



A Detail in Kronecker's Program

Author(s): E. T. Bell

Source: *Philosophy of Science*, Vol. 3, No. 2 (Apr., 1936), pp. 197-207

Published by: The University of Chicago Press on behalf of the Philosophy of Science Association

Stable URL: <https://www.jstor.org/stable/184346>

Accessed: 24-03-2020 22:49 UTC

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at <https://about.jstor.org/terms>



JSTOR

The University of Chicago Press, Philosophy of Science Association are collaborating with JSTOR to digitize, preserve and extend access to *Philosophy of Science*



A Detail in Kronecker's Program

BY

E. T. BELL

THE PROGRAM

IT WAS Kronecker who sought to avoid the use in mathematics of all numbers (negatives, fractions, irrationals) other than the positive integers, and he outlined the means for carrying through this program.¹ In the introductory sections of his memoir he briefly indicates the personal philosophy which made such a project appear desirable.

It does not seem surprising that Kronecker's program has inspired controversies and created its own opposition. The program itself has been called bizarre, impracticable, and idle even if it were possible of achievement. The general sentiment on the hostile side has been briefly summed up as follows by Hobson.²

"His [Kronecker's] ideal is that every theorem in analysis shall be stated as a relation between integral numbers only, the terminology involved in the use of negative, fractional, and irrational numbers, being entirely removed. This ideal, if it were possible to attain it, would amount to a reversal of the actual historical course which the science has pursued; for all actual progress has depended upon successive generalizations of the notion of number, although these generalizations are now regarded as ultimately dependent on the whole number for their

¹ L. Kronecker, *Über den Zahlbegriff*, *Journal für die reine und angewandte Mathematik* vol. 101 (1887) pp. 251-280; *Werke*, vol. III 1, pp. 251-280.

² E. W. Hobson, *The Theory of Functions of a Real Variable*, etc., (1907) Art. 17.

foundation. The abandonment of the inestimable advantages of the formal use in Analysis of the extensions of the notion of number could only be characterized as a species of Mathematical Nihilism.”

The doubt whether it is possible to attain Kronecker's ideal has recently been repeated.^{3,4} It must be remembered, however, that Kronecker wrote his sketch at a time when it was not customary, as it is now, to state carefully the postulates upon which a particular mathematical theory is based before proceeding to the construction of the theory. Further, parts of his exposition are quite concise and might easily be misinterpreted by a reader as antipathetic to Kronecker's program as Couturat was. Couturat let himself go; he attacked the program with gusto and damned it in general and in detail. Some of his objections are easily seen to be based on a simple misunderstanding of parts of Kronecker's elementary algebra. This applies in particular to some of the strictures on Kronecker's theory of negatives, and a similar oversight occurs in connection with objections to the treatment of irrationals and fractions.

Although it may be presumptuous to attempt to convince anyone temperamentally opposed to Kronecker's program that it is not the bizarre futility it is sometimes said to be, nevertheless it may be recalled that some of the techniques outlined or used by Kronecker in his memoir and in its companion on algebraic “magnitudes” have had, and still have, wide application in theory of algebraic numbers, the theory of algebraic functions and the theory of modular systems, all of which are severely technical mathematical disciplines untainted by speculative impracticality or mathematical nihilism. In short, Kronecker's mathematics in his sketch of the program, *as mathematics*, needs no defense. Nor is it necessarily true that the historical development of the number system is the best for a modern presentation. The historical development is, in fact, not followed: we

³ A. C. Black, *The Nature of Mathematics* (1933), p. 177. Black refers “for a full discussion and criticism of Kronecker's views” to

⁴ L. Couturat, *De l'Infini Mathématique*, (1896), pp. 603-616. This book had a wide circulation a generation ago.

do not torture ourselves as the ancients vainly did to produce a civilized theory of common fractions; we do not repeat, even in the elementary schools, the endless arguments which the early algebraists found necessary before they would admit negative numbers to a parity with the positives; nor do we trouble our souls with profound doubts about "sophistical quantities" when some equation incontinently presents us with an imaginary root. To attack Kronecker's program on the ground that it is unhistorical is to render aid and comfort to the enemy.

Before going on to the simple detail in connection with negative numbers, we recall that Cauchy⁵ originated the device of algebraic congruences as an alternative, "real," way of handling complex numbers. This device is that which Kronecker extends and exploits to the limit to give him the algoristic half of his theory. The other, less tangible, half concerns Kronecker's theory of adjunction and is much harder to justify to a hostile critic of the program and to clear once and for all of the charge of circularity. The historical origin of the abstract principles behind the theory of adjunction can be traced, I believe, to Kummer, who was one of Kronecker's teachers. Kronecker's specific application of the principles is entirely his own.

NEGATIVE NUMBERS

The theory is based on the concept of what is now called a *semi-field*. It will be sufficient to define the terms used, state the postulates, and give only enough of the theorems deduced from the postulates to dispose of one objection which has been raised against Kronecker's algorithms. The proofs of the theorems are almost immediate from the definitions and postulates. What follows is an abstract of the first part of a paper by Wedderburn.⁶ The postulates for equality, =, are presupposed.

⁵ A. L. Cauchy, *Exercices d'Analyse et de Physique Mathématique*, Tome 4, (1847), pp. 87-110. One remark of Cauchy's is rather amusing, coming as it does from the inventor of the theory of functions of a complex variable:

"In the theory of algebraic equivalences [congruences] substituted for the theory of imaginaries, the letter i will cease to represent the symbolic sign $\sqrt{-1}$, which we repudiate completely, and which we can abandon without regret, because nobody knows what this sham sign signifies, nor what meaning is to be attributed to it."

⁶ J. H. M. Wedderburn, Algebraic Fields, *Annals of Mathematics, Second Series*, vol. 24 (1923), pp. 236-264.

Let D denote a set of elements (or "marks") a, b, c, \dots , finite or infinite in number, which satisfy the following postulates.

P. If a, b are any elements of D , not necessarily distinct, there exist two single-valued functions of a, b , denoted by $a + b$ and $a \times b$ respectively, and these functions have the following properties.

A₁. $a + b$ is an element of D .

A₂. $a + b = b + a$.

A₃. $a + (b + c) = (a + b) + c$.

A₄. If $a + b = a + c$, then $b = c$.

A₅. There is an element o such that $o + o = o$.

M₁. $a \times b$ is an element of D .

M₂. $a \times b = b \times a$.

M₃. $a \times (b \times c) = (a \times b) \times c$.

M₄. If $a \times b = a \times c$, but $a + b \neq b$, then $b = c$.

M₅. There is an element $1 \neq o$ such that $1 \times 1 = 1$.

AM₁. $(a + b) \times c = a \times c + b \times c$.

AM'₁. $c \times (a + b) = c \times a + c \times b$.

AM₂. If $a \times c + b \times d = a \times d + b \times c$, and $a \neq b$, then $c = d$.

The " o " in A₅ might be denoted by z , and the " 1 " in M₅ by u , to emphasize that these are not necessarily the zero and unity of common arithmetic. But as there can be no confusion, we let $o, 1$ stand as they are.

A set D satisfying these postulates is called a *semi-field* (because the inverses of $+$, \times , which would give subtraction and division, as in a field, are not postulated). Note that the elements a, b, c, \dots of D are *any* marks satisfying the postulates. The point of departure is thus set farther back than Kronecker's, in which the positive integers are taken as the starting point. This (as Wedderburn remarks) is merely a matter of convenience for what is to follow. It is evident that an *instance* of a semi-field is obtained from D when we take as the elements the positive integers and zero, and for $+$, \times the plus, times of common arithmetic. To prevent a possible misunderstanding, the $+$, \times of the postulates might be enclosed in circles, as is sometimes done, but this is unnecessary.

The argument will be clearer if we state first what is to be done, following Cauchy and therefore also Kronecker. What immediately follows is merely descriptive. Assuming, known say, the real numbers, we can *classify* all the polynomials with real coefficients in the *real variable* i by means of the "division transformation" with respect to a given polynomial, say $i^2 + 1$, as follows. Dividing the polynomial $f(i)$ by $i^2 + 1$ we get a quotient $q(i)$ and a remainder $r(i)$, both of which are polynomials with real coefficients, and the degree of $r(i)$ is less than that of the divisor. Thus, when the divisor is $i^2 + 1$, we can express $f(i)$ in the form

$$f(i) = q(i) (i^2 + 1) + ai + b,$$

where a, b are real. Different polynomials may give the same remainder. All those polynomials which give the same remainder $ai + b$ are defined to belong in the same *class*. A particular class contains one and only one remainder, say $ai + b$. Hence this class, being completely specified by the unique remainder $ai + b$, may be denoted by $\{ai + b\}$, and $ai + b$ may be taken as the *representative* of the class. Any two polynomials belonging to a given class are said to be *congruent* with respect to the *divisor* as a *modulus*, or *congruent mod the divisor*. Here, two polynomials $f(i), g(i)$ in the class $\{ai + b\}$ are congruent mod $i^2 + 1$, and this is written

$$f(i) \equiv g(i) \pmod{i^2 + 1},$$

which is merely an expression of the fact that $f(i)$ and $g(i)$, when divided by $i^2 + 1$ give the same remainder $ai + b$. We need not go into the excellent reasons for adopting this seemingly involved manner of stating an elementary fact; it is sufficient to emphasize here that the *remainders* $ai + b$ and the corresponding *classes* $\{ai + b\}$ are the important things for our present purpose. If the divisor is any polynomial with real coefficients, the procedure is the same.

Suppose, however, that we are not operating with polynomials whose coefficients are any *real* numbers (positive, negative, fractional), but have restricted ourselves to polynomials whose

coefficients are elements of the set $0, 1, 2, 3, \dots$ of common arithmetic. Then it is easily seen that, *in the form of the division transformation furnished by common division, as in elementary algebra, the preceding classification breaks down.* For there will be remainders in which the coefficients are *negative* or *fractional*, and *neither the negatives nor the fractions* are included in the set $0, 1, 2, 3, \dots$. For example, dividing $x^2 + 2x$ by $x^2 + 1$ we get

$$x^2 + 2x = 1(x^2 + 1) + 2x - 1;$$

the remainder is $2x - 1$, and we might be tempted to say that $x^2 + 2x$ belongs to the class $\{2x - 1\}$. But as we have now restricted ourselves to zero and the *positive* integers $1, 2, 3, \dots$, the symbol -1 in $2x - 1$ has no meaning, and $\{2x - 1\}$ does not denote a class, but is entirely meaningless.

We have elaborated this because it is an example of the type of objection to Kronecker's algorithms which is based upon a simple misunderstanding of his elementary algebra. This is the kind of objection with which we are concerned here. To be specific, I shall quote (in translation) exactly what Couturat says (loc. cit. p. 613) in part with regard to Kronecker's project for avoiding the negatives, $-1, -2, -3, \dots$.

"The congruence $7 + 9x \equiv 3 + 5x \pmod{x + 1}$ states that the remainders of the two members, divided separately by the modulus, are equal. Now if we divide each of the binomials $(7 + 9x)$ and $(3 + 5x)$ by $(x + 1)$, we get in each case the remainder -2 , that is to say, the negative number which would result from the subtractions, impossible by hypothesis."

Here it is a question of *avoiding the negatives*, and Couturat is pointing out that if we go through the elementary algebra of dividing as demanded by the congruence, then we get the negative -2 , which is forbidden, negatives being, by hypothesis, meaningless when the set of permissible coefficients is restricted to be $0, 1, 2, 3, \dots$. He gives further examples to emphasize his point. If Kronecker's algorithm did anything of this sort, the objection would be well taken. But the algorithm was carefully constructed so as to avoid this and similar pitfalls. It is clear that if we postulate only a semi-field as the domain of the coeffi-

cients, neither subtraction nor division of coefficients as in common algebra is permitted, as subtraction and division are undefined for a semi-field. Hence it must be shown that the division transformation can be constructed in a *semi-field*. Continuing with Wedderburn's paper, we abstract enough of his theorems to reach the correct form of the division transformation for a *semi-field*.

A polynomial $f(x)$ is said to be in the semi-field D if its coefficients are elements of D . Instead of "element of D " we shall say "element"; $\circ, \mathbf{1}$ are as in the postulates A_5, M_5 .

DEFINITION. Any element z such that $a + z = a$ for every a (in D) is called a *null element*.

THEOREM 1. \circ is the only null element in D .

THEOREM 2. $a \times \mathbf{1} = a$.

DEFINITION. An element x such that $a \times x = a$ for every element of D which is not a null element is called an *identity element*.

THEOREM 3. $\mathbf{1}$ is the only identity element in D .

THEOREM 4. If a is any element, then $a \times \circ = \circ$.

Let x denote any element. Then, if n denotes a positive integer, x^n is uniquely defined, by M_2, M_3 .

DEFINITION. A polynomial in x is the sum of a finite number of elements and a finite number of terms of the form $a_i x^{n_i}$, where a_i ($i = 1, 2, \dots$) are given elements and x is a variable element and n_i ($i = 1, 2, \dots$) are positive integers.

We shall say that the polynomial is *in D* . Since $(a + b)x^m = ax^m + bx^m$, for any elements a, b, x and any positive integer m , it follows that any polynomial in x in D can be expressed in the form $a_0x^n + a_1x^{n-1} + \dots + a^n$, where n is a positive integer and a_i are elements of D . If the degree of the polynomial is one, the polynomial is called *linear*.

The next definition is of importance in reaching the correct form of the division transformation.

DEFINITION. Two polynomials in D in the same variable x are said to be *identically equal* if, and only if, they have the same value for every value of x in D . The sign for "identically equal" is \equiv .

THEOREM 5. *If two linear polynomials in D are identically equal, corresponding coefficients are equal.*

That is, if $ax + b$ and $cx + d$ are in D and are identically equal, then $a = c$ and $b = d$.

THEOREM 6. *If $f(x)$ is any polynomial in x in D , then there exist two polynomials $p(x)$, $q(x)$ in x in D , and a linear polynomial $ax + b$ in D such that*

$$f(x) + p(x)(x + 1) \equiv ax + b + q(x)(x + 1).$$

It is this theorem which, in the semi-field D , replaces the "division transformation" of common algebra when the divisor is $x + 1$. The "divisor" $x + 1$ is that appropriate for Kronecker's theory of negatives; $x^2 + 1$ is the "divisor" for Cauchy's and Kronecker's theory of complex numbers, and so on; for every "divisor" which it is necessary to discuss in Kronecker's theory there is an appropriate theorem replacing the corresponding "division transformation" of common algebra, and each such theorem is the expression of an identity, corresponding to that concerning $f(x)$ in THEOREM 6. The important point to be noted in this particular case is that on each side of the sign \equiv of identical equality in the theorem there is a polynomial which is in D . We have not passed out of the semi-field D from which we started.

DEFINITION. When, as in THEOREM 6,

$$f(x) + p(x)(x + 1) \equiv ax + b + q(x)(x + 1),$$

we say that $f(x)$ is congruent to $ax + b$ with respect to the modulus $x + 1$, and we write⁷

$$f(x) \equiv ax + b \pmod{x + 1}$$

The identical equality and the congruence express the same fact. Namely, if we assert the congruence, we might, if we wished, replace the congruence by the following assertion: "There exist polynomials $p(x)$ and $q(x)$ in x in D such that

$$f(x) + p(x)(x + 1) \equiv ax + b + q(x)(x + 1)."$$

⁷ The sign \equiv of identical equality in the first formula is not in danger of confusion with the same sign in the second formula, for in the latter \equiv is part of the compound sign " $\equiv \dots \pmod{\dots}$ " of congruence. The "mod" indicates that congruence, not identical equality is meant.

The precise forms of the $p(x)$, $q(x)$ corresponding to a particular $f(x)$ are of no importance for our purpose.

COROLLARY (to THEOREM 6). *If the polynomials $f(x)$, $g(x)$ in x in D are such that*

$$f(x) \equiv ax + b \pmod{x + 1}$$

and

$$g(x) \equiv ax + b \pmod{x + 1},$$

(where $ax + b$ is in D), then there exist polynomials $P(x)$, $Q(x)$, in x in D such that

$$f(x) + P(x)(x + 1) \equiv g(x) + Q(x)(x + 1).$$

The next definitions and immediate consequences of THEOREM 6 and the COROLLARY provide the basis for separating the totality of polynomials in x in D into classes.

DEFINITION. Polynomials in x in D which are congruent to the same linear polynomial in x in D with respect to the modulus $x + 1$ are said to be congruent to each other modulo $x + 1$.

From the definition of congruence, it follows that if

$$f(x) \equiv g(x) \pmod{x + 1},$$

and

$$g(x) \equiv h(x) \pmod{x + 1},$$

then

$$f(x) \equiv h(x) \pmod{x + 1}.$$

DEFINITION. The set of all polynomials in x in D which are congruent to the same polynomial $f(x)$ in x in D modulo $x + 1$ constitute the *residue class*, or simply *class*, denoted by $[f(x)]$, corresponding to $f(x)$.

DEFINITION. Two classes $[f(x)]$, $[g(x)]$ are equal if, and only if, any polynomial in x in D which is a member of $[f(x)]$ is also a member of $[g(x)]$, and every member of $[g(x)]$ is a member of $[f(x)]$.

By THEOREM 6, every class contains a polynomial of the form $ax + b$, which may be taken as the representative of the class.

THEOREM 7. The classes $[f(x)]$ and $[g(x)]$ are equal if, and only if, $f(x) \equiv g(x) \pmod{x + 1}$.

DEFINITIONS. $\circ, \mathbf{1}$ being as in A_5, M_5 , the class $[\circ]$ is called the *zero class*, and the class $[\mathbf{1}]$ the *identity class*. The *sum* of the classes $[f(x)]$ and $[g(x)]$ is the class $[f(x) + g(x)]$, and is denoted by⁸ $[f(x)] + [g(x)]$; the *product* of $[f(x)]$ and $[g(x)]$ is the class $[f(x)g(x)]$, and is denoted by $[f(x)] \times [g(x)]$. With these definitions we have

THEOREM 8. *The set, denoted by K , of all classes of polynomials in x in D forms a semi-field.*

The *elements* in K are the classes; the $+$, \times are the operations just defined in connection with classes, and the $\circ, \mathbf{1}$ are $[\circ], [\mathbf{1}]$. The proof of this theorem is somewhat detailed; see Wedderburn, loc cit. pp. 247–249.

THEOREM 9. If α is any element of K there exists a unique element β of K such that $\alpha + \beta = [\circ]$.

We have just seen in THEOREM 8 that K is a semi-field. Hence, in particular, the elements (residue-classes mod $x + 1$) of K satisfy the postulates A_1 to A_5 for addition in a semi-field. Suppose now that we write THEOREM 9 after A_5 , as is legitimate, since it has been deduced from the postulates for D , and merely re-label it A_6 . Then A_1 to A_6 , with $K, \alpha, \beta, \gamma, \dots, [\circ], [\mathbf{1}]$, in place of $D, a, b, c, \dots, \circ, \mathbf{1}$ are identical with the postulates for “addition” in a *field* (not merely a semi-field), in which subtraction, as understood in arithmetic and common algebra, is uniquely possible.⁹ The element β in THEOREM 9, merely to give it a name, may be called the “negative” of α in K . Thus every element α in K has a unique negative, which may be denoted by $-\alpha$, merely as a matter of writing. We have not committed the solecism of “solving” $\alpha + \beta = [\circ]$ for β and getting $\beta = [\circ], -\alpha, = -\alpha$; all we have done is to give β a new name and a new symbol, $-\alpha - \beta$, to indicate that it is the particular β prescribed by THEOREM 9 when α is given.

⁸ The “+” in $[f(x)] + [g(x)]$ refers to addition of *classes*, as defined; the “+” in $[f(x) + g(x)]$ refers to addition in the semi-field D . Similarly for x .

⁹ For the postulates of a field see L. E. Dickson, *Algebras and their Arithmetics*, p. 201, or the papers by Dickson or E. V. Huntington in *Transactions of the American Mathematical Society*, vol. 4 (1903) pp. 13–20, vol. 6 (1905) pp. 181–204.

It has been shown, therefore, that from any semi-field D a new set can be constructed in which "subtraction," and "negatives," having the properties of subtraction and negatives in common algebra or arithmetic, can always be constructed. The like follows for "division" and "reciprocals." Hence, from a semi-field, in which neither "subtraction" nor "division" is defined, we can construct a field. This is what was to be done.¹⁰

California Institute of Technology.

¹⁰ Since this note was written, a paper by H. S. Vandiver has appeared (*Proceedings of the National Academy of Sciences*, vol. 20, November 1934, pp. 579-584) bearing partly on Kronecker's program. It would be of considerable historical interest to know the exact date of Schatunovsky's first work on objections to the unrestricted use of the law of excluded middle, as some of his examples are even more illuminating than some of Brouwer's.

