_x^2 + S_y^2 + S_z^2 = S^2.$$

Direct measurement of the z component excludes attributing definite values to the other components, but realism specifically supposes that there are *independent* "elements-of-reality" that can be subjected to *indirect* measurements.

Léon Rosenfeld, a harsh defender of the Copenhagen interpretation, summarizes the instrumentalist view:

> A phenomenon is therefore a process (endowed with the characteristic quantal wholeness) involving a definite type of interaction between the system and the apparatus (1967, p. 82).

Thus, the probability calculus must be inherent to the quantum-mechanical measurement process. The tacit assumption of a classical probability structure must be questioned and a better adjustment of the analytical apparatus and its physical interpretation remains a lasting problem for foundational research. The completeness of Quantum Mechanics, despite Bell's pronouncement, is such a problem, may it be of a quantum-logical or mathematical nature. The topological solution suggested here has instrumentalist overtones, but it aims essentially at explaining Quantum Mechanics as the physics of "local" experiments. Although the metaphysics of wholeness or non-separability is not totally dispelled by such an attempt, it might provide the sceptic with some good reasons not to despair about the so-called incompleteness of Quantum Mechanics in his search for reality. As Redhead (1987, p. 45) puts it, on Bohr's complementarity interpretation, the value of an observable Q, when the state of the system is not an eigenstate of Q, is undefined or "meaningless" and one cannot impugn such an interpretation by denying a locality principle which says that a previously undefined value for an observable cannot be defined by measurements performed "at a distance". On Redhead's reckoning, the charge of incompleteness cannot be levelled against Bohr's view, unless staunch realism and non-constructive *reductio ad absurdum* arguments are invoked. But if the Indeterminacy or Uncertainty Principle has given rise to a non-commutative geometry and analysis (A. Connes), Bohr's Complementarity Principle could yield on a par a non-classical logic and probability calculus. And this militates for a proportionate anti-realist or, as I prefer to say, a constructivist (instrumentalist) interpretation of *QM*.

5.6 Riemannian Geometry

Hermann Weyl's foundational stance in mathematics is many-faceted. From the predicative mathematics of *Das Kontinuum* (1917) to the constructivist Kroneckerian point of view of *Algebraic theory of numbers* (1939), Weyl has sustained a continuous effort to defend a constructivist philosophy in mathematics, physics and science in general. I do not want to put any emphasis on his philosophical inspirations from Kant and Fichte to Husserl and Brouwer. I shall rather insist on the motivations internal to his mathematical work and particularly on his appraisal of Riemannian geometry, which has played a major role in Weyl's theoretical endeavours.

I recall the main ideas of Riemann's 1867 paper "*Über die Hypothesen welche der Geometrie zu grunde liegen*", "On the hypotheses of the foundations of geometry" (Riemann 1990). The concept of an n-dimensional manifold or space (*Mannigfaltigkeit*) is a topological one, that is, it is to be treated with continuous (real and complex) functions. As a metric space, it is endowed with the metric invariant ds^2 and here Riemann refers to Gauss' theory of curved surfaces.

The fundamental quantity for any surface is the element of arc length

$$ds^2 = dx^2 + dy^2 + dz^2.$$

Gauss had given a general form to this notion of distance by introducing parameters u and v to represent the coordinates (x, y, z) of any point on the surface and had obtained

$$ds^2 = e(u, v)dv^2 + 2f(u, v)dudv + g(u, v)dv^2$$

(where e, f, g are functions of the parameters u and v). The general formula for the ds^2 is

$$ds^2 = g_{mn}dx_m dx_n$$

where dx_m and dx_n are the infinitesimal transformations of the parameterized curves on the surface; and the g_{mn} are the quantities that depend on those curves. The curvature of a surface is then determined from this fundamental quadratic form; this is the point of departure of Riemann's work. The local or infinitesimal approach favoured by Riemann allows for a generalization of Gauss' surfaces into the n-dimensional manifold with the metrical groundform or fundamental metrical tensor (Weyl 1950, p. 39)

$$ds^2 = g_{uv} dx^u dx^v \text{(for } u, v = 1, \ldots, n)$$

which controls the behaviour of the geodesics for a point and a direction in an n-dimensional manifold.

The local infinitesimal point of view insures that the Pythagorean theorem is valid in the infinitely small and in his remarks on Riemann's lecture, Weyl insists again on the fact that the differential form ds^2 is not only the simplest, but also the most appropriate one for the classification of all possible geometries, as I have said above. Group theory enters the picture as, for example, in the case of the alternate subgroup of even permutations of a given group for the distinction between geometries of various dimensions. But Pythagorean-Riemannian geometry is a special case and Weyl adds that one has to supplement the names of Lie and Helmholtz in order to have infinitesimal mobility (*Beweglichkeit*) in an n-dimensional manifold.

The infinitesimal Lie group of rotations obeys the same positive definite quadratic form and also validates the Pythagorean theorem in the infinitely small. Weyl points out that his solution to the new problem of space implied in Relativity Theory, as he says, had urged him to construct a different solution, that is the affine geometry of parallel displacement which Weyl will put to use in his *Raum, Zeit, Materie*, ("Space, Time, Matter") of 1918 (Weyl 1950).

5.7 Riemann's "Hypotheses"

Weyl has put the emphasis on Riemann's achievement for being the first to define the idea of a physical geometry. Against all former mathematicians and philosophers, Weyl says it is Riemann who maintains that the metric field is determined by the material content of the world and has the same status as the electromagnetic field. In a Riemannian manifold of constant curvature, free mobility is guaranteed by the Lie group of rotations. But this again implies that the physical content of the space participates in the metric in such a way that it is the distribution of matter which defines ultimately the metric field, an idea rediscovered by Einstein, Weyl tells us. It is not doubtful that Riemann did have such a scientific objective. In his *Pariser Arbeit*, for example, he deals with the linear transformations involved in second-order differential equations to tackle the problem of an isothermic system again in terms of a fundamental quadratic form. In many of his works, Riemann could be considered as a mathematical physicist, as Weyl suggests, and I would suggest that he could be considered also as a philosopher of science, at least to the extent that he has expressed himself even so briefly on matters philosophical. Take, for instance, Riemann's notion of hypothesis.

As a student of the Kantian Herbart, who had defended a kind of physical *a priori*, Riemann distinguishes his sense of hypothesis from the Newtonian notion found in *Philosophiae naturalis principia mathematica*:

> *Quidquid enim ex Phaenomenis non deducitur, Hypothesis vocanda est*.

Riemann prefers to define hypothesis as anything (concepts and principles) that goes beyond phenomena, and not as figments of one's imagination:

> *Man pflegt jetzt unter Hypothese Alles zu der Erscheinungen Hinzugedachte zu verstehen* (Riemann 1990, p. 525).

For Riemann, hypotheses and facts <*Thatsachen*> share a common status as conceptual structures that supervene on phenomena; the law of inertia, for example, as a law of motion is a hypothesis, not different from an axiom, since it belongs to the transempirical or empirical *a priori* realm, while an axiom in the traditional sense should be analytical. By the same token, one could say that facts are the same as hypotheses and Helmholtz' 1868 work <*Über die Thatsachen die der Geometrie zugrunde liegen*> stands in perfect continuity with Riemann's notion of hypothesis. As a matter of fact, Riemann states the law of inertia as a counterfactual conditional, much in the manner of later logical positivism:

> If there were only a single material point in the world moving in space at a definite velocity, it would always move with the same velocity. (My translation of Riemann 1990, p. 525).

Riemann's notion of hypothesis reaches beyond Kant to Descartes and Aristotle. One could justify the hypothetico-deductive method by quoting Descartes who says in his *Principles of Philosophy* (IV, 204):

> For the things that our senses cannot reach, it suffices to explain how they could be.

Descartes adds: it is exactly what Aristotle has done and he refers here to Aristotle's *Meteors* (I, p. 7):

> If it is true that for phenomena which escape our senses we deem to have given a rational explanation by ascending to their possible causes, it is certainly true for those phenomena which we now study (the meteors).

This anagogical way has been called abduction by Peirce and it is certainly part of what has been termed ≪ inference to the best explanation ≫. In any case and without pouring too much philosophy into Riemann's sparse remarks, one should not neglect the foundational motivations in Riemann's mathematical work.

5.8 Physical Geometry

In the Special Theory of Relativity, the Minkowskian four-dimensional manifold is Euclidean, but the quadratic form here is not positive definite, it has an index of inertia of 1; it is then called semi-Riemannian as in the case of Special Relativity

$$ds^2 = dx^2 + dy^2 + dz^2 - c^2dt^2$$

while in the General Theory, the manifold is Riemannian, since the gravitational material content of the world forces a curvature onto the structure of the metric field.

Incidentally, Riemann points out in his lecture that such a curved space or spherical universe could be unlimited in extension without being infinite from the point of view of measurement. In the case of a space with positive curvature, however small it is, an unlimited spherical surface is necessarily finite (Riemann 1990, p. 284).

In his paper "*Reine Infinitesimalgeometrie*", Pure Infinitesimal Geometry (1918), Weyl declares that Riemann is not always consequent, for infinitesimal geometry forbids to relate two finite elements when they are at an arbitrary finite distance from each other, as Riemann supposes. The relation is possible only in infinitesimal affine geometry for infinitely near points. As Weyl puts it in *Space, Time, Matter*, it is:

> The principle of gaining knowledge of the external world from the behaviour of its infinitesimal parts. In a Riemannian geometry, geodesics have a stationary length, which is not the case in affine geometry (Weyl 1950, p. 193).

I want to comment briefly on the fate of Weyl's own geometrical idea of affine geometry, an idea which has been instrumental in his unified field theory of electromagnetism and gravitation in *Raum, Zeit, Materie*.

Weyl indicates that an affine relationship or transfer of direction and not only of length in infinitesimal parallel displacements is inherent in metric space. The metric field is still dominated by the quadratic form ds^2 while the electromagnetic field is endowed with a linear fundamental form $\varphi_i dx_i$ which has its origin in the metric field. Weyl will admit later that the gauge invariance between the electromagnetic and the gravitational fields was to be grounded on a more fundamental quantum theory. He had also introduced a cosmological constant as Einstein did, but Weyl thought that Einstein's lambda (λ) was arbitrary, as Einstein later admitted, for it was meant only to insure spatial closure of a stationary universe, while Weyl claims an inner necessity for his own λ, because his affine geometry accounts for the electromagnetic potentials and fully obey Maxwell's equations which demand the equilibrium state of the total mass of a closed universe. An inner necessity however which finally vanished like Einstein's blunder. The fact that it is revived today in supersymmetry theories is evidence that blunders have their own constancy, if not their own cosmology. There remains though Weyl's fundamental idea of a unified theory based on gauge invariance which is still a major building block in contemporary physics. But Weyl has also emphasized the Minskowskian world picture in Relativity Theory.

5.9 Minkowski's Spacetime

I am interested here in the connection of Minkowski's spacetime formulation of Special Relativity with his geometry of numbers or *Geometrie der Zahlen* which Minkowski had developed prior to his famous 1908 paper *"Raum und Zeit"*. There is an inner mathematical connection between the two enterprises and I want to argue that spacetime diagrams are an illustration in physical geometry of a central scheme in the geometry of numbers which was the main endeavour of Minkowski's mathematical career. Minkowski's work in physics belongs to mathematical physics and his statement at the end of the *"Raum und Zeit"* paper can be counted as the philosophical motto of the mathematical physicist:

> With the elaboration of its mathematical consequences, there will be plenty of hints for the experimental confirmation of the postulate (of the absolute world), so that anyone who feels uncomfortable with the loss of traditional pictures (*Anschauungen*) will find himself compensated with the idea of a preestablished harmony between physics and pure mathematics. (Minkowski 1967, my translation)

Such a declaration of principle echoes Minkowski's assessment of Dirichlet's achievements in mathematical physics—see his 1905 address *"Peter Gustav Lejeune Dirichlet und seine Bedeutung für die heutige Mathematik"* (in Minkowski 1967, II, pp. 449–461). Minkowski says that the two directions of number theory and mathematical physics, though they seem to diverge, are harmoniously integrated in Dirichlet's work by the use of the integral calculus. Here Minkowski mentions Dirichlet's results on the convergence of Fourier series and the Dirichlet principle on the minima of the potential function. In praising Dirichlet for having introduced discontinuous factors in the multiple integrals of the potential function, Minkowski evokes Leibniz's idea of a grand scheme for a perfectly harmonious world. This mathematician's dream was encapsulated in Minkowski's postulate of the absolute world and I want to explore now its mathematical motivation.

Hermann Weyl credited Minkowski for having recognized that:

> The fundamental equations for moving bodies are determined by the principle of relativity if Maxwell's theory for matter at rest is taken for granted. (Weyl 1960)

He also said, referring to Minkowski's 1907 paper *"Die Grundgleichungen für die elektromagnetischen Vorgänge in bewegten Körper"* (in Minkowski 1967, II, pp. 352–404) or "The Fundamental Equations for the Electromagnetic Processes in Moving Bodies", that:

> The adequate mathematical formulation of Einstein's discovery was first given by Minkowski: to him we are indebted for the idea of four-dimensional world-geometry. (Weyl 1960)

Minkowski had distinguished in the aforementioned paper the theorem of relativity from the principle of relativity; the first is purely mathematical in terms of the covariance of Lorentz transformations and the second, the principle of relativity, allows, in Minkowski's words, for the derivation of the laws of mechanics solely from the principle of the conservation of energy. The language here is still of spacetime vectors and does not anticipate on the 1908 paper on *"Raum und Zeit"* where the vocabulary of worldpoints and worldlines is canonized and serves as the basic ingredient for a graphic representation, as Minkowski says, of the group of spatiotemporal transformations. Minkowski then suggests that the terminology for the postulate of relativity is rather dull—*"matt"* in German—when one wants to stress the invariance properties of the group of the transformations and he comes up with his "postulate of the absolute world" (*Postulat der absoluten Welt*). Let me point out that at one time Einstein himself had wanted to rename relativity theory as invariant theory.

My contention is that Minkowski's idiom has essentially a mathematical meaning as a representational means for the spatiotemporal structure of the physical world. And

I assume that Weyl did not interpret the Minkowskian mathematical picture otherwise (see Gauthier 2005). I shall give some reasons to substantiate that claim in the following.

5.10 Geometry of Numbers

Minkowski's work on physical problems (hydrodynamics, capillarity, etc., and on relativity theory) is marginal compared to his endeavour in number theory, geometry and especially what Minkowski called the geometry of numbers. It is in the geometrical representation of number-theoretic relations that Minkowski introduces the notion of *Zahlengitter* or number grids. Minkowski defines there a three-dimensional number grid as a geometrical representation of three integers in rectangular coordinates—see *"Über Geometrie der Zahlen"* (Minkowski 1967, I, pp. 264–265). These three integers correspond to discrete points in space; and these points in turn represent bodies (*Körper*) and the main question is the content of the surface (*Flächeninhalt*) on which those bodies float or are immersed in, so to speak. To illustrate this train of thought, let us look at a diagram drawn by Minkowski to define the approximation of a real quantity (number) by rational numbers (Fig. 5.1):

The three grid points H, J and K on the straight line $Y = 1$ stand in the following relation: $HJ = JK = OA$ for O the null point at the center of the grid and A a point corresponding to K on the straight line G parallel to $Y = 1$. The inscribed parallelogram does not contain any other grid point besides O in its interior. Minkowski uses such diagrams to show that two relatively prime numbers x and y can be represented by linear forms $\zeta = \alpha x + \beta y, \eta = \gamma x + \delta y$ for the straight lines ζ and η with arbitrary coefficients $\alpha, \beta, \gamma, \delta$ and a determinant $\alpha\delta - \beta\gamma = 1$ so that the norm or the length between x and y (not both zero) is

$$|\zeta\eta| \leq 1/2.$$

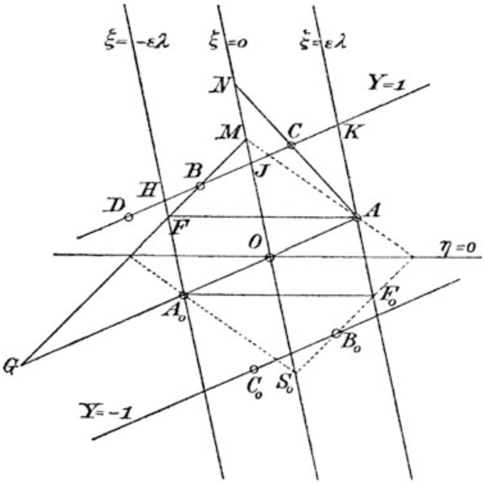


Fig. 5.1 From Minkowski (1967, I, p. 327)

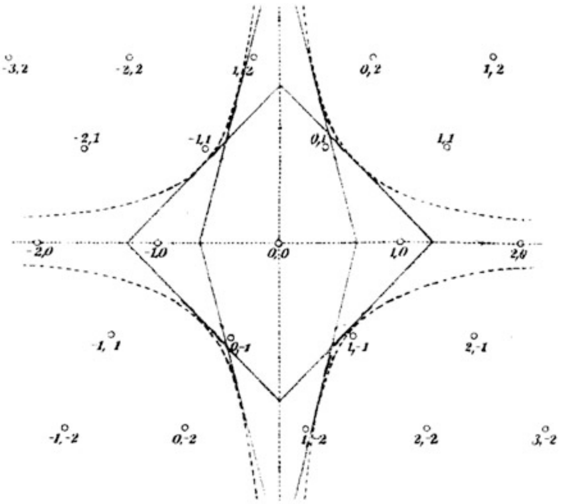


Fig. 5.2 *"Diagonalketten"* (diagonal chains) from Minkowski (1967, II, p. 45)

$$\text{(1)} \qquad f(z) = c_m z^m + \cdots + c_0 + \frac{c_1}{z} + \frac{c_2}{z^2} + \cdots$$

$$= F_0(z) - \cfrac{1}{F_1(z) - \cfrac{1}{F_2(z) - \cdots}};$$

$$\text{(2)} \qquad \bigl(P(z) - f(z)\,Q(z)\bigr)\,Q(z).$$

$$\text{(3)} \qquad \frac{x}{y} - a < \frac{1}{2y^2}, \qquad \text{(4)} \qquad a = g_0 - \cfrac{1}{g_1 - \cfrac{1}{g_2 - \cdots}}$$

$$\text{(5)} \qquad \xi = \alpha x + \beta y, \quad \eta = \gamma x + \delta y, \quad \alpha\delta - \beta\gamma = 1;$$

$$\text{(6)} \qquad -\tfrac{1}{2} < \xi\eta < \tfrac{1}{2}.$$

Minkowski's diagrams and calculations are quite involved as is shown by the following diagram intended to illustrate the "very intuitive link between all the possible solutions of the inequality $|\zeta\eta| \leq 1/2$ in whole numbers without common divisors" in Minkowski's words (Fig. 5.2):
Here Minkowski uses continued fractions to obtain the desired inequality

$$-1/2 < \zeta\eta < 1/2$$

for what he calls diagonal chains of continued fractions (*Diagonalkettenbrüche*).

This geometry of numbers has an arithmetical core, while geometry has an intuitive appeal. The main idea is to inscribe triangles or parallelograms in rectangular Cartesian coordinates in order to represent geometrically the reticular system or grid (*Gitter*) of all grid points (*Gitterpunkte*) of positive quadratic forms with integer coefficients. A number grid or mesh or point lattice (as it is now called when points have integer coefficients) is most important for the representation of the volume of a body and its fundamental arithmetical property is the generalization of the length of a straight line into the principle that in a triangle the sum of the lengths of two sides is never smaller than the length of the third side. As a special case, one easily points to the Pythagorean Theorem for right triangles:

$$c^2 = a^2 + b^2$$

which is at the foundation of the differential form

$$ds^2 = dx_1^2 + dx_2^2$$

in Euclidean coordinates. Weyl pointed out that the differential form ds^2 is not only the simplest, but also the canon for the classification of possible geometries since the positive quadratic form generates all linear transformations of the variables involved as a unique mathematical structure. Of course, the ds^2 is the fundamental (quadratic) form

$$ds^2 = c^2dt^2 - dx^2 - dy^2 - dz^2$$

for the invariant metric element in Special Relativity. Let me remark that if one lifts the quadratic restriction, one gets Finsler spaces which are akin to Riemannian spaces. I do not need to mention that Minkowski devoted much of his work to the theory of quadratic forms, i.e. homogeneous polynomials of the second degree, which were the main object of study in number theory from Gauss to Kronecker. Rather than elaborate on this, I can only mention that number grids are clearly connected to what we now call Minkowski diagrams.

5.11 Spacetime Diagrams

In his mathematical diagrams, Minkowski depicts grid points and intersection points for the approximation of a real number (or quantity) by rational numbers or diagonal chains of continued fractions that illustrate the fact that in a triangle the sum of the lengths of two sides cannot be smaller than the length of the third one. Here entire rational functions are used as denominators of continued fractions. What we have is an intuitive representation of solutions of a real inequality in terms of integers without common divisors.

Those diagrams do not differ essentially from the ones which are to be found in the paper *"Raum und Zeit"*. What is represented here as a grid point is the notion of an arbitrary point like charge or electron or potential field (with vector potential and scalar potential components) in a light cone. The world postulate or the postulate of the absolute world is nothing more than the totality of those grid points along grid lines in a gridded universe without any ontological import.

To obtain a physical picture for Minkowski's diagrams, one has to make the assumption of a correspondence between the energy vector *of motion* and the energy vector *in motion*, as Minkowski clearly said:

> *Der Kraftvektor der Bewegung ist gleich dem bewegenden Kraftvektor.* (Minkowski 1967, II, p. 441)

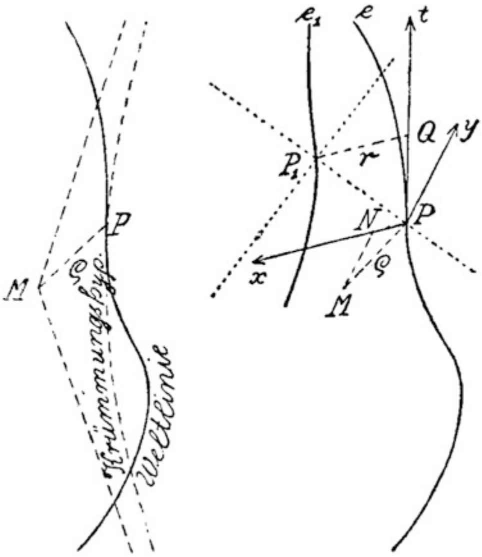


Fig. 5.3 From Minkowski (1967, II, p. 442)

What this means is that motion can only be represented by the picture of a moving vector on a continuous line, a worldline as a moving world point; diagrams can then be drawn to picture motion in a physical geometry as grids were used to cover the content of a surface (*Flächeninhalt*) in a geometry of numbers (arithmetical geometry). The parallel between the two tasks, to cover a surface with numerical grids and to fill up a two-dimensional space with diagrams, strongly suggests that there is a continuous path in Minkowski's mathematical *Weltanschauung* or theoretical construction of the world, to use Weyl's terminology. Let us examine in detail the following diagram (Fig. 5.3).

The diagram depicts an electron e in motion along its worldline through worldpoints P, $P1$ and Q. Minkowski wants to describe here a moving pointlike charge in the "absolute world", that is in a four-dimensional continuum with three space coordinates x, y and z and a time coordinate t. The vector $P1Q$ has a norm or length r, whereas the vector PQ has a length e/r since P lies on the tangent orthogonal to $P1Q$ which cuts through the worldline of e. All this combined with c, the speed of light in the light cone, defines the potential field of the pointlike electron e at point $P1$. Set against the negative curvature hyperbola of the timelike world line, the diagram should provide the appropriate scene for the equations of the ponderomotive force in an electromagnetic field.

Let us remark that this diagram is meant to represent a four-dimensional world—there are continuous curved lines—while the diagrams in the geometry of numbers were meant to represent a three-dimensional world of spatial bodies (*Körper*)—there were only continuous straight lines. The four-dimensional world is of course expressed in the quadratic form

$$dt^2 = -dx^2 - dy^2 - dz^2 - ds^2$$

or equivalently for the invariant metric element

$$ds^2 = c^2dt^2 - dx^2 - dy^2 - dz^2$$

which is the central formulation of Minkowski's version of Special Relativity.

5.12 Physical Axiomatics

Is this Minkowskian representation a physical or a mathematical one? In view of Minkowski's pronouncements on mathematical physics, one would be tempted to advocate a purely mathematical treatment. This might be the reason why Einstein was reluctant at first to adopt Minkowski's formulation. I would rather put Minkowski's achievements in the Hilbertian tradition of the axiomatization of physics. We know that Hilbert was a close friend of Minkowski's and he praised him on many occasions.

One is reminded that Hilbert had put the problem of "The mathematical treatment of the axioms of physics" as the number 6 item on his famous 1900 list of mathematical problems. Hilbert names probability theory and mechanics as the two major candidates for axiomatization. The central problem in physical theories is the consistency problem in Hilbert's view because a fundamental physical theory proceeds like geometry from general axioms to more specific ones and the extension from the first principles to the secondary ones must preserve consistency. Consistency is not a matter of feeling or experimentation, but of logic (or mathematics), Hilbert insists.

Hilbert's ideas of the foundations of Quantum Mechanics have been made to work by von Neumann in the Hilbert space formulation, which is the standard formulation of Quantum Mechanics. From my point of view, Minkowski's diagrams belong to the models of a canonical analytical apparatus and I want to come back to Minkowski's other works in mathematical physics. I see Minkowski's endeavour as part of the Hilbertian program for the axiomatization of physics. Hilbert had mentioned as candidates for axiomatization limit processes and laws of motion for solid bodies in continua: it is precisely that kind of problem that Minkowski had already tackled in a 1888 paper on "The Motion of a Solid Body in a Liquid" (*"Über die Bewegung eines festen Körpers in einer Flüssigkeit"*) in the line of Kirchoff's work. His subsequent work on capillarity is a sequel to that first work and it is in 1907 paper mentioned above on "The fundamental equations for electromagnetic processes in moving bodies" that he states his relativity theorem (*Theorem der Relativität*) for the pure mathematical fact of the covariance of Lorentz transformations and then proceeds to formulate his relativity principle in a canonical (axiomatic) fashion, for which everything follows from the sole principle of the conservation of energy. In that paper, Minkowski declares that

> It is not a serious difficulty for the mathematician accustomed to n-dimensional manifolds and non-Euclidean geometry to adapt the concept of time (as a fourth dimension) to the concrete Lorentz transformations. (Minkowski 1967, II, p. 366, my translation).

This is in accordance with Einstein's account of Special Relativity, Minkowski concludes. Minkowski's efforts in the axiomatization of physics are continued in the paper on “The derivation of the fundamental equations for electromagnetic processes in moving bodies from the point of view of the theory of the electron” (Minkowski 1967, II, pp. 405–430). But that text had to be rewritten by Max Born on Hilbert’s invitation after Minkowski’s death. Born says that he had to work with a hundred-page manuscript full of formulas but with no helpful advice; needless to say, it is not a conclusive treatment of the theory of electrons.

What philosophical conclusions can be drawn from my analysis? For the ontology of space-time, a grid universe could be empty or devoid of any substance, or *Substanz* if we want to use Minkowski’s word for matter. Substantial points or worldpoints constitute worldlines which embrace the whole world, Minkowski insisted (Minkowski 1967 II, 434) and the universal validity of the world postulate points to the pre-established harmony of pure mathematics and physics (Minkowski 1967, II, p. 444). Since the postulate of the absolute world can be given a purely mathematical signification in virtue of its arithmetico-geometrical foundations, I would grant it, following Weyl, only a transcendental status, that is the status of an a priori structure in the theoretical construction of the world, as Weyl put it in his *Philosophy of Mathematics and Natural Science* (Weyl 1960, p. 235). Minkowski diagrams belong to the analytical apparatus—*der analytische Apparat* as Hilbert had termed it in his work on the foundations of Quantum Mechanics. The diagrams do not belong to a model of the physical world. From that standpoint, a realist interpretation of the Minkowskian world view is thereby excluded on Minkowski’s own terms. Although Minkowski states that his intuitions of space and time rest on the solid ground of experimental physics, their validity must be sought in the mathematical justification of the intuitive content. Behind or below the physical geometry, *“physikalische Geometrie”*, as Helmholtz called it, lies a geometry of numbers, the heart of which is arithmetic or number theory or simply number. Minkowski’s four-dimensional manifold is an instance of the concept of n-dimensional manifold and the mathematician has no problem in dealing—or toying, one might say—with that notion.

Weyl had of course novel ideas beyond Special and General Relativity theories and he has emphasized the probabilistic world view of Quantum Mechanics. His idea in the 1920s could indeed be seen as anticipating the free-will theorem of Conway and Kochen and also the no-cloning philosophy in *QM* and multiverse cosmology.

5.13 Hermann Weyl and the Free-Will Theorem[3]

Hermann Weyl has defended a probabilistic approach to quantum physics as early as 1920. At the time (Weyl 1920), Weyl shared with the intuitionist Brouwer the idea that the mathematical continuum was a process of becoming <*ein Prozess im Werden*> (Weyl 1918). For Weyl, the physical world is also in an infinite process of becoming and the notion of the end of time is only a limit idea <*Grenzidee*>. While the causal outlook

[3] The Content of this Paragraph has Originally Appeared Partially in *Reports in Mathematical Physics* **72** (2013), 191–199.

is bound to the eternal cycle of causal chains, the statistical or probabilistic view privileges decisions that are autonomous and causally absolutely independent of each other <*selbständige, kausal voneinander absolut unabhängige Entscheidungen*> (Weyl 1920, p. 541). Weyl adds that these <decisions> are the real ingredients of the world. The causal static view describes only the world scene <*Schauplatz*>, not the real events (of the statistical probabilistic worldview), Weyl concludes—see (Busek and Hillery 1996) for Weyl's view on the causal universe of Relativity Theory.

To me, Weyl's foundational stance offers a strong supportive hypothesis to the Conway-Kochen free will theorem and I would like to add a combinatorial probabilistic argument to defend the idea. Weyl himself uses the binomial distribution (Weyl 1920, p. 539) to stress the probabilistic independence of physical events and I shall use the argument against the naïve thesis of a current cosmological view on infinite worlds with infinite reproduction of true copies or doubles (or *Doppelgänger*)—Weyl had insisted on the one world of infinitely novel becoming. Let us start with the binomial distribution

$$p(k) = \tbinom{n}{k} p^k q^{n-k}$$

and the expansion of the binomial coefficient given by the factorial

$$\sum_{k=0}^{n} \tbinom{n}{k} = 2^n \text{ for } \frac{n!}{k!(n-k)!} = C_n^k$$

for the combinations C with the power set 2^n of a set of n elements. By Cantor theorem the power set $P(X) > X,\ P(X) = 2^X$ and for a countable set $\aleph_0$

$$P\{\aleph_0\} = 2^{\aleph_0} = c \text{ (the continuum)}$$

and $P\{\aleph_0\} = \{\emptyset\}$, {finite subsets}, {countable subsets $\aleph_0$}, $2^{\aleph_0}$. Thus the continuum has cardinality $2^{\aleph_0}$ and—independently of the Continuum Hypothesis which asserts that $2^{\aleph_0} = \aleph_1$ or the Generalized Continuum Hypothesis $\forall\sigma(\aleph_\sigma < 2^{\aleph_\sigma} = \aleph_{\sigma+1})$—Cantor has shown that all continua in any dimension are *isomorphic*, but Brouwer has subsequently shown that they are not *homeomorphic*, that is the bijection is not continuous, for example there is no continuous transformation between points on a circle and points on a sphere. The argument shows that finite subsets are indistinguishable in the continuum; in terms of measure-theoretic probability theory (Borel-Kolmogorov), they are negligible or of measure zero, so that there is no infinite reproduction of a finite configuration (combination) in an indeterministic universe. In a deterministic universe, eternal return is possible only in a spatially finite world. Poincaré's recurrence theorem states that an isolated mechanical system will come back arbitrarily close to its initial state or conditions in a universe of *finite volume* on an arbitrarily long temporal sequence (see Gauthier 2009a).

The combinatorial argument points to infinististic hypotheses in contemporary physics, from quantum theory (e.g. Everett's multiverse theory) to cosmology (e.g. parallel universes) as well as to logical or mathematical theories which postulate actual infinities.

In the case of Everett's multiverse hypothesis, the fact there is no bijection between $\aleph_0$ and $2^{\aleph_0}$ can be invoked against the thesis of the universal ramification of the wave function in *QM*. The universal ramification has $2^{\aleph_0}$ branches (the real or complex values of the wave function). We assume that there are at most $\aleph_0$ observers in an infinite multiverse, otherwise there would be an instantaneous realization of the $2^{\aleph_0}$ values, which means that measurement results would be indistinguishable and the universe (multiverse) would be in all its states simultaneously (*toto universo simul*). Therefore no distinct (finite) measurement results would be available to any local observer and this is sufficient to refute Everett's thesis with the collateral thesis that the formalism generates its own interpretation! From a quantum-thoretical probabilistic point of view, a single experiment would deliver the infinite decimal expansion of a real number in one blow—no need here to pinpoint the inconsistency! Everett's relative state formulation has been taken anew by the physicist Carlo Rovelli (1996), but with the proviso that the new formulation takes into account the relational structure between the measured system and the measuring system, which I call the local observer (see Gauthier 1983a,b). My argument here is in accord with Special Relativity where there are no simultaneous measurable events and also with General Relativity since the invariant ds^2 applies to cosmic events through the covariance principle.

Hermann Weyl as a constructivist logician and mathematician who was also deeply involved in physics and its philosophy could not conceive of the continuum, mathematical or physical, as a static set-theoretic transfinite universe. This accords well with a finitistic worldview which grants the physical world with a spontaneous self-determining becoming or evolution as advocated in the Conway-Kochen proposal (Conway and Kochen 2006, 2009). The Conway-Kochen argument dispenses with probability or random processes; for Weyl, the causal (deterministic) independence of decisions <*Entscheidungen*> is likely indistinguishable from the statistical (stochastic) <indecisions> in the constructive theory of a becoming continuum (Weyl 1920, p. 541) from the point of view of local observers (see Gauthier 1983a,b).

5.14 The Conway-Kochen Free-Will Theorem

In their paper, Conway and Kochen (2009) quote Hermann Weyl's saying: <The objective world simply is, it does not happen> and reject this block-universe vision of an eternal spacetime arena for General Relativity, but they neglect to add that Weyl mentions the <gaze of consciousness> (Weyl 1963, 116) as the sequential order of events in the transcendental world which is a physico-mathematical construction of our own. This last view is certainly coherent with the free will idea that Conway and Kochen put forward in their papers.

To make explicit their idea of free will in Quantum Mechanics, they have formulated three axioms:

1. the SPIN axiom says that a triple experiment, that is an experiment in a three-axes x, y, z coordinate system, yields the outcome $1, 0, 1$ for spin-1 particles

2. the TWIN axiom asserts that spatially separated coupled spin-1 particles can give the same answer when they are asked the same question as in the well-known EPR experiment with the spin-$1/2$ statistics

$$\Phi = 1/\sqrt{2}[(\varphi_{+} \otimes \psi_{+}) + (\varphi_{-} \otimes \psi_{-})]$$

3. finally, the FIN axiom states a causal antecedence (relativistic causality) of the source of a signal over its reception.

The FIN axiom is put in a stronger form in Conway and Kochen (2009) under the name MIN claiming that two experimenters exchanging on the 33 particular directions (with 40 triples x, y, z) of the Kochen-Specker coordinate frame for spin-1 particles are free to pick any direction and any triple on their side of the exchange: the Strong Free Will Theorem declares that the freedom of choice is not <a function of properties of that part of the universe that is earlier than a response in this exchange with respect to any initial frame of reference> (Conway and Kochen 2009, p. 228). Notice the ontological import of the exchange process, since it is a spin-1 particle responding to the call, so that if an experimenter is free to experiment or to set up an experiment, the <objects> of the experiment, that is the particles experience an equal amount of freedom in such a way that the independence of both outcome and set-up parameters is preserved. Conway and Specker are clearly defending an objective realist interpretation of free will and if experimenters (human, robotic or otherwise) have a share of that freedom, it is imparted on them by Nature! This view is a far cry from Weyl's transcendental standpoint, but is in line with the assumed realism of the EPR experiment, the Bell theorem on non-contextual local hidden-variable theories or Bohm's version of *QM* and various no-go theorems in *QM*. The question of determinism is at the philosophical center here and of course it is not settled by the free will theorem, nevertheless there is an immediate profit to be gained by the foundational discussion and we can compare briefly the Conway-Kochen way with Weyl's views in the first section.

While Weyl puts the emphasis on the statistical worldview, Conway and Kochen insist that they do not need any notion of probability or stochastic process to establish their result. They argue for an overarching indeterminism that is grounded in the very nature of the quantum-mechanical world. Weyl's views in 1920 were expressed in the infancy of quantum physics and although he had a clear understanding of the distinction between causal and statistical theories, he did advocate the idea that decisions or free will choices are ≪autonomous and causally absolutely independent of each other≫ and that they are the real ingredients of the world in an everlasting process of becoming. This is, in my opinion, in complete agreement with the Conway-Kochen ontological posture, but once again one should not ignore that there is a deep philosophical divide between the two positions. Let me emphasize the rôle that quantum logic has played in the evolution of ideas in that context. Hermann Weyl was among the first to advocate the concept of a quantum logic that is at the heart of the contemporary debate. Gleason's theorem on the measure of closed subspaces of a Hilbert space and Kochen-Specker theorem on the non-embeddability of the partial Boolean algebra of observables in a commutative Boolean algebra can be seen as the final blows on non-contextual hidden-variable theories;

those results among others belong to quantum logic and non-standard logic including intuitionistic logic and maybe non-classical probability theory (see Nelson 1987a,b). Surely, Conway and Kochen are not reluctant to consider logical issues, but they seem to be more inclined to adopt a general philosophical perspective, maybe along Lucretius'poem *De rerum natura* in which the Roman philosopher and disciple of Epicurus defends the idea that man's free will is deducible from free will in nature through the <clinamen>, the deviation or declination of particles (or atoms for Lucretius) in the void of the universe or universes, since Lucretius proclaims a multiplicity of universes in an infinite world much in the spirit of multiverse theory.

5.15 A General No-Cloning Theorem in the Multiversal Cosmology

There is strong analogy between the Conway-Kochen theorem and the general no-cloning proposal: both have to do with the non-reproducibility of measurements and their outcomes in an indeterministic setting. But there is also a deep difference between the two for free will cannot be demonstrated mathematically, while the general no-cloning theorem has a rigorous mathematical proof based on set theory and algebraic topology. Let us begin with some preliminaries.

5.15.1 The No-Cloning Theorem in QM

The argument for the no-cloning theorem in *QM* goes back to the papers of Wootters and Zurek (1982) and Dieckx (1982). The fundamental idea is quite simple: a single quantum (or quantum state) cannot be cloned. Wooters and Zurek even question the very notion of quantum state (Wootters and Zurek 2009). One singles out an arbitrary state and shows that due to the time evolution operator and linearity and unitarity (bounded linearity) conditions, all states—for the single-out state is arbitrary—cannot be cloned in a copy-multiplier experiment. Quantum Mechanics is couched in an infinite-dimensional Hilbert in a second-order language whose cardinality is $2^{\aleph_0}$ in the set-theoretic idiom. Infinite-dimensional means $\aleph_0$ dimensions, that is the countable infinity of the set N of positive integers—$2^{\aleph_0}$ is uncountable and it corresponds to the set $\mathbb{R}$ of real numbers. There is no bijection between $\aleph_0$ and $2^{\aleph_0}$ which is also the power set of $\aleph_0$. It is in that context that Cantor formulated his Continuum Hypothesis as stated above in section 1. The first occurrence of the continuum Hypothesis appears in a 1878 paper <Contributions to the theory of multiplicities (manifolds)> (Cantor 1966, pp. 119–133) in which Cantor attempts to prove that all continuous manifolds are of the same denumerable dimension using the concept of the uncountable cardinality (*Mächtigkeit*) of the reals $2^{\aleph_0}$. In a subsequent paper <On a proposition in the theory of continuous manifolds> (Cantor 1966, pp. 134–138), Cantor gives a defective proof that all continua are of the same dimension, this time using the Riemannian notion of a multivalued function. One has to wait till Brouwer's papers in 1910 and the following years (Brouwer 1912a,b) to get the right concept: continua of different dimension might be isomorphic (have the same cardinality), but they cannot be homeomorphic. It is in his 1910 paper <Proof of the invariance of the dimension number> that Brouwer proves the following statement:

> An m-dimensional manifold cannot contain a one-to-one continuous function of a domain of a greater dimension number. (My translation of Brouwer 1910, p. 165)

The same is true for $l < m$ and this means that there is homeomorphism or a bicontinuous mapping between manifolds of different dimension. Brouwer uses various concepts like simplicial maps and the fixed-point theorem. In particular, Brouwer's fixed-point theorem was inspired by Kronecker's notion of the winding number <*Windungszahl*> or indicatrix. The fixed-point theorem states that a one-to-one continuous transformation of an n-dimensional element in itself posesses a fixed point; in contemporary idiom, the indicatrix is called an index or a topological degree for a continuous function to itself on the closed unit ball D^n such that it has at least one fixed point (see Gauthier 2009b). In the language of general (set-theoretic) topology, Brouwer's proof says simply that if U is an open subset of a Euclidean space R^n and we have an injective map $f : U \to R^n$, then the image of $f(U)$ is open and homeomorphic: R^n is not homeomorphic to R^m if $m \neq n$.

I use those notions to formulate a general theorem to the effect that there cannot be exact copies of elements (states, objects or persons) that could be clones or doppelgangers in an infinite multiverse. There are cosmologists like A. Vilenkin (see 2006 and 2010) and string theorists like B. Greene who would be inclined to think that there is an exact reproduction of states of affairs in an infinite universe of finite (or infinite) dimension. The following theorem shows that it cannot be the case (see Gauthier 2013b).

5.15.2 A No-Cloning Theorem in the Multiverse Cosmology

I state now the main argument as the following:
Theorem.

> In an n-dimensional infinite universe, there cannot be an exact reproduction or homomorphic images of items (finite or countably infinite) in any finite or countably infinite $\aleph_0$ subuniverse of the uncountable multiverse of the power of the continuum.

Proof. We take the notion of multiverse in its original sense of Everett's many-universe interpretation of QM—as the universal ramification of the wave function—but the notion excludes any finite renormalizable cosmological theory like herotetic string theory in 10, 11 or 26 dimensions even with at least 10^{500} universes attempting a unification of cosmology or General Relativity with Quantum Mechanics. The most general setting is set-theoretic combinatorial: an arbitrary subset X of a countably infinite set $\aleph_0$ is included in the power set of that set, that is

$$X \subseteq P(X)$$

and by the Cantor theorem on cardinalities

$$\forall X\ (\text{card}\, X < \text{card}\, P(X))$$

Recall that the power set 2^n, the set of all the subsets of a given set n, represents all the combinations C of the elements or members of the set, as in the binomial theorem used by Weyl (see above) in his probabilistic picture of a universe in a process of infinite becoming. There is no bijection between $\aleph_0$ and $P(\aleph_0)$ and *a fortiori* there in no continuous bijection between an arbitrary subset (subuniverse) and the multiverse or between of a finite member of a (countable) subuniverse and the (uncountably) superuniverse. Turning to the topological setting, we have topological spaces (manifolds) which are locally Euclidean R^n to refer to Cantor's original faulty argument; here we deal with homeomorphic images and since Brouwer's proof on the invariance of the dimension number works for open sets and the system of their neighbourhoods, the argument is straightforward: there is no homeomorphic image of an n-universe to an m-universe for $m \neq n$. We can still specify our argument to metric topological spaces, for example a Hilbert space which is also a Banach space where we have the open mapping theorem which sends open sets to open sets between Banach spaces. Moreover, the sequence of linear subspaces of a Banach space has a local open complement by the following argument:

Let B be an n-dimensional Banach space and let $F^{\perp}$ be the sequence of closed linear manifolds or subspaces $F^{\perp}$ of B . Set $F^{\perp} = F^{-}$, the closure of all $F^{\perp}$. The local complement F^{+} of F^{-} such that

$$F^{\perp} = F^{+} - F^{-}$$

is an open subset of B. If we take a locally convex space as the space B, the sequence G of open subsets g containing a neigbourhood of each of their points admits readily a local complement which is also open (by locality), since the metric complement

$$-A \equiv \{x : x \in X, \rho(x, A) > 0\}$$

of a located subset A, i.e.

$$\rho(x, A) \equiv \inf\{\rho(x, y) : y \in A\}$$

(if this distance from x to A exists $\forall x \in X$) is open, for we have

$$\rho(x, A) \leq \rho(x, y) + \rho(x, A) \quad (\forall y \in A)$$

(see Bishop 1967 for the notion of located subset). A still more special case can be obtained, if we restrict ourselves to a fixed point and a local homeomorphism, a fiber in the language of sheaves, defined by the restriction on a function $f : X \to Y$ for topological spaces X and Y with

$$f|X : X \to f(X)$$

and the inverse image $f^{-1}(y)$ for $y \in Y$. Here again we have an open set (and neighbourhoods) and it is only that in spaces of the same dimension that this obtains, since as Brouwer's theorem shows that for spaces of different dimensions $n \neq m$, there is no homeomorphic image (or open map) in the neighbourhood of an open set in a Banach space, even at infinitesimal distance $\square$.

Although Brouwer's fixed point theorem is notably non-constructive, there are constructive versions which are approximations or approximative of the fixed-point theorem. Our own version of Bishop's located subset provides with a local fixed point which accentuates the impossibility of a <proximate> cloning in a multidimensional universe. One should not forget in that context that the origin of the fixed-point theorem is to be found in Kronecker's notion of the winding number (*Windungszahl*) which he introduced in his 1869 work on functions of several variables. In algebraic topology, the winding number is called an index or a topological degree for a continuous function to itself on the closed unit ball D^n; the winding number is generated by a finite iteration of the progression principle (*Fortgangsprinzip*) for closed curves. The notion is central to (constructive) approximation theory as it deals essentially with approximating polynomials. Even though our result looks non-constructive at first sight since it is based on set-theoretic concepts, it is constructively justified insofar as it deals with infinite totalities that are subjected to a combinatorial procedure defined in the finite, that is the power set of a given finite set. The non-constructive burden rests on those who believe in the existence of infinite sets and the applicability of the power set to those transcendental powers... Of course, the result obtained above is independent of the continuum hypothesis which is nowadays believed to be false (by Woodin and alli). Our result depends only on the combinatorial content of the power set of any infinite set of cardinality $\aleph_0$.

The immediate effect of that result is that there cannot be any reduplication of an open map in manifolds of dimensions $n > 1$ and a particle cannot meet its exact double in the free world of the multiverse! In *QM*, the phenomenon of entanglement of states is invoked, but our result is equally valid for disentangled dual states—duality is not an internal mathematical property in Banach spaces, nor an intrinsic feature of the physical world. The ontological indiscernability principle of Leibnizian inspiration and reduced to the statistical principle of invariance permutation by van Fraassen in the quantum-mechanical context (see for example van Fraassen 1991, Chap. 11) is used to the same effect and is thereby included in the no-cloning theorem which could be termed the homeomorphic *indiscernability* principle, since it is a *domain invariance* theorem and not a simple state invariance condition. Our result also strengthens the no-cloning theorem in *QM* and imposes also limitations on approximate clonings as in the paper of Busek and Hillery (1996) in which they imagine copying states in the (undefined) neighbourhood of a given state or hyperinstances or *almost exact* copies in multidimensional cosmology. For supersymmetric theories, one should remember that homeomorphisms and diffeomorphisms reduce to automorphisms in spaces of the same dimension and should not expect superpartners at near range or in a nearby dimension. The no-cloning idea applies equally to the <transdimensional> cosmology suggested by Vilenkin and others in the measure problem of the multiverse, since the essential use of the notion of hypersurface refers to an m-dimensional manifold with an m-1 dimensional submanifold in differential topology. And again from the point of view of the combinatorial topology of knot theory, higher-dimensional knots become n-dimensional spheres emerging from an m-dimensional Euclidean space and thus losing their homeomorphic images as untied strings or loose loops…

From a geometrical point of view, this result is in accordance with Poincaré conjecture (solved by Perelman) on the homeomorphism between simply connected, closed 3-manifolds to the 3-sphere, since they are of the same dimension for all integers n; fixed points are present in the Riemann surface of the Thurston geometrization conjecture which inspired Perelman and such manifolds are also homotopy equivalent, but homeomorphy is not reducible to homotopy. Incidentally, it is the polynomial constitution of the moduli space—as objects in a Grothendieck scheme—of a Riemann surface that earned a Fields medal in 2014 to the Iranian Maryam Mirzhakani, the first woman ever to win the prize. Homotopy equivalence comes down to identity and indiscernability, which means that homotopy morphisms are coarser than homeomorphisms and they trespass dimensional frontiers, for homotopy equivalence becomes weaker in infinite dimensions! Here fibers from fiber bundles as surjections on the same space come into play, but fibrations as generalized fibers can go across borders and build a common path between different spaces or spaces of different dimensions. This is why the common path of homotopy theory becomes narrower in an infinite dimension. From a cosmological point of view, supersymmetry theories introduce superpartners of elementary particles like the selectron for the electron or the fotino for the photon which cannot replicate exactly the original particles for they would have to transfer their quantum numbers over dimensions with non-homeomorphic consequences… Indeed, in the abstract framework of anabelian geometry conjectured by Grothendieck and pursued by Mochizuki in his inter-universal geometry, the infinite multiverse has no commutative subsets, since all sit far and apart from an abelian nuclear group. But how could those specimens of a non-commutative species (Mochizuki's idiom) could reassemble in a set-theoretic superuniverse under the leading of an inaccessible cardinal, as Mochizuki suggests, is a very open question.

In any case, our general no-cloning theorem stated above supersedes other theorems on no-cloning. Take for example Lindblad's (1999) on the operator algebra of observables in the Hilbert space of *QM* or Barnum et alii result on the no-broadcasting of exact copies of mixed states from the information-theoretic viewpoint; those results are limited to the quantum-mechanical scene. Even the more ambitious (and most problematic) <constructor theory> of D. Deutsch et *alii* aiming at a unified theory of Quantum Mechanics and General Relativity cannot account for the most general no-cloning setting. In both cases, a superfluous objectivist ontology does not make place for the local observer, the real informant or the only <constructor>, the outsider in the observable scene (Lindblad 1999).

In the quantum-mechanical context, an infinite-dimensional (of cardinal $\aleph_0$ and ordinal ω) Hilbert space has $2^{\aleph_0}$ states inhabited by real numbers, all distinct between them. In the abstract category-theoretic framework of dagged categories—categories with an involution—one can reproduce the no-cloning result in compact spaces of the same dimension for finite-dimensional Hilbert spaces, but not for infinite-dimensional ones. And finally, in the most general combinatorial set-theoretic setting, the subsets of $\aleph_0$ form a totality $2^{\aleph_0}$ of distinct combinations. Let us remark that the general no-cloning or no-homeomorphism theorem applies equally to abstract theories of sets, types, classes, categories and topoi where are involved many universes or multiverses of higher transfinite dimensions; it is also valid for anabelian higher-dimensional algebraic varieties in the sense of Grothendieck or anabelian inter-universal geometry in the sense of Mochizuki! If we come down to finite dimensions, algebraic topology with Brouwer's result teaches us that there is no transdimensional identity (even with Poincaré recurrence in a finite volume). Here approximations accentuate distinctions and indiscernability comes down to unique identity, which means that there cannot be clones of exact status in any universe or multiverse of different dimension. The lesson that could be drawn here is maybe that if you have to live an eternal life (before and after forever), you will never (have been) be exactly the same self. This lesson should not however be considered as a plea for a theory of multiple reincarnation!

From the perspective of the local observer (Gauthier 1983a,b), the cosmological holographic principle (introduced by Gerhard 't Hooft among others) which reduces the dimensions of the multiverse to a two-dimensional surface is certainly compatible with our result, since everything happens *outside* the local observer and the physical universe appears as a homeomorphic image to the *same* local observer. That the two-dimensional image or information is a projection of a three-dimensional spatial structure or form forbids any homeomorphic transmission of information to the local observer who lives in a three-dimensional world, but the local observer *qua* observer is indifferent to dimensions, it is a zero-dimensional observer. Put differently, the local observer is a fixed-point observer in interaction with the observable universe. Otherwise, the highly speculative theory of eternal and infinite observers is not immune to serious foundational criticisms and even though string theory (superstring or M-theory in 11 dimensions) is a viable theory as a finitary renormalizable theory, it should be free of *doppelgängers* or ghost observers… The philosophical shortcomings of cosmologists and string theorists are no excuse when it comes to logico-mathematical foundations.

The general result is congenial to Weyl's views on the ever-becoming world and Brouwer's idea of the (mathematical) continuum as a process. In the classical Cantorian view, the continuum is made of uncountable *distinct* real numbers, while in the Brouwerian-Weylian view the continuum as an ever-becoming process is made of *indistinguishable* elementary processes. In both cases, as we have seen, there is no exact reproduction or copying of arbitrary individuals, may they be items of a countably infinite species, animal, human, robotic, alien or supernatural, entities, Lebnizian monads, Nietzschean <cyclists> in an infinite return or physical objects in general in an infinite-dimensional universe. It may seem that the modern cosmologists who speculate on infinite copies of the same make the error of thinking that there is only a finite number of combinations or subsets in an infinite set (universe). The French writer Auguste Blanqui believed so in his 1872 book *L'éternité par les astres* and concluded that there was an infinite number of duplicates of himself in an eternal and infinite universe. Blanqui was also a revolutionary and the fact that he was imprisoned at the time of his writing probably led him to imagine infinite possibilities under finite circumstances! But speculations of the kind are not rare though among thinkers and writers, from the Presocratic philosophers to Giordano Bruno, Fontenelle and Edgar Allan Poe and they are not all devoid of interest.

Our result is also compatible with the Conway-Kochen free will approach for even in the absence of time, particles have the choice of a countable infinity of directions and not just the 33 directions of the triple x, y, z experiment—of course an actual experiment requires time and is limited to a finite number of decisions, as Weyl puts it. Those decisions take $1/10$ of a second for human experimenters as Conway and Kochen admit (2006, p. 1142), but they also take place in Weyl's transcendental (*a priori*) time for observers. From an information-theoretic point of view, transmission of signals also takes time and there is a limit above, may it be the speed of light or more generally causal antecedence of the emission of a signal over its reception and this also can be accounted for in a non-realist constructivist way as the transcendental channel of intersubjective communication that can even be quantified—counting is an objective activity of a free agent…

As far as the philosophy of free will is concerned, our result means that the question is not of ontological import, as Conway and Kochen claim in their realistic posture, but is essentially of a constructivist nature, as Weyl describes (1963 and 1968) the theoretical or symbolic construction of the world in physico-mathematical terms.

5.16 Conclusion

The consistency problem for physical theories raised by Hilbert in his axiomatization programme has taken a new turn in recent years with the renormalization idea. Consistent theories in quantum field theories and the theories of critical phenomena must be renormalizable, that is they have to remove their infinities or their divergences in order to be granted a physical meaning as theories of finite measurable quantities. The two cases of Quantum Electrodynamics (QED) and Quantum Chromodynamics (QCD)—for the unified theory of the electroweak field—are exemplary. Here the consistency question could be termed <external> in the sense that the procedures of renormalization (and regularization) are applied to the mathematical or analytical apparatus of a physical theory and are meant to get rid of inconsistencies and anomalies (infinite divergences). In this way, F. Dyson a pioneer in the renormalization programme made the distinction between an ideal observer capable of infinite precision and the real observer limited to finite measurements. Others, like J. Schwinger separate the dynamical variables at the mathematical level of a theory from the observed particles at the physical level. Dirac and Feynman expressed serious doubts about the relevance of renormalization, but subsequent work by K.G. Wilson, M. Veltman and G. 't Hooft among others have introduced new techniques for renormalization that proved successful (see Gauthier 2002, Chap. 6). But one should not hide the fact that the renormalization procedures are somewhat artificial as they consist in simply cutting off divergences or substract infinite quantities and make the theory fit for finite measurements while at the same time using infinitary mathematical tools like analytic continuation in the toolbox of classical mathematics (and physics)—for the Hamiltonian and the Lagrancian formalisms. This means that there is no overt constructive aim in the renormalization process, only a pragmatic goal and the <physical logic> or physical axiomatics that Hilbert had in view is not practicable to its full extent in physical theories. The <consistent histories> approach of Gellmann and Hartle does not fare better as far as <internal> consistency is concerned, since it does suppose an objective decoherence of superpositions of states, so as to make the theory consistent and the physical world coherent before the Schrödinger wave even reaches any measurement apparatus, as if quantum-mechanical (and cosmological) probable histories were predetermined or predestined by Nature or some other metaphysical entity. Theories renormalizable from the start, like string theory, might be more likely candidates for constructivization, since they are finitely generated from discrete objects and not from point-like particles. In any event, internal consistency as we have it in mathematical or logical theories is not yet available for physical theories and the external consistency of renormalization is only from the outside, not the inner consistency that Hilbert hoped for his metamathematical programme of finitist proof theory in the foundations of logic and arithmetic and by extension of the whole of mathematics.

On the proper pragmatic side of the consistency question, one should emphasize the interaction between the analytical apparatus and the experimental apparatus, if a coherent philosophy of physics is desired. Experimental physics depend upon theoretical physics to probe physical facts and achieve precision measurements. Technology itself, e.g. the laser apparatus, telescopes or laboratories like CERN, is aimed at confirming or infirming models of theories while the statistics of measurement are not always adequate—the Opera faster-than-light neutrino programme failed, but the Higgs apparently succeeded—till further test and testimony beyond the mass of 125 GeV. And black holes might not exist after all as witting white holes with no loss of information, at least without wormholes and other serpentine or stringy creatures—one might say in French that these are indeed $\ll$ *de troublants trous blancs* $\gg$! Conservation of information is the issue here and since entropy is a local phenomenon, an open universe, cyclic or bouncing or infinite in both or all directions would not suffer from any loss of information, which is just an other form for energy, energy being itself in any kinematical or thermodynamical form in action—for those notions, see Gauthier (2009a). The postulated gravitational waves have been *dusted* by a Planck experiment in recent observations, but they do not confirm a definite cosmological model, may it be inflation (eternal or not), a multiverse scenario in principle unobservable or a string theory alternative with as many possible models as a consistent finitely renormalizable theory permits. The most precise measurements of our own inflationary universe seem to indicate that the observable cosmos is very flat (not fat!) with a corresponding Euclidean model and our best experimental theory, quantum electrodynamics (QED), requires fifteen decimals for the tuning of the fine structure constant of the electron.

What this means is also that discoveries are not haphazardly or by happenstance, experimental physicists find what they are looking for being guided by theories and their models, but they rarely find it, statistically speaking. And statistics themselves have to be as refined as the observation apparatuses are fine-tuned to precision measurements, in the lab or in the outer world (within five sigma, that is 99.9999 % in terms of the standard deviation). There again, a physical phenomenon, may it be a quantum-mechanical one or a relativistic (special or general) is subjected to the interaction between the observed (small or large scaled) and the observer, who is always local. That interaction can be subsumed under a quadratic polynomial in the internal logic which assigns a rôle and a locus or a place to the local observer of the observable world in the binomial combination observed-observer.

But how far can one (the local observer) see beyond the event horizon of a black hole or the Big Bang as a singular black hole? Only the theoretical eye can fathom the outer worlds and it is on the ultimate fluctuating vacuum field, the physical counterpart of the chaotic tohu-wa-bohu of the Bible or the Tiamat of the Babylonians, that the universal or multiversal observer comes to rest in the search of a global vision, a unified theory of everything. In this quest, physics takes the place of ancient religions and obsolete metaphysics in order to make sense of it all in the terms of science. That does not mean however that the field of vision is devoid of any unphysical impurity and that speculative research can totally obviate fictional dreams and inconsistent views. There is always the sanction of empirical verification, but it is not possible in all interesting cases, e.g. string theory still awaiting to go beyond the Higgs field and see the larger multidimensional picture of a supersymmetric universe. Here again the horizon is receding and any original account or final story of the origin and the end is an unending tale that will remain to be told.

5.17 Appendix to Chapter 5

5.17.1 Principles for a Theory of Measurement in QM

1. Principle of denumerability (or distinguishability) for results; measurement results must be distinguishable from one another (finitely or at most with the limit cardinality $\aleph_0$).
2. Quantum states could be indistinguishable in the wave function ψ which represents the probability density as a continuum (of cardinality $2^{\aleph_0}$)—here the experimental setting or apparatus is needed to obtain a finite measurement result.
3. A measurement result must be realized in order to count as a measurement (in a successful experiment in an experimental setting).
4. An ideal measurement result is not a *real* result and although it could be integrated to a thought experiment, it must also be denumerable or distinguishable.
5. There is no bijection between $\aleph_0$ and $2^{\aleph_0}$.
6. The combinatorial theory of measurements forbids any simultaneous measurement giving for an $\aleph_0$ universe $2^{\aleph_0}$ measurement results which would be indistinguishable, in other words, all possible states of the system would be realized at the same time or simultaneously, the system would be in all its states <*simul*> and this would make impossible any single measurement with discrete values of a given state of the system.

Those principles are the foundations of a measurement theory for QM and they allow for a probability theory *à la* Kolmogorov compatible with a QM where Schrödinger's wave function describes the time evolution of a quantum system and where Heisenberg's indeterminacy relations define the parameters of a denumerable probability theory in agreement with the constructivist theory stipulating that a quantum phenomenon is an interactive process between an observed system and an observer (observing system or apparatus). There follows Bohr's complementarity thesis between the causal and the spatiotemporal descriptions for QM. The internal logic of QM calls here for a pseudo-boolean logic where the observer occupies the position of a relative or local complement in a measurement experiment as expressed in the following formula:

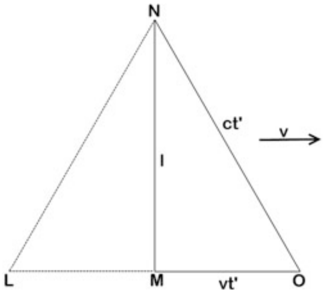
$$a \to b = In((X - a) \cup b)$$

which can be transformed into a modular polynomial expression as I show in Chap. 7.

Admittedly, no-go theorems for hidden variable theories in QM like Gleason, Bell, Kochen-Specker and Conway-Kochen theorems designed for ideal measurements (in the analytical apparatus) are valid in the theoretical framework and the recent work of Meyer, Kent and others on the finite precision loophole in quantum information theory do not invalidate them. The finite precision requirement is still a theoretical constraint and does not apply to concrete measurements, since real measurements by a local observer are always finite and precision is realized through finite approximations closing effectively any measurement loophole *numerically*. Again, the internal physical logic points to an arithmetical foundation not only of the analytical apparatus, but also of the experimental apparatus in the *same measure*.

Along those lines, the recent attempt by Couder, Fort and others to draw a hydrodynamic picture of the quantum-mechanical world has resulted only in a surface analogy (or a toy model) of the de Broglie-Bohm pilot wave deterministic interpretation of orthodox QM; the de Broglie-Bohm theory is not naturally Lorentz invariant and it doesn't modify the standard statisticical measurement theory of an essentially stochastic quantum regime, it only superposes a macroscopic analogue of a supposedly causal (deterministic) substratum or subquantum world. We know that work on hydrodynamics in the 18th century gave rise to partial differential equations and subsequently to Navier-Stokes equations for fluid dynamics on the model of classical mechanics. Apparently, this is the physico-mathematical background of Couder's enterprise. Couder's water or oil drop experiments with an artificial *zitterbewegung* seem to point to a nonlocal hidden-variable theory overriding relativistic constraints of parameter independence or outcome independence or both for spatially separated and correlated systems in line with Bell's theorem and the Einstein-Podolsky-Rosen thought experiment in the reformulation of Bohm, as discussed above. More importantly though, any hidden-variable theory faces the bijection problem $\aleph_0 \nLeftrightarrow 2^{\aleph_0}$ for quantum states and their measurement, a paradox that affects Everett's multiverse interpretation as well as any hidden-variable theory in QM, relativistic as non-relativistic alike.

It is clear that the macroscopic picture cannot recapture the quantum-mechanical behaviour beyond the classical limit or below the quantum limit. Here in the unobservable (meta of infra-physical) underworld, there is no place for observers, nor for measurement. Indeed, all this is a far cry from the analytical apparatus of QM with its usual Hilbert space formalism (with possible substitutes like the C^* von Neumann algebras or Connes' non commutative analysis or even string and M-brane theory), but that does not mean that graphical analogies or pictorial analogues cannot be useful, for example as aids in thought experiments, for instance the classical <*Gedankenexperimente*> from Zeno to Galileo, Newton, Einstein and Schrödinger among many others. I give here a simple illustration of my own for the derivation of the main formulas of Special Relativity with the Pythagorean theorem as the sole tool from the analytical apparatus and the two postulates of SR, Galilean relativity or inertia principle and the constancy of the velocity of light c in a vacuum. We have the following image of a sailboat, the sailboat of time as I would like to call it :



The sailboat moves with velocity v and l is the length or height of the (stationary) mast *MN*. A light signal is sent from a source L to N when the boat is at rest and is sent down to O with ct' the distance traveled by the light signal when the boat is traveling the distance vt' between the points M and O. We take ct' as the hypothenuse of this square rectangle and we get the following derivation from the Pythagorean theorem : $c^2 = a^2 + b^2$ with sides a and b and hypotenuse c.

Derivation of $\sqrt{1 - v^2/c^2}$ or $(1 - v^2/c^2)^{1/2}$

0. $ct'^2 = l^2 + vt'^2$
1. $l = \sqrt{ct'^2 - vt'^2}$
2. $t = \sqrt{ct'^2 - vt'^2/c^2} = t'\sqrt{c^2 - v^2/c^2}$
3. $t'\sqrt{1 - v^2/c^2}$
4. $t' = t/\sqrt{1 - v^2/c^2}$ □

Consequences : Lorentz-Fitzgerald

1. $t' = t/\sqrt{1 - v^2/c^2} \leq 1$ for time dilation.
2. $l' = l/\sqrt{1 - v^2/c^2} \geq 1$ for length contraction.

The sailboat of time seems to be a reflection of the relativity of simultaneity as it drifts silently on a uniform sea under a starlight signal flowing down from the canopy of heaven! This seems to be a nice thought experiment compared to Einstein's horseback riding a light beam as he imagined himself in his 1905 paper on the electrodynamics of moving bodies. In both cases though, the sailer and the rider, there is an observer aboard! The final outcome is that Relativity Theory (Special and General) and Quantum Mechanics are observer dependent and cannot do without the measurement of an observable universe. There is no doubt that beyond the observable universe, measurement takes on a new meaning and inevitably cosmological hypotheses (eternal inflation, ekpyrotic or cyclic universes, homogeneous or heterogeneous multiverses) or unified theories of General Relativity and Quantum Gravity border on metaphysical speculations and some hypothetical anthropic principle must sometimes come to the rescue to save the phenomena in a soft atonement like fine tuning; the detour is needed for the task of measuring the apparently immeasurable, if only by indirect means like the CMB (Cosmic Background Radiation) or other tracking devices that can only register traces of the unobservable. The frontiers of the observable are those that are traced above and below by the grand unified theories (GUTs) that hope to link gravitation (General Relativity or alternative theories like loop quantum gravity) with the electromagnetic, weak and strong fields (Quantum Mechanics). For cosmology, the limit is the standard model of the Big Bang with or without inflation beyond the singularity, for particle physics, the frontier is below the Higgs bosons at 125 GeV/c^2. In both cases, new physics looms large on the observable horizon (and far beyond) to absorb dark matter or energy, supersymmetric partners or exotic particles even parallel universes to supplement or complement the local observable landscape. In the no man's land of the unobservable, string theory seems to be the proximate probe to explore the *terra incognita*. Strings, superstrings or M-branes need to have "all strings attached" to cope with the physical continuum which can be considered as a combinatorial superstructure of discrete units (finite strings with the minimal length l_s of 10^{-34} m) that need to be stuck together in accordance with our view of an evolving, chaotic universe described earlier. In that sense, the physical continuum is not different from the mathematical continuum, if as H. Weyl envisioned, even the mathematical continuum is nowhere and never a completed totality from a constructivist viewpoint. The continuum is filling up all the time, since it is a combinatorial process in motion or a process in becoming <*ein Prozess im Werden*>, as Brouwer would have it. The local observer still remains unique in his capacity to combine cosmos and chaos in the finite polynomial equations that puts him ahead of the broken order of a hidden and fearful symmetry (or supersymmetry!), knowing that his own location *qua* observer is at the center of the observable universe or of any universe. As a local gauge, if one may say, the (theoretical) observer is absolutely stable in a thermodynamical instable or metastable universe insofar as any quantum field, including any hypothetical field beyond the Higgs field of the Standard Model, must preserve symmetry above or below any spontaneous symmetry breaking for the sake of a consistent model of the persistence of the universe(s). The local observer literally sees worlds revolving around him as if they were immersed in the sphere containing all things, as the Ancients thought.

Physical logic or the logic of physics, from quantum logic to cosmological logic or cosmologic as a true universal logic, that is the logic of the cosmos, the universe or the multiverse also rests on the firm ground of arithmetical logic to the extent that the fixed-point observer is the one who measures all things, as Pythagoras proclaimed, and is at the center of it all.

Chapter 6
The Internal Logic of Constructive Mathematics

6.1 Transcendental Versus Elementary: The Gel'fond-Schneider Theorem

Mathematical constructivism could be summarized by the phrase: "Arithmetical statements proven by analytical means can be proven without them, that is by elementary non-analytical means". Herbrand expressed the idea clearly in the 1920s. It was repeated recently by H. Friedman, following Avigad (2003). The classical example in this connection is Dirichlet who proved in 1837 the prime number theorem and the theorem on arithmetical progressions by analytical means; the elementary proofs were provided only in 1949 by Selberg and Erdös. A less known example is the 1933 Gel'fond-Schneider theorem for which Gel'fond gave a constructive version in the 1960s. I give here a brief account of the theorem and its foundational implications.

6.2 Transcendental Number Theory

To illustrate the excluded middle principle of classical logic, Dummett (2000, p. 6) cites the well-known example of a theorem in classical logic which gives a rational solution to two irrational numbers x^y:

> There are solutions of $x^y = z$ with x and y irrational and z rational. Take $\sqrt{2}^{\sqrt{2}}$ as either rational or irrational:
>
> If $\sqrt{2}^{\sqrt{2}}$ is rational, take (as irrational) $x = \sqrt{2}$ and $y = \sqrt{2}$, so that $z = \sqrt{2}^{\sqrt{2}}$ which by hypothesis is rational.
>
> If on the other hand $\sqrt{2}^{\sqrt{2}}$ is irrational, put $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ so that $z = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2$, which is certainly rational.

Thus in either case a solution exists, but the excluded middle principle is unable to tell us what is the case. Intuitionistic logic requires that one of the disjuncts of a disjunction

Y. Gauthier, *Towards an Arithmetical Logic*, Studies in Universal Logic,
DOI 10.1007/978-3-319-22087-1_6

be proven or instantiated (as for the existential quantifier). Of course, we know now that $\sqrt{2}^{\sqrt{2}}$ is irrational and even transcendental, due to the Gel'fond-Schneider theorem: here an intuitionist logician like A.S. Troelstra (2003) (see his *Proof theory and Constructivism*) is content to say that there is a constructive proof and simply refers to the Gel'fond-Schneider theorem without further comment!

The Gel'fond-Schneider theorem (1934) 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 (1934a,b) puts the problem in the form:

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

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 (1934) 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 $f(x) = 0$.

Baker (1975) extended and generalized those results in transcendental number theory using auxiliary functions or polynomials—which he calls fundamental polynomials—linear forms and logarithms for approximations of algebraic numbers in order to establish algebraic independence by contradiction or *reductio ad absurdum*.

It is only in 1962 that Gel'fond produced an elementary (constructive) proof for real algebraic numbers ω, $a > 0$, b for e^{ω} with e the base of natural logarithms and a^b (see Gel'fond and Linnik 1965, Chap. 12). Gel'fond relates that he used only Rolle's theorem as an analytical tool—here a radical constructivist could mention that a constructive version of Rolle's theorem is to be found in Bishop (1967). Essentially, Rolle's theorem says 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 2002). Bishop has admitted (Bishop 1970) that his foundational project was closer to Kronecker's finitist programme than to Brouwer's intuitionism.

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 (1965, Chap. 12) states that « if $\omega \neq 0$ is an algebraic real, than 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 (Gel'fond and Linnik 1965, Chap. 10), Hasse's theorem on integral solutions for the equation :

$$y^2 \equiv x^3 + ax + b \; (mod \, p)$$

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

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

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 1941). 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 (analytic) 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 and Weil has repeatedly referred 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). In the same context, Weil stated his main conjectures on the Riemann hypothesis in finite fields in (Weil 1949) and states that the case for curves being settled, he was working on varieties of higher dimensions. Weil's conjectures were proven in full generality by P. Deligne in 1973 using also a form of descent, i.e. cohomological descent (see above, Chap. 4). Weil's work in this area has emphasized the deep analogy or rather the internal connection between finite number fields and (algebraic) function fields as extensions of finite degree of the field Q of rational numbers and also of the ring Z of integers. The main reason for this is certainly the finite character of the polynomial arena, as Kronecker had conceived it in his theory of forms or general arithmetic. And it is in that arena where divisor theory naturally applies that Fermat's descent comes to play.

Fermat's infinite or indefinite descent, as Fermat qualified it, is in fact a finite process. Weil describes infinite descent in the following :

> Infinite descent *à la* Fermat depends ordinarily upon no more than the following simple observation: if the product $\alpha\beta$ of two ordinary integers (resp. two integers in an algebraic number-field) is equal to an m-th power, and in the g.c.d. of α and β can take its values only in a given finite set of integers (resp. of ideals), then both α and β are m-th powers up to factors which take their values only in some assignable finite set. For ordinary integers this is obvious; it is so for algebraic number-fields provided one takes for granted the finiteness of the number of ideal-classes and Dirichlet's theorem about units. In the case of a quadratic number-field $\mathbb{Q}(\sqrt{N})$, this can be replaced by equivalent statements about binary quadratic forms of discriminant N. (see Weil 1984, pp. 335–336)

What interests us here in this modern terminology is the finiteness results and the character of *effectivity* that attaches to the proofs by infinite descent. In that context, Fermat's infinite descent is a generalized Euclidean algorithm or a division algorithm in finite number fields and in finite function fields. The original idea of Fermat's infinite or indefinite descent appears in his 1670 commentary on Diophantus:

> Eodem ratiocinio dabitur et minor istâ inventa per viam prioris, et semper in infinitum minores invenientur numeri in integris idem praestantes. Quod impossibile est quia, dato numero quovis integro, non possunt dari infiniti in integris illo minores (Fermat 1899).

I translate the last quotation as:

> By the same calculation it is supposed that a smaller number is found in a descending procedure and that one can always find numbers smaller than the preceding one *ad infinitum*, which is impossible, since for an arbitrary integer there cannot be found an infinity of smaller ones in integers.

Let us remark that the method of infinite descent can be applied to a variety of problems, starting with the proof of the irrationality of $\sqrt{2}$ or the impossibility of

$$x^4 + y^4 = z^2$$

for all $z > 0$ and $x, y \neq 0$. Infinite or indefinite descent is, in fact, finite; it does not transcend the finite and the *reductio ad absurdum* is innocuous here, since the ensuing double negation is finitary. The finiteness of the procedure is still more evident when it is applied to "positive" questions, as Fermat says. Take the theorem: ≪Any prime number which is greater than a multiple of 4 by one must be composed of two squares≫. If there was such a prime number greater than a multiple of 4 by one, but which would not be composed of squares, there would be a smaller one of the same nature and still smaller ones till one reaches 5, which is the smallest number having the said property. One must then conclude that the theorem is true. What we have here is simply a generalization of Euclid's division algorithm, but it has been used variedly from Fermat to contemporary arithmetic geometry as a proof-theoretical device of reduction (Legendre's term), Kronecker's elimination theory or decomposition of forms (homogeneous polynomials) in divisor theory and diverse descent techniques as in Grothendieck's programme. Of course, not all those techniques are effective, even in number theory, that is, they do not necessarily provide calculations with explicit bounds. In some cases, like in n-category theory (infinity or ω-categories), descent can be encapsulated as a fly down escape from the aether of higher-dimensional categories, the totality of which live in the Ω-universe of all ordinals—described by Cantor as an absolutely inconsistent plurality ≪*eine absolut inkonsistente Vielheitgg*. But even without the Ω totality of universes, categorical foundations still need an inaccessible cardinal of higher set theory, that is transfinite induction beyond ϵ_0, as V. Voevodsky admits in his univalent foundations for homotopy type theory (see Voevodsky 2010). The same is true for Martin-Löf intuitionistic (or so-called constructive) type theory with dependent or contextual types together with the program proof assistant Coq also needed in Voevodsky's categorical foundations. However, descent is still lurking in the background under the clothings of the axiom of foundation introduced by von Neumann for the cumulative rank structure of axiomatic set theory. Mochizuki (2012) is keen on keeping the axiom of foundation as a descent procedure in the set-theoretic foundations of his ambitious programme of inter-universal geometry for the putative proof of the so-called *ABC* conjecture in number theory.

I would qualify such foundational programmes as *descriptive*—like in descriptive set theory—as opposed to *reductive* foundational programmes, meaning that foundations should incorporate a critical evaluation and a justification for mathematical practice hopefully within mathematics itself with a minimal (constructivist) philosophy, not just a unifying language. Although descriptive theories may have a computational or algorithmic intent, as in Voevedsky's univalent foundations or in Mochizuki inter-universal geometry, the abstract or general framework in higher category theory or higher topos theory, which both need transfinite induction (and recursion), is not constructive or so feebly constructive that the computational output seems to be a by-product, rather than a natural outcome of the theory—the algorithmic results are most of the time grounded on polynomial arithmetic as a basis for higher (alien) structures or creatures! Note that the *ABC* conjecture mentioned above has been demonstrated for polynomials constructively, that is by elementary (non-analytic) means. In the theorem about polynomials, for coprime polynomials $A(t)$, $B(t)$, $C(t)$ with $A+B=C$, one uses simply the maximum of the degrees which is smaller or equal to the number n_0 of roots of ABC

$$max(deg\{A, B, C\} \leq n_0(ABC) - 1.$$

For coprime positive integers A, B, C and the product of distinct prime factors or radical of (ABC), the conjecture states that

$$rad(ABC) < C = A + B$$

and that there is only a finite number of such triples A, B, C.

This is a finiteness result and if it were to be proven conclusively for integers, many other finiteness results would follow constructively, for example Faltings' result for Mordell's conjecture on the finite number of rational points on an elliptic curve or Wiles' result for Fermat's last theorem. If this programme is going to succeed, instead of Mochizuki's inter-universal geometry, one could speak of universal arithmetic in the sense of Newton's *arithmetica universalis* or of general arithmetic in the sense of Kronecker's *allgemeine Arithmetik*!

Let us remark that there is connection between the *ABC* conjecture and Pythagorean triples like $a^2 + b^2 = c^2$ at the basis of the Pythagorean theorem which is the foundation of differential geometry—and physical geometry. We have thus a thorough arithmetization from pure mathematics to theoretical physics in a constructivist perspective.

6.3 The Internal Logic

The logical outcome of this can be stated in a few words : both disjuncts in number theory must have a number-theoretic content, while intuitionistic logic requires only that one of the disjuncts be instantiated in order that a disjunction may have a truth-value or rather a verification value—the same for the existential quantifier. What our example shows is that a constructivist logic must be dependent upon an external resource, a numerical content, in order to be effective in arithmetic. This means that the logic is derived and comes after or is posterior to what Hilbert called <*inhaltliches logische Schliessen*>, a terminology I have translated as <internal logic> (see Gauthier 2002 for details). Formal logic, in Hilbert's view, was an external metamathematical means <*äusseres Handeln*> to treat the internal logic of mathematical theories or the inferences pertaining to mathematics proper, not to the metamathematics or the proof theory of formal systems.

But if we follow Hilbert's lead, formal logic must depend upon mathematics' inner workings and Brouwer, who is not a Hilbertian by any means, would follow suit and concur by saying that the excluded middle principle is not admissible particularly in the mathematical analysis of infinite sequences or infinitely proceeding sequences (of natural numbers). Kolmogorov was well aware of the significance of intuitionistic logic which he interpreted as a logic of problems (and solutions) and he made a distinction between real mathematics and the classical mathematics of pseudo-truth (*pseudoistinosti*) where transfinite induction is operative. Problems, in Kolmogorov's mind, are essentially well-posed mathematical problems, since in the Hilbertian spirit, they must have a solution. We know that Brouwer was suspicious of logic and we could ask if intuitionistic logic, following Heyting and his successors, is faithful to Brouwer's original intent. I give only one example or counterexample in line with Brouwer's practice, the attempt to confound Gentzen's transfinite induction with Fermat's infinite descent ; the former is designed to provide a consistency proof for Peano arithmetic while, the latter is a constructive method of proof in classical number theory, from Fermat, Euler, Gauss, Lagrange, Legendre, Kummer, Kronecker to contemporary number theory and algebraic-arithmetic geometry in the hands of Mordell, Hermann Weyl, André Weil, Gert Faltings among others.

6.4 Descent or Descending Induction

Infinite descent in classical number theory from Fermat to Kronecker and Weil is not infinite descent in the set-theoretic setting of an infinite set of natural numbers. It is in fact a finite arithmetical procedure that has little to do with the transarithmetical process of transfinite induction.

As A. Baker explains in his major work on transcendental number theory (Baker 1975), Gel'fond's and Schneider's proofs proceed by construction of auxiliary functions and polynomials and they then derive their results by induction on an arbitrary (finite) large integer n by assuming that if the result holds for $n-1$, it holds for all n. In the same vein, J.-P. Serre defines descending induction as ≪acting on two (positive) integers m and N with $m > N$ descending to N ≫ (see Serre 2009). For integers or numerical predicates, the procedure looks like

$$Ax_n$$

$$Ax_{n-1}$$

$$\vdots$$

$$Ax_{n-(n-1)}$$

$$Ax_0 = Ax_{n-n}.$$

Ax_n is what Bourbaki has called a general term. While classical infinite descent works with the descending sequence of finite ordinals (natural numbers), designated as *weak* well-ordering by Kreisel, transfinite induction calls for the *strong* well-ordering of transfinite ordinals up to ϵ_0 of Cantor's second number class. This well-ordering has to deal with the subsets of $\mathbb{N}$. Here the logician must pick up a certain quantifier-free subset of the ordinal ω hierarchy, because he knows that the set of all countable ordinals of the ω's including the ϵ's is the uncountable ω_1 corresponding to the cardinal $\aleph_1$—Cantor suggested that the continuum c was $\aleph_1 = 2^{\aleph_0}$. The power set of the set of natural numbers is significant in that connexion, since the well-ordering principle says

$$\forall S \subseteq \mathbb{N}(S \neq 0 \wedge Ax(x \in S)) \rightarrow (\exists y < x \wedge y \in S),$$

that is, there exists a strictly decreasing sequence for all elements of the subsets of the set $\mathbb{N}$ of natural numbers. This is the *strong strict* well-ordering of $\mathbb{N}$ requiring the excluded middle on the power set of $P(\mathbb{N}) = 2^{\aleph_0}$! Transfinite induction runs along an initial segment of the ω-sequence *beyond* the first ω up to its limit ϵ_0, while infinite descent starts with an arbitrary integer *n below* the first ω. Here is one main cleavage between finitist and infinitist proof theory, but Gentzen wanted to believe that classical infinite descent was a disguised form of complete induction in order to justify transfinite induction over the denumerable ordinals (see Gentzen 1969) Following suit, Kreisel has simply noticed that it was a form of infinite descent that Gentzen had used (see Kreisel 1976).

Polynomials as the finite support of infinite power series are the natural extension of natural numbers and provide with a finitist alternative to set-theoretic Peano-Dedekind arithmetic. For polynomials of the form

$$P(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

in decreasing powers for integer coefficients a's and indeterminates x's, one works with their degrees (exponents or powers) and heights (the maximum of the absolute values of the coefficients) and the idea is to come down to irreducible polynomials, i.e. polynomials that cannot be factorized over the integers.

I have emphasized the finitist character of infinite descent and I want now to contrast it with the infinitist dimension of transfinite induction.

6.5 Induction Principles

Let us see the classical formulation of various induction principles

1. Peano's induction postulate (first order)

$$\text{(PIP)} \qquad \forall x Ax(A0 \rightarrow (\forall x Ax \rightarrow ASx)) \rightarrow \forall x Ax$$

—one replaces A by X (for subsets) to obtain Peano's second-order postulate.

2. Axiom of infinity in Z-F (correspond to second-order PIP)

$$\text{(IA)} \qquad \exists x(\emptyset \in x \wedge \forall y(y \in x \to y \cup \{y\} \in x))$$

—this is Peano's original formulation in Peano's *Opere scelte* (Peano 1959)

3. Complete induction

$$\text{(CI)} \qquad \forall x(\forall y(y \prec x)Ay \to Ax) \to \forall x Ax$$

4. Transfinite induction

$$\text{(TI)} \qquad \forall\sigma[(\forall\tau)(\tau \prec \sigma)A(\tau, x) \to A(\sigma, x)] \to \forall\sigma A(\sigma, x)\ ;$$

—for ordinals σ and τ

5. Least number principle

$$\text{(LNP)} \qquad \exists x Ay \to \exists y(Ay \wedge \forall z(z \prec y)\neg Az)$$

6. Set-theoritic infinite descent

$$\text{(STID)} \qquad \forall x(Ax \to \exists y(y \prec x)Ay) \to \forall x \neg Ax.$$

By successive transformations on classical equivalences (tautologies)

$$\forall x \neg Ax \vee \exists y Ay$$

and

$$(\neg\forall x \neg Ax \wedge \neg\exists y Ay) \vee \forall \neg Ax$$

and by

$$(\neg\forall x \neg Ax) \leftrightarrow \exists x Ax$$

I obtain

$$\forall x \neg Ax \vee \exists x Ax$$

i.e. the excluded middle.

This way 3, 4, 5 are equivalent from the classical point of view (by contraposition or indirect way), 5 and 6 are not from the intuitionistic point of view, since one would have

$$\forall x Ax \leftrightarrow \neg\exists x \neg Ax,$$

with the passage

$$\neg\exists x\neg Ax \rightarrow \forall x Ax$$

prohibited in intuitionism, although 3 and 6 are supposed to be equivalent since Peano's postulate (PIP) is admitted. Markov's rule allows only the passage

$$\text{(MR)} \qquad \neg\neg\exists A(x, y) \rightarrow \exists x A(x, y),$$

Kolmogorov had allowed the excluded third for finitary judgments and he had recognized that transfinite induction implied the axiom of choice (and excluded third) in the classical framework of *pseudoistinosti* (pseudo-truth). (Kolmogorov 1925, Gauthier 2002, pp. 666–667).

I conclude that intuitionistic logic should reject the identification of transfinite induction with Fermat's infinite descent, since it does involve a double negation of the denumerable (infinite) set ω of natural numbers or ordinals numbers ϵ_0.

6.6 Intuitionistic Logic and Transfinite Induction

In classical logic and mathematics, the least-number principle (LNP) is equivalent to transfinite induction on the infinite set of finite ordinals

$$\text{(LNP)} \qquad \exists x Bx \rightarrow \exists x(Bx \wedge \forall y < x \neg By)$$

Substitute $\neg Bx$ for Bx to obtains *bq* contraposition

$$\text{(TI)} \qquad \forall y[\forall x < yAx \rightarrow Ay] \rightarrow \forall x Ax.$$

From the intuitionistic view point, LNP replaces the excluded third for Heything arithmetic (see Troestra and van Dalen 1968).

Suppose that I have a predicate A much that :

$$Ax = \begin{cases} 0 \wedge P \\ 1 \wedge \neg P \\ n \end{cases}$$

I have $\exists x Ax$; if I had a smallest y much that Ay and $y = n$, then $\neg A0$, $\neg\ A1$ hence $\neg(0 = 0 \wedge P)$ and $(1 = 1 \wedge \neg P)$, which gives P et $\neg\neg P$ (contradiction). If $y = 0$, I have P and if $y = 1$, I have $\neg P$.

The intuitionist has a final recourse through Markov's principle

$$\neg\neg\exists A(x, y) \rightarrow \exists x A(x, y)$$

and he can assert with a double negation on the existential quantifier that

$$\neg\neg[\exists x A x \to \exists x(Ax \wedge \forall y < x \neg Ay)].$$

From a proof-theoretical viewpoint (here in a sequent calculus) one will suppose that the universal quantifier is isolated from the positive instances of the existential quantifier and from disjunction (Mints-Orevkov condition). Of course, intuitionistic logic requires that in a disjunction $(A \vee B)$, one of the member has a proven instance and the same is true for existential quantifier $\exists x A x$ that must exhibit an instance An.

One can then show that

$$\exists x A x \to \neg\neg\exists x(Ax \wedge Ay < x \neg Ay)$$

is equivalent to

$$\forall x[Ax \to \neg\neg\exists z(Az \wedge \forall y < z \neg Ay)],$$

but here one must use the transfinite induction principle which is supposedly equivalent to complete induction in Heyting's arithmetic. Complete induction is admitted by intuitionists for all constructive properties of natural numbers. But there is a gap, since it can be shown that the equivalence between CI and TI (and STID) rests on a double negation over an infinite set. It suffices to repeat the preceding exercise with the least-number principle

$$\text{(LNP)} \qquad \exists x A y \to \exists y(Ay \wedge \forall z(z \prec y)\neg Az).$$

I substitute $\neg Ay$ for Ay

$$\neg\exists y(Ay \wedge \forall z(z \prec y \to \neg Az))$$

and I obtain by transformation on classical equivalences and MP

$$\forall y(\neg Ay \wedge \forall z(z \prec y \to \neg Az))$$

and

$$\forall y(\forall z(z \prec y \to \neg Az)) \to Ay$$

and

$$\forall y \neg Ay$$

which is the consequent of the descent with

$$\text{(STID)} \qquad \forall y(Ay \to \exists z(z \prec x)Az) \to \forall y \neg Ay$$

obtained classically from the induction rule

$$(A0 \text{ and } \forall y Ay \to ASy)$$

and from Peano's induction postulate

$$\text{(PIP)} \qquad \forall x Ax(A0 \to (\forall x Ax \to ASx)) \to \forall x Ax$$

by MP.

The equivalence between LNP and STID is classically proven, but LNP is not deducible from TI in intuitionistic logic (because of the excluded third principle). Otherwise, TI is equivalent to CI and STID both classically and intuitionistically. There is a dilemma or rather a trilemma: either CI, TI and STID are not equivalent in intuitionistic logic or LNP cannot be derived from TI (or CI), nor from STID.

In order to contrast infinite descent with transfinite induction, let us introduce the version of Fermat's descent with the effinite quantifier ∓ for the unlimited sequences of natural numbers.

I. Positive descent.

$$\mp x\{([Ax \wedge \exists x(y \prec x)Ay] \to \exists y Az(z \prec y)Az) \to \exists z(z = 0 \vee 1 \vee n)Az\}\mp x Ax$$

II. Negative descent

$$\mp x\{[Ax \wedge \exists y(y \prec z)Ay] \to \exists y[z(z \prec y)Az]\} \to \mp x \neg Ax$$

Positive descent excludes clearly the excluded third by

$$Az = \begin{cases} 0 \\ 1 \\ n \end{cases} \qquad \text{for } 0 \text{ or } n = A_{x_n} \vee \ldots \vee A_{x_1} \vee A_{x_0}$$

As "finite" descent stops at 0, 1 or n. It is only in that context that a quadratic polynomials or a diophantine equation can have an infinite (unlimited or effinite) number of solutions. For negative problems, as Fermat says, double negation must come down to 0 or 1 with $1 \neq 0$. This is the very meaning of *reductio ad absurdum* which boils down to the reduction of a false premise to a contradictory conclusion in a finite number of steps, which is a proper proof procedure for finite sequences (sets) in constructive logic and mathematics.

Brouwer had clearly criticized the excluded middle principle in his 1923 paper on "*The meaning of the excluded middle principle in mathematics, especially in the theory of functions*" (Brouwer 1975). What Brouwer calls the reciprocity principle for the complementary species (set)

$$\forall x(\neg\neg Ax \to Ax)$$

or the global decidability principle for a predicate P

$$\forall x(Px \vee \neg Px)$$

is essentially from the "local" testability or decidability principle.

$$\neg A \vee \neg\neg A$$

for a constructible element $x_0 = x$ or a sequence of such elements. The said principle, Brouwer insists, does not apply indifferently to finite and infinite species—species or collections of properties in Brouwer's intuitionism.

In his programme for the revision of classical analysis, Brouwer introduced intuitionistic principles for the well-ordering of choice sequences, this is sequences of choice of values in the well-ordered sequence of natural numbers. The bar theorem, the fan theorem, and the uniform continuity theorem on the compact interval [0, 1] are such principles. The bar theorem stipulates that "if a property is true for any sequence a (inhabited by initial value) and is true for initial segment of values for a and if it is true for the concatenation $a^* < n >$ for all n, then it is true for all sequences in S (the universal spread, Dutch "*spreiding*")—for these notions see Gauthier (1976, Chap. 2) and Gauthier (1997a,b, Chap. 5). There is a close or "barred" induction relationship between the bar theorem and Peano's induction postulate and S.C. Kleene has shown (Kleene and Vesley 1965) that the general principle of barred induction implied the excluded third and there was the need to restrict the induction to local decidability for sequences in order to constructively validate the bar theorem. Kleene's results and others are duly reported in Dummett's *Elements of Intuitionnism* (Dummett 2000). See also Troelstra (1969) and Troelstra (1976) for the intuitionistic theoy of choice sequences.

Choice sequences are generated by successive choice of values that are stratified by continuous operations or functionals on a reticular set of anterior choices to give rise the to spread of choice sequences. A first valid principle for choice sequences is intensional continuity stated as

$$X\alpha \rightarrow \exists\Gamma(\exists\beta(\alpha = \Gamma\beta) \wedge \forall\beta X(\Gamma\beta))$$

i.e. if a choice sequence possesses an extensional predicate or belongs to a given species (set of properties), it is always possible to find a continuous functional on another choice sequence which corresponds to the first choice sequence, since it possesses the same extensional predicate or belongs to the same species having the same initial segment of values. One can also define an extensional continuity (Brouwer's principle for numbers)

$$\forall\alpha\exists x X(\alpha, x) \rightarrow \exists X\forall x\forall y\forall\beta(\bar{\alpha}x = \bar{\beta}x \rightarrow X(\beta, y))$$

meaning that if we have for an arbitrary choice sequence a procedure which can determine a natural number x, then for all other choice sequences having the same initial segments, we can have the same procedure for a natural number y; in other terms, the existence a given numerical value for a choice sequence implies that there is a continuous lawlike functional acting on that choice sequence.

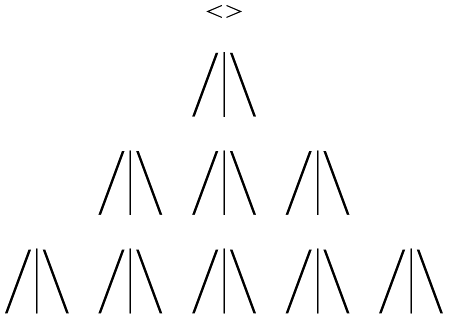
An important consequence of the principles is the fan theorem for spreads. The notion of spread is defined by two laws, a spread law represented by a lawlike function a with the following rules:

1) $a0 \neq 0$
2) $\forall n \forall m (a(n * m) \neq 0 \rightarrow an \neq 0)$
3) $\forall n \exists x (an \neq 0 \rightarrow a(n* \prec x \succ \neq 0))$

a fourth finiteness rule

4) $\forall \; n \exists z \forall \; x(a(n* \prec x \succ \neq 0) \rightarrow x \leq z \,)$

defines a finitary spread law of fan. Here $*$ denotes again the concatenation $< x >$, a sequence containing one element. A fan law can be represented by a tree with the top being the empty sequence.



The other law defining a spread is a complementary map ξ of a spread law which associates positive natural numbers to the members of a given species. A given spread is either dressed or naked, according to the map ξ being in a species or not and a sequence is a member of a spread if it immediately follows in the spread (tree).

$$\forall \alpha \exists x X(T_\alpha \alpha, x, \alpha_0, \ldots) \rightarrow \exists y \forall \alpha \forall \beta (\Gamma_\alpha \alpha y = \Gamma_\beta \beta y \rightarrow X(\Gamma_\alpha \beta, x, \alpha, \ldots)).$$

The fan theorem is in essence a finiteness theorem for choice sequences: in words if to each element x of a fan α is associated a natural number x, a natural number y can be specified in such a way that x be determined by the y first choices which generate a by the fan law α. König's classical lemma is the contrapositive of the fan theorem for a detachable species, i.e.

$$\forall x \in X(x \in Y \vee x \notin Y)$$

for species X and Y. König's lemma says that any infinite tree with finite branching displays a infinite branch (the trunk!) and requires the excluded third and the axiom of choice of classical logic. It is therefore necessary to have a weaker form of the fan theorem to make it constructively acceptable.

The fan theorem has been used by Brouwer in his proof of an important theorem in intuitionistic analysis: "Any real-valued functions defined on the compact interval $[0, 1]$ is uniformly continuous." Intuitively, one can see that ay real-valued $\phi(x)$ defined iteratively everywhere on the real line must also be so by the n first choices of values for $\phi(x)$ in such a way that the difference between two functions $\phi(p)$ and $\phi(q)$ for two points p and q is always smaller than a rational number 2^{-n}, whence uniform continuity—note the contrast with the classical $\epsilon - \delta$ formulation.

Let us finally remark that the induction principles on ordinals (the well-orders) have the same meaning in classical and intuitionistic logic, except that one supposes species to be decidable, that is for a strictly descending arbitrary sequence (or subsequence) F, one has $x_0 \notin F$ or $x_0 \in F$ (see Troestra 1969). To the set-theoretic notion of well-order on the subsets of N corresponds the intuitionistic notion of well-founded tree for which there is no strictly decreeing (descending) sequence—a statement perfectly similar to the axiom of foundation in Z-F set-theory. In both cases, if we want to pass to Fermat's infinite or indefinite descent, we have to use the double negation bridge on the denumerable infinite set of natural numbers N, while finite descent, the true meaning of Fermat's descent, is exclusive of the excluded third by

$$\neg(\neg FD) \leftrightarrow FD$$

in a polynomial calculus for constructive logic and mathematics.

6.7 Transfinite Induction

The transfinite induction principle says:

$$\forall\sigma[(\forall\tau)(\tau \prec \sigma)A(\tau, x) \rightarrow A(\sigma, x)] \rightarrow \forall\sigma A(\sigma, x)$$

for σ and τ as ordinals in the ϵ_0 segment of Cantor's second number class defined by

$$\lim_{n \to \omega} \left.\omega^{\omega^{\cdot^{\cdot^{\cdot^{\omega}}}}}\right\}^{n} = \epsilon_0$$

where epsilon naught is the limit ordinal of the omega hierarchy with n tending to ω, the limit of finite natural numbers n. Infinite descent in set-theoretic terms with a universal quantifier on natural numbers boils down to

$$\forall x(Ax \rightarrow \exists y(y \prec x)Ay) \rightarrow \forall x \neg Ax.$$

By successive transformations (classical equivalences and tautologies), I get

$$\forall x \neg Ax \vee \exists y Ay$$

and

$$(\neg\forall x\neg Ax \wedge \neg\exists yAy) \vee \forall x\neg Ax$$

and by

$$(\neg\forall x\neg Ax) \leftrightarrow \exists xAx$$

I get

$$\forall x\neg Ax \vee \exists xAx$$

which is the excluded middle. What we end up with is a derivation of the excluded middle obtained from a double negation operation on the infinite set of natural numbers. This is equivalent to the double negation elimination rule, not admissible in intuitionistic logic where the excluded middle principle is prohibited in general and specifically in non-finite situations. Kolmogorov thought that the principles of excluded middle and double negation were involved in some forms of transfinite induction (Kolmogorov 1925, 666–667). The fact that intuitionists after Heyting (see Troelstra and Dalen 1988) accept complete induction on the infinite set of natural numbers

$$\forall x(\forall y(y \prec x)Ay \rightarrow Ax) \rightarrow \forall xAx$$

leads them naturally to accept transfinite induction, which is just complete induction on ordinals up to ϵ_0. A similar exercise can be made with the smallest number principle (equivalent to infinite descent as classically interpreted, but not intuitionistically valid)

$$\exists yAy \rightarrow \exists y(Ay \wedge \forall z(z \prec y)\neg Az)$$

By substituting $\neg Ay$ to Ay, we have

$$\neg\exists y(Ay \wedge \forall z(z \prec y \rightarrow \neg Az))$$

and I obtain by classical equivalences and MP (*Modus Ponens*)

$$\forall y(\neg Ay \wedge \forall z(z \prec y \rightarrow \neg Az))$$

and

$$\forall y(\forall z(z \prec y \rightarrow \neg Az)) \rightarrow Ay$$

and

$$\forall y\neg Ay$$

which is the consequent of infinite descent derived from Peano's induction postulate

$$\forall yAy(A0 \to (\forall yAy \to ASy)) \to \forall yAy$$

and the induction rule

$$A0 \text{ and } \forall yAy \to ASy$$

by MP. □

6.8 Conclusion: A Finitist Logic for Constructive Mathematics

A simple idea for the internal logic of finite arithmetic is that such a logic should be arithmetical, that is, it should represent or translate the logic of arithmetic in arithmetical terms. The idea is to interpret logical operators, expressions and formulas in arithmetic and that arithmetic is polynomial arithmetic. Logic can be embedded in polynomial arithmetic, since it is a larger arena than integral arithmetic with all the arithmetic operations and it constitutes a field, in particular a finite field where infinite (indefinite or finite descent) can be freely enacted. The main advantage of the polynomial translation is that it is not simply an assignment of integers to logical expressions (like Gödel numbers), but a direct interpretation of logic in a purely arithmetical syntax. Such a direct translation would look like the following:

$$\begin{array}{ll}
a \wedge b & := a \cdot b \\
a \vee b & := a + b \\
\neg a & := \bar{a} \text{ for } 1 - a \\
a \to b & := \bar{a} + b \\
\exists x & := \Sigma(a_1, a_2, a_3, \ldots, a_n) \\
\forall x & := \Pi(a_1, a_2, a_3, \ldots, a_n) \\
\mp x & := \Pi(a_1, a_2, a_3, \ldots, a_n, \ldots)
\end{array}$$

Remarks: The new quantifier $\mp$ is meant to express quantification over the unlimited sequence of natural numbers or Brouwer's infinitely proceeding sequences beyond the finite sets subjected to the classical quantifiers. A way to formalize infinite descent in Fermat-Kronecker arithmetic would be to use the unlimited or «effinite quantifier » in the following formulation:

$$\mp x\{([Ax \wedge \exists y(y < x)Ay] \to \exists y \mp z(z < y)Az\} \to \mp x \neg Ax$$

which is the «negative » version of infinite descent. This means unlimited or indefinite quantification on an arbitrary sequence (not an infinite set) of natural numbers. The positive formulation looks like this :

$$\mp x\{([Ax \wedge \exists y(y < x)Ay] \to \exists y \forall z(z < y)Az\} \to \exists z(z = 0 \vee 1 \vee n)Az\} \to \mp xAx$$

and it means that a descent could stop at 0 or 1 or any positive integer (like 5) in order to give way to an unlimited number of solutions for diophantine equations, for example. This quantification is not bounded quantification, nor quantification in predicative arithmetic *à la* Nelson, it just reveals a formal contrast to Peano's induction postulate or complete induction on the (completed) infinite set of natural numbers.

The numerical expression "1" refers to the unlimited arithmetical universe. The arithmetical expression $\bar{a}$ for $1 - a$ stands for a *local* negation in stead of the set-theoretic topological relative complement. Such a logic could be called a modular polynomial logic if we add a *Modus Ponens* in the form of

$$1 - a_0x \equiv b_0x \ (mod \ a_0x)$$

where a_0x and b_0x are monomials (see Gauthier 2010 for details) and from the point of view of Gentzen's sequent calculus, the cut rule equivalent to *MP* is innocuous, since it is *modular*, that is, taken into account and then discarded in a pure (cut-free) equational calculus. Such a calculus is a calculus of polynomial content and could be considered as an internal logic for Kronecker's theory of forms in his general arithmetic (see Chap. 7 for a detailed construction of the calculus).

The arithmetical logic I have sketched should be finitely decidable—the theory of finite fields is decidable. Of course, the arithmetic in question is not Peano arithmetic (or Dedekind-Peano) with its induction postulate on the denumerable set of natural numbers, but rather Fermat-Kronecker arithmetic with infinite descent substituting for infinite induction and acting on forms, that is the homogeneous polynomials with integer coefficients and indeterminates of Kronecker's general arithmetic (*allgemeine Arithmetik*).

After the arithmetization of analysis by Cauchy and Weierstrass—one can include also Dedekind and Cantor—and the arithmetization of algebra by Kronecker, my contention is that Hilbert has inaugurated the arithmetization of logic pursued in the work of Skolem, Gentzen and Gödel and particularly active in contemporary theoretical computer science after Turing.

As far as number theory is concerned, the Gel'fond-Schneider theorem is a revealing instance of constructive (see Gauthier 1978) proofs. Liouville's and Lindemann's proofs on the existence of transcendental numbers were not constructive, Dirichlet's analytical proof on the infinity of prime numbers in arithmetic progressions had to wait for the 1949 Selberg's constructive proof. The French logician and number-theorist Jacques Herbrand, a follower of Hilbert (see Coquand 2008), even formulated a general hypothesis to the effect that theorems in non-analytic (elementary) number theory must have a non-analytic, i.e. constructive proof (Herbrand 1968). It is an intrinsic feature of transcendental number theory that the existence of transcendental numbers is only negatively or indirectly demonstrated by *reductio ad absurdum*, but direct elementary proofs provide more information on the content of a theorem in the case of constructive mathematics and more so in finitist foundations. The emphasis is on what Hilbert called «*Sicherheit*» and «*Sicherung*», certainty or certification of the tools and means of the mathematician or the logician who wants to count on more information in order to rely on the concrete proof procedures at work in constructive mathematics and in its internal logic.

Chapter 7
The Internal Consistency of Arithmetic with Infinite Descent: A Syntactical Proof

7.1 Preamble

The question of the consistency or non-contradiction of arithmetic is a philosophical question, that is the certainty of a mathematical theory and it has become a logical problem requiring a mathematical solution. It is Hilbert who has put the original question and who has attempted a first answer. Having demonstrated in 1899 the consistency of elementary geometry on the basis of a consistent arithmetic of real numbers, he turned to the question of that arithmetic (the second problem of his 1900 list) which included besides the axiom of elementary arithmetic an axiom of continuity, i.e. the Archimedean axiom with syntactic completeness. Hilbert introduces functionals, that is second-order functions or functions of functions, in order the use induction over the ordinals. Transfinite induction proved successful in the hands of Gentzen, and thereafter Gödel's second incompleteness results which aimed to show that Peano's arithmetic cannot contain its own consistency. Skolem had already indicated in 1923 that a finitary consistency proof could be attained only by finite processes, as Skolem says following Kronecker.

Gödel himself has not relinquished the problem of the consistency of arithmetic and in his 1958 *Dialectica* paper, he came back to Hilbert's functionals using complete induction on finite types rather than transfinite induction over the ordinals. The extension of the finitist point of view meant only that one has to transcend the formal system of finite arithmetic in order to encompass all finite types, that is the totality of natural numbers. Gödel will seek relentlessly philosophical (foundational) justifications for the functional interpretation, as he admits (see Gödel 1990, vol. II, p. 305), but Gödel will insist repeatedly that Hilbert programme is not doomed, it is the finitist stand that has to be extended or enlarged (*erweitert*). My proposed consistency proof is grounded in

A first version of the proof was published in *Modern Logic*, VIII (1/2), 47–87 (2000) and contained some extraneous semantical and set-theoretical elements which have been removed here. See also Chapter 4 of my book *Internal Logic. Foundations of Mathematics from Kronecker to Hilbert*, Kluwer, Dordecht, 2002.

Y. Gauthier, *Towards an Arithmetical Logic*, Studies in Universal Logic,
DOI 10.1007/978-3-319-22087-1_7

Fermat-Kronecker arithmetic, Kronecker's general arithmetic of forms or homogeneous polynomials with Fermat's infinite descent. It is primitive recursive arithmetic without induction on the infinite sequence of natural numbers, the denumerable set $\aleph_0$ from a set-theoretical point of view. I call the unlimited sequence of natural numbers an "effinite" sequence adopting Brouwer's idea of an infinitely proceeding sequence, effinite meaning then indefinite extension of the finite. There is no infinite set in Fermat-Kronecker (F-K) arithmetic only finite fields with extensions (possibly infinite extensions) provided by the adjunctions of indeterminates (*Unbestimmte*). The adjunctions are processes performed in a finite number of steps for indeterminate quantities that can be iterated indefinitely. Fermat's infinite or indefinite descent is also a finite process since it starts with an arbitrary finite natural number and it stops at 0, the only limit-ordinal accepted in F-K arithmetic, there is no ω, the first transfinite ordinal without an immediate predecessor. Of course, we have here the dividing line between the Fermat-Kronecker arithmetic and Peano arithmetic with its Cantorian set-theoretic universe underlying the semantics of first-order and higher-order logic.

The problem of the consistency of arithmetic from an internal point of view is purely syntactical and consists in separating theorems from non-theorems (sentences from their negations) and in showing that only theorems are provable, i.e. $a = a$ or $\neg(0 = 1)$. The decidability follows by enumerating the theorems and syntactic completeness ends up by listing exhaustively the requiring axioms of the consistent arithmetic theory; above and beyond, semantic completeness is external to arithmetic, since it requires that theorems be true in a model—here consistency means "have a model" and it is in a set-theoretic universe that a model is located in general.

The arithmetical (polynomial) translation or interpretation of logic allows for the direct passage from the ring of integers to the ring of polynomials (and then to finite number fields and function fields), in other words, from the ordinary arithmetic of integers to the general arithmetic of polynomials. Such a course is defined by a finitary finitist constructivism without the detour via recursive functions in a set-theoretic setting, since polynomials are already recursive having the property of continuity.

The idea of arithmetical logic is in line with E. Bishop's constructivist stand of mathematics as a numerical language. Bishop had confessed that his endeavor in constructivist analysis was closer to Kronecker's finitism then Brower's intuitionism (see Bishop 1967). But my programme of an arithmetical logic originated in my discovery of Fermat's infinite descent in the writings of André Weil.

It is also André Weil who has directed me to Kronecker's arithmetical theory of algebraic quantities which Weil considers as the foundation of algebraic geometry (see Gauthier 1994 for early indications of an arithmetical logic).

7.2 Introduction

The primary goal of an arithmetical logic consists in substituting infinite descent *à la* Fermat to Peano's induction postulate. From the point of view of classical logic, infinite descent and complete induction are equivalent principles. However, in order to demonstrate that equivalence, one has to use the excluded middle principle with a double negation over the denumerable (infinite) set of natural numbers, a procedure forbidden by the constructivist. Transfinite induction or complete induction on ordinals in Cantor's first and second classes up to the limit ($lim\ \omega = \epsilon_0$) cannot correspond to infinite descent on finite number fields without violating the very idea of finite descent. Fermat, Euler, Lagrange, Legendre, Dirichlet, Kummer and Kronecker have all used descent in the spirit of finite elementary arithmetic. And Poincaré, Mordell, Weyl and Weil have followed suit in their work on algebraic-arithmetic geometry. And Kronecker being a pioneer of algebraic geometry, as Weil has emphasized, has elaborated a general arithmetic (*allgemeine Arithmetik*) or the arithmetical theory of algebraic quantities, which has all the essential characteristics of ordinary arithmetic of integers. For instance the unique factorization of polynomials in prime polynomials, which Kronecker points out as one of his fundamental results (see Kronecker 1968a). The main tool here is the theory of polynomial content at the heart of general arithmetic: the actual formulation states

> that two forms (homogeneous polynomials) F and F' are equivalent, if they have the same coefficients (i.e. arithmetical content).

The coefficients are integral and one can perform linear substitutions on such forms provided that one substitutes integral coefficients for the variables or indeterminates of the forms. Indeterminates, Gauss' *indeterminatae*, play a fundamental rôle in the sense that they give the mathematical theory its greatest generality and invest sufficient means in the theory of forms for the integral representation of algebraic quantities. This notion of polynomial representation avoids any recourse to semantics (notions of model or set-theoretic interpretation). The needed syntactic instruments are formulated in a minimal reduced formal apparatus.

The term "reduction" refers to the Euclidian algorithm for divisors or decomposition of composite numbers. Infinite descent is here applied as a generalized Euclidian algorithm extended to the field Q of rational numbers. The content of a polynomial in the context of divisibility can be seen as the greatest common divisor of its coefficients.

It is the ring $K[x]$ of irreducible (prime) polynomials with coefficients in the finite number field $K(x)$ which is going to be the principal theater of our operation and $F(x)$ will serve as the finite field of decomposition where descent is effective. Vandiver (1936) inspired by Kronecker has shown how to recompose the decomposition field $F(x)$ of a rational number field Q of algebraic numbers by adjoining indeterminates one at a time, that is in a linear time algorithm. Vandiver has therefore recomposed by finite induction the decomposition field Q by finite descent.

What is represented in the polynomial theory? First what we call Gödel's polynomials rather than Gödel's numbers which are assigned to logical formulas on the one side and on the other side the logical operations which are responsible for the composition of formulas i.e. logical constants while variables are represented by the indeterminates in the polynomials. The calculus has the goal of producing a final inequation $0 \neq 1$ as a proof of consistency for arithmetic. It is a double bijection that we finally have in the polynomial representation; first a bijection between integers and their polynomial representatives and second a bijection between formulas and their polynomial representatives—in this case we have an isomorphism. Here we have an internal isomorphism since we are all along in general arithmetic, while the Curry-Howard isomorphism between types and formulas can be deemed as external, since it is without arithmetic, not within. Finally, arithmetical logic exhibits the features of a modular polynomial logic. Polynomial signifies "multiple division" as in the generalized Euclidean algorithm (Fermat's infinite descent) and modularity pertains to Kronecker's theory of forms which is at the same time a theory of modular systems.

Our first-order language $L(T)$ for our first-order theory T has an *effinite* supply of atomic symbols:

1. letters for formulas (and sentences), A, B, C together with their punctuation signs, points, commas, parentheses, brackets, etc.
2. letters for constants or coefficients $a, b, c, \ldots$ and variables or indeterminates $x_1, x_2, \ldots, x_n$,
3. predicate letters p_j^n and the predicate symbol $=$ plus the arithmetical symbols $+, \cdot, (\times), -, \neq, \cong, \equiv, mod, 0, 1$, polynomial symbols $P_n Q_n, a_0 b_0$ the absurdity symbol $\perp$, and the symbol $\Box$ for the end of a proof.
4. functions letters f_j^n—when f is 0-ary, we consider it as a constant, plus function letters, ϕ, ψ, χ
5. the connectives $\wedge, \vee, \neg, \rightarrow$
6. the quantifiers $\forall, \exists$ and $\mathbf{\Xi}$.

Remarks: the quantifiers $\forall$ and $\exists$ quantify over finite sequences (sets), while the effinite quantifier $\mathbf{\Xi}$ quantifies over effinite (unlimited) sequences with a pre-positional bound or initial term without a post-positional bound or final term (for instance the sequence of natural numbers).

The terms consist exclusively of:

1. variables and constants
2. sequences composed of terms and functions letters, e.g. $f_j^n, t_1, \ldots, t_n$—for the terms $t_1, \ldots, t_n$.

Formulas or *wffs* consist exclusively of:

1. atomic formulas composed of terms and predicate letters, e.g. $p_j^n t_1, \ldots, t_n$ for the terms $t_1, \ldots, t_n$
2. any wff with connectives and quantifiers

Remarks: sentences are closed formulas, that is, formulas are "open" sentences with the free occurrence of variables. An instance or an exemplar $(t_1, \ldots, t_n / x_1, \ldots, x_n)$ of a formula A is the result of a substituting terms for the occurrences of a free variable.

The minimal logic has only one axiom, the axiom of identity

$$A \vdash A$$

for an arbitrary formula A. As logical rules, one adopt intelim rules for the introduction and the elimination of connectives and quantifiers in a natural deduction system *à la* Gentzen. Intelim rules are less systematic than the equivalent rules in a calculus of sequents, but they are "closer" to the deductions in a constructive logic.

$$\text{Axiom} \quad A \vdash A$$

$$(\mathrm{I}\wedge) \quad \frac{A \quad B}{A \wedge B} \qquad\qquad (\mathrm{E}\wedge) \quad \frac{A \wedge B}{A} \quad \text{and} \quad \frac{A \wedge B}{B}$$

$$(\mathrm{I}\vee) \quad \frac{A}{A \vee B} \quad \frac{B}{A \vee B} \qquad\qquad (\mathrm{E}\vee) \quad \frac{A \vee B \quad \begin{array}{c}[A]\\ \vdots\\ C\end{array} \quad \begin{array}{c}[B]\\ \vdots\\ C\end{array}}{C}$$

$$(\mathrm{I}\rightarrow) \quad \frac{\begin{array}{c}[A]\\ \vdots\\ B\end{array}}{A \rightarrow B} \qquad\qquad (\mathrm{E}\rightarrow) \quad \frac{A, A \rightarrow B}{B}$$

$$(\mathrm{I}\neg) \quad \frac{\begin{array}{c}[A]\\ \bot\end{array}}{\neg A} \qquad\qquad (\mathrm{E}\neg) \quad \frac{A, \neg A}{\bot}$$

(*Remark:* intuitionistic logic has the rule

$$(\mathrm{E}\neg) \quad \frac{\begin{array}{c}[A]\\ \bot\end{array}}{A}$$

while classical logic admits

$$(\mathrm{E}\neg) \quad \frac{\begin{array}{c}[\neg A]\\ \bot\end{array}}{A}$$

to obtain the double negation $\neg\neg A = A$).

$$(\mathrm{I}\,\forall) \quad \frac{Ax}{\forall x A x} \qquad\qquad (\mathrm{E}\,\forall) \quad \frac{\forall x A x}{A t}$$

$$\text{(I }\exists)\quad \frac{At}{\exists x Ax} \qquad\qquad \text{(E }\exists)\quad \frac{\exists xA \quad \begin{matrix}[Ax]\\ \vdots \\ B\end{matrix}}{B}$$

$$\text{(I }\mp)\quad \frac{Ax_n}{\mp x Ax} \qquad\qquad \text{(E }\mp)\quad \frac{\mp x Ax}{At_0}$$

Remarks: it is understood that the variable of quantification is not free, Ax_n meaning that we have an unlimited sequence of variables and the meaning that with the elimination of the effinite quantifier $\mp x$, we get an initial numerical term. We still have the intuitionistic properties of the disjunction—$A \vee B$ is provable if A or B is provable—and the provable instance for $\exists x Ax$ which is provable if we can find a numerical instance t. Moreover, our logic is endowed with constructive properties that apply only locally on finite sequence (sets) and effinite sequences (unlimited iterations). In the same manner, the sequent calculus in the forms $\Gamma \vdash A$ for Γ the antecedent and A the consequent—unique in the case of intuitionistic logic—the rules for → have the following form:

$$\text{(I }\rightarrow)\quad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \qquad\qquad \text{(E }\rightarrow)\quad \frac{\Gamma \vdash A \qquad \Gamma, B \vdash C}{\Gamma, A \rightarrow B \vdash C}$$

and the cut rule

$$\frac{\Gamma \vdash A \qquad \Gamma', A \vdash B}{\Gamma, \Gamma' \vdash B}$$

says that if we have A from Γ and if we have deduced B from another antecedent Γ and from A, then we can infer B from Γ and Γ by "cutting" A. The cut rule corresponds to the "*Modus Ponens*" or detachment rule.

$$\frac{\begin{matrix}A \rightarrow B\\ B\end{matrix}}{A}$$

As for structural rules, we have simply

$$\frac{\Gamma \vdash A}{\Gamma' \vdash A}$$

and this serves only to order antecedents following various combinations like additions, contractions or omission and exchanges. In our restricted syntax, the combinatory principle is latent and any permutation of the lexicographic order, ascending or descending—like the ordering of powers in polynomials—is allowed. The symmetry of inference rules in he sequent calculus can be achieved only in classical logic where double negation is permitted

$$\frac{\vdash A, \neg A}{\neg\neg A \vdash A}$$

as is the excluded third from the cut rule. The cut rule itself does not show explicitly in our formulation, since the polynomial calculus is a uniform calculus which rests on the chain continuity of polynomial sequences (or finite series) which have an inherent subformula property. Finally there is no ω rule, nor a $\aleph_0$ set; there is no set-theoretic semantics and *a fortiori* no completeness theorem, completeness and other semantical properties being excluded for finite structures by Trakhtenbrot's theorem (1950). The infinite is only a "*façon de parler*" following Gauss' dictum and it is not a manner of speech we use.

7.3 Arithmetic

R.M. Robinson's minimal arithmetic (see Nelson 1987a,b, Chap. 3) will serve as a point of departure. Robinson's theory $R =< 0, S, +, \cdot >$ has the following axioms:

1. $Sx \neq 0$
2. $Sx = Sy \rightarrow x = y$
3. $x + 0 = x$
4. $x + Sy = S(x + y)$
5. $x \cdot 0 = 0$
6. $x \cdot Sy = x \cdot y + x$
7. $Px = y \leftrightarrow Sy = x \vee (x = 0 \wedge y = 0)$

Axiom 7 for predecessor has been introduced by Nelson and replaces Robinson's formulation for successors

$$x \neq 0 \rightarrow \exists y Sy = x.$$

The last formula is then a theorem and as Nelson mentions, axioms of associativity, distributivity and commutativity are assumed to hold. Nelson has shown that R (rather a variant Q or its formal system Q_0) is self-consistent. This minimal arithmetic is an open theory, that is without quantifiers $\forall_{x_{x<y}}$ and $\exists_{x_{x<y}}$ for finite sequences (sets). For effinite sequences, e.g. the effinite sequence of natural numbers we have the effinite quantifier $\mp x$ or

8. $\mp x[Ax \wedge \mp x(Ax \rightarrow APx)] \rightarrow \mp x\neg Ax$

for a first-order formula A with variables $x_0, x_1, \ldots, x_n$ and for $P(x)$ the predecessor of x. This formulation of infinite descent means that for given n, there is no unlimited sequence of predecessors to n. For positive problems, as Fermat said, one as a positive version of descent in the following formulation

$$8' \quad \mp x_1 \ldots \mp x_n\{[Ax \wedge \forall x(Ax \to APx)] \to \exists x(x = 0 \vee 1 \vee m < n)Ax\} \to \mp xAx.$$

The postulate of infinite descent or Fermat's postulate, as we can call it, is substituted here for Peano's postulate and it is manifest that there is no infinite set in our axiomatization. Fermat's postulate allows for descending induction on the predecessors of an arbitrary natural number n and it also allows a generalized Euclidean algorithm for polynomial reduction and decomposition in Kronecker's general arithmetic; exponentiation is also bounded by the finite degree polynomials. For our present purpose though, we refer to Weil's algebraic version of infinite descent (see Chap. 6) as a finite decomposition process in number fields (for ordinary and algebraic integers) as finite extensions $\boldsymbol{Q}(\alpha)$ of the field of rational numbers $\boldsymbol{Q}$ where algebraic integers are roots of polynomials. The finite decomposition process is closely related to the Euclidean division algorithm for quadratic forms, i.e. homogeneous polynomials. Finite descent as a generalized Euclidean algorithm is the method we use in the following. Here finite descent could be called positive in the sense that it descends to 0 as the first ordinal or 1 for the first positive integer or n as an arbitrary integer and for polynomials to degree 1 for linear polynomials or $n = p$ for prime polynomials or 0 for the constant polynomial (the zero polynomial is noted—∞). As Davenport (1968, p. 159) points out, Fermat's version of descent was meant for insolubility of Diophantine equations while Legendre's version (and many others, e.g. Lagrange's reduction) was designed for solubility of polynomial equations as it is the case for Kronecker's theory of forms and polynomial division for modular systems which is a main ingredient of our proof for the internal consistency of Fermat-Kronecker arithmetic formalized in a modular polynomial logic. Since the effinite quantifier is not itself bounded, it can be used as an induction principle, but as we have shown, it is not equivalent to the classical principles of complete induction, transfinite induction or to the least number principle which are all equivalent classically via the indirect route of the excluded middle and the double negation principles, a route that is not practicable by the direct orientation of the constructivist logician and number theorist or arithmetician.

7.4 Arithmetization of Syntax

In his classical results on the incompleteness of Peano's arithmetic, Gödel supposed the ω-consistency of the arithmetic on the infinite set of natural numbers. The weaker 1-consistency for Σ_1^0 sentences on recursively enumerable sets in the arithmetic hierarchy derives from ω-consistency for existential sentences and still needs the infinite set of natural numbers. Peano's original second-order formulation of the induction principle is based on the existence of the same infinite set

$$\exists x\{\phi \in x \wedge \forall y(y \in x \to Sy \in x)\} \to \forall y \in x.$$

A formal system S in the sense of Hilbert has a finite characterization and Gödel devised a way to assign natural numbers (Gödel numbers) to the primitive signs of S and to the finite sequence of such signs (the formulas of S); the bijection between a finite sequence of natural numbers in $\mathbb{N}$ and a finite sequence of signs in S is defined by a map

$$\phi : \mathbb{N}_s \to \mathbb{N}$$

in such a way that a sequence $n_1, n_2, \dots, n_k$ is assigned a number

$$2^{n_1} \cdot 3^{n_2} \dots \cdot p_k^{n,k}$$

where p_k denotes the k^{th} prime number; Gödel is than able to immerse the formal system S into Peano arithmetic. This is the arithmetic of primitive recursive functions generated by substitution and composition (or recursion) from the initial functions, the successor function, the constant functions like zero

$$\forall x (Zx = 0)$$

and identity functions. If one has also the μ function for the least number k such

$$\phi(k+1, x_2, \dots, x_n) = \mu(k, \varphi(k, x_2, \dots, x_n), x_2, \dots, x_n),$$

one obtains the general recursive functions. Here, if recursive functions are arithmetical functions, they have as domain the denumerable set $\mathbb{N}$ of natural numbers. In Gödel's words, ω-consistency is defined for the properties $F(x)$ of natural numbers, since it runs through all the values of a function applied to the set of natural numbers. Rosser's simple consistency result for Peano's arithmetic only substitutes to ω consistency the concept of recursive enumerability which is equivalent by the fact that $\aleph_0 = \mathit{card}\ \aleph$.

Our polynomial representation operates on a different stage. Take for the instance the binary quadratic forms $x^2 + y^2$. These are homogeneous polynomials of degree 2 with two variables and they induce equivalent representations of integers (see Davenport 1968). By the isomorphism between polynomials p and integers a

$$\sum_{k \leq n} a_k^{p_k}$$

for an integer a and p prime or not, signs and sequences of signs can be represented by polynomials. A reduced polynomial in a finite field $F(x)$ of g elements is simply a polynomial of a lesser degree $< q$ in each variable. Any polynomial

$$f(x) \in F[x_1, \dots, x_n]$$

in that context is equivalent to a reduced polynomial (see Ireland and Rosen 1980).

If we go to general recursive functions with the μ operator, we can avoid the least number principle with the help of the minimal reduced polynomial which is irreducible (being linear or of degree 1); we can also descend or reduce down to the zero polynomial (noted—∞). Since we can use the Chinese remainder theorem on congruences with our generalized Euclidean algorithm (infinite descent), we reach down to a minimal polynomial of degree 1 or of degree 0 for the constant polynomial or—∞ for the zero polynomial. Besides, the least integer in a finite field is obviously a finite integer and it corresponds to the degree of the minimal polynomial (of minimal degree); that polynomial is indeed irreducible.

One can immediately see how the polynomial representation works for Gödel numbers that are replaced by what we can freely call Gödel polynomials. Take for a specific example Gödel's function β which served to represents sequences of natural numbers (and their associated sentences); it is a somewhat artificial device using the Chinese remainder theorem in order to obtain a primitive recursive function. In order to have a more natural representation, one has only to introduce the notion of reduced polynomial in the following formulation

$$P(\bar{x}) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

or

$$P(\bar{x}) = \sum_{i=0}^{n} a_i x^{c'}$$

for $\bar{x}$ representing the sequence of natural numbers $(x_1, \ldots, x_n)$, in the same fashion, to the Gödel number of a sequence x, one can substitute the monomial

$$M(\bar{x}) = a_i x^{i_1} a_i x_2^{i_2} \ldots a_i x_n^{i_n}$$

with the sum $\sum(i_1, i_2, \ldots, i_n)$ over the indices i's.

We are going to need elementary facts about polynomials in one indeterminate with our principal tool, the convolution (or Cauchy) product for polynomials. Polynomials of the form

$$f = f_0 + f_1x + f_2x^2 + \ldots + f_nx^n$$

where the f_i are the coefficients with the indeterminate x build up the subring $K[x]$ of the ring $K[[x]]$ of formal power series. The degree of a polynomial is the degree of the last non-zero coefficient $k = n$, while the leading coefficient of a polynomial f of degree k is the constant f_k and f is called monic if its leading coefficient is 1. Thus polynomials are power series having only a finite number of non-zero coefficients. The convolution or Cauchy product of two polynomials will play an important role in our translation; we write it

$$f \cdot g = \Big(\sum_m f_m x^m\Big)\Big(\sum_n g_n x^n\Big)\Big(\sum_m \sum_n f_m g_n x^{m+n}\Big).$$

The sum $f + g$ of polynomials f and g is obtained by simply adding corresponding coefficients. Homogeneous polynomials have all their non-zero terms of the same degree and they can be put in the following convenient form

$$a_0x^m + a_1x^{m-1} + \ldots + a_mx.$$

We are interested in irreducible (= prime in $K[x]$) polynomials. Every linear polynomial is irreducible. $K[x]$ has the property of unique factorization and this fact will be crucial in our future developments.[1] We are going to make an essential use of Kronecker's notion of the content of forms in (1968b, p. 343). A form M is contained in another form M' when the coefficients of the first are convoluted (combined in a Cauchy product) in the coefficients of the second. This idea of a content "*Enthalten-Sein*" of forms can be summarized in the phrase "The content of the product is the product of the contents (of each form)" which can be extracted from Kronecker's paper (1968, pp. 419–424). Thus, for a form to be contained or included in another form is simply to be linearly combined with it (to have its powers convoluted with the powers of the second form).

We can adopt here a general principle of substitution—elimination formulated by Kronecker (1882). We state the *Substitution Principle*:

> 1) Two homogeneous forms (polynomials) F and F° are equivalent if they have the same coefficients (*i.e. content*);
> 2) Forms can be substituted for indeterminates (variables) provided the (linear) substitution is performed with integer coefficients.

We have immediately the following Proposition 1 (proposition X in Kronecker):

> Linear homogeneous forms that are equivalent can be transformed into one another through substitution with integer coefficients.[2]

We have also the following Proposition 2 (proposition X° in Kronecker):

> Two forms F and F° are absolutely equivalent, if they can be transformed into one another.

[1] Kronecker had proven the unique factorization theorem in the following formulation: "Every integral form (= polynomial) is representable as a product of irreducible (prime) forms in a unique way" (see Kronecker 1882, p. 352). Kronecker is interested in the theory of divisibility for prime forms (forms with no common divisors greater than 1), rather than prime polynomials in his work. The notion of integral domain and unique factorization domain are direct descendants to that theorem.

[2] This can be seen as the precursor of the problem of quantification over empty domains. We know that we have

$$\frac{A, A \supset B}{B}$$

in an empty domain, provided that A and B have the same free variables. But Kronecker had a more general theory of inclusion or content of forms in mind and the transformation in question is a composition of contents, an internal constitution of polynomials (forms) where indeterminates are not the usual functional variables.

These propositions can be considered as lemmas for the unique factorization theorem for forms which Kronecker considered as one of his main results. The substitution procedure is simultaneously an elimination procedure, since indeterminates "*Unbestimmte*" are replaced by integer coefficients. Thus an indefinite (or effinite) supply of variables can be made available to a formal system and then reduced by the substitution-elimination method to an infinitely descending or finite sequence of natural numbers, as will be shown in the following. The equivalence principle makes it possible to have a direct translation between forms (polynomials) and (logical) formulas.

The substitution process takes place inside arithmetic, from within the Galois field F^*, i.e. the minimal, natural or ground field of polynomials which is the proper arena of the translation and indeterminates—Kronecker credits Gauss for the introduction of "*indeterminatae*"—are the appropriate tools for the mapping of formulas into the natural numbers. The main idea is that indeterminates in Kronecker's sense can be freely adjoined and discharged and although Kronecker did not always suppose that his forms were homogeneous, we restrict ourselves to homogeneous polynomials.

We introduce an isomorphism:

$$\psi : Form \rightarrow Poly$$

between formulas and polynomials together with two more valuation maps:

$$\phi : Form \rightarrow (0, 1)$$

which evaluates formulas into $[n]$ and

$$\chi : Poly \rightarrow (0, 1)$$

which evaluates polynomials into n, the degree of a polynomial.

We define the polynomial translation in eight clauses.

Clause 1) An atomic formula A can be polynomially represented by the isomorphism:

$$\psi : (A)[n] \cong a_0x(\text{for an arbitrary } A)$$

(where the a_0 part is called the determinate and the x part the indeterminate and ψ is the polynomial valuation function or map). Here the coefficient a_0 corresponds to a given natural number (the "valuator") and indicates that it is the first member of a sequence, x being its associate indeterminate. The "valuator" of the formula A is indicated by n and $[n]$ represents the Gödel number of the formula associated to a natural number n; it is thus a Gödel polynomial—here a monomial. Molecular formulas are built up from monomials.

Clause 2) The negation of an atomic formula, that is $\neg A$, is translated as

$$\psi : (\neg A)[n] = (1 - a_0x).$$

Clause 3) The conjunction A and B is translated as $\psi(A \wedge B)(n \times m) \cong (a_0x) \cdot (b_0x)$ for the product of monomials (a_0x) and (b_0x).

Clause 4) The disjunction A or B is rendered by

$$\psi : (A \vee B)(n+m) = (a_0 x + b_0 x)$$

Clause 5) Local implication $A \rightarrow B$ is rendered by $\psi(A \rightarrow B)(m^n) \cong (\bar{a}_0 x + b_0 x)^n$ for $\bar{a}_0 x = 1 - a_0 x$.

Remarks: How is implication to be interpreted polynomially? A developed product of polynomials has the form

$$a \cdot b = \Big(\sum_i a_i x^i\Big)\Big(\sum_j b_j x^j\Big) \cong \sum_i \sum_j a_i b^j x^{i+j}.$$

For a^b we could simply write $(a+b)^n$ for the binomial coefficients and put

$$(a_0 x + b_x o)^n \cong a_0^n x + n a^{n-1} x b x + [n(n-1)/2!] a_2^{n-2} x^2 b_2 x^2 + \ldots + b_0^n x^n$$

in short

$$(a_0 x + b_x o)^n_{i<n} \cong \sum_{i+j=n} (i+j) a^i b^i x^n.$$

The rationale for our translation is that we want to express the notion of inclusion of a in b by interwining or combining their coefficients in a "crossed" product, the sum of which is 2^n which is also the sum of combinations of n different objects taken r at a time

$$\sum_{r=0}^{n} C^n_r.$$

Linear combination of coefficients is of course of central importance in Kronecker's view and one of his fundamental results is stated: "Any integral function of a variable can be represented as a product of linear factors" (1968a, pp. 209–247). In his (1968b, pp. 147–208), Kronecker refers to Gauss's concept of congruence and shows that a modular system with infinite (indeterminate) elements can be reduced to a system with finite elements. This is clearly the origin of Hilbert's basis theorem (1965, III, pp. 199–257) on the finite number of forms in any system of forms with

$$F = A_1 F_1 + A_2 F_2 + \ldots + A_m F_m$$

for definite forms $F_1, F_2 \ldots F_m$ of the system and arbitrary forms $A_1 A_2 \ldots A_m$ with variables (indeterminates) belonging to a given field or domain of rationality "*Rationalitätsbereich*". The fact that exponentiation is not commutative is indicated by the inclusion $a \subset b$. The combinatorial nature of implication is made more explicit in the polynomial expansion and is strengthened by the symplectic (interlacing) features of local inclusion of content. We may also define implication, in analogy with the relative complement, as

$$(1^n - a_0x) + b_0x$$

where 1^n is the arithmetic universe polynomially expanded.

Clause 6) $\psi : (\exists xAx)[m + n + \ell \ldots] \cong \sum_{0\ldots}(a_0x + b_0x + c_0x)_{i<n}$ where $\sum$ is an iterated sum of numerical instances with a_0 as the first member of the sequence.

Clause 7) $\psi : (\forall xAx)[n \times x \times \ldots \times \ell] \cong \prod_0(a_0xb_0xc_0x)_{i<n}$.

Clause 8) $\psi : (\text{∃̶}xAx)[n \times x \times \ell \ldots] \cong \prod_{0\ldots}(a_0xb_0xc_0x\ldots)_n$.

Remarks: The effinite quantifier calls for some clarification. While the classical universal quantifier stands here for finite sets only, the effinite quantifier is meant to apply to infinitely proceeding sequences or effinite sequences (with the three dots at the end signifying a continuing process). These are not sets and do not have a post-positional bound; we put an n to such sequences and 2^n to sequences of such sequences

$$0, 1, 2, \ldots, n, \ldots, 2^n$$

with the understanding that n signifies an arbitrary bound. It should be pointed out that Boole in his *Mathematical Analysis of Logic* (1847) had also a universe (of classes) denoted by 1; negation was interpreted as $1 - x$. The fact that the ring $K[x]$ of polynomials enjoys the unique factorization property exhibited by infinite descent coupled with the proof by infinite descent of the infinity of primes makes essential use, from our point of view, of the effinite quantifier.

We then have a combinatorial formulation

$$\prod_{0\ldots}^{n}(a_0xb_0xc_0x\ldots n_nx^n)$$

for the effinite quantifier; since $n! = \prod_{c<n} c$, the combinations of n, I call this scheme the absolute or standard scale. Any other scale is an associate scale (of indeterminates) and it is reducible by substitution to the standard scale.

As a foundational precept, there is no ω. Any transnatural or transarithmetic (transfinite, in Cantorian terminology) ordinal scale, e.g. up to ϵ_0, is an associate scale and is by definition reducible. It is clear, from a Kroneckerian point of view, that Cantor's transfinite arithmetic becomes a dispensable associate (with an indeterminate pay-off!). The arithmetic universe N is naturally bounded by 2^n and not by $2^{\aleph_o}$ for infinite power series!

The internal consistency proof for (FK) Fermat-Kronecker arithmetic is following the course of the radical translation or interpretation of logic into polynomial arithmetic, the embedding of arithmetic into polynomials—with indeterminates as variables—where the degree of a polynomial substitutes for the Gödel number of a given formula (or sentence) in the arithmetical universe and finally infinite descent which reduces polynomials according to the decreasing order of their powers down to linear irreducible polynomials of degree 1 or down to the zero polynomial. What we have then is $1 \neq 0$, hence consistency or non-contradictory by

$$\chi : P_{(\text{deg } 1})=1$$

$$\chi : P_{(\text{deg}—\infty)}=0.$$

In that proof, Cauchy diagonal (the convolution product)does not transcend the domain of rationality of polynomials and the combinatorial nature of polynomials is preserved or conserved as a natural extension of elementary arithmetic. The elimination of logic in that process is not alien to the quantifier elimination procedure in model theory which originates in Kronecker's elimination theory, as we have seen (Chap. 2). By replacing the rank of a formula by the degree of the corresponding polynomial, we obtain a reduction by unique factorization, that is a finiteness result for arithmetic with infinite descent.

7.5 Reducibility and Divisibility

The method of descent we used in our proof and which is most common could also be called the method of decomposition, as Weil has called it—see Weil (1979a). The decomposition process necessarily stops and this form of the descent is the one most commonly used for the positive solutions of Diophantine equations. After Fermat, Legendre used the method which he called reduction and it is the way it is used by most contemporary authors from Mordell and Weil on.[3] Local decomposition of forms in a descent corresponds to a division process as in the Euclidean algorithm. Kronecker has outlined in (1968b, pp. 419–424) the most general setting for the decomposition of polynomial content. His notion of inclusion or content is expressed in terms of the convolution product. The general form of the convolution product of two polynomials (forms) encloses or contains higher-order forms and the substitution-elimination method enables one to remain within the confines of integral forms. The product of forms

$$\sum_{h=0}^{m} M_h U_h \cdot \sum_{i=1}^{m+1} M_{m+2} U_{m+1}$$

satisfies an algebraic equation of order r which defines a form containing the product of forms

$$\prod_{h=1}^{r} M_k U_{hk}.$$

[3] Mordell says of infinite descent in 1922 that you start with an arbitrary n—an arbitrary choice made once and for all—and descend finitely. Hasse's principle of local solvability implying global solvability for quadratic forms relies on the same principle and is related to Legendre "positive" infinite descent (see Davenport 1968).

Hence, the notions of inclusion and of equivalence (reciprocal inclusion) of forms are valid generally, i.e. for both forms and divisors.[4] Factor decomposition—which we may call devolution—is a descending technique perfectly similar to the division algorithm for integers or the Euclidean algorithm for polynomials. The notion of greatest common divisor of a finite set of elements is an equivalence class of polynomials and Kronecker's main result says as stated above.[5]

> Every integral algebraic form is canonically representable as a product of irreducible (prime) forms.

For this unique decomposition (devolution) of polynomials, descent is used to arrive at irreducible polynomials, much in the same way as in Euclid's proof of the divisibility of composite numbers by primes. Take a polynomial

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

of degree n. Suppose that n is not prime, then it must be divisible by two factors i and j one of which, say j, must be prime; if not, j must be divisible by two factors, h and g, one of which, say i, must be prime; if not, we go on in that process, until we reach an n which is necessary prime, since there is no infinite descent and we must stop at 1, that is linear (and irreducible) polynomials. Formally,

$$\mp x\{[Ax \wedge \exists y(y < x)Ay] \rightarrow \exists y \mp z(z < y)Az\} \rightarrow \mp x \neg Ax.$$

By *reductio ad absurdum*, there are irreducible polynomials. Now the fact (Gauss lemma) that the product of two primitive polynomials (with 1 as the greatest common divisor of their respective coefficients) is primitive can also be had with infinite descent and *reductio ad absurdum*. This fact combined with the fact that there is unique decomposition into irreducible (= prime) polynomials, we obtain unique prime factorization. Kronecker's version of unique decomposition rests on the formula quoted above

$$\prod_{h=1}^{r} M_k U_{hk}.$$

and

$$\prod_{i=j+k} c_i = \sum_{j+k=i} a_j b_k$$

[4] My emphasis is different from Edwards (1987a,b) who has chosen to look at divisor theory rather than the theory of forms which is, in my view, the encompassing theory.

[5] See Kronecker (1889). Edwards (1987a,b) rightly says that Dedekind's Prague theorem—a generalization of Gauss lemma to the algebraic case—is but a consequence of Kronecker's result. See also Edwards et al. (1982).

with $j = (0, \ldots, m)$ and $k = (0, \ldots, n)$. We shall read it in the form (remembering that $a^{b-1} \equiv (mod\, p)$ from a divisibility point of view)

$$\prod_{i=1}^{m+n}(1 + c_i x_i) + \sum_{i=0}^{m+n}(c_i x^{m+n-1}) = \sum_{m+n=1}(a_m b_n)$$

to prove the eliminability of the effinite quantifier. The procedure is quite similar to the process of elimination of implication which now appears as a decomposition of content—the notion of inclusion "*Enthalten-Sein*" which has been translated by "content". With the elimination of the effinite quantifier by infinite descent, we shall be done.

7.6 Elimination of Logical Constants

The connectives negation, disjunction and conjunction are directly eliminable in the polynomial representation, since one can interpret them as difference, sum and product of polynomials with a finite number of terms (coefficients and indeterminates).
Proof: we rewrite the logical intelim rules in the polynomial language. The unique identity axiom becomes the equality $A = A$.

$$(\text{I} \wedge) \quad \frac{A \quad B}{A \wedge B} \qquad ;\ a_0x, b_0x \equiv a_0x \cdot b_0x$$

$$(\text{E} \wedge) \quad \frac{A \wedge B}{A} \quad \text{and} \quad \frac{A \wedge B}{B} \qquad ;\ a_0x \cdot b_0x \equiv a_0x, b_0x$$

$$(\text{I} \vee) \quad \frac{A}{A \vee B} \quad \frac{B}{A \vee B} \qquad ;\ a_0x{+}b_0x \equiv a_0x,\ a_0x{+}b_0x \equiv b_0x$$

$$(\text{E} \vee) \quad \frac{A \vee B \quad \begin{array}{c}[A]\\ \vdots \\ C\end{array} \quad \begin{array}{c}[B]\\ \vdots \\ C\end{array}}{C} \qquad ;\ \begin{array}{l} a_0x + b_0x \equiv c_0x \ (\text{mod } b_0x) \\ a_0x + b_0x \equiv c_0x \ (\text{mod } a_0x)\end{array}$$

$$(\text{I} \rightarrow) \quad \frac{\begin{array}{c}[A]\\ \vdots \\ B\end{array}}{A \rightarrow B} \qquad ;\ a_0x \equiv b_0x(\text{mod } a_0x + 1)$$

$$(\text{E} \rightarrow) \quad \frac{A, A \rightarrow B}{B} \qquad ; 1 - a_0x \equiv b_0x(\text{mod } a_0x)$$

$$(\mathrm{I}\neg)\quad \frac{\begin{array}{c}A\\ \perp\end{array}}{\neg A} \qquad ;\ 1 - a_0x \equiv 1(\mathrm{mod}\ a_0x)$$

$$(\mathrm{E}\ \neg)\quad \frac{A, \neg A}{\perp} \qquad ;\ 1 - a_0x \equiv 0(\mathrm{mod}\ a_0x)$$

$$(\mathrm{I}\ \forall)\quad \frac{Ax}{\forall xAx} \qquad ;\ \prod_n a_0x^n \equiv a_0x(\mathrm{mod}\ n)$$

$$(\mathrm{E}\ \forall)\quad \frac{\forall xAx}{At} \qquad ;\ a_0x \equiv \prod_n a_0x^n(\mathrm{mod}\ 1)$$

$$(\mathrm{I}\ \exists)\quad \frac{At}{\exists xAx} \qquad ;\ \sum_n a_0x \equiv a_0x^n(\mathrm{mod}\ 1)$$

$$(\mathrm{E}\ \exists)\quad \frac{\begin{array}{cc} & [Ax] \\ \exists xA & \vdots \\ & B\end{array}}{B} \qquad ;\ a_0x \equiv \sum_n b_0x^n(\mathrm{mod}\ 1)$$

$$(\mathrm{I}\ \mp)\quad \frac{Ax_n}{\mp xAx} \qquad ;\ \prod_{n\ldots} a_0x \equiv a_0x^n(\mathrm{mod}\ n \times n)$$

$$(\mathrm{E}\ \mp)\quad \frac{\mp xAx}{At_0} \qquad ;\ a_0x \equiv \prod_{n\ldots} a_0x^n(\mathrm{mod}\ 1)$$

In translating logical formulas into congruent forms, we want to represent logical constants in a polynomial language in order to integrally arithmetize (polynomialize) logic. It is manifest in that context that deduction expressed in a turnstile $A \vdash A$ or A/A is a congruence relation in a modular calculus. Implication is rewritten

$$(\bar{a}_ox + b_ox)^n$$

for $\bar{a}_ox = 1 - a_ox$, the local negation (complement) of logic; exponent n denotes the degree of the polynomial (content) of implication that we reduce in the following way by a calculus on symmetrical polynomials (forms).

7.7 The Elimination of Implication

We want to arithmetize (local) implication. We put $1 - a = \bar{a}$ for local negation. We have $(\bar{a}_o x + b_o x)^n$ and we want to exhaust the content of implication—in Gentzenian terms, this would correspond to the exhibition of subformulas (the subformula property). We just expand the binomial by decreasing powers

$$(\bar{a}_o x + b_o x)^n) = \bar{a}_0^n x + n\bar{a}^{n-1} x b_0 x + [n(n-1)/2!]\bar{a}^{n-2} x b^2 x + \ldots + b_0^n x$$

where the companion indeterminate x shares the same power expansion. By an arithmetical calculation (on homogeneous polynomials that are symmetric i.e. with a symmetric function $f(x, y) = f(y, x)$ of the coefficients)

$$\begin{aligned}
(\bar{a}_o x + b_o x)^n) &= \bar{a}_0^n x + \sum_{k=1}^{n-1} (n-1/k-1)\bar{a}_0^{k-1} x + (n-1/k) a_0^k x b_0^{n-k} x + b_o^n x \\
&= \sum_{k=1}^{n} (n/k-1) a_0^k x b_0^{n-k} x + \sum_{k=0}^{n-1} (n-1/k) a_0^k x b_0^{n-k} x \\
&= \sum_{k=0}^{n-1} (n-1/k) a_0^{k+1} x b_0^{n-k} x + \sum_{k=0}^{n-1} (n-1/k) a_0^k x b_0^{n-k} x \\
&= \bar{a}_0 \sum_{k=0}^{n-1} (n-1/k)(\bar{a}_0 - 1)^k b^{n-1-k} x + \\
&\quad \sum_{k=0}^{n-1} (n-1/k)\bar{a}_0^k x (b_0 - 1)^{n-1-k} x \\
&= (\bar{a}_1 x + b_1 x)(a_1 x + b_1 x - 1)^{n-1}
\end{aligned}$$

and continuing by descent and omitting the x's, we have

$$(\bar{a}_2 + b_2)(\bar{a}_2 + b_2 - 2)^{n-2}$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots$$

$$(\bar{a}_{n-2} + b_{n-2} + \bar{a}_{n-2} +_{n-2} -(n-2))^{(n-(n-2))}$$

$$(\bar{a}_{n-1} + b_{n-1} + \bar{a}_{n-1} +_{n-1} -(n-1))^{(n-(n-1))}$$

$$(\bar{a}_n + b_n)(\bar{a}_n + b_n)^{n-n}.$$

Applying descent again on $(\bar{a}_n + b_n)$, we obtain

$$(\bar{a}_0 + b_0)$$

or, reinstating the x's

$$(\bar{a}_0 x + b_0 x).$$

Remembering that

$$(\bar{a}_x + b_x)^n_{k<n} = \sum_{k+m=n} (k + m/k)\bar{a}^k b^m x^n$$

we have

$$(\bar{a}_x + b_x)^{n+m=n}_{k<n} = \prod_{k+m=n} (k, m) = 2^n$$

or more explicitly

$$\sum_{i=0}^{m+n} c_1 x^{m+n=1} = \bar{a}_0 x \cdot b_0 x \prod_{i=1}^{m+n} (1 + c_i x) = 2^n$$

where the product is over the coefficients (with indeterminates) of convolution of the two polynomials (monomials) a_0 and b_0. We could of course calculate the generalized formula for polynomials

$$(a_0 x + b_0 x + c_0 x + \ldots + k_0 x)^n = \sum_{p,q,r\ldots s} a^p b^q c^r \ldots k^s$$

in the same manner, but we shall postpone the general case till we come to the effinite quantifier for a unified treatment.

The combinatorial content of the polynomial is expressed by the power set 2^n of the n coefficients of the binomial. I contend that this combinatorial content expresses also the meaning of local (iterated) implication. Convolution exhibits the arithmetic connectedness that serves to render the logical relation of implication. Implication is seen here as a power of polynomials, a^k and b^m with $k < m$ having their powers summed up and expanded in the binomial expansion. Some other formula may be used for the product, but it is essential to the constructive interpretation that the arithmetic universe be bounded by 2^n. One way to make things concrete is to analyse $a \to b$ in terms of

$$a \to b = C((2^n - a) + b)$$

where C can stand for combinations or coefficients. The formula is an arithmetical analogue of the topological interpretation of intuitionistic implication.

Theorem. Local implication $a \to b$ can be eliminated by interpreting it as $(\bar{a} + b)^n$.
Proof. By the above construction.

7.8 The Elimination of the Effinite Quantifier Through Infinite Descent

There is an intimate connection between implication as inclusion (filling in a content) and effinite quantification as an iterated product. We have introduced the effinite quantifier in the form

$$\varphi_!(\mp xAx)[n \times m \times \ell \ldots] < n \times m \times \ell \ldots >= 1$$

we can translate the effinite quantifier as an iterated product.

$$\prod \ldots \prod (a_n x^m)(a_n x^n)$$

which we write as

$$\begin{aligned} \textstyle\prod_{i=1}^{m} a_i \left(\textstyle\prod_{j=1}^{n} \ldots a_{m+j} \right) \ldots &= \textstyle\prod_{i=1}^{n+1} a_i = \left(\textstyle\prod_{i=1}^{n} a_i \right) a_{n+1} \\ &\vdots \\ &= \textstyle\prod_{i=1}^{n+m} a_i = \left(\textstyle\prod_{i=1}^{n} a_i \right) a_{n+1}, \ldots, a_{n+n} \end{aligned}$$

which we calculate by descending. We set

$$\prod_{i=1}^{m+n} (C_i)_n = a_m \cdot b_n \prod_{i=1}^{m+b} (1 + c_i x)_1 \ldots (1 + c_i)_n.$$

The lower index $(1 \ldots n)$ is the height of the polynomial. We take up again our calculation of coefficients. We put $((a_0 x) \cdot (b_0 x)^n$ to indicate that we have a product of monomials

$$(a_0 x \cdot b_0 x) = ((a_0 x) \cdot (b_0 x)^n$$

$$= \left[\begin{array}{l} a_0^n x + \prod\limits_{i=1}^{n} \sum\limits_{k=1}^{n-1} (n - 1/k - 1)_1 a_0^{k-1} x + (n - 1/k)_1 + b_0^n x_1 \\ \vdots \\ a_0^n x + \prod\limits_{i=1}^{n} \sum\limits_{k=1}^{n-1} (n - 1/k - 1) n a_0^{k-1} x + (n - 1/k)_n + b_0^n x_n \end{array} \right]$$

$$= \left[\begin{array}{l} \prod\limits_{i=1}^{n-1} \left(\sum\limits_{k=1}^{n} \right) (n/k - 1)_1 (a_0^k x b_0^{n-k} x)_1 + \sum\limits_{k=0}^{n-1} (n - 1/k - 1)_1 (a_0^k x b_0^{n-k} x)_1 \\ \vdots \\ \prod\limits_{i=1}^{n-1} \left(\sum\limits_{k=1}^{n-1} \right) (n/k - 1)_n (a_0^k x b_0^{n-k} x)_n + \sum\limits_{k=0}^{n-1} (n - 1/k - 1)_n (a_0^k x b_0^{n-k} x)_n \end{array} \right]$$

$$= \begin{bmatrix} \prod_{i=1}^{n} \left(\sum_{k=1}^{n-1} \right) (n/k-1)_1 (a_0^{k+1} x b_0^{n-1-k} x)_1 + \sum_{k=0}^{n-1} (n-1/k)_1 (a_0^k x b_0^{n-k} x)_1 \\ \vdots \\ \prod_{i=1}^{n} \left(\sum_{k=1}^{n-1} \right) (n/k-1) n (a_0^{k+1} x b_0^{n-1-k} x)_n + \sum_{k=0}^{n-1} (n-1/k)_n (a_0^k x b_0^{n-k} x)_n \end{bmatrix}$$

$$= \begin{bmatrix} a_n \prod_{i=1}^{n} \Bigg[\sum_{k=0}^{n-1} (n-/k)_1 \big((a_0-k)^k x\big)_1 (b^{n-1-k} x)_1 + b_n \sum_{k=0}^{n-1} (n-1/k)_1 (a_0^k x) \\ \qquad + b_n \sum_{k=0}^{n-1} (n-1/k)_1 (a_0^k x)_1 ((b_0 - 1^{n-1-k} x)_1) \Bigg] \\ \vdots \\ a_n \prod_{i=1}^{n} \Bigg[\sum_{k=0}^{n-1} (n-/k)_n \big((a_0-k)^k x\big)_n (b^{n-1-k} x)_n \\ \qquad + b_n \sum_{k=0}^{n-1} (n-1/k)_1 (a_0^k x)_n ((b_0 - 1^{n-1-k} x)_n) \Bigg] \end{bmatrix}$$

$$= (a_0 x + b_1)_1 (a_1 x + b_1 x - 1)_1^{n-1}$$

$$\cdots \quad \cdots \quad \cdots$$

$$= (a_1 x + b_1)_n (a_1 x + b_1 x - 1)_n^{n-1}$$

and continuing by descent we have (again omitting the x's)

$$= \begin{bmatrix} (a_2 + b_2)_1 (a_2 + b_2 - 2)_1^{n-2} \\ \vdots \\ (a_2 + b_2)_2 (a_2 + b_1 - 2)_n^{n-2} \end{bmatrix}$$

$$\cdots \quad \cdots \quad \cdots$$

$$= \begin{bmatrix} (a_{n-2} + b_{n-2})_1 (a_{n-2} + b_{n-2} - n - 2)_1^{n-(n-2)} \\ \vdots \\ (a_{n-2} + b_{n-2})_n (a_{n-2} + b_{n-2} - n - 2)_1^{n-(n-2)} \end{bmatrix}$$

$$\cdots \quad \cdots \quad \cdots$$

$$= \begin{bmatrix} (a_{n-1} + b_{n-1})_1 (a_{n-1} + b_{n-1} - n - 1)_1^{n-(n-1)} \\ \vdots \\ (a_{n-1} + b_{n-1})_n (a_{n-1} + b_{n-1} - n - 1)_n^{n-(n-1)} \end{bmatrix}$$

$$\cdots \quad \cdots \quad \cdots$$

$$= \begin{bmatrix} (a_n + b_n)_1(a_n + b_n)_1^{n-n} \\ \vdots \\ a_n + b_2)_n(a_n + b_n)_n^{n-n} \end{bmatrix}$$

which is

$$= \begin{bmatrix} (a_0 + b_0)_1 \\ \vdots \\ a_0 + b_0)_n \end{bmatrix}$$

which is just $(a_0 \cdot b_0) = \prod_0^n (a_0 + b_0)$. Infinite descent terminates with 0 or 1. If it does terminate with 1 (degree 1), we have linear polynomials irreducible as are prime polynomials, if the descent stops with 0, the zero polynomial has no degree (but noted—∞). Thus $1 = \neg 0$ and

$$a_0 x \not\equiv \bar{a}_0 x$$

which is $1 \neq (1 - 1 = 0)$. □

Our proof is in agreement with Hilbert's original formulation (1904) for the consistency in terms of homogeneous (polynomials) equations

$$a = a$$

and inequations

$$a \neq a$$

Hilbert's axiom 1 is the identity (or equality) axiom which we have adopted and the consistency problem is summarized in the derivation

$$a \neq a$$

or

$$\neg(a = a)$$

from a logical point of view.

7.9 Conclusion: The Polynomial Extension from a Finitist Point of View

In his 1958 *Dialectica* paper, Gödel introduced his idea of the consistency of arithmetic as an extension of the finitist point of view and instead of using the traditional Gentzen-style transfinite induction, he conceived of functionals of finite types inspired by Hilbert's himself inspired by Kronecker, as I have shown in Gauthier (2013a). The proof exposed above could be seen as a polynomial extension of the finitist arithmetical point of view and I would like to review briefly Gödel's attempt from a polynomial perspective. Presumably, Gödel who had insisted on an internal proof of consistency for arithmetic was dissatisfied with the proof in transfinite induction and proposed induction on all finite types. A polynomial interpretation of the functional *Dialectica* interpretation is thus suggested. The central notion of the *Dialectica* interpretation is the notion of computable function of finite types over the natural numbers. Types are derived by the following classes, type 0 is the type of natural numbers and the rule for generating types that stipulates that if σ and $\theta_1, \dots, \theta_n$ are types, then $(\sigma, \theta_1, \dots, \theta_n)$ is also a type. These are really functions on arguments from θ_1 to θ_n, that is functionals since these functions are over other functions for types > 0 i.e. beyond the natural numbers considered as individuals in the universe of types, the logic of the functional interpretation is intuitionistic in principle or constructivist in a loose sense, since Gödel considers that his interpretation is independent of intuitionist logic. Gödel's idea consists in translating a formula A of Heyting arithmetic into a computable function

$$\exists x \forall y A(x, y)$$

where A is quantifier-free.

We have then for the definitional equality for logic:

$$\begin{array}{ll} A \wedge B) & := \exists xu \forall vy (A \wedge B)' \\ (A \vee B) & := \exists zxu \forall vy (z = 0 \vee 1) \wedge (A \vee B)' \\ \forall z A z & := \exists x \forall zy A(xz, y)' \\ \exists z A z & := \exists zx \forall y A(x, z, y)' \\ A \rightarrow B) & := \exists UY \forall xv (A(x, Yxv) \rightarrow B(Ux, v))' \end{array}$$

For two recursive functionals, we have

$$F' = \exists y \forall z A(y, z, x)$$

and

$$G' = \exists v \forall w B(v, w, u)$$

where z, y, v and w are finite sequences or typed variables.

Implication

$$(F \supset G)' = \exists VZ\forall y, w[A(y, Z(y, w), x) \supset B(V(y), w, u)]$$

exhibits two functionals (with their proper variables) which subordinates "*zuorden*" the consequent to the antecedent. One could think here that the convolution product fulfills the role of computational extraction of the content in a more direct way if we translate

$$\exists x\forall x \supset \exists yBy = \sum_{0}^{n}\left(\sum \bar{a}_0 x + \sum b_0 x\right)^n$$

and

$$\forall xAx \supset \forall yBy = \prod_{0}^{n}\left(\prod \bar{a}_0 x \cdot \prod b_0 x\right)^n$$

in order to gain the formal content of forms (homogeneous polynomials) with implication or inclusion of contents "*Enthalten-Sein*" as in Kronecker.

In view of Gödel's Dialectica interpretation, one could wonder if logic is concrete or abstract, since it is the meaning of the concept which is at stake here. Gödel says—thinking probably of Gentzen—that the notion of accessibility "*Erreichbarkeit*" is an abstract concept which involves a kind of reflection on finite constructions. The notion of functional of finite simple type over the integers is such a concept. Gödel shows how to eliminate logic (implication and the quantifiers) by using a recursive functional

$$F = \exists y\forall yA(y, z, x)$$

where y and z, z and w are finite sequences of variables of arbitrary type and A is a quantifier-free expression with the variables x, y, z. In the case of implication,

$$\exists xHx \supset \exists yRy$$

formulas are simply identified with (two) functionals (with their proper variables) which coordinate "*zuordnen*" the consequent with the antecedent. I claim that the convolution product achieves the aim (of the computational extraction of the content) of implication in a direct fashion.

The formal content of forms (polynomials) in Kronecker's sense of entailment or inclusion "*Enthalten-Sein*" seems to call for such an interpretation by adjunction of indeterminates. Whether the calculus of content needs an abstract (intensional) setting is of foundational import. There is no doubt that the requirement of constructivity is satisfied, while the requirement of finiteness might be relaxed (with the effinite quantifier and infinite descent?). In any case, those requirements were the motivation for Gödel's extension of the finitist point of view in order to prove the consistency of arithmetic.

Recall that the *Dialectica* interpretation has inspired subsequent important work by Kreisel, Spector, Luckhardt, Scarpellini, Girard and more recently Kohlenbach (1998), Fereira, Oliva and Schwichtenberg in the proof mining project of classical analysis.[6] Note also that the functional interpretation is close to the no-counterexample interpretation introduced by Herbrand and pursued by Kreisel who introduced higher type functionals—Herbrand had used a negative interpretation, following Hilbert and Bernays (see Herbrand 1968), with his notion of primitive recursive function in the form

$$\neg A \equiv \neg B(x_\gamma f(x)_\gamma, z, g(x, z))$$

Kreisel (1961) has also wanted to use extensionally defined sentences in a "strong" interpretation of logical constants in a classical framework of truth conditions. Disjunction has here the form

$$a, M, X||B(a) \vee C(a)$$

and means

$$a, M, X||B(a) \text{ or } a, M, X||C(A),$$

that is, we have either B(a) or C(a) in all the submodels M of a theory X for the sentences of a finite type theory in the style of the *Dialectica* interpretation. Kreisel's attempt was not successful, but one may think that it is on this track that Cohen had his idea of forcing in his proof the independence of the continuum hypothesis in Zermelo-Fraenkel axiomatic set theory.

The forcing condition C for disjunction reads

$$C \Vdash (A \vee B) \leftrightarrow C \Vdash A \vee C \Vdash B$$

and for implication →

$$C \Vdash (A \to B) \leftrightarrow_{\text{def}} C \Vdash B \vee C \Vdash A$$

with

$$C \Vdash \neg\neg A \nleftrightarrow C \Vdash A.$$

Forcing conditions are compatible with intuitionistic logic, even if they were not intended to prove the consistency of arithmetic as in Gödel, but the consistency of the

[6] One may notice in that context that Kohlenbach with collaborators has adopted the *Dialectica* interpretation for Kreisel's proof mining project instead of Kreisel's own no-counter-example interpretation. This turn in logic is somewhat ironical when one remembers that Kreisel downgraded the *Dialectica* Interpretation in his *Gödel obituary* in the *Bibliographical Memoirs of the Royal Society* **26**, 1980.

negation of the continuum hypothesis in a minimal (transitive) model of Z-F. It is worth mentioning here that the injection of generic elements in the minimal model obeys closely the patterns of field extensions to the minimal Galois field, with the proviso that the procedure here is not constructive, since the generic extension comes in a block or a gender, while Kronecker introduces new indeterminates one by one—generic sets comes as infinite bunches of indeterminates in a set-theoretic universe!

Such a context is alien to Hilbert's finitism (see Hilbert 1904, 1926). Hilbert formulated the consistency problem in terms of primitive homogeneous equations that are conservative over logical inferences with consequences "*Folgerungen*" coded in homogeneous sequences "*Folgen*" regulated by the definitional equality = which Gödel has recuperated. For Hilbert, definitional equality provides the basis for consistency through the conservation of polynomial equations

$$x = x$$

and

$$x = y \wedge w(x) \rightarrow w(y)$$

where w is an arbitrary combination of objects x and y. Hilbert mentions composition and decomposition of numerical signs or numerals "*Auf – und Abbau der Zahlzeichen*" to which the proof procedure is reducible and he invokes here a kind of internal induction "*inhaltiche Induktion*" different from (external) mathematical induction. This is perfectly in agreement with Kronecker's line of thought in his finitist enterprise. Moreover, the elimination of ideal elements and the transfinite epsilon function in Hilbert and Bernays (1968–1970) proceeds in the same way as it is a true descent "*Abstieg*" in the sense of Fermat's arithmetic and Kronecker general arithmetic of forms. The recurrence process, as Herbrand calls it, must terminate in the finite and in accordance with Hilbert's idea of internal induction, it is not equivalent to complete induction as I have shown above (Chap. 5).

Gödel, who late in his philosophical career, was still preoccupied with a finitist (internal) proof of consistency of arithmetic, was unsatisfied with transfinite induction, but could not escape the impredicative theory of functionals over all finite types and by the same token could not match the finitist requirements of Kronecker and Hilbert, since Gödel wished to eliminate logic (the formal system) in his consistency proof of arithmetic. Our proof is meant to achieve that goal by appealing to a polynomial interpretation of the arithmetical syntax of the ring $K[x]$ of irreducible polynomials with coefficients in the field $k(x)$ under the guidance of finite descent in the Galois field $f(x)$ of finite elements. The descent is an eliminative procedure and we come down to the bottom polynomial equation with degrees

$$\deg 0 \neq \deg 1$$

or

$$\deg—\infty \neq \deg 0$$

which essentially means that the arithmetical content of a polynomial or polynomial function is computable in a finite time, a performance out of reach for the *Dialectica* functional interpretation reserved for the classical set-theoretic notion of recursive function.

Modular polynomial logic as the internal logic of arithmetic with its embedding in the general arithmetic of polynomials does not need a truth-conditional or set-theoretic semantics for the verification of $a = a$, only a syntax, the correction of which is secured by a calculus—from the Latin *calculi* meaning those small stones on which one can walk step by step (*Schritt zu Schritt*), following in Kronecker's steps. Since the polynomials in one variable (indeterminate) I have used in my proof define a decidable theory (like monadic first-order predicate logic),[7] I am confident I have kept pace with Kronecker's ascent in his finitist theory of higher forms (homogeneous polynomials) and at the same time with Fermat's descent in the finite field of modular polynomial arithmetic. I have shown that Fermat-Kronecker is internally consistent when embedded in a modular polynomial logic which reflects the polynomial structure. Undecidability as in Robinson-Davis-Putnam-Matijasevich theorem for Hilbert's 10th problem begins in polynomials with thirteen indeterminates. Polynomials in two variables are believed to be decidable with the gap between two and thirteen still undecided.

In our case, polynomials in one variable (indeterminate) with coefficients the natural numbers are sufficient to translate logical contents into a modular polynomial logic which reproduces the internal structure of Fermat-Kronecker arithmetic. In any case, multivariate polynomials from a computational point of view can be factored down to univariate polynomials with the use of a modular algorithm (e.g. Gröbner basis) for evaluation maps where the Euclidean algorithm or the generalized Euclidean algorithm, as we called Fermat descent, is at work.

[7] The analogy is misleading though, since the algebrization of logic from Boole for the sentential calculus to Tarski (cylindrical algebra) and Halmos (polyadic algebra) for the predicate calculus does not have the generality or the extent of the polynomial calculus which is, as Kronecker has emphasized, a general arithmetic with purely arithmetical content. In contrast then to the algebra of logic, the polynomial calculus of the theory of forms pertains to the arithmetization of logic. Categorical logic as an algebraic logic does not fare better since it does only translate isomorphically logical calculi into categorical structures (from Lawvere's elementary topos to closed cartesian categories or monoidal categories) only reflecting the surface features of deductive systems.

Chapter 8
Conclusion: Arithmetism Versus Logicism or Kronecker Contra Frege

8.1 Introduction: Arithmetical Philosophy

I understand arithmetical philosophy on the model of Russell's mathematical philosophy as an internal examination of arithmetical concepts—in the case of Russell, the internal examination of logical and general mathematical concepts (Russell 1919). From the mathematical point of view, Kronecker's general arithmetic could be seen as a successor to Newton's *Arithmetica Universalis* in the sense that both Newton and Kronecker wanted to integrate algebra into a general or universal arithmetic. The two texts "On the concept of number" (Kronecker 1887a,b) and his last lectures in Berlin "On the concept of number in mathematics" (see the German text edited by Boniface and Schappacher 2001) summarize Kronecker's conception of number or whole number (integer). Kronecker shares with Gauss the idea that the concept of number is in the mind or *a priori* while space is a property or relation in the external world; geometry and mechanics do not belong to the realm of pure mathematics since they have to represent and picture natural processes by using the concept of continuity whereas number inhabits the discrete universe of ordinals. Cardinals are invariants for the counting of groups of objects and equivalence is an intensional relation. The concrete combinatorial procedures (*Verfahren*) of addition, multiplication, congruence, etc. join with the general concepts of forms or homogeneous polynomials and their properties in the process of arithmetization.

There is a Kantian background to Kronecker's conception of number and Kronecker could not help but mock the philosophy of mathematics of post-Kantian philosophers like Schelling and Hegel.[1] Philosophical definitions of number are useless and one must start with the basic facts of a science (arithmetic here) and then fully elaborate the

[1] Kronecker does not reject all of Hegel and he quotes him approvingly on certain occasions, but he has not taken Hegel's conception of number seriously. One should mention however that contemporary mathematicians, like Lawvere in category theory, logicians in non-standard analysis and philosophers of logic (dialetheism and paraconsistent logic) have tried to make good of some of Hegel's ideas.

Y. Gauthier, *Towards an Arithmetical Logic*, Studies in Universal Logic,
DOI 10.1007/978-3-319-22087-1_8

conceptual determinations (*Begriffsbestimmungen*) of the subject matter. In that sense, pure mathematics was for Kronecker an experimental science in the construction of concepts in accord with Kant's dictum "Mathematics constructs concepts, philosophy analyzes them". Beyond this motto, Kronecker has hoped for a thorough arithmetization of mathematics, especially algebra; arithmetization of algebra has been the main task of his mathematical life as Kronecker confesses in a letter to Lipschitz (Kronecker 1886, pp. 181–182)

> On that occasion (the publication of his 1882 paper), I have found the long-sought foundations of my entire theory of forms which somehow brings to completion "the arithmetization of algebra" which has been the goal of my whole mathematical life; it is evident to me that at the same time arithmetic cannot dispense with the "association of forms" and that without them, it can only go astray in meandering thoughts (*Gedankengespinste*) as is the case with Dedekind, where the true nature of the matter is obscured rather than illuminated.
>
> (my translation)

Beyond the polemical tone, one sees the central role of his 1882 formulation and it is especially in that connection that Hermann Weyl has asserted the superiority of Kronecker's algorithmic approach in algebraic number theory with his domains of rationality (*Rationalitätsbereiche*) over Dedekind's concept of field (*Körper*). Association of forms means in that context homogeneous polynomials with integer coefficients and indeterminates, the central topic of Kronecker's major work (1882) "*Die Grundzüge einer arithmetischen Theorie der algebraischen Grössen*" ("On the Fundamental Features of an Arithmetical Theory of Algebraic Quantities").

As far as analysis is concerned, Kronecker has sought arithmetical invariants in the theory of elliptic functions and Weil has granted him the status of the pioneer of algebraic-arithmetic geometry. In those lectures of 1891, Kronecker comes back to the approximation method which he calls localization (*Isolierung*) of real roots of an algebraic equation in well-defined intervals of values for algebraic equalities and inequalities. In his criticism of Bolzano's theorem on intermediate values, Kronecker villifies Bolzano for having used the crudest means (*mit den rohesten Mitteln*) to obtain an analytical result which cannot be applied to the roots of an entire function. He also mentions Dirichlet's celebrated analytical proof on the infinity of primes in any arithmetical progression which he has discussed in his *Vorlesungen über Zahlentheorie* (Kronecker 1901). As K. Hensel puts it in the Preface, the methods of arithmetic and algebra rest on a finite number of steps, "*eine endliche Anzahl von Versuchen*", while analysis is built upon the concepts of continuity and limit. Here Kronecker tackles Dirichlet's transcendental proof on the infinity of primes in any arithmetical progression and introduces an arithmetical extension on a finite interval ($\mu \ldots \nu$) for two integers μ, ν where one must find at least one prime of the form $hm + r$ for m and r with no common divisors. Kronecker says that it is one case among others where arithmetic can do more than analysis and go beyond analytical methods. Dirichlet had used infinitesimal analysis (infinite series) in his proof and had confessed that what was still lacking were the right principles or conditions under which transcendental relations between indeterminate integers could be removed.

Kronecker defines arithmetic as pure mathematics free from space and time (see Boniface and Schappacher 2001, p. 227) and pays tribute to Gauss for having defined the true nature of arithmetic with the introduction of the concepts of composition (and decomposition into roots) of algebraic systems, in this case quadratic forms (*ibid.*, 262), and he credits him also with the introduction of the notion of indeterminates (*indeterminatae*). In his opposition to the analytical concepts of continuity and limit, Kronecker is echoing Gauss who in a 1831 letter to Schumacher did denounce the use of completed infinite quantities (*vollendete unendliche Grösse*) with the maxim "The infinite is only a manner of speech", "*Das Unendliche ist nur eine Façon de parler*". Kronecker could have made that maxim his own, but Leibniz had already qualified those infinitesimal quantities as useful fictions in the calculus. Kronecker would have been surprised though, had he studied more seriously Hegel's conception of the mathematical infinite, to learn that Hegel espoused the Leibnizian-Gaussian idea of a differential calculus dealing with the relative character of quantities rather than with the absolute limits of an infinite iterative process. In any case, Kronecker's view of the matter is in total agreement with Gauss' arithmetical philosophy and it is no surprise this time if he has opposed Cantor's practice of transfinite arithmetic which he has discarded as mathematical sophistry.

Kronecker even invited Cantor on one occasion to do real mathematics rather than theology! But both were in agreement that mathematics was a free creation of the human mind. They would disagree though on the kind of creations that could constitute real mathematics. For the finitist or constructivist mathematician there is a divide between tractable and intractable problems, as contemporary theoretical computer science would name it. Transfinite arithmetic in that sense is only tractable maybe in God's mind or in some ideal realm, as Cantor (or a Platonist) would believe. Only well-posed problems could have a definitive solution, Hilbert would advise. One example is Cantor's continuum hypothesis. Hilbert's failed attempt at a solution was ill-advised as the problem is intractable within Zermelo-Fraenkel set theory, since Gödel's and Cohen's results indicate that it is not decidable in Z-F, meaning that it is not a well-posed problem within that theory. Another example is E. Nelson's failure at proving the inconsistency of Peano arithmetic with a variant (Chaitin's incompressibility) of Gödel's incompleteness argument, Chaitin's and Gödel's ideas are couched in the infinististic language of Peano arithmetic with induction on the set of natural numbers and Gentzen had to resort on induction on transfinite ordinals while Gödel admitted that he had to adopt a transcendent point of view on finite arithmetic to obtain his incompleteness result. Of course, Robinson arithmetic, a weak subsystem of Peano arithmetic, does without Peano's induction postulate and is still subjected to Gödel's results, but it is only due to the fact that Robinson arithmetic is also a set-theoretical arithmetic with an unbounded quantification over the set of natural numbers as its *natural* universe and this confirms again the idea that consistency or inconsistency of Peano arithmetic is not provable by finite means. Constructivist or finitist foundations do not lead to philosophical fundamentalism, they serve only as a guide to clarify the distinction between the finite and the infinite or the non-finite. Poincaré, who was also an adversary of transfinite set theory, would have added that it is the infinite that is an approximation of the finite and not vice versa, a motto that Kronecker would have certainly endorsed and that could well serve as a finitist slogan.

8.2 Kronecker Today

Kronecker is present in contemporary mathematics as we have seen and his arithmetical theory is at the core of today's mathematical investigations in number theory and algebraic-arithmetic geometry. But his work remains unchartered territory to many mathematicians and most logicians and philosophers. From Hermann Weyl who has emphasized the supremacy of Kronecker's algebraic number theory over Dedekind's theory of ideals to André Weil who has ranked Kronecker as a most important pioneer in algebraic geometry and to Grothendieck and Langlands, all have been inspired by Kronecker's arithmetical foundations. Brouwer, Hadamard and Poincaré have borrowed his notion of winding number <*Windungszahl*> for the fixed-point theorem in analysis, but it is Kronecker's theory of finite fields (domains of rationality in Kronecker's idiom) and their extensions that constitutes the heart of the matter. Of course, it is in the tradition of Fermat, Gauss, Galois and Kummer that the idea of finite field has played a central rôle. Finite fields and their generalizations in algebraic varieties in the work of Weil, Chevalley and Grothendieck have become the basis of much current research, e.g. motivic integration and higher category or topoi theory. In that context, Grothendieck's notion of scheme is of Kroneckerian inspiration or, as Grothendieck says, is derived from the Kroneckerian point of view. As we have shown, it is Kronecker's theory of forms or homogeneous polynomials and divisor theory (modular systems) which serve as the foundation for the theory of algebraic varieties.

Arithmetic or general arithmetic as arithmetization of algebra in the hands of Kronecker means that arithmetical foundations reach up to the higher stages of the mathematical edifice. It is that far that arithmetic goes with arithmetical means alone and the direction of the search is the reverse of Frege's intention of seing how far he could go in arithmetic with logical means alone. We know that Frege stopped short at an early stage of the arithmetic of real numbers without gaining much mathematical terrain in his logicist programme. Frege's legacy rests with logicians and philosophers of mathematics or philosophers of language. Despite the efforts of contemporary logicists, Frege's programme cannot be rescued by logical means alone. The only outcome of mathematical interest seems to be the complexity theory of Frege's propositional systems and it has nothing to do with the logicist thesis. As far as logic is concerned, the salvage move deals with a second-order Hume principle of equality for numbers, transformed for the occasion as an extensional equality for number concepts. The end effect is that second-order Fregean arithmetic is equivalent to Peano arithmetic with no logical gain, if one adopts the Quinean dictum that second-order logic is no more <pure> logic. In any case, some have asked for a change of paradigms in philosophy of mathematics. H. M. Edwards, a mathematician and historian of mathematics has urged for a foundational shift from set theory and logic to Kronecker's constructivism and the logician and philosopher J. Hintikka has also pleaded for a retreat from Frege and logicism. But Kronecker remains ignored by a majority and a paradigm shift is not looming large at the time being.

From the mathematical point of view, there is no doubt that Kronecker's arithmetism is winning over Frege's logicism. From the philosophical point of view, there is not much philosophy in the strict sense in Kronecker's writings or in his mathematical practise beyond the decidedly finitist posture. The foundational motive of finitism is the leading force in the continuation of Kronecker's programme of arithmetization by logical means. Here comes Hilbert. Hilbert is the true initiator of mathematical logic which he called metamathematics—for proof theory or the theory of formal systems—and the first contender for the arithmetization of logic. I pretend that Hilbert has not only taken up Kronecker's programme of arithmetization of algebra, as is evident from Hilbert's *Nullstellensatz* and other algebraic results, but he has also followed Kronecker's lead in his introduction of functionals in his attempt to prove the consistency of arithmetic by arithmetical means, a project that was taken anew by Gödel in his extended finitist *Dialectica* Interpretation. Hilbert, as I have mentionned, may have been helped in that direction by his former student Hermann Weyl, who introduced in his *Das Kontinuum* (1918) procedures of iteration and substitution for ideal elements on the basis of the sequence of natural numbers in the spirit of Kronecker's general arithmetic. Philosophically speaking, Weyl was inspired by Husserl's phenomenological theory of judgment as is the contemporary Martin-Löf's idea of a constructive type theory, this time though without the Kroneckerian heritage of constructive general arithmetic.

The pivotal question of computability theory is the decision problem <*Entscheidungsproblem*> in Hilbert's terms. A decision method for a formal system S consists in determining in a finite number of steps if a given sentence is a theorem of S or not; the decision problem is then to find for the formal system S in question such a decision method or show that there is no such method. Hilbert's terminology in that context is <a finite number of operations> (Hilbert 1935, III, p. 154). What Hilbert called internal consistency <*innere Widerspruchslosigkeit*> is accessible from without through the axiomatization of logic, a finite process which must end up on the question of decidability. The procedure has to do with the internal logical deduction <*das innere logische Schliessen*> which must remain as close as possible to the inner structure of arithmetic. Hilbert gives here the example of his 1890 theorem on rational algebraic invariants which reduce to a finite number of invariants for the entire system of invariants; this is the theological proof denounced by Gordan—who produced later a one page proof!—but then Hilbert gave a proof of his result in 1893 after Kronecker's fashion of a finite number of steps (or operations). Hilbert there pays homage to Kronecker who had created the tools for the calculation of rational invariants in his theory of modular systems—see Gauthier (2002, p. 20 and ss). for mathematical and historical details. But Hilbert's notion of decidability has also given rise to the host of undecidable problems as negative answers to his 10th problem on a general or universal algorithm for rational solutions of diophantine equations (polynomials with integer coefficients). The undecidability results are stated in a set-theoretic context from Gödel to Turing (the halting problem) to Matijasevich and problems outside the field of logic in number theory, algebraic geometry and computer science as couched in the set-theoretical universe of abstract algorithmic methods. Particular questions in those fields have usually positive answers and applied proof theory having also more precise goals has more concrete results in extracting constructive content from non-constructive logic and mathematics.

Transcendental arithmetic, as I have called it, is inhabited by transcendent ideal creations like a supercompact cardinal in the universe V of higher set theory, but its inner models touch the ground of mundane arithmetic by downward transitive sets, other creatures in category theory or in the topos-theoretic multiverse are linked also to the same ground level through various descent techniques, arithmetic geometry is focused on the finite accounting of rational points on elliptic curves—Wiles' proof of Fermat's last theorem with the tools of algebraic geometry has a natural arithmetic grounding in the ring-theoretic Noetherian chain condition for prime numbers while Matijasevich's undecidability proof for Hilbert's 10th problem follows the path of a Fibonacci sequence of even integers. What this means is that if π is in the sky, the sky is still anchored in the earthly arithmetic of counting, if not in the rule-and-compass geometry of the terrestrial plane. In any event, the anchoring is secured in algebraic geometry by the general (polynomial) arithmetic of rational points as solutions of polynomial equations in a (finite) field K of an algebraic variety or scheme of finite type. Scheme is a Grothendienck creature of Kroneckerian ancestry, as we have seen; although Weil and Chevalley have worked on the concept, Grothendieck's abstract notion is derived from Kronecker's conception of modular systems. Finiteness (polynomial arithmetic) is all over the place (geometry), if one may say, and the internal logic of finite arithmetic grounds it all…

If Hilbert's proof theory is a <logical arithmetic> and Tarski's model theory a <logical algebra> to some extent dependent on Kronecker's arithmetism as I have attempted to show, one could suggest that constructive algebra in the steps of Kronecker's general arithmetic may become the arithmetic of the logic of computer science or the true algorithmic logic. The notion of Gröbner basis is a nice illustration of such a programme with its organon of primitive elements in a polynomial ring furnishing finite algorithms for the Euclidean division of large common divisors or for Gaussian elimination in matrix theory and further in integral linear programmation where the programme variables are integers. Of course, algorithms abound in arithmetic and number theory, from Euclidean division algorithm and Erastothenes sieve to the various sieve methods. But the computer science agenda looks like a combination of Fermat's descent and Kronecker's divisor theory. The procedures are concrete here and cannot be compared with the abstract computation techniques associated with the logical representation and translation of computer programmes; the symbolic concrete implementation is of the essence in constructive algebra and could be compared with the recent result of Agrawal et al. (2004) which use Fermat's <little> theorem,

$$a^{p-1} \equiv 1 (mod\, p)$$

where p is a prime number and a is a prime relative to p. It is such a congruence which provides the algorithm for the factorization of large primes and one can think that the polynomial time needed for the actual computation is derived from a phenomenon anterior to the computational programme, a phenomenon ingrained in the internal logic of modular polynomial arithmetic (the FK or Fermat-Kronecher arithmetic). On a different scale, Voevodsky's idea of univalent foundations is a far cry from radical constructive mathematics although it is supposedly representable in type theory (Martin-Löf's intuitionistic type theory) and implementable in Coq's system for the registration of proofs. Algebraic theories in a categorical setting cannot provide either the concrete foundations of constructive algebra since they rest on formal analogies (interpretations) between logic, algebra and topology ultimately based on polynomials in an abstract general nonsensical! picture. For example, the univalence axiom in homotopy theory says simply that isomorphic structures are identical and that amounts to homotopical equivalence possibly implementable in a computer programme for proof assistance or verification. The alleged content of the theory is geometric, while the formal calculus, if successful as it is assumed to be, must rely on polynomial arithmetic in order to be consistent. Eventually, the abstract construction must be grounded on concrete finite proof derivations with a reduction of higher-level structures to elementary ones, which is the domain of arithmetic.

I could have argued in that connection that Kronecker's higher-order form theory is the mother (or the paradigm) of all type theories, at least in the tradition of Hilbert's functionals, von Neumann's cumulative rank structure for set theory, Gödel's functional interpretation and constructive type theories. Russell didn't probably know about Kronecker's construction, but his idea of a finite logical type hierarchy is close enough to be translated into the arithmetical polynomial structure. It should be noted that Frege used the notion of <*Stufe*> or level in his 1893 *Grundgesetze der Arithmetik*, but they were not meant as Kronecker's levels or ranks of polynomials, but the ordering of concepts and concepts of concepts (of numbers), and it is not clear that the Fregean logical hierarchy of concepts has a mathematical (Kroneckerian) origin, but it is certainly the inspiration for the Russellian simple theory of types with a first level of individuals and higher levels of properties or predicates like in higher-order logic.

Since the notion of *Stufe* was originally used in the algebraic theory of quadratic forms, it could be couched naturally in Kronecker's general theory of forms or homogeneous polynomials, as I have shown in Chap. 1. As for transfinite type theories of set-theoretic descent, may they be called intuitionistic or constructive, they rely on resources beyond finitistic foundations and as such should be considered as transarithmetical ideal copies of the higher-order polynomial theory originated by Kronecker. Predicativity in the context of constructive type theory means simply that one doesn't want the full universe of sets ($U \in U$) in one embrace, but stops at a high enough cardinal to crown large (big) sets, categories, types, topoi and homotopoi. From beyond and above there, it is hard to imagine a safe descent to the firm ground of *real* classical arithmetic (elementary number theory)! The claim of constructivity for constructive type theory (and related theories) consists mainly in the rejection of LEM, the law of excluded middle, but once you have climbed to ω or ω^{ω} and so on up the Church-Kleene recursive ordinals or to ϵ_0, the limit ordinal of the ω hierarchy, you have transgressed the prohibition, since you have used a double negation on an infinite set to identify transfinite induction *à la* Gentzen with infinite descent, as we have seen in Chap. 6. Even if you use quantifier-free induction, you have to pass over **all** finite ordinals to get to the first ω and then proceed to ω^{ω} for the ordinal of primitive recursive arithmetic PRA or down to ω^3 for elementary function arithmetic EFA with bounded quantifiers. One could argue under those circumstances that formalized arithmetic, Peano arithmetic and its subsystems e.g. Robinson arithmetic, cannot bypass ω for having essentially a set-theoretical, metamathematical, undercover clothing. Indeed, classical arithmetic (elementary or constructive number theory) is an entirely different apparel with an internal logic of its own with (in) finite descent and finite polynomials, the (FK) Fermat-Kronecker arithmetic. However, constructive type theory claims to be able to get beyond ω to higher inductive types with the help of a well-founded induction – induction on the subsets of the infinite set $\aleph_0$ of natural numbers

– equivalent to transfinite induction. The protocole, ordinal encoding, is reflected in Coq (after Thierry Coquand), a proof assistant for checking and verifying proofs once they are done, that is after the fact. Coq as a calculus of constructions and constructors of operations in a functional programming language with types is a computerized representation of proofs that mimick constructive type theory through specification and implementation of programmes for value-dependent inductive types. The procedure indeed constructs types inductively or iteratively as they come in as mathematical data, but here constructive is meant in the broad sense of construction at large in a building site. Homotopy theory *à la* Voevodski is an attempt to combine different approaches into a unified univalent scheme—the univalent axiom—whose foundational significance is still unclear despite some high expectations. Rather, the homotopical or homotopological enterprise should be looked upon as an interesting general framework for the presentation and representation of abstract logical and mathematical structures, an unexpected progeny maybe of the Bourbaki structuralist school or alternatively as a hybrid creature between a functional language (typed λ-calculus) and a geometric theory (of topological spaces) couched in the univalent language of equivalence classes (isomorphisms) reducible to logical identities. What is the gain for logic and mathematics in that joint enterprise remains to be seen. From the finitist stance, a consistency proof for classical mathematics is hopeless, as is the inconsistency proof for Peano's arithmetic as advertised by Ed Nelson, for it is only from a transcendental point of view (or *the view from above*) advocated by Gödel in his incompleteness result that one could raise such questions. Of course, the finitist views those questions from below and cannot but refuse to imagine a Platonic realm of ideal mathematics beyond the horizon of mathematical activity and its foundational justification.

Arithmetical logic is the internal logic of arithmetic in the precise sense that there is a correspondence between logical propositions (sentences) and arithmetical formulas (polynomials) with logical constants translated into arithmetical operations. Set-theoretic foundations are still present in type theory à la Martin-Löf and in homotopy theory *à la* Voevodsky as an inaccessible ordinal is needed to cap the higher-order or higher-dimensional structures and constructs. No doubt that these ideal entities would be deemed transcendental by Kronecker and reducible or removable as ideal elements by Hilbert. And the transfinite induction required, as a kind of analytic continuation, cannot be constructively justified. Arithmetical foundations are devoid of geometric or set-theoretic content insofar as they espouse the concrete procedures of a finite calculus on integers and rational numbers. Polynomial arithmetic with integer coefficients and indeterminates (free variables) is a straightforward generalization of elementary arithmetic into Kronecker's general arithmetic in the passage from the ring of polynomials to the field of rational numbers and other finite fields. Arithmetical logic is likewise extended to a modular polynomial logic—with a congruence relation to accommodate division for the field of rational numbers—if one considers that Kronecker's general arithmetic is associated to a divisor theory which is itself in a close relationship to the generalized Euclidean division algorithm, that is essentially Fermat's (in)finite descent on finite fields. Thus Fermat-Kronecker (FK) arithmetic is the right characterization of an internal logic of arithmetic, a modular polynomial logic intended as a descriptive theory of arithmetical foundations for mathematics.

Surprisingly, the predicativist Nelson thought that he could use an incompressibility argument *à la* Chaitin while Chaitin's own incompleteness theorem is inspired by Berry's paradox and assumes at the same time the denumerable set $\aleph_0$ of natural numbers with its implied consistency. As a related issue, Voevodsky's ill conceived discussion of the possible inconsistency of Peano arithmetic is symptomatic of a foundational disarray in infinitary mathematics, may it be in category theory, (higher) topoi theory, homotopy theory and its companion constructive type theory (despite its name). All these theories reach beyond PA to higher ZF theory looking for at least an inaccessible cardinal in the transfinite cumulative hierarchy of ordinals. Even Gentzen's proof of the consistency of PA using the limit ϵ_0 is transcendent in that respect, despite the constructivist claim on the part of many logicians. The transcendent or transcendental viewpoint from above cannot be recovered or descended to the finitist standpoint and there is simply no hope for a consistency (or inconsistency) proof for infinitary mathematics as there is no use of the consistency question for univalent foundations of homotopy theory or constructive type theory with or without a Coq verifier as a witness. Grothendieck himself didn't care much about doing mathematics in U-topia as the totality of all topoi and their respective universes. It is no surprise then to see one of the main promoters of homotopy theory, S. Awodey, expressed his scepticism as to the foundational significance of the univalent foundations of homotopy theory. On the opposite side of presumed abstract or ≪ continuous ≫ foundations, finite computability and finite results with finitistic concrete or ≪ discrete ≫ objects constitute the safe haven and the solid rock of constructive mathematics.

8.3 Arithmetization of Geometry: From Algebraic Geometry to Arithmetic Geometry

From the arithmetic of the triangle with a quadratic form to the arithmetic of the circle in Kummer's cyclotomy theory and what could be called *ellipotomy* in Kronecker's theory of the ellipse through the arithmetic theory of the plane, the surface and the sphere from Descartes and Desargues to Gauss and Riemann, arithmetization of geometry seems to be a major trend in contemporary mathematics and results like Perelman's proof of Poincaré's conjecture (with the idea of a finite fundamental group) or Mochizuki's putative proof of the *abc* conjecture in number theory using the arithmetic of the elliptic curves, as the celebrated results of Weil, Deligne, Faltings and Wiles, all point to a vast programme of arithmetization of geometry. Mochizuki's intended proof points to an arithmetic version of Teichmüller theory of holomorphic (continuous complex) structures with indeterminates or an indeterminate isomorphism, notions which suggest an extended Kroneckerian landscape in Mochizuki's own programme of general arithmetic geometry. Whether the proof of the abc conjecture can be carried out is still an unresolved question, but it remains that the conjecture itself is central in the mathematical panorama (see for example Granville and Tucker 2002, It's as easy as *abc*, *Notices of the AMS*, pp. 1224–1231). One could conclude here that if arithmetic is not always the point of departure of mathematical theories, it is often their finishing line or their ultimate outcome, as Kronecker had stressed in his time and as one should still emphasize nowadays. One important conjecture yet unproven is the celebrated Riemann Hypothesis. Riemann had conjectured in a 1859 paper that the zeros (roots) of the zeta function $\zeta(s)$ over complex numbers > 1 have all real part $1/2$; $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ is related to the prime numbers through the identity:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod \frac{1}{1-p^s} \qquad \text{for the primes } p \text{ of the Euler product.}$$

It has also connections with physics via the generalization of global Dirichlet L-functions from statistical mechanics to noncommutative geometry, quantum field theory, M-theory, etc., but these connections or analogies may not be deep enough to help with the proof of the conjecture. Riemann had left aside his hypothesis saying in a note that it was secondary to his main arithmetical objective—which was the search for the number of primes below a given n. And Riemann turned decidedly to geometry and its hypotheses, but not without arithmetic underpinnings.

In his 1867 *Über die Hypothesen welche der Geometrie liegen*, Riemann points out that the construction of manifolds (*Mannigfaltigkeiten*) or n-dimensional spaces is based on arithmetical metrical measures and their realization rests ultimately on the application of the Pythagorean theorem in the infinitely small. A Riemanniann surface as a complex analytic manifold can be subjected to the same treatment when metrics are introduced into the one-dimensional surface. I recall that Cantor had originally called his set theory (*Mengenlehre*) by the name *Mannigfaltigkeitslehre* or theory of multiplicities. The name itself, translated into English as manifold (in French <*variétés*>) means the same thing as polynomials or multiple divisions. The connexion between the two is not accidental and Brouwer who knew the meaning of words had adopted the name <spreads> (*spreiding* in Dutch) to convey the same idea—the connexion extends to a bridge between geometry and algebra! An other extended bridge can be built that connects Brouwer's algebraic topology to algebraic and arithmetic geometry. Among the many generalizations of Brouwer's fixed-point theorem, Lefschetz' theorem with its fixed-point counting formula plays an important rôle, for example, in Deligne's proof of the Weil conjectures for arbitrary algebraic varieties.

In the Riemannian context, the infinitesimal ideas are derived from Gauss' theory of curved surfaces with the metric invariant ds^2, the quadratic (polynomial) groundform. This arithmetical geometry is the foundation of the theory of abstract spaces from the vector calculus on metric spaces in Grassmann's *Ausdehnungslehre* (theory of extension) to Hausdorff and Fréchet (theory of metric spaces) or Choquet (theory of capacities). Nowadays, Konsevich's motivic integration or Voevodsky's homotopy theory (and higher topoi theory) look at geometric forms and spatial volumes in search of an arithmetical content which they recover by descending to discrete (simplicial) sets and to fundamental polynomials—also called forms by Kronecker. In the case of Voevodsky, it is instructive to know that he started with finite-valued homotopy types with an integer n to make them correspond to algebraic varieties (as untyped spaces) and then come back in the so-called univalent foundational programme to type theory with transfinite types in the hope of recovering some constructive content beyond the univalent axiom of (logical) identity expanding into homotopic equivalence through paths between isomorphic structures or spaces. Homotopy type theory is then typified in a companion so-called constructive type theory climbing up a parallel transfinite scale assisted by a programming language (Coq or Agda) that typically recopy proofs of theorems. In another parallel universe the amplituhedron, a recent invention in quantum field theory, is a geometric form endowed with a positive Grassmannian, that is an internal arithmetical structure for the calculation of amplitudes in terms of *k*-planes filling up an *n*-dimensional space.

The hypothesis I have been defending here is that mathematical imagination can freely create abstract spaces or geometric forms, but these are abstractions that acquire concrete meaning through the arithmetical operations which innervate all mathematical structures. For example, motives in Grothendieck's programme of algebraic geometry were designed as a systematic study of algebraic varieties in order to articulate the numerical equivalences embodied in their fundamental groups (of cycle classes on subvarieties that is, algebraic correspondences defined on the integers). One can find a similar <motivation> in Descartes' *Dioptrics* where he speaks of geometric motives in order to compose the <embroidery> of geometric motives for algebraic curves, a theme which Descartes introduced at the birth of arithmetic algebraic geometry. After Riemann, geometry has become a Riemannian manifold and the notion of space in algebraic geometry has been algebrized as notions of vector spaces and algebraic spaces (and even arithmetic spaces); at the same time, topology as study of spaces has been algebrized from Brouwer on to Grothendieck and the notion of topos as a generalization of topological space has transformed into étale topology a generalization of Euclidean space, itself an algebraic object.

The geometry of algebraic varieties bears upon arithmetic geometry, since it has to do with rings, number fields and function fields in the tradition of Kronecker's theory of moduli systems which has guided Grothendieck's <schematic> programme (with the notion of <*schème*>), as well as Langland's programme with its number-theoretic <correspondences>. Diophantine equations and Diophantine approximation also belong to arithmetic geometry which could be defined as the study of the intrinsic arithmetical structures of algebraic varieties. If the starting point of algebraic geometry was the study of systems of polynomial equations, it has lifted up to the height of abstract spaces and varieties, the modern name for manifolds, but from the higher planes of abstraction, there is a natural descent to the ground level of effective calculations and the internal operations of arithmetical logic. The abstract language of geometric forms and abstract structures is nonetheless necessary to achieve the ultimate goal of reconciling the abstract and the concrete the continuous and the discrete, geometry and arithmetic. What we could call Grothendieck's dream is summarized in those few words: in his unpublished testament *Récoltes et semailles*, he speaks of a river where all the king's horses would come and drink "tous les chevaux du roi pourraient y boire ensemble" (drawn from a beautiful traditional *French song Aux marches du palais*). Let me remark that Grothendieck's dream is similar to Kronecker's dream of unifying *arithmetic*, algebra and analysis, but without geometry which was not an apriori mathematical theory for Kronecker. Grothendieck had chosen to express his dream in a categorical language and a topos-theoretic vernacular idiom, but his dream transcends those linguistic *limitations*. Category theory, a descendant of homological algebra and topoi theory, a generalization of the notion of topological space, are the favorite candidates for mathematical generality and geometric abstraction, but they must toil hard to redescend to the ground level of concrete content. Fortunately, descent techniques in homology and cohomology devised by Weil are successful in regaining most of the ground, especially in arithmetic geometry. However, higher topoi theory and homotopy theory still need to climb down the transfinite ladder of the set-theoretic and type-theoretic universes, as we have seen.

Arithmetic is the common ground of all mathematical theories, including the all-encompassing category theory. There is no category-theoretic foundation of arithmetic or number theory, let alone pure number theory. Category theory has evolved from homological algebra to a general theory of symmetrical situations in mathematics with functors and natural transformations or equivalences (isomorphisms for homology and homotopy) and logic (equivalence classes). Here the notion of morphism, that is a map between objects or structures, becomes a functor between categories and even that most general notion can be approximated by *polynomial* functors in the Goodwillie calculus mimicking the approximation of a Taylor series by finite polynomial functions of an entire (complex-valued) function . Category theory is a diagrammatic art and a calculus of diagrams designed to represent graphically algebraic relations by analogies between different mathematical structures. As a theory of classification of structures, model theory stands in clear opposition to category theory. Here a theory of infinite structures uses definable sets (defined by first-order logic) to access categoricity in uncountable power via the compactness and the Löwenheim-Skolem theorems to reach out to higher planes of parent mathematical theories where stability and invariance describe common features in various mathematical theories like algebraic and arithmetic geometry, complex manifolds, differential equations, finite structures in search for a unified theory. The work of Morley, Shelah and Hrushovski among other model theorists in that connection remains unmatched by “structuralist” category theorists, but again the unification in this case has to boil down to some arithmetic foundational common ground which is not yet in view. In the case of category theory, analogies extend beyond mathematics into logic, physics and linguistics among many other disciplines. For logic, closed cartesian—with a cartesian product—categories provide a link (isomorphism) between simply-typed lambda calculus and intuitionistic logic via the Curry–Howard isomorphism while braided monoidal categories reach larger or more numerous logical systems with enriched categorical structure. The same is true for the notion of topos which once baptized elementary topos (by Lawvere) becomes a powerful machinery with adjoint functors as substitutes for logical notions. By the way, the notion of topos, invented by Grothendieck as a generalization of the notion of topological space is endowed with a categorical structure, but the category of topological spaces is not cartesian closed and therefore is not a topos : the general notion of topos does not <cover> the notion of topological space, there is no topos of topoi therefore the many universes imagined by Grothendieck! In that connection, a full universe of sets or classes, categories and topoi might be inconsistent, as Voevodsky admits, but then the inaccessible ordinal his univalent foundations scheme seems to require could belong to an inconsistent universe. Needless to say, Max Tegmark own mathematical (Platonist or Pythagorean) universe—see his book *Our Mathematical Universe*—is saturated with inconsistencies and nonsensical analogies. I recall here that the general no-cloning or no-homeomorphism theorem forbids analogies of any kind beyond crude isomorphisms. As I have said (Chap. 5), the theorem applies to any many-dimensional not only physical, but also mathematical universe (multiverse) of any dimension in any theory of sets, classes, types, categories or topoi and <homotopoi> (from homotopy theory). It is in a way a no-go theorem for universal or inter-universal (strict, exact or deep) analogies. On the logical, philosophical and metaphysical side of things, not everything is possible in one world, because there is a unique (zero to *n*-dimensional) actual world (like a point or a line a surface at infinity) and Leibniz could dream of such a world as the best of all the possible worlds only God could dream of and even in God's view that infinity of infinities, as Leibniz expressed himself in his 1697 opusculum *De rerum originatione radicali*, could only be an *imperfect* analogous multitude of combinations—*pace* possible worlds semantics which also falls prey to the combinatorial argument! Apologists of the possible worlds hypothesis like David Lewis invoke a recombination or patching principle of parts provided they occupy different spacetime locations and this calls for higher dimensions for which the no-homeomorphism idea is valid along with the indiscernability and domain invariance corollaries as explained in Chap. 5.

The analogical way is not the pure logical direct route. That is not to say however that pictures and patterns are not useful in logic and mathematics as representations of concepts and surely category theory is a study of concepts, mathematical and extra-mathematical, sometimes reduced to a taxonomy of structures. But in the context of the connectedness of the abstract and the concrete the paradigmatic case is Grothendieck's motivic theory of geometrico-arithmetical correspondences in algebraic geometry. Here again there is a *counting* of rational points or measures in motivic theory (e.g. motivic integration). However some category theorists have followed the lead of Grothendieck and have built (silk or lace?) inter-theoretical or inter-universal bridges between mathematical continents as if categories and structures (after the 1965 book title of Charles Ehresmann) and topoi were to achieve the grand unification that was dreamed of by the Bourbaki school—Grothendieck is a rebellious child of that school—although the axiomatic ideal of French mathematical structuralism was alien to the American categorical spirit of Eilenberg and MacLane. Analogies abound in mathematics and the most fruitful ones are deeply rooted in mathematical theories. A paradigmatic example is the analogy (deep relationship, correspondence or inner connection are better words here) between number fields and function fields, an idea which originated in Kronecker's theory of forms and which has been pursued by a long chain of major mathematicians in algebraic number theory from Hilbert to Hermann Weyl and André Weil, as well as in Grothendieck's and Langlands' programmes (see Chaps. 4 and 6). Here analogies work more like undercurrents or tectonic plates moving towards each other to create a uniform stratum. In any case, bridges (mobile or not) themselves don't hang in the air and they eventually land and sit down both ends on their fulcrum, the solid rock of the finite arithmetic of polynomials.

8.4 From Geometry of Numbers to Physical Geometry and Physics

The scope of arithmetical foundations is not limited to pure mathematics, it extends to mathematical physics and to theoretical physics, as I have tried to show. Hilbert, von Neumann, Weyl had an idea of a <*physikalische Logik*>, a physical logic with a polynomial probability calculus as an arithmetical foundation. Hilbert wished to axiomatize the notion of probability to deprive it of its mystical character and Kolmogorov has succeeded in providing such an axiomatization. A physics based on algorithms and probability theory with local notions (states and observers) is certainly in line with a constructivist outlook that privileges computations over metaphysical constructions, e.g. determinism and ontological realism. In relativity theory, Minkowski's spacetime is a good candidate for an arithmetical treatment (with the geometry of numbers in the background) and in quantum theory and cosmology renormalization procedures are meant to dissipate infinities in the field of physics. In his 1926 paper <On the Infinite>, Hilbert stated that the infinite is nowhere to be found in the physical world or even in physical theories, but that the infinite could have a place in our thought. The radical constructivist posture here consists in eradicating the infinite from our mathematical, logical and scientific thought altogether. Arithmetical logic can achieve that goal if it obeys the Kroneckerian incentive of proceeding in a finite number of steps <*eine endliche Anzahl von Versuchen*> as echoed by Hensel in Kronecker (1901).

8.5 Arithmetization of Logic

The arithmetization of logic began with Hilbert and was pursued by Skolem, Herbrand, Gödel, Tarski—for the algebrization of logic—Turing and theoretical computer science. Brouwer has not contributed to logic—his heir Heyting did—or number theory, but he has introduced the creating subject and its construction of the mathematical continuum as a process in becoming <*ein Prozess im Werden*> in his theory of sequences, lawlike sequences , choice sequences and lawless sequences on the foundation of the arithmetical unlimited (*effinite*) sequence of natural numbers. A natural consequence of the arithmetization of logic should be an arithmetical logic as an internal logic of arithmetic, as I have argued, and if pure number theory, not formalized <external> Peano arithmetic, uses Fermat's infinite descent as an induction or *récurrence*—Poincaré's preferred idiom—procedure instead of complete induction on the infinite set of natural numbers or transfinite induction on the infinite set of denumerable ordinals and if the deductive process must be made secure (Hilbert's <*Sicherheit*>), it has to be performed within arithmetic itself, as Kronecker claimed internal truth and provability <*innere Wahrheit und Folgerichtigkeit*> for his general arithmetic. Besides Fermat's descent, Kronecker's theory of forms provides with the internal content—contentual or internal logic—of the modular polynomial logic sufficient to encompass the conservative extensions of finite arithmetic and logic. Internal consistency or self-consistency is achieved with arithmetical syntactical means alone—with elementary arithmetic as a minimal model, if one wishes some semantical additional flavor. No set-theoretic model notion is invoked and we do not refer anywhere to the $\aleph_0$ set of natural numbers, only to the unlimited sequence of natural numbers equipped with the arithmetical operations of addition, multiplication, substraction, division (for the field of rational numbers) and polynomial (limited) exponentiation. Our interpretation of implication is crucial, we use a binomial formulation of $a \to b$ as $(a^- + b)$ for $\neg a \vee b$ to express the arithmetical content of logical inference. There is no involvement of logic proper, since logical operations are directly interpreted in a polynomial calculus with a congruence relation to cover inequality as a local negation. Logic in the arithmetical setting has only a secondary role, it serves as an ancillary formal device for the presentation or the exhibition of the arithmetical content. The designation <modular polynomial logic> might sound as a misnomer, insofar as logic is concerned, but insisting on internal logic, Hilbert's <*inhaltiches Schliessen*>, removes the logical or formal stint. This is not to say that formal logic is of no import for mathematics, only that as the hygiene of the mathematical discourse, as Weil ventured to say to the displeasure of many a logician, it must be used strictly at the threshold of internal logic. Internal logic of arithmetic could be looked at as first-order arithmetic without the formal apparatus of classical logic and as a constructive foundational theory for the whole of mathematics, it could also constitute the basis for the hierarchy of logics by weighing their constructive content, from arithmetic to algebra to geometry to algebraic and arithmetic geometry up to higher set theory and category or topoi theory (and *homotopoi* theory!). In that perspective, arithmetical logic as a building stone for the internal logic of mathematics is only a starting point.

References

W. ACKERMANN (1940) : Zur Widerspruchsfreiheit der reinen Zahlentheorie. *Mathematische Annalen*, 117(2):162–194.

M. AGRAWAL, N. KAYAL and N. SAXENA (2004) : PRIMES is in P. *Annals of Mathematics*, 160:781–793.

J. AVIGAD (2003) : Number Theory and Elementary Arithmetic. *Philosophia Mathematica*, XI:257–284.

A. BAKER (1975) : *Transcendental Number Theory*. London, Cambridge, University Press.

E. BISHOP (1967) : *Foundations of Constructive Analysis*. New York, McGraw-Hill.

E. BISHOP (1970) : Mathematics as a Numerical Language. *In Intuitionism and Proof Theory*, 53–71. North-Holland, Amsterdam and New-York.

J. BONIFACE and N. SCHAPPACHER (2001) : Sur le concept de nombre en mathématique. Cours inédit de Leopold Kronecker à Berlin en 1891. *Revue d'histoire des mathématiques*, 7:207–275.

N. BOURBAKI (1970) : *Théorie des ensembles*. Hermann, Paris.

L. E. J. BROUWER (1910) : Beweis der Invarianz der Dimensionenzahl. *Math. Annalen*, 70:161–165.

L. E. J BROUWER (1912a) : Beweis der Invarianz des n-dimensionalen Gebietes. *Math. Annalen*, 71:305–313.

L. E. J. BROUWER (1912b) : Über Abbildungen von Mannigfaltigkeiten. *Math*, 38(71):97–115.

L.E.J. BROUWER (1975) : *Collected Works, vol. I*. North-Holland, Oxford, Amsterdam.

J. BURGESS (2005) : *Fixing Frege*. Princeton University Press, Princeton, NJ.

V. BUSEK and M. HILLERY (1996) : Quantum Copying: Beyond the No-Cloning Theorem. *arXiv:quant-ph/19607018v1*.

S.R. BUSS (1986) : *Bounded Arithmetic*. Bibliopolis, Napoli.

S.R. BUSS and P.J. SCOTT, eds (1990) : *Feasible Mathematics*. Birkhaüser, Basel.

G. CANTOR (1947) : *Abhandlungen mathematischen und philosophischen Inhalts, hrsg. v. Zermelo u. A. Fraenkel*. Gauthier-Villars, Paris.

G. CANTOR (1966) : Über einer Satz aus der Theorie der stetigen Mannigfaltigkeiten. *Abhandlungen mathematisch und philosophischen Inhalts, Georg Olms, Hildesheim :134–138*.

A. CARBONE and S. SEMMES (1997) : Making proof without *modus ponens*: an introduction to the combinatorics and complexity of cut elimination. *Bulletin (new Series) of the American Mathematical Society*, 34(2):131–159.

A. CAUCHY (1847) : *Oeuvres complètes, IIe série, tome III*. Gauthier-Villars, Paris.

J. CONWAY and S. KOCHEN (2006) : The free will theorem. *Found. Physics*, 36:1441–1473.

J. CONWAY and S. KOCHEN (2009) : The strong free will theorem. *Not. Amer. Math. Soc.*, 56:226–232.

S. COOK and A. URQUHART (1993) : Functional Interpretations of Feasibly Constructive Arithmetic. *Annals of Pure and Applied Logic*, 63:103–200.

T. COQUAND (2008) : Herbrand et le programme de Hilbert. *Gazette des Mathématiciens*, 118:17–28.

A. DAVENPORT (1968) : *The Higher Arithmetic*. Chap. VI. Hutchinson University Library, London.

Y. Gauthier, *Towards an Arithmetical Logic*, Studies in Universal Logic,
DOI 10.1007/978-3-319-22087-1

P. de FERMAT (1899) : *Oeuvres*, volume II. Gauthier-Villars, Paris.

R. DEDEKIND (1965) : *Was sind und was sollen die Zahlen. Stetigkeit und irrationale Zahlen*. Fried. Vieweg und Sohn, Braunschweig.

D. DIECKS (1982) : Communication by EPR devices. *Phys. Lett. A*, 92:271–272.

J. DIEUDONNÉ (1974) : *Cours de Géométrie Algébrique 1*. PUF, Paris.

J. DOWKER and D. KENT (1996) : On the Consistent Histories Approach to Quantum Mechanics. *Journal of Statistical Mechanics*, 82((5/6)):1575–1646.

M. DUMMETT (2000) : *Elements of Intuitionism*. Oxford University Press, Oxford, 2nd édition.

H. M. EDWARDS (1987a) : *Divisor Theory*. Birkhaüser, Basel.

H. M. EDWARDS (1987b) : An appreciation of Kronecker. *The Mathematical Intelligencer*, 9(1):28–35.

H. M. EDWARDS (1992) : Kronecker's arithmetic theory of algebraic quantities. *Jahresbericht der Deutschen Mathematiker Vereinigung*, 94(3):130–139.

H. M. EDWARDS, O. NEUMANN and W. PURKERT (1982) : Dedekinds "Bunte Bemerkungen" zu Kroneckers "Grundzüge". *Archive for History of Exact Sciences*, 27(1):49–85.

G. FALTINGS and G. WÜSTHOLZ (1984) : *Rational Points*. Vieweg Verlag, Braunschweig-Wiesbaden.

S. FEFERMAN (1960) : Arithmetization of metamathematics in a general setting. *Fundamenta mathematicae*, XLIX:35–92.

G. FREGE (1983) : *Grundgesetze der Arithmetik*. H. Pohle, Jena.

Y. GAUTHIER (1976) : *Fondements des mathématiques. Introduction à une philosophie constructiviste*. P.U.M., Montréal.

Y. GAUTHIER (1978) : Foundational Problems of Number Theory. *Notre Dame Journal of Formal Logic*, 19:92–100.

Y. GAUTHIER (1983a) : Le constructivisme de Herbrand. *Journal of Symbolic Logic*, 48(4):1230.

Y. GAUTHIER (1983b) : Quantum Mechanics and the Local Observer. *Int. J. Theor, Physics*, 72:1141–1152.

Y. GAUTHIER (1985) : A Theory of Local Negation. The Model and Some Applications. *Archiv für mathematische Logik und Grundlagenforschung*, 25:127–143.

Y. GAUTHIER (1989) : Finite Arithmetic with Infinite Descent. *Dialectica*, 43(4):329–337.

Y. GAUTHIER (1991) : *De la logique interne*. Vrin, Paris.

Y. GAUTHIER (1994) : Hilbert and the Internal Logic of Mathematics. *Synthese*, 101:1–14.

Y. GAUTHIER (1994b) : Review of A. Weil The Apprenticeship of a Mathematician. *Modern Logic*, Vol 4. no. 1 (1994):97–100.

Y. GAUTHIER (1997a) : *Logique et fondements des mathématiques*. Diderot, Paris.

Y. GAUTHIER (1997b) : *La logique interne. Modèles et applications*. Diderot, Paris.

Y. GAUTHIER (1998) : A Polynomial Translation of Gödel's Functional Interpretation. *Bulletin of the Section of Logic, University of Łódź*, 27(3):130–137.

Y. GAUTHIER (2000) : The Internal Consistency of Arithmetic with Infinite Descent. *Modern Logic*, VIII(1/2):47–87.

Y. GAUTHIER (2002) : *Internal Logic. Foundations of Mathematics from Kronecker to Hilbert*. Kluwer, Synthese Library, Dordrecht/Boston/London.

Y. GAUTHIER (2005) : Hermann Weyl on Minkowskian Space-Time and Riemannian Geometry. *International Studies in the Philosophy of Science*, 19:262–269.

Y. GAUTHIER (2007) : The Notion of Outer Consistency from Hilbert to Gödel (abstract). *Bulletin of Symbolic Logic*, 13(1):136–137.

Y. GAUTHIER (2009a) : The Construction of Chaos Theory. *Found. Sci.*, 14:153–165.

Y. GAUTHIER (2009b) : Classical Functional Theory and Applied Proof Theory. *International Journal of Pure and Applied Mathematics*, 56(2):223–233.

Y. GAUTHIER (2010) : *Logique Arithmétique. L'arithmétisation de la logique*. Presses de l'Université Laval, Québec.

Y. GAUTHIER (2011) : Hilbert Programme and Applied Proof Theory. *Logique et Analyse*, 213:46–68.

Y. GAUTHIER (2013a) : Kronecker in Contempory Mathematics. General Arithmetic as a Foundational Programme. *Reports on Mathematical Logic*, 48:37–65.

Y. GAUTHIER (2013b) : A General No-Cloning Theorem for an Infinite Multiverse. *Reports in Mathematical Physics*, 72:191–199.

A. O. GEL'FOND (1934) : Sur le Septième Problème de Hilbert. *Comptes Rendus Acad. Sci. URSS Moscou*, 2:1–6.

A. O. GEL'FOND and U. V. LINNIK (1965) : *Elementary Methods in Analytic Number Theory*. Rand McNally and Co.

G. GENTZEN (1969) : *Collected Papers.* E. Szabo, ed. North-Holland, Amsterdam.

J. GIRAUD (1964) : *Méthode de la descente*. Mémoire 2 de la Société Mathématique de France.

A.M. GLEASON (1957) : Measures on the Closed Subspaces of a Hilbert Space. *Journal of Mathematics and Mechanics*, 6:885–893.

K. GÖDEL (1931) : Über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38:173–198.

K. GÖDEL (1958) : Über eine noch nicht benüzte Erweiterung des finiten Standpunktes. *Dialectica*, 12:230–237.

K. GÖDEL (1967) : *On formally undecidable propositions. In Jean van Heijenoort, editor, From Frege to Gödel: a source book in mathematical logic 1879–1931.* Harvard University Press.

K. GÖDEL (1990) : *Collected Works.* S. Feferman, ed., volume II, 217–251. Oxford University Press, New York/Oxford.

O. GOLDREICH (1995) : Probabilistic Proof System. *Proceedings of the International Congress of Mathematicians*, 443–452.

S. GOLDSTEIN and D.N. PAGE (1995) : Linearly Positive Histories Probabilities for a Robust Family of Sequences of Quantum Events. *Physical Review Letters*, 74:19.

A. GRANVILLE and T.J. TUCKER (2002) : It's as Easy as ABC. *Notices of the AMS*, 1224–1231.

I. GRATTAN-GUINNESS (1970) : *The Development of the Foundations of Mathematical Analysis from Euler to Riemann.* M.I.T. Press, Cambridge, Mass.

R.B. GRIFFITHS (1984) : Consistent Histories and the Interpretation of Quantum Mechanics. *Journal of Statistical Physics*, 36:219.

A. GROTHENDIECK (1960) : *Technique de descente et théorèmes d'existence en géométrie algébrique I, Généralité. Descente par morphisme fidèlement plats.* Séminaire Bourbaki, 5 (1958–1960) Exp. No. 90, 29 p.

A. GROTHENDIECK and M. RAYNAUD (1971) : *Revêtements étale et Groupe fondamental (SGA1), Séminaire de Géométrie algébrique du Bois-Marie 1960–1961.* Lecture Notes in Mathematics, Springer-Verlag.

Y. GUREVITCH (1988) : *Current Trends in Theoretical Computer Science.* E. Börger, ed., Logic and the Challenge of Computer Science: 1–57. Computer Science Press, East Lansing, MI.

P. HÁJEK and P. PUDLÁK (1993) : *Metamathematics of First-Order Logic*. Springer, Berlin.

M. HALLETT (1998) : Hilbert and logic. *In* M. MARION and R. S. COHEN, éditeurs : *Quebec Studies in the philosophy of science, Part I :135–187.* Kluwer, Dordrecht.

P. HALMOS (1957) : *Introduction to Hilbert Space and the Theory of Spectral Multiplicity*. 2nd ed., New York, Chelsea.

J. HERBRAND (1968) : *Écrits logiques.* J. van Heijenoort, ed. PUF, Paris.

D. HILBERT (1890) : Über die Theorie der algebraischen Formen. *in Hilbert, vol. II :199–257.*

D. HILBERT (1893) : Über die vollen Invariantensysteme. *in Hilbert, vol. II :287–365.*

D. HILBERT (1904) : *Über die Grundlagen der Logik und Mathematik*, 174–185. in: A. Krazer (Hrsg.) Verhandlungen des III. Internationalen Mathematiker-Kongresses in Heidelberg vom 8. bis 13. August 1904. Leipzig, Teubner.

D. HILBERT (1905) : Über die Grundlagen der Logik und der Arithmetik. *in Verhandlungen des dritten internationalen Mathematiker-Kongresses in Heidelberg, Krazer (ed.) Leipzig : B.G. Teubner, 1905*, 95:174–185.

D. HILBERT (1926) : Über das Unendliche. *Mathematische Annalen*, 95:161–190. trad. par A. Weil sous le titre "Sur l'infini", *Acta Mathematica* 48 : 91–122.

D. HILBERT (1930) : Die Grundlegung der elementaren Zahlenlehre. *Mathematische Annalen*, 104:485–494.

D. HILBERT (1932) : *Gesammelte Abhandlungen III.* Chelsea, New York.

D. HILBERT (1935) : *Gesammelte Abhandlungen 3 vols.* Chelsea, New York.

D. HILBERT and P. BERNAYS (1968–1970) : *Grundlagen der Mathematik I et II.* Springer, Berlin, 2 édition.

D. HILBERT, J. von NEUMANN and L. NORDHEIM (1928) : Über die Grundlagen der Quantenmechanik. *Mathematische Annalen*, 98:1–30.

W. HODGES (1993) : *Model Theory*. Cambridge University Press, Cambridge.

E. HRUKOVSKI and I. PITKOWSKY (2004) : Generalizations of Kochen and Specker's Therorem and the effectiveness of Gleason's Therorem. *Studies in History and Philosophy of Science Part B*, 35(2):177–184.

D. HUME (1978) : *A Treatise of Human Nature.* L. A. Selby-Bigge, ed. Clarendon Press, Oxford.

K. IRELAND and M. ROSEN (1980) : *A Classical Introduction to Modern Number Theory*. Springer, New York/Heidelberg/Berlin.

J.M. JAUCH (1968) : *Foundations of Quantum Mechanics*. Reading, Mass.

R. KAYE (1991) : *Models of Peano Arithmetic*. Clarendon Press, Oxford.

S. C. KLEENE and J. VESLEY (1965) : *Foundations of Intuitionistic Mathematics*. North-Holland, Amsterdam.

S. KOCHEN and E.P. SPECKER (1967) : The Problem of Hidden Variables in Quantum Mechanics. *Journal of Mathematics and Mechanics*, 17:59–87.

U. KOHLENBACH (1998) : *Arithmetising Proofs in Analysis. In Lascar D. Larrazabal, J.M. and G. Mints, editors*. Logig Colloquium 96, volume 12 of Springer Lecture Notes in Logic.

U. KOHLENBACH (2008a) : Functional Interpretations and their Use in Current Mathematics. *Dialectica*, 62:223–267.

U. KOHLENBACH (2008b) : *Applied Proof Theory: Proof Interpretations and their Use in Mathematics*. Springer, Heidelberg.

A. N. KOLMOGOROV (1925) : O printsipe *tertium non datur*. *Matematicheskii sbornik*, 32:646–667.

G. KREISEL (1961) : *Set-theoretic problems suggested by the notion of potential totality*, 103–140. in: Infinitistic Methods. Pergamon Press, Oxford.

G. KREISEL (1976) : What have we learnt from Hilbert's Second Problem? Mathematical Developments arising from Hilbert's Problems. *Providence, Rhode Island: American Mathematical Society.*, 93–130.

G. KREISEL (1981) : *Extraction of bounds: interpreting some tricks of the trade. In P. Suppes, editor*. University-level computer-assisted instruction at Stanford: 1968–1980, Stanford University Institute for Mathematical Studies in the Social Sciences.

S. KRIPKE (2009) : The Collapse of the Hilbert Program: Why a System Cannot Prove its Own 1-consistency. *The Bulletin of Symbolic Logic*, 15(2):229–230.

L. KRONECKER (1883) : Zur Theorie der Formen höherer Stufen. *Werke*, II:419–424.

L. KRONECKER (1884) : Über einige Anwendungen der Modulsysteme auf elementare algebraische Fragen. *Werke*, III:47–208.

L. KRONECKER (1886) : Zur Theorie der elliptischen Funktionen. *Werke*, IV:309–318.

L. KRONECKER (1887a) : Ein Fundamentalsatz der allgemeinen Arithmetik. *Werke*, II:211–241.

L. KRONECKER (1887b) : Über den Zahlbegriff. *Werke*, III:251–274.

L. KRONECKER (1889) : Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *Werke*, II:47–208.

L. KRONECKER (1901) : *Vorlesungen über Zahlentheorie I. K. Hensel, ed.* Teubner, Leipzig.

L. KRONECKER (1968a) : Über Systeme von Funktionen mehrerer Variablen. In K. Hensel, editor, Werke, volume I. Teubner, Leipzig.

L. KRONECKER (1968b) : *Werke,* éd. K. Hensel, volume III, Grundzüge einer arithmetischen Theorie der algebraischen Grössen, 245–387. Teubner, Leipzig.

L. LAFFORGUE (2002) : Chtoukas de Drinfeld et correspondance de Langlands. *Inventiones Mathematicae*, 197(1):11–242.

R. P. LANGLANDS (1976) : *Some Contemporary Problems with Origins in the Jugendtraum, Mathematical Developments arising from Hilbert's problems*. American Mathematical Society, Providence R.I.

G. LEJEUNE-DIRICHLET (1969) : *Werke I.* L. Kronecker, ed. Chelsea, New York.

G. LINDBLAD (1999) : A General No-Cloning Theorem. *Letters in Mathematical Physics*, 47:189–196.

S. LIPSCHITZ (1896) : *Briefwechsel mit Cantor, Dedekind, Helmholtz, Kronecker, Weierstrass*. Vieweg Verlag, Braunschveig.

J. LURIE (2009) : *Higher Topos Theory*. Annals of Mathematics Studies, Princeton University Press, Princeton.

M. MARION (1998) : *Wittgenstein. Finitism and the Foundations of Mathematics*. Oxford University Press, Oxford.

H. MINKOWSKI (1967) : *Gesammelte Abhandlungen,*. hrsg. v. D. Hilbert (Chelsea, New York).

D. MIRIMANOFF (1917) : Les antinomies de Russell et Burali-forti et le problème fondamental de la théorie des ensembles. *L'enseignement mathématique*, 19:17–52.

S. MOCHIZUKI : Inter-universal Teichmüller Theory iv. Log-volume Computations and Set-theoretic Foundations. Homepage of S. Mochizuki (2012).

J. MOLK (1885) : Sur une notion qui comprend celle de la divisibilité et sur la théorie générale de l'élimination. *Acta Mathematica*, 6:1–165.

MYCIELSKI (1981) : Analysis without actual infinity. *Journal of Symbolic Logic*, 46:625–633.

E. NELSON (1987a) : *Predicative Arithmetic*. Number 32 of Mathematical Notes. Princeton University Press, Princeton, N.J.

E. NELSON (1987b) : *A Radically Elementary Probability Theory*. Princeton University Press, Princeton, N. J.

R. PARIKH (1971) : Existence and feasibility in arithmetic. *Journal of Symbolic Logic*, 36:494–508.

G. PEANO (1959) : *Opere scelte, vol. II*. Edizione Cremonese, Roma.

H. POINCARÉ (1951) : Sur les propriétés arithmétiques des courbes algébriques. *Oeuvres*, II:483–550.

M.C.G. REDHEAD (1987) : *Incompleteness, Nonlocality and Realism*. Oxford, Clarendon Press.

B. RIEMANN (1990) : *Gesammelte mathematische Werke, wissenschaftlicher Nachlass und Nachtrage. Collected Papers*. neu hrsg. v. R. Naramsihan, (B.G. Teubner, Springer-Verlag, Berlin, New York, Leipzig).

C. ROVELLI (1996) : Relational Quantum Mechanics. *Int. J. Theor, Physics*, 35:1637–1678.

B. RUSSELL (1919) : *Introduction to Mathematical Philosophy*. Allen and Unwin, London, UK.

B. RUSSELL (1966) : Mathematical logic as based on the theory of types. *In* J. van HEIJENOORT, éditeur : *From Frege to Gödel*, 150–182. Harvard University Press, Cambridge, Mass.

V. Yu. SAZONOV (1995) : On feasible numbers. *In* D. LEIVANT, éditeur : *Logic and Computational Complexity*, 30–51. Lecture Notes in Computer Science, Springer, Berlin Heidelberg.

T. SCHNEIDER (1934a) : Transzendenzuntersuchungen periodischer Funktionen. *J. reine angew. Math.*, 172:65–69.

T. SCHNEIDER (1934b) : Transzendenzuntersuchungen periodischer Funktionen. ii. *J. reine angew. Math.*, 172:70–74.

J. R. SCHOENFIELD (1967) : *Mathematical Logic*. Addison-Wesley, Reading, Mass.

D. SCHWARZ-PERLOW and A. VILENKIN (2010) : Measures for a Transdimensional Universe. *arXiv: 1004. 4567v2*.

J.-P. SERRE (2009) : How to use finite fields for problems concerning infinite fields. *Proc. Conf. Marseille-Luminy (2007), Contemporary Math. Series, AMS.*, 1–12.

W. SIEG (1999) : Hilbert's Program : 1917–1922. *Bulletin of Symbolic Logic*, 5(1):1–44.

T. SKOLEM (1970) : Einige Bemerkungen zur axiomatischen Begründung der Mengenlehre. *In* J. E. FENSTAD, éditeur : *Selected Works in Logic*. Universitetsforlaget, Oslo.

A. TARSKI (1951) : *A Decision Method for Elementary Algebra and Geometry*. University of California Press, Berkeley and Los Angeles, 2nd édition.

B. A. TRAKHTENBROT (1950) : Nevozmozhnosty Algorifma dla Problemy Razreximosti Konechnyh Klassah, (The impossibility of an algorithm for the decision problem in finite classes). *Dokl. Akad. Nauk, SSSR*, 70:569–572.

A. S. TROELSTRA (1969) : *Principles of Intuitionism*. Numéro 95 de Lectures Notes in Mathematics. Springer, Berlin Heidelberg New York.

A. S. TROELSTRA (1976) : *Choice Sequences*. Clarendon Press, Oxford.

A. S. TROELSTRA (2003) : *Constructivism and Proof Theory*. ILLC, University van Amsterdam.

A. S. TROELSTRA and D.van DALEN (1988) : *Constructivism in Mathematics. vol. I*. North-Holland, Amsterdam.

L. van den DRIES (1988) : Alfred Tarski's Elimination Theory for Real Closed Fields. *Journal of Symbolic Logic*, 53:7–19.

B. van FRAASSEN (1991) : *Quantum Mechanics. An Empiricist View*. Oxford, Clarendon Press.

H. S. VANDIVER (1936) : Constructive Derivation of the Decomposition Field of a Polynomial. *Annals of Mathematics*, 37(1):1–6.

A. VILENKIN (2006) : A Measure of the Universe. *arXiv: hep-th/0609193v3*.

V. VOEVODSKY (2010) : *Univalent Foundation Project*. (A modified version of an NSF grant application). October 1.

J. von NEUMANN (1932) : *Mathematische Grundlagen der Quantenmechanik*. Berlin, Springer.

J. von NEUMANN (1961) : *Collected Works*, volume I, Eine Axiomatisierung der Mengenlehre, 24–33. Pergamon Press, Oxford.

K. WEIERSTRASS (1894–1927) : *Mathematische Werke, 7 Bände*. Mayer u. Müller, Berlin.

A WEIL (1941) : On the Riemann Hypothesis in Function Fields. *Proc. Natl. Acad. Sci. USA*, 27:345–347.

A. WEIL (1949) : Numbers of solutions of equations in finite fields. *Bull. Am. Math. Soc.*, 55:497–508.

A. WEIL (1976) : *Elliptic Functions according to Eisentein and Kronecker*. Springer, Berlin.

A. WEIL (1979a) : *Oeuvres scientifiques*. Collected Paper, Vol. I, Springer-Verlag, New York.

A. WEIL (1979b) : *Number Theory and Algebraic Geometry*. In: *Weil*, Vol. III :442–452.

A. WEIL (1979c) : *L'arithmétique sur les courbes algébriques*. In: *Weil*, Vol. I :11–45.

A. WEIL (1984) : *Number Theory. An Approach through History. From Hammurabi to Legendre*. Birkhäuser. Boston-Basel-Berlin.

A. WEIL (1992) : *The Apprenticeship of a Mathematician*. Translated from the French by Jennifer Cage. Birkhäuser, Basel.

H. WEYL (1918) : Das Kontinuum, Veit, Leipzig.

H. WEYL (1920) : Das Verhältnis der kausalen zur statistischen Betrachtungsweise in der Physik. *Schweizerische Medizinische Wochenschrift*, 50:537–541.

H. WEYL (1940) : *Algebraic Theory of Numbers*. Princeton University Press, Princeton, N. J.

H. WEYL (1950) : *Space, Time, Matter*. trans. By H. L. Brose (Dover Publications, New York).

H. WEYL (1960) : *Philosophy of Mathematics and Natural Science*. Atheneum, New York.

H. WEYL (1968) : *Gesammelte Abhandlungen*. hrsg. v. K. Chandrasekharan (Springer-Verlag, Berlin, Heidelberg, New York).

W. WOOTTERS and W. ZUREK (2009) : The no-cloning theorem. *Phys. Today*, 62(2):76–66.

W.K. WOOTTERS and W.H. ZUREK (1982) : A single quantum cannot be cloned. *Nature*, 299:802–803.

E. ZERMELO (1908a) : Neuer Beweis für die Möglichkeit einer Wohlordnung. *Mathematische Annalen*, 59:107–128.

E. ZERMELO (1908b) : Untersuchungen über die Grundlagen der Mengenlehre i. *Mathematische Annalen*, 59:261–281.

E. ZERMELO (1909) : Sur les ensembles finis et le principe de l'induction complète. *Acta Mathematica*, 32:185–193.