ELEMENTARY MATHEMATICS FROM AN ADVANCED STANDPOINT

John Stillwell
Department of Mathematics, University of San Francisco, U.S.A.
School of Mathematical Sciences, Monash University, Australia.

Keywords: History of mathematics, arithmetic, computation, algebra, geometry, calculus.

Contents

Summary

A survey of elementary mathematics, using the insights and general concepts made available by higher mathematics. We also observe how the "advanced standpoint" has changed over the last century, by reference to the works of Felix Klein on this topic.

1. Introduction: Klein's View of Elementary Mathematics

In 1908, the German mathematician and mathematics educator Felix Klein published a series of three books (in German) under the title of *Elementary Mathematics from an Advanced Standpoint*, henceforth called EMAS for short. The first volume was subtitled *Arithmetic, Algebra, Analysis*, and the second volume was subtitled *Geometry*. Both of these volumes were translated into English in the1930s, and they have been popular with English-speaking mathematicians and students ever since. It is a tribute to Klein's influence, and foresight, that his "standpoint" remains clearly comprehensible to mathematicians today, though of course our "standpoint" is somewhat different. One of the goals of this article is to compare Klein's view of elementary mathematics with the views of mathematicians today.

Klein's third volume was *not* published in English and it has been almost forgotten. Evidently, his subject matter (the mathematics of approximations) was of lesser interest to English-speaking mathematicians of his time, and one doubts that it would be of much interest today, now that computers have completely revolutionized the practice of numerical and graphical approximation. Indeed, computers have strongly influenced our standpoint on the material in Klein's first two volumes as well, albeit in a more subtle way. Klein's view of arithmetic, algebra, analysis, and geometry has not been rendered obsolete by computers, but the modern view has to take them into account.

2. Arithmetic

Klein begins his account of arithmetic with the "fundamental laws of reckoning," by which he means general properties such as the commutative and associative laws,

$$a+b=b+a, \quad ab=ba,$$

$$a+(b+c)=(a+b)+c, \quad a(bc)=(ab)c,$$

and what he calls *monotonic laws*:

If $b<c$ then $a+b<a+c$ and $ab<ac$.

Thus Klein initially assumes that numbers are positive, so his abstract "laws of reckoning" do not define a standard algebraic structure of today, such as a ring. He generally does not take abstraction so far as giving names to structures defined by abstract laws, as we probably would today (see the section on algebra below).

In any case, Klein is well aware that the natural numbers are more than just an algebraic structure. Their "fundamental laws" actually follow from a deeper property, namely the *inductive* property of natural numbers:

> If a theorem holds for a small number, and if the assumption of its validity for a number *n* always ensures its validity for *n*+1, then it holds for every number. This theorem, which I consider to be really an intuitive truth, carries us over the boundary where sense perception fails. (EMAS, p. 11)

Instances of proofs by induction can be found as far back as Euclid, but the foundational role of induction was not really recognized until the 19th century. Klein gives credit to Grassmann, whose *Lehrbuch der Arithmetik* of 1861 used induction to *define* addition and multiplication of natural numbers and to prove their "fundamental laws." He also notes Peano's formal theory of numbers of 1889, where induction and other axioms are written in a symbolic language and theorems are derived from them by formal rules of logic. Finally he emphasizes the problem of proving the consistency of Peano's system PA (as it is now called, abbreviating "Peano arithmetic"), posed by Hilbert in 1904. He shows a good understanding of the so-called *Hilbert program*, whose goal was to prove the consistency of all mathematics by analyzing the operation of formal systems, using only intuitively obvious assumptions about finite strings of symbols.

Klein seemed to approve of the Hilbert program because he believed that in mathematics

> … *one must retain something, albeit a minimum, of intuition*. One must always use a certain intuition in the most abstract formulation with the symbols one uses

> in operations, in order to recognize the symbols again, even if one thinks only about the shapes of the letters. (EMAS, p. 14).

However, neither Klein nor Hilbert realized just how problematic the "intuitively obvious assumptions about finite strings of symbols" would be. It is reasonable to take this set of assumptions to be PA, because

1. Finite strings of symbols can be interpreted as numerals.
2. Operations on strings can then be defined arithmetically.
3. The axioms of PA are intuitively obvious.
4. Obvious assumptions about operations on strings are basic theorems of PA.
5. All theorems about operations on strings – for example, whether the formal rules of PA lead to a contradiction – should therefore be provable in PA.

But then, if one follows this train of thought a little further, one arrives at the stunning theorem of Kurt Gödel (1931) that the consistency of PA is expressible by a sentence of PA but is *not* provable in PA.

Thus the "advanced standpoint" today must acknowledge that the consistency of PA is a very slippery problem. Nevertheless, the problem can be better appreciated by the modern audience, thanks to its connection with the concept of *computation*. In Klein's time, computation was mainly confined to addition, subtraction, multiplication, division, and extraction of roots. Since these operations were generally carried out by hand, Klein's readers were considerably more familiar with these operations than most people are now. On the other hand, mathematics students today are at least aware of the concept of a *computer program*, and many have written programs, so there is a greater understanding of the potential complexity of computation (see next section).

Like us, Klein assumes that the rules for reckoning with decimal *numerals* are known, and he merely gives some simple examples that illustrate the use of general laws in particular computations. Then, as now, it was not fully appreciated how much *more* complex are the rules for reckoning with numerals than the abstract laws governing addition, multiplication, and ordering of numbers. However, Klein embraces applied arithmetic -- numerical computation – more enthusiastically than we generally do today, by describing the operation of early 20th-century calculating machines. It takes him four pages to describe what he admits is "merely a technical realization of the rules which one always uses in numerical calculation."

In one respect, arithmetic is a much more applied subject now than it was in Klein's day. The transforming event was the discovery of *public key cryptosystems* in the 1970s, particularly the RSA system (named after its discoverers, Rivest, Shamir, and Adelman) of 1977. The RSA system is an application of the classic theorem of Euler and the concept of an inverse mod n – both standard, fare in elementary number theory – so RSA has now become a common topic for beginners. Thanks to the everyday occurrence of encryption in internet commerce, interest in cryptography generally has surged, and interest in number theory has surged with it. Topics such as the greatest common divisor (gcd), factorization, and the recognition of prime numbers have been revitalized due to attention of computer scientists interested in the making and breaking of codes. In particular, the workability of the RSA cryptosystem depends on the existence of a fast algorithm for the gcd (the classical Euclidean algorithm), a fast algorithm for generating large prime numbers (a recent discovery), and the presumed *non*-existence of a fast algorithm for factorization (still an open problem).

The importance of algorithms in applied mathematics today is a second reason to include computation in our “advanced standpoint.”

But before moving on to computation, we should mention another remarkably prescient section of Klein’s chapter on arithmetic: his account of *quaternions*. Klein introduces quaternions as a 4-dimensional extension of the complex numbers, and he evidently finds the quaternions much more interesting than the complex numbers. He thoroughly discusses their addition, subtraction, multiplication, and division, also the quaternion conjugate and absolute value, with particular attention to geometric interpretation. In particular, he shows how convenient the quaternions are for representing rotations of 3-dimensional space. It was by no means clear in Klein’s day that quaternions had a future (if anything, they were already falling into obscurity), but history has come down on his side. Today, just as complex numbers are in the toolkit of every electrical engineer, quaternions are in the toolkit of every programmer in the field of video games or computer animation.

3. Computation

Computation was a common activity of mathematicians in Klein’s day, but it was not a branch of mathematics, because the field had not yet been organized around a concept of computability. And, surprisingly, the concept of computability did not arise from the practice of computation but from *logic*. More precisely, it arose from Hilbert’s program for proving the consistency of mathematics.

Hilbert wanted a consistency proof because, around 1900, there were serious doubts about the foundations of mathematics. This was the time when the concept of *set* began to emerge as the fundamental mathematical concept. It was found to be possible to define numbers, functions, points, geometric figures – and seemingly everything else in mathematics – as sets of one kind or another; but what *are* sets, exactly? A problem with the set concept comes to light when one asks the more specific question: is the collection of all sets itself a set? Or more specifically still: what about the collection of all sets that are not members of themselves? If the latter collection X is a set, then X is either a member of itself, or not. But since the condition for membership of X is *not* being a member of oneself, one quickly reaches the conclusion that *X is a member of itself if and only if X is not a member of itself.*

We can escape from this contradiction (known as the *Russell Paradox*) by deciding that the collection of all sets is not itself a set. However, that is not very reassuring. Sets and membership are fundamental concepts of mathematics, and if they lead so easily to contradiction, who knows what other contradictions may be lurking? Hilbert’s program was supposed to ensure consistency by writing axioms in a formal language, deriving theorems from the axioms by simple symbol-manipulation rules, and proving (by intuitively obvious principles) that the rules do not lead to a contradiction. As mentioned in the previous section, the proof of non-contradiction was pushed beyond the “intuitively obvious” range by Gödel’s theorem about consistency proofs. However, the idea of proving theorems by symbol manipulation – without regard to the meaning of the symbols – was important for more than the intended reasons.

Hilbert’s intention was to make the concept of “rule of inference” so precise that the claim that “the axioms and rules do not lead to a contradiction” was itself a mathematical sentence; hopefully, a provable sentence. A side-effect of making rules mathematically precise is that human intervention in mathematics is not required – in principle, proofs can be generated by a machine. 100 years ago, this effect was not of interest, because machines capable of complicated symbol manipulations did not exist. But in the 1920s (unbeknownst to Hilbert and Klein) the American mathematician Emil Post began a serious study of symbol-manipulation rules. Post’s investigations eventually led to a precise definition of the concept of computability.

Post began, in the spirit of Hilbert’s program, with the aim of simplifying a known system of symbolic logic, the *Principia Mathematica* of Whitehead and Russell. His aim was to prove that the *Principia* is *complete* (that is, all its true sentences are derivable from its axioms) and consistent. He was pleased to find that all theorems of *Principia* could in fact be derived by very simple manipulations – essentially, by removing sequences of symbols from the left hand end of words and attaching sequences on the right – so he had high hopes of proving the completeness and consistency of *Principia*.

But when it came to analyzing the behavior of such symbol-manipulation systems, Post was surprised to find intractable complexity in even very simple systems.

Post’s most famous example is the system in which the words are strings of 0s and 1s, and the rules are:

1. If the string begins with 1, remove the first three symbols, and attach 1101 to the right hand end.
2. If the string begins with 0, remove the first three symbols, and attach 00 to the right hand end.

It appears that, for any initial string, these rules lead either to termination or to periodic behavior, but this has never been proved. The unexpected complexity of simple rules stopped Post in his tracks and he made a dramatic change of direction. Instead of trying to predict the outcome of symbol-manipulation rules, he decided to show that outcomes are *not* always predictable. More precisely, he aimed now to show that *no machine can correctly predict the outcome of every computation.*

It turns out, by an argument not unlike Russell’s paradox, that this is indeed the case. Each machine M has finite *description*, $\text{des}(M)$, which can be input to M, so the problem of predicting outcomes of computations includes the questions:

Q_M: Does M, given input $\text{des}(M)$, eventually halt with output NO?

It is fair to assume that any machine T that answers these questions receives question Q_M in the form of the word $\mathrm{des}(M)$, since this input contains all necessary information. But then T then cannot give the correct answer to question Q_T. Hence there is no machine that can correctly predict the outcome of every computation. Since "computations" include proofs of theorems in formal systems, Post's discovery reveals profound limitations in the formalization of mathematics, as Post realized. Among them are the incompleteness of PA (already noticed by Post in 1921) and the unprovability of consistency by methods of PA, later discovered by Gödel.

However, Post's argument for the incompleteness of PA, unlike Gödel's, depended on being able to formalize the concept of computation. Today, this is the familiar fact that each algorithm can be encoded by a program (and hence by a finite string of symbols), but in Post's time the formalization of computation was an entirely new and untested idea. Gödel, in particular, did not at first believe it could be done. The idea became generally accepted when the English mathematician Alan Turing introduced a new concept of machine in 1936 – one now known as the *Turing machine*. Turing's paper included a detailed analysis of the process of computation, and a description of a *universal machine* that can simulate the computation of any particular machine. Turing also gave a formal version of the unsolvability of the *halting problem* (described informally by the questions Q_M above), and deduced from it the impossibility of predicting which sentences are proved by certain formal systems.

Thus, before any universal computing machines were actually built, mathematicians knew that computation had its limits. The limitations discovered by Post, Gödel, and Turing have receded somewhat in mathematical consciousness today, but other limitations have come to the fore; particularly, *speed* limits. We are now aware of many problems that are solvable in principle, but for which the known solution is too slow to be of any use. One such problem is the factorization of large numbers. As mentioned at the end of the previous section, a fast algorithm for factorization is not known – and not desirable, as this would break the RSA cryptosystem. At present, it seems feasible to factorize numbers with only a few hundred digits, whereas it is feasible to generate prime numbers with thousands of digits. This should keep the RSA system secure for now, but the seemingly elementary questions of factorization and prime generation are sure to remain important for the foreseeable future.

-
-
-

Bibliography

Dedekind, R. (1963). *Essays on the Theory of Numbers*, Dover. [Two essays by Dedekind: one from 1872, on the nature of irrational numbers; the other from 1888, on the role of counting and induction in the arithmetic of positive integers.]

Dedekind, R. (1996). *Theory of Algebraic Integers*, Cambridge University Press. [English translation of an 1877 essay of Dedekind on algebraic numbers and ideals, together with a historical introduction by the translator, John Stillwell.]

Euclid (1956). *The Thirteen Books of Euclid's Elements* (3 volumes), Dover. [Euclid’s geometry and number theory, complete, with notes by Sir Thomas Heath. Heath’s notes are helpful in interpreting the archaic style of Euclid and relating it to later developments, though they miss the developments that originate with Hilbert.]

Gauss, C.F. (1986). *Disquisitiones Arithmeticae*, Springer-Verlag. [English translation of the Gauss’s seminal 1801 book on number theory. In this book, Gauss solves many problems left unsolved by Fermat, Euler, and others, and paves the way for much number theory and algebra of the 19^{th} century.]

Grassmann, H. (1861). *Lehrbuch der Arithmetik* (Textbook of arithmetic), Enslin, Berlin. [Grassmann’s construction of number theory from the induction principle. In particular, Grassmann proves the ring properties of the integers by induction.]

Grassmann, H. (1844). *Ausdehnungslehre* (Theory of extension) An English translation is available as *A New Branch of Mathematics: The Ausdehnungslehre of 1844 and Other Works*, Open Court (1994). [Grassmann’s approach to geometry, via linear algebra.]

Hilbert, D. (1971). *The Foundations of Geometry*, Open Court. The 1950 edition is available free from www.gutenberg.org/ebooks/17384 [Hilbert fills the gaps in Euclid’s axioms, and shows the algebraic significance of the Pappus and Desargues theorems.]

Klein, F. (1945). *Elementary Mathematics from an Advanced Standpoint*, Dover. [Two-volume survey of arithmetic, algebra, analysis, and geometry at the high-school and undergraduate level. Klein’s standpoint is that of German higher mathematics as of 1900.]

Klein, F. (2003). *Lectures on the Icosahedron and the Solution of Equations of Fifth Degree*, Dover. [English translation of Klein’s 1884 book relating polynomial equations to group theory and the geometry of polyhedra.]

König, D. (1990). *Theory of Finite and Infinite Graphs*, Birkhaüser. [English translation of König’s 1936 *Theorie der Endlichen und Unendlichen Graphen*, the first book on graph theory.]

Whitehead, A.N. and Russell, B. (1913). *Principia Mathematica*, Cambridge University Press. [Three volumes on symbolic logic and mathematics, building basic number theory and geometry from simple principles about sets. The aim of the volumes is to show in principle that all mathematics is derivable from a few axioms and rules of inference.]

Biographical Sketch

John Stillwell was born in Melbourne, Australia, in 1942 and was educated at Melbourne High School and the University of Melbourne. He received an M. Sc. from the University of Melbourne in 1965, for a thesis on the subject of recursively enumerable sets. From 1965 to 1970 he was a graduate student at MIT, in Cambridge, Massachusetts, where he received a Ph.D. in 1970. His thesis was entitled *Reducibility in generalized recursion theory*. At this time, his interests were mainly in set theory and mathematical logic.

In 1970 he moved back to Australia, where taught at Monash University in Melbourne until 2001. During this period

his interests expanded to encompass group theory, topology, geometry, number theory and algebra. He is inspired by the great mathematicians who have contributed to these fields – such as Dirichlet, Dedekind, Klein, Poincaré, and Dehn – and has translated many of their works into English. His involvement in the history of mathematics led to his best-known book, *Mathematics and Its History* (Springer 1989 and 2002), and to several invited addresses at prestigious conferences, among them the International Congress of Mathematicians in 1994, and the Joint Meetings of the AMS and the MAA in 1998.

In 2002 he took a new position at the University of San Francisco, where he spends one semester each year and teaches a variety of topics in mathematics. He continues to write books and articles. His most recent books include *The Four Pillars of Geometry* (Springer 2005), *Yearning for the Impossible* (A K Peters 2006) and *Naïve Lie Theory* (Springer, to appear). One of his articles, *The Story of the 120-Cell*

(Notices of the AMS, January 2001) was awarded the Chauvenet Prize for mathematical exposition by the Mathematical Association of America in 2005.