

WEIERSTRASS'S FINAL THEOREM OF ARITHMETIC IS NOT FINAL

F. G. ASENJO and J. M. MCKEAN

Weierstrass proved that the system of complex numbers C is the first and last algebraic extension of the field of real numbers \mathcal{R} which has the properties that (i) it is itself a field, that (ii) it is algebraically closed, and that (iii) it is a finite dimensional vector space over \mathcal{R} . As a consequence, the so-called "final theorem of arithmetic" follows:

It is impossible to extend the number system beyond C into structures that preserve all the formal laws of arithmetic (most significantly, the field-theoretic ones)—that is, full-fledged arithmetic ends with C .

This theorem is principally based on the fact that C is a finite dimensional vector space over \mathcal{R} ; however, this puts too much reliance on a condition extraneous to both the program and the spirit of Hankel's classical formal laws of arithmetic. Since C is both algebraically closed and a vector space over \mathcal{R} , one tends to lose sight of the obvious fact that property (iii) is not a consequence of (i).

This problem arises: Is it possible to generalize the final theorem of arithmetic to fields obtained by adjoining the root of $x^2 + 1 = 0$ to any field \mathcal{R}^* that contains \mathcal{R} and is obtained from \mathcal{R} by strictly finitistic procedures (i.e., finitistic rules of formation, quotient structures, and the like) rather than by ultraproducts or some other infinitistic device? The answer to this question is no, as we shall outline. To be specific, an extension \mathcal{R}^* of \mathcal{R} can be finitistically constructed in which $x^2 + 1 = 0$ is not solvable, and in which the field C^* obtained by adjoining i to \mathcal{R}^* is not algebraically closed, and such that from \mathcal{R}^* an unlimited number of algebraic field extensions can be obtained. These extensions yield an infinite sequence of number systems, all of which are fields and none of which is algebraically closed. Thus, the final theorem of arithmetic fails for C^* as well as for all its algebraic extensions. It is possible to expand the concept of number from \mathcal{R}^* indefinitely.

In [1] a number system \mathcal{N}^* was introduced that is an extension of the system of natural numbers \mathcal{N} . Members of \mathcal{N}^* —term-relation numbers—are obtained as by-products of formalizing some of the properties of

internal relations. The method for constructing \mathcal{N}^* is entirely finitistic and can be applied in turn to obtain an extension \mathcal{J}^* of the system \mathcal{J} of all integers (see [2] and [3]). The arithmetic of \mathcal{J}^* possesses some properties that should be emphasized: \mathcal{J}^* is a commutative ring with proper zero divisors, and since the least ideal that contains all of these zero divisors is the whole ring, it is not possible to map the ring \mathcal{J}^* into a field by the usual method of forming the difference ring. However, the ring \mathcal{J}^* does raise the question of whether or not it can be mapped by other means into an integral domain. Further, it also raises the question of whether or not it is possible to obtain finitary extensions \mathcal{R}^* of the field \mathcal{R} for whose respective extensions $\mathcal{C}^* = \mathcal{R}^*[i]$ the Weierstrass theorem would not apply.

Why is it that such a question has not been raised before? Chiefly because there is something fixed and prototypical about the ordinary number systems. If one starts with the ring of integers \mathcal{J} , as then the extensions to new arithmetic systems follow a step-by-step path that has become (and with good reason) a well-worn groove: from \mathcal{J} one inevitably reaches \mathcal{C} through established classical procedures. This also explains why Skolem's non-standard models of arithmetic, for example, were looked upon for a long time simply as logical curiosities; in fact, it was not until A. Robinson actually put these and other non-standard models to good use that the existence of radically different systems of arithmetic were for the first time seriously considered.

Non-standard models did not open the question, however, because being essentially infinitistic in the most interesting cases, they only provide a view from the outside, so to speak, of \mathcal{R} and \mathcal{C} . Further, in Robinson's non-standard models of analysis all sentences valid in \mathcal{R} hold, so that for each of them there can be only one algebraic extension before reaching algebraic closure—which means that they provide no counter-example to the Weierstrass theorem.

What actually stimulated an investigation of the matter from the inside is the fact that system \mathcal{N}^* described in [1] represents an extension of \mathcal{N} that opens the way to circumventing \mathcal{J} , thus avoiding the tendency to fall into well-trodden paths. The only difficulty with \mathcal{N}^* —or with \mathcal{R} , for that matter—is that in order to obtain the required extensions one has to resort to trial and error within finitistic bounds, since all classical methods fail.

A field \mathcal{R}^* is presented in [4] which is not a non-standard model of analysis, but which is a non-standard model of the field-theoretic part of \mathcal{R} . \mathcal{R}^* is obtained piecemeal in the following way. Assume the field of real numbers \mathcal{R} is formally given, with the constants $a_1, a_2, \dots, b_1, b_2, \dots$ denoting individuals of that field. With the individuals of \mathcal{R} we form the set R' of all variable-free terms formed by the following rules:

- (i) The constants $a_1, a_2, \dots, b_1, b_2, \dots$ (2^{\aleph_0} in number) are terms and so are the variables ranging over them.
- (ii) If y_1, y_2, \dots, y_n are terms (n a positive integer), then $y_1 + y_2 + \dots + y_n$ is a term.
- (iii) If $y_1, y_2, u_1, \dots, u_{2n-3}$ are terms obtained without using rule (ii), then $y_1 [y_1, u_1, \dots, u_{2n-3}, y_2] y_2$ is a term.
- (iv) If y_1 and y_2 are terms, so is $y_1 \cdot y_2$.

Notice that in (iii) the terms $y_1, y_2, u_1, \dots, u_{2n-3}$ may themselves have been obtained by applications of the same rule. The bracket structure of the term indicates the order of generation (see example in the next paragraph).

The postulates for R' divide into two groups. The first one establishes the commutativity and associativity of the formal addition given by rule (ii). The effect of the second group is to introduce an equivalence relation in the set R' of all variable-free terms. These reduction postulates allow for formal addition to be actually performed in R' in terms of addition in \mathcal{R} when the numbers added have the same formal structure. (Thus, for example,

$$3[3, 1, 2] 2[3[3, 1, 2] 2, 4, 0] 0 + 2[2, 4, 1] 1[2[2, 4, 1] 1, 3, 2] 2$$

reduces to $5[5, 5, 3] 3[5[5, 5, 3] 3, 7, 2] 2$.) Also, for any terms $y_1, y_2, \dots, y_{2n-1}$, the term

$$y_1[y_1, 0, y_2, 0, y_3, 0, \dots, 0, y_{2n-1}] y_{2n-1}$$

reduces to $y_1[y_1, y_2, \dots, y_{2n-2}, y_{2n-1}] y_{2n-1}$. Finally $0[0, 0, \dots, 0] 0$, with $2n - 1$ zeros between brackets, reduces to 0.

These reduction postulates taken together induce an equivalence relation in R' . Let us call R'' the quotient set of R' with respect to such relation. In R'' addition can be carried out between any two members by choosing adequate representatives of each equivalence class of R' , using the reduction postulates to either reduce or expand terms to identical formal structure. (Each class, incidentally, also has a unique *reduced form*, i.e., one with a minimum number of individuals from R .) It can be proved that R'' is an additive group.

Multiplication is postulated as follows:

- (i) For individuals of \mathcal{R} in R'' , just as in \mathcal{R} .
- (ii) If x is an individual from \mathcal{R} in R'' and y is the equivalence class determined by $a_1[a_1, b_1, \dots, b_{2n-3}, a_2] a_2$, then $x \cdot y$ is the class determined by

$$xa_1[xa_1, xb_1, \dots, xb_{2n-3}, xa_2] xa_2,$$

a product that is of course commutative.

- (iii) If $z_1 = y_1[y_1, u_1, \dots, u_{2n-3}, y_2] y_2$ and $z_2 = y_3[y_3, v_1, \dots, v_{2m-3}, y_4] y_4$, then $z_1 \cdot z_2$ is the class determined by

$$y_1 y_3 [y_1 \cdot y_3, y_1 v_1, \dots, y_1 v_{2m-3}, y_1 y_4, u_1 y_3, u_1 v_1, \dots, u_1 v_{2m-3}, u_1 y_4, \dots, u_{2n-3} y_3, u_{2n-3} \cdot v_1, \dots, u_{2n-3} v_{2m-3}, u_{2n-3} \cdot y_4, y_2 \cdot y_3, y_2 \cdot v_1, \dots, y_2 \cdot v_{2m-3}, y_2 \cdot y_4] y_2 \cdot y_4.$$

- (iv) If y_1 is any term and y_2 is $u_1 + u_2 + \dots + u_n$, then

$$y_1 \cdot y_2 = y_1 u_1 + y_1 u_2 + \dots + y_1 u_n \quad \text{and} \quad y_2 \cdot y_1 = u_1 y_1 + u_2 y_1 + \dots + u_n y_1.$$

This operation is associative and R'' is proved to be a ring. In order to imbed R'' into an integral domain, a new equivalence relation must be introduced. We say that y_2 divides y_1 iff there exists a term y_3 such that

$y_1 = y_2 \cdot y_3$ (which is not always the case in R'' for arbitrary terms y_1 and y_2); a term y_1 is a *unit* iff y_1 divides 1; two terms y_1 and y_3 are *associates* iff $y_1 = y_2 \cdot y_3$, where y_2 is a unit; a non-zero term y_1 is *irreducible* iff in any factorization $y_1 = y_2 \cdot y_3$ either y_2 or y_3 is a unit. It can then be proved that every term that is neither zero nor a unit can be factored into a product of a finite number of irreducible terms. Further, given two factorizations $v_1 \cdot v_2 \dots v_m$ and $u_1 \cdot u_2 \dots u_m$ of a term y into irreducible terms, then $m = n$ and the v 's and u 's form pairs of associates.

In terms of such factorization, an equivalence relation ρ can be defined such that the difference ring of R'' modulo ρ is a commutative integral domain R''' with identity. The imbedding of R''' into its field of fractions gives us \mathcal{R}^* , the desired field. \mathcal{R}^* can be totally ordered and is, of course, non-Archimedean. Further, in \mathcal{R}^* $x^2 + 1 = 0$ is not solvable. However, in adjoining i to \mathcal{R}^* , the field C^* obtained (which contains an image of the standard complex field C) is not algebraically closed, and no finite number of algebraic extensions of C^* yields the algebraic closure of C^* .

REFERENCES

- [1] Asenjo, F. G., "Relations irreducible to classes," *Notre Dame Journal of Formal Logic*, vol. IV (1963), pp. 193-200.
- [2] Asenjo, F. G., "The arithmetic of the term-relation number theory," *Notre Dame Journal of Formal Logic*, vol. VI (1965), pp. 223-228.
- [3] Asenjo, F. G., "Rings of term-relation numbers as non-standard models," *Notre Dame Journal of Formal Logic*, vol. VIII (1967), pp. 24-26.
- [4] McKean, J. M., "Term-Relation Numbers and Weierstrass's Final Theorem of Arithmetic," Doctoral dissertation, University of Pittsburgh, 1970. (Misprint: On page 2, line 7 from the bottom, "is a non-standard model" should read "is not a non-standard model.")
- [5] Weierstrass, K., *Mathematische Werke*, II, Johnson Reprint Corp. (original 1895).

University of Pittsburgh
Pittsburgh, Pennsylvania