THE JOURNAL OF SYMBOLIC LOGIC
Volume 8, Number 4, December 1943

A SYSTEM OF AXIOMATIC SET THEORY

PART V. GENERAL SET THEORY (CONTINUED).[53]

PAUL BERNAYS

13. General recursion. We have still to consider the extension of the methods of number theory to infinite ordinals—or to *transfinite numbers* as they may also, as usual, be called.

The means for establishing number theory are, as we know, recursive definition, complete induction, and the "principle of the least number." The last of these applies to arbitrary ordinals as well as to finite ordinals, since every non-empty class of ordinals has a lowest element. Hence immediately results also the following generalization of complete induction, called *transfinite induction*: If A is a class of ordinals such that (1) $0\eta A$, and (2) $a\eta A \rightarrow a'\eta A$, and (3) for every limiting number l, $(x)(x\epsilon l \rightarrow x\eta A) \rightarrow l\eta A$, then every ordinal belongs to A.

So for the generalization of the methods of number theory to arbitrary ordinals it remains only to inquire how recursive definition is to be generalized. The theorem answering this question (*the theorem of transfinite recursion*) can be derived from a more general theorem on recursion (*the general recursion theorem*) which is one of the fundamental theorems of set theory.[54] Before stating it, we introduce as a preliminary the *general concept of a sequence.*

By a *sequence* we understand a functional set whose domain is an ordinal. In particular, if n is an ordinal, an *n-sequence* is a sequence with the domain n. The elements of the converse domain of a sequence will be called the *members* of the sequence—so that a set is a member of a sequence s if and only if it is the second member of a pair which is in s.

By a *sequence* (or *n-sequence*) *of elements of* C, where C is a class, we mean a sequence (n-sequence) whose members belong to C. In this sense we speak in particular of a *sequence* (or *n-sequence*) of ordinals. And we speak also of a *sequence* (or *n-sequence*) *of elements of a set* c, meaning a sequence whose members are in c.

If G is a function whose domain is the class of all ordinals, a sequence which is a subset of G will be called a *segment* of G. For any ordinal n, the set which (by axiom V b) represents the class of elements $\langle a, c\rangle$ of G such that $a\epsilon n$, is a segment of G and will be called *the n-segment of* G. Similarly, if g is an m-sequence and $n\epsilon m$, the n-sequence representing the class of elements $\langle a, c\rangle$ of g such that $a\epsilon n$, will be called *the n-segment of* g.

Received June 9, 1941, with additions to §§14, 15 received August 26, 1941, and an addition to §13 received September 24, 1942.

[53] Parts I–IV appeared in this JOURNAL, vol. 2 (1937), pp. 65–77; vol. 6 (1941), pp. 1–17; vol. 7 (1942), pp. 65–89, 133–145.

[54] General recursion in the frame of the Fraenkel axiomatic set theory (with the strong form of the *Ersetzungsaxiom*, equivalent to our axiom V*) was established by von Neumann, on the basis of his independent theory of ordinals, in his paper *Über die Definition durch transfinite Induktion und verwandte Fragen der allgemeinen Mengenlehre*, ***Mathematische Annalen***, vol. 99 (1928), pp. 373–391.

According to these definitions we have in particular, for any class C, that the null set is a 0-sequence of elements of C, and the only one; and likewise for any set c the null set is a 0-sequence of elements of c, and the only one. And the 0-segment of any function whose domain is the class of all ordinals, or the 0-segment of any n-sequence, where n is an ordinal $\neq 0$, is the null set.

It is easily shown that, if n is an ordinal and $k \epsilon n$, the k-segment of the n-segment either of a sequence s whose domain is higher than n, or of a function G whose domain is the class of all ordinals, is identical with the k-segment of s, or of G.

We insert here at once some remarks on *ascending sequences of ordinals*. A sequence of ordinals will be called *ascending* if it is a numeration in the natural order. As is easily shown by transfinite induction, each member of an ascending sequence of ordinals is at least as high as the ordinal to which it is assigned.

An ascending sequence of ordinals whose domain is a limiting number is said to *have a limit* if the sum of its members is represented by a set. This set is then the lowest of those ordinals which are higher than every member of the sequence, and it is at least as high as the domain of the sequence. We call it *the limit of the sequence*. Every limiting number l is the limit of an ascending sequence of ordinals; for in particular the set of pairs $\langle n, n\rangle$, such that $n \epsilon l$, has the limit l.

A limiting number l will be called *irreducible* if every ascending sequence of ordinals whose limit is l has the domain l.

For every limiting number l there is a lowest of those limiting numbers k such that there exists an ascending k-sequence of ordinals whose limit is l. The ordinal so determined is an irreducible ordinal, as follows easily by the composition lemma and axiom V b. We shall call it *the lowest domdin for the limit l*.

Now we state the *general recursion theorem*: For any class A and any function F which assigns to every sequence of elements of A an element of A, there exists a function G whose domain is the class of all ordinals and whose value for an ordinal n is the value assigned by F to the n-segment of G.

Proof. Let us call a sequence s *adapted to F* if, for each of its elements $\langle n, c\rangle$, c is the value assigned by F to the n-segment of s.

If n is an ordinal and $r \epsilon n$, the r-segment of any n-sequence adapted to F is itself adapted to F. By the class theorem, there exists the class C of ordinals m such that there is one and only one m-sequence adapted to F.

Let k be an ordinal every element of which belongs to C. There exists the class of pairs $\langle n, c\rangle$ such that $n \epsilon k$ and c is the value assigned by F to the uniquely determined n-sequence which is adapted to F. This class, by V b, is represented by a set s which is a k-sequence of elements of A. We shall now show that s is adapted to F. For this purpose we have to verify that, if $n \epsilon k$, the value $s(n)$ is identical with the value of F for the n-segment of s. Let n be an element of k and let t be the uniquely determined n-sequence which is adapted to F. If $\langle r, a\rangle \epsilon t$, then $r \epsilon n$, $r \epsilon k$, and a is the value of F for the r-segment of t. But this r-segment, by our remark above, is adapted to F; hence it is the uniquely determined r-sequence which is adapted to F, and a is the value of F for this sequence. Thus we have $t(r) = s(r)$ for every $r \epsilon n$, so that t is the n-segment of s, and the value $s(n)$, which is the value assigned by F to the n-sequence t, is the value of

F for the n-segment of s. So in fact s is adapted to F. Furthermore, if s_1 is any k-sequence adapted to F, and $n \epsilon k$, then the n-segment of s_1 is the uniquely determined n-sequence which is adapted to F, so that $s_1(n) = s(n)$. Accordingly we have $s_1 = s$. So s is the only k-sequence adapted to F, and $k \eta C$.

Thus we have that, if every element of an ordinal k belongs to C, then k itself belongs to C. So the class of ordinals not belonging to C cannot have a lowest element and consequently must be empty; in other words, every ordinal belongs to C.

In consequence, it follows by the class theorem that the function G exists whose domain is the class of all ordinals and which assigns to the ordinal k the value of F for the k-sequence adapted to F. From the above considerations it follows further that, for every ordinal k, the k-sequence adapted to F is the same as the k-segment of G, so that $G(k)$ is the value of F for the k-segment of G. Thus G is the function (depending on A and F) whose existence is asserted in our theorem.

For this proof, besides the axioms I–III, only V a, V b are required—and V a only for the theory of ordinals (so that instead of it here axiom VII would suffice).

Of the general recursion theorem there are, of course, many applications. As a particular consequence of it we note first the following theorem: If A is a class of ordinals such that, for every sequence of elements of A, there exists an element of A higher than every member of the sequence, then there exists a one-to-one correspondence C between the class of all ordinals and A, such that to the higher of any two ordinals is assigned the higher element of A—so that every segment of C is an ascending sequence.

This results by applying the general recursion theorem to the case that F is the function whose domain is the class of sequences of elements of A and which assigns to each of these sequences the next higher element of A. Thus there follows first the existence of a one-to-one correspondence C between the class of all ordinals and a subclass B of A, with the property that every segment of C is an ascending sequence. Then by means of the principle of the least number it is easily shown that $B = A$.

Let us further show how by means of the general recursion theorem we can obtain the Max Zorn *maximum principle*, which for many purposes in connection with abstract algebras may suitably be used instead of the well-ordering theorem, as has been noted by Zorn.[56]

For simpler formulation of the principle we introduce the following definitions of Zorn (slightly modified):

A set of sets is a *chain* if, for every two elements a, b of it, either $a \subset b$ or $b \subset a$.

(Under this definition, in particular, the null set is a chain, and, for every set a, the set (a) is a chain.)

A class A (or a set a) is *closed* if for every chain which is a subset of A (or a) the sum of its elements is represented by an element of A (or a).

(We note that every closed class, or set, has the null set as an element.)

---

[56] M. Zorn, *A remark on method in transfinite algebra*, ***Bulletin of the American Mathematical Society***, vol. 41 (1935), pp. 667–670.

We further define an element of a class (or a set) to be a *maximal* element if it is not a proper subset of any other element of that class (or set).

Now a formulation of Zorn's principle adapted to our present axiomatic frame is: *Every closed class of subsets of a set has a maximal element.*

Concerning this formulation of the principle we make the following remark. Zorn's original statement is that *every closed set has a maximal element.* From this our statement of the principle follows if we use V d, since by V d and V a every class of subsets of a set is represented by a set. On the other hand, from our statement, that of Zorn follows immediately if we apply V c. However, this application of V c can be avoided: in fact, as we shall see, Zorn's statement of his principle can be derived from our statement on the basis merely of the axioms I–III and V a. Moreover, under our distinction of classes and sets, our form of the statement is more advantageous for the applications for which the principle is intended. So it will be justified to speak here of the "Zorn maximum principle" in the sense of our above formulation, and to distinguish from this the "original statement" of the principle.

In order to derive the Zorn maximum principle from our axioms I–IV, V a, b it will be sufficient to show the following: If A is a closed class satisfying the condition that each of its elements is a proper subset of another element, then the elements of A cannot all be subsets of a set b. This in turn will follow if we show that, under the same assumptions on A, there exists a function L whose domain is a subclass of the sum S of the elements of A and whose converse domain is the class of all ordinals. In fact, if every element of A were a subset of b, then S would be a subclass of b, and therefore by V a every subclass of S would be represented by a set; thus from the existence of the function L it would follow by the theorem of replacement that the class of all ordinals were represented by a set, whereas we know it is not so represented.

Now the existence of the function L, under the stated conditions on A, results as follows, by means of the general recursion theorem. By one of the conditions on A, in consequence of the axiom of choice, there exists a function P assigning to each element c of A an element d of A such that $c \subset d$. Moreover, since A is closed, there exists, by the class theorem, a function F assigning to every sequence of elements of A an element of A in such a way that the following relations hold: $F(0) = 0$ $(0 \eta A)$; for every k'-sequence q, $F(q) = P(q(k))$; for a sequence q whose domain is a limiting number, in case the converse domain of q is a chain, $F(q)$ is the value of P for the element of A which represents the sum of the members of q, and in the contrary case $F(q) = 0$. Thus the general recursion theorem can be applied, and it follows by it that there exists a function G whose domain is the class of all ordinals and whose value for an ordinal k is the value of F for the k-segment of G. This function G, as is easily shown with the aid of transfinite induction, has the property that, for every ordinal m, $G(m)$ has an element which is not in $G(n)$ for any ordinal n lower than m.

Consequently, if H is the sum of the elements of the converse domain of G, and L is the function assigning to each element c of H the lowest of the ordinals m such that $c \; \epsilon \; G(m)$, the converse domain of L is the class of all ordinals. And the domain of L, being the sum of the values of G, which are elements of A, is a subclass of the sum S of the elements of A.—Thus L is a function of the required kind. And so the Zorn principle is seen to be provable by means of our axioms I–IV, V a, b.

There is another principle of a similar kind, intended for the same purposes as is that of Zorn, which was proposed by Oswald Teichmüller—who in his paper, *Braucht der Algebraiker das Auswahlaxiom?*,[56] not knowing of Zorn's publication, showed this principle to be sufficient for abstract algebras. Teichmüller's principle, of which he gives three equivalent statements, can be formulated as follows: *If A is a class of subsets of a set, such that a set c belongs to A if and only if every finite subset of c belongs to A, then A has a maximal element.*

This principle can be derived from the Zorn maximum principle. In fact it is easily shown, with an application of V a, that every class satisfying the hypotheses of the Teichmüller principle is closed.

On the other hand, from the Teichmüller principle we can obtain the original statement of the Zorn principle in two steps as follows. Observing first that a set is a chain if and only if every finite subset of it is a chain, we deduce from the Teichmüller principle the *theorem of the maximal chain*, viz.: *The class of those subsets of a set which are chains has a maximal element.*

Now let a be a closed set. By the theorem of the maximal chain, there exists among the subsets of a which are chains a maximal chain m; and the sum of the elements of m, since a is closed, is represented by an element s of a. The set s cannot be a proper subset of an element t of a. For if it were, the set n having as elements the sets c such that $c \epsilon m \vee c=t$ would be a subset of a and at the same time a chain, and m would be a proper subset of n; but this contradicts the defining property of m. Therefore s is a maximal element of a. So it results that every closed set has a maximal element.

In this way, finally, we have derived Zorn's original statement of his maximum principle from our statement by means of the axioms I–III, V a.

Remark. As has been observed for each of the two maximum principles by its author, there is the possibility of deducing from it the well-ordering theorem, but for this the power axiom V d is necessary. On the other hand, the axiom of choice in the form of our axiom IV, referring to arbitrary classes of pairs, apparently is not deducible from the maximum principles even with the aid of V d.

There is also an easy proof of the theorem of adapted numeration as a consequence of the general recursion theorem, as follows. Let c be a non-empty set (the theorem being obvious in the case of the null set), let a be an element of c, and let F be a function which assigns to every proper subset p of c an element of $c \dot{-} p$. Then the sum T of F and the class whose single element is $\langle c, a\rangle$ is a function which assigns to every subset of c an element of c. Furthermore by the class theorem there exists a function P assigning to every sequence of elements of c the value of T for the converse domain of this sequence. By the general recursion theorem there exists a function G whose domain is the class of all ordinals and which assigns to every ordinal n the value of P for the n-segment of

[56] ***Deutsche Mathematik***, vol. 4 (1939), pp. 567–577. See the review by Rózsa Péter in this JOURNAL, vol. 6 (1941), pp. 65–66.

G. This function G cannot be a one-to-one correspondence; for if it were, then, since the the converse domain of G is a subclass of c and therefore (by V a) is represented by a set, it would follow by V b that the domain of G, namely the class of all ordinals, were represented by a set.

There must, therefore, exist different ordinals for which the value of G is the same; and the class of those ordinals for which the value of G is the same as for some lower ordinal has a lowest element m. Now the m-segment of G, which is a sequence of elements of c, is a one-to-one correspondence. Its converse domain must be the set c itself. For if it were a proper subset p of c, then $G(m)$, which is the value of P for the m-segment of G, i.e. $T(p)$, would be identical with $F(p)$ and thus not in p; then the m'-segment of G would still be a one-to-one correspondence, contrary to the definition of m. It follows that the m-segment of G is a numeration of c; and obviously this numeration is adapted to F.

In this way the numeration theorem and the well-ordering theorem can be derived from the general recursion theorem.

We now still have to apply the general recursion theorem, as originally intended, to the derivation of a theorem of transfinite recursion, extending the theorem of finite recursion to arbitrary ordinals. Within general set theory as we have defined it this application is not at all immediate. But a direct passage from the general recursion theorem to a satisfactory theorem of transfinite recursion becomes possible as soon as the axiom V c is adjoined. In fact, as we know, this axiom in combination with the theorem of replacement yields the sum theorem,[57] and from the latter theorem it follows directly that the sum of the members of any sequence is represented by a set. Using this in connection with the general recursion theorem, we obtain immediately the following *strong theorem of transfinite recursion*: If A is a class, a an element of A, and P a function assigning, to every pair $\langle n, c\rangle$ of an ordinal n and an element c of A, an element of A, then there exists a function K, uniquely determined by a and P, whose domain is the class of all ordinals and which satisfies the conditions that $K(0) = a$, and $K(n') = P(\langle n, K(n)\rangle)$ for every ordinal n, and, for every limiting number l, $K(l)$ is the set representing the sum of the members of the l-segment of K.

For the existence of such a function K follows from the general recursion theorem by taking for F the function whose domain is the class of sequences of elements of A and whose value for an n-sequence s of elements of A is a if $n = 0$, or, if n is the successor m' of an ordinal m, is P $(\langle m, s(m)\rangle)$, or, if n is a limiting number, is the set by which the sum of the members of s is represented (in consequence of the sum theorem). And by transfinite induction it follows immediately that the value of K for an ordinal n is uniquely determined by n, a, and P.

This (strong) theorem of transfinite recursion may be applied to the case that A is the class of all ordinals, and it then allows the introduction of functions of arbitrary ordinals by recursive definitions, in the usual fashion.

In this way a comparatively simple foundation of transfinite arithmetic is possible. And for this purpose it might seem desirable to adjoin the axiom

[57] See Part II, §4, p. 3.

V c to the axioms of general set theory—or, what amounts to the same thing, to take the axioms I–IV and V** as basis for general set theory. This stronger conception of general set theory—we shall call the axiomatic system to which it gives rise the *strengthened system of general set theory*—is of course advantageous in some respects. But it conflicts with our idea (expressed in §11) of separating from general set theory the existential statements concerning cardinal numbers which lead to the Cantor hierarchy of powers. In fact, in the strengthened system of general set theory it follows, as a consequence of the theorem that the sum of the members of any sequence is represented by a set, that for every sequence of cardinals which has no highest member there exists a higher cardinal.

If our idea of §11, for general set theory (proper), is to be found practicable, we must show how a general method of transfinite recursion, applying in particular to the recursive introduction of functions of arbitrary ordinals, can be established on the basis merely of the axioms I–IV, V a, b. For this purpose we require a number of preliminary results, including the proof of the pair class axiom from the axioms I–IV, V a, b.

14. Sum and product of arbitrary ordinals. Proof of the pair class axiom. We wish next to introduce the notion of the sum of arbitrary ordinals. For this purpose we begin by defining the *sum* $a+n$ *of an arbitrary ordinal* a *and a finite ordinal* n as the value for n of the iterator on a of the function which assigns to every ordinal c the value c'. By complete induction it follows that, for an arbitrary ordinal a and any finite ordinals m and n, we have $a+(m+n) = (a+m)+n$.

Corresponding to any ordinal a there are ordinals c for which there exists a finite ordinal n such that $a = c+n$; and it is easily seen that the lowest such ordinal c cannot be a successor. Thus for any ordinal a there exist ordinals b and n, n being finite and b either 0 or a limiting number, such that $a = b+n$. Moreover, for a given a, b and n are uniquely determined, as is easily shown. The finite ordinal n will in particular be called *the finite residual of* a.

By means of finite residuals we can extend the familiar distinction between even and odd numbers to arbitrary ordinals, calling an ordinal *even* or *odd* according as its finite residual is expressible in the form $n+n$ or in the form $n+n'$.

If a is a limiting number, the class of pairs $\langle b+n, b+(n+n)\rangle$, such that b is either 0 or a limiting number lower than a, and n is a finite ordinal, is readily shown to be a one-to-one correspondence between a and the class of even elements of a. Similarly, the class of pairs $\langle b+n, b+(n+n')\rangle$, with b and n satisfying the same conditions as before, is a one-to-one correspondence between a and the class of odd elements of a.

Further, if a is any infinite ordinal, n the finite residual of a, and b the limiting number for which $a = b+n$, then the class of pairs which have either the form $\langle b+k, k\rangle$ with $k \epsilon n$, or the form $\langle m, n+m\rangle$ where m is a finite ordinal, or the form $\langle r, r\rangle$ where r is an infinite ordinal lower than b, is a one-to-one correspondence between a and b. Thus every infinite ordinal number a is of equal power with some limiting number not higher than a. It follows in particular that *every infinite cardinal number is a limiting number.*

Now we prove readily that *if the classes A and B are represented by sets, their sum is represented by a set.* As previously remarked,[58] we may, in consequence of V a, restrict ourselves to the case that A and B have no common element. Let r and s be the respective cardinal numbers of the sets representing two classes A and B having no common element. Since our conditions on A and B are symmetrical, we may suppose that r is not higher than s. If r is finite, we prove by complete induction the existence of a one-to-one correspondence between the ordinal $s+r$ and the class $A \mathbf{+} B$, and the latter, by V b, is therefore represented by a set. If r is infinite, s is also infinite, and r and s, being cardinals, are limiting numbers. As above, there exists a one-to-one correspondence between r and the class of even elements of r. The even elements of r are also even elements of s. Further, there exists a one-to-one correspondence between s and the class of odd elements of s. From this, using the composition lemma, we infer that there is a one-to-one correspondence between a subclass of s and the class $A \mathbf{+} B$, and the latter, by V a and V b, is therefore represented by a set. Thus in either case the sum of A and B is represented by a set.

Now (as we did in §11 on the basis of the pair class axiom) we may define the *set-sum* $a \mathbf{+} b$ of sets a and b as the set representing the sum of the classes represented by a and b.

From the preceding, in consequence of the Bernstein theorem, it follows also that if a set a is not of higher power than b and b is infinite, then $a \mathbf{+} b \backsim b$. Hence if $a \prec c$, and $b \prec c$, and c is infinite, then $a \mathbf{+} b \prec c$.

We may now introduce the *sum $a+b$ of arbitrary ordinals a and b*, as follows. We first consider the class of pairs $\langle r, 0\rangle$ such that $r \epsilon a$, and the class of pairs $\langle r, 1\rangle$ such that $r \epsilon b$. By V b these classes are represented by sets p, q, and so their sum is represented by the set-sum $p \mathbf{+} q$. A well-ordering of the latter set is constituted by the class of those pairs which have one of the three forms:

$\langle\langle r, 0\rangle, \langle s, 0\rangle\rangle$ with $s \epsilon a$ and $r = s \vee r \epsilon s$;

$\langle\langle r, 1\rangle, \langle s, 1\rangle\rangle$ with $s \epsilon b$ and $r = s \vee r \epsilon s$;

$\langle\langle r, 0\rangle, \langle s, 1\rangle\rangle$ with $r \epsilon a$ and $s \epsilon b$.

Moreover this well-ordering, by the theorem of adapted numeration, is associated with a certain numeration of $p \mathbf{+} q$. The domain of this numeration of $p \mathbf{+} q$ we define to be the *sum* $a+b$.

Under this definition, the relation $a+b = c$ between ordinals a, b, c amounts, as is easily seen, to the following: a is not higher than c (and thus is a subset of c) and b is the domain of the numeration of $c \div a$ in the natural order. This relation can be formulated by a constitutive expression, and from the preceding reasoning it follows that, for any ordinals a, b, there is a unique ordinal c such that $a+b = c$. Hence there exists the class of triplets $\langle\langle a, b\rangle, c\rangle$ such that a, b, c are ordinals and $a+b = c$; and this class is a function whose domain is the pair class of the class of all ordinals.

An ordinal b for which there exists an ordinal a such that $a+b = c$ will be called a *residual of* c.

From our definition of $a+b$ it follows further that for arbitrary ordinals a and b we have $a+0 = a$ and $a+b' = (a+b)'$. Hence our general definition of

[58] See Part IV, §11, p. 134.

$a+b$ is in agreement with the one previously given for the special case that b is finite.

Another consequence of our definition of the sum of ordinals is that, if a and c are ordinals and c is not lower than a, there exists an ordinal b such that $a+b = c$. Moreover, for given a and c, the ordinal b is uniquely determined. In fact, for arbitrary ordinals a, b, c, as is easily proved, we have $b \epsilon c \rightarrow a+b \;\epsilon\; a+c$. Hence in particular, if c is an ordinal other than 0, every ordinal a is lower than the ordinal $a+c$. And also, if l is a limiting number, the sum $a+l$ is the lowest ordinal that is higher than every sum $a+c$ for $c \epsilon l$; hence if l is a limiting number and a is any ordinal, then $a+l$ is also a limiting number.

That, for arbitrary ordinals a and b, b is not higher than $a+b$, can be proved by transfinite induction. Also by transfinite induction we obtain the associative law, $a+(b+c) = (a+b)+c$, for arbitrary ordinals a, b, c.

As for the power of the sum $a+b$ of ordinals a and b, since $a+b$ is the set-sum of a and a set of equal power with b, it follows from the properties of the set-sum which we derived above, that if at least one of a and b is infinite, then either $a+b \backsim a$ or $a+b \backsim b$. In particular, if c is an infinite cardinal and $a \epsilon c$ and $b \epsilon c$, then $a+b \prec c$ and consequently $a+b \;\epsilon\; c$; hence further, if $a \epsilon c$, then $a+c = c$. Thus every residual, $\neq 0$, of an infinite cardinal c is identical with c.

We come now to the proof of the pair class axiom as a theorem of general set theory. It will be derived as a consequence of the following *pair class theorem*: If the class C is represented by an infinite cardinal, then $C \times C \backsim C$.

Remark. Of course the one-to-one correspondence here stated is well known; but we have to show that it can be proved on the basis merely of our axioms I–IV, V a, b. As a matter fact, it will not even be necessary to use the axiom of choice, IV, in the proof.

Proof. We first observe that the condition on a cardinal c, that $C \times C \backsim C$, where C is the class represented by c, is equivalent, by V b, to the existence of a functional set representing a one-to-one correspondence between $C \times C$ and C. Hence we see that the condition in question can be formulated by a constitutive expression with c as its only free variable. And so the class of those infinite cardinals which do not satisfy the condition exists. Unless this class is empty, there must be a lowest cardinal belonging to it. Consequently it is sufficient to consider the case of an infinite cardinal c such that, for every lower infinite cardinal q, the class Q represented by q satisfies the condition $Q \times Q \backsim Q$.

A further reduction results from the following consideration. For any class of ordinals C, the class exists of those pairs $\langle a, b\rangle$ such that $a \eta C$, $b \eta C$, $a \epsilon b$; let us call it (for purposes of this proof) the *reduced pair class of* C. If E is the class of pairs $\langle b, b\rangle$ such that $b \eta C$, and H is the reduced pair class of C, and L is the converse class of H, then $C \times C = E \boldsymbol{+} (H \boldsymbol{+} L)$.

Obviously $E \backsim C$ and $L \backsim H$. And if C has at least three elements, it is of equal power with a subset of H. Now let C be the class represented by the infinite cardinal c. If it can be shown that H is of equal power with a subset of C, then by the Bernstein theorem it will follow that $H \backsim C$. Moreover, since C is represented by an infinite cardinal, it will follow from $H \backsim C$, $E \backsim C$, $L \backsim H$ that $E \boldsymbol{+} (H \boldsymbol{+} L) \backsim C$, or $C \times C \backsim C$.

Thus it remains only to show that, if c is an infinite cardinal, C the class represented by c, and H the reduced pair class of C, then H is of equal power with a subclass of C, and for this purpose we may assume that every class represented by an infinite cardinal lower than c is of equal power with its pair class.

We consider[59] the well-ordering R of H constituted by the class of elements $\langle\langle a, b\rangle, \langle d, e\rangle\rangle$ such that $\langle a, b\rangle \eta H$, and $\langle d, e\rangle \eta H$, and either $b \epsilon e$ or $b = e$ & $(a \epsilon d \vee a = d)$.

Let F be a function assigning to every sequence s of elements of H, according as the converse domain p of s is a proper subset of H or represents H, the first element of H in the order R which is not in p, or the first element of H in the order R. By the general recursion theorem there exists a function G whose domain is the class of all ordinals and whose value, for every ordinal n, is the value of F for the n-segment of G.

Three cases must be considered: (1) that G is a one-to-one correspondence between the class of all ordinals and a proper subclass H_1 of H; (2) that G is a one-to-one correspondenbe between the class of all ordinals and H; (3) that G is not a one-to-one correspondence.

Case (1) is, however, impossible. For if $\langle a, b\rangle\ \eta\ (H \div H_1)$, then, by the definition of F and G, every element $\langle d, e\rangle$ of H_1 must precede $\langle a, b\rangle$ in the well-ordering R, and hence either $e \epsilon b$ or $e = b$, and also $d \epsilon e$, therefore $d \epsilon b$. Consequently H_1 must be a subclass of the pair class P of the class represented by b'. Now if q is the cardinal number of b' (which is the same as the cardinal number of b) and Q is the class represented by q, then since q is lower than c we have $Q \times Q \sim q$ and therefore $P \sim q$. So by V b it follows that P is represented by a set, and therefore, by V a, H_1 is represented by a set. From the one-to-one correspondence between H_1 and the class of all ordinals then follows that the latter class is represented by a set; but this is impossible.

In case (3), there exists a one-to-one correspondence between some ordinal n and the class H, as follows by an argument which we have used already in our last proof of the theorem of adapted numeration.[60] This one-to-one correspondence, as also the one-to-one correspondence of case (2), has, by the definition of F and G, the property that the element of H assigned to the lower of two ordinals (belonging to the domain of the one-to-one correspondence) precedes, in the well-ordering R, that assigned to the higher ordinal. Thus in either case (2) or case (3) there exists a one-to-one correspondence K between a transitive class of ordinals and H, such that, for all elements k and l of the domain of K,

$$k \epsilon l \rightarrow \langle K(k), K(l)\rangle\ \eta\ R.$$

Let m be an element of the domain of K. Then $K(m)$ is an element $\langle a, b\rangle$ of H, and if M is the class of elements of H which precede $\langle a, b\rangle$ in the well-order-

[59] The following argument has been substituted for an earlier one which was more complicated, and which besides required the axiom of choice. This simplification was suggested by Gödel's proofs of the theorems 7.811 and 8.62 in his monograph ***The consistency of the continuum hypothesis*** (Princeton 1940). However, these proofs are based on the theorem 5.18 (proved by means of the power axiom), which coincides with our pair class axiom. Hence we here need to modify Gödel's method of proof.

[60] §13, p. 94.

ing R, we have $m \backsim M$. Let q be the cardinal number of b', Q the class represented by q, and B the class represented by b'. Then M is a subclass of $B \times B$, and

$$\begin{aligned} B \times B &\backsim Q \times Q \\ &\backsim Q. \end{aligned}$$

Therefore the cardinal number of m is not higher than q, and consequently $m \epsilon c$.

So the domain of K is a subclass of C, and therefore the converse domain of K, namely H, is of equal power with a subclass of C. But just this is what had to be shown.

This now completes the proof of the pair class theorem. (In order to see that the proof really avoids use of the axiom of choice it must be observed that for our definition of the cardinal number of a set, in the special case that this set is an ordinal, the reference to the numeration theorem is not needed.)

As a consequence of the pair class theorem we are now able immediately to prove the pair class axiom as a theorem. For let a and b represent the classes A and B respectively. If a and b are both finite, the pair class $A \times B$, as the sum of the elements of a finite class of finite sets, is finite; so in this case the pair class of A and B is represented by a set. If at least one of the sets a, b is infinite, the class $A + B$ and the set-sum $a + b$ are infinite. Let c be the cardinal number of $a + b$, and C the class represented by c. Then $A + B \backsim C$, and by the pair class theorem $C \times C \backsim c$, hence by the composition lemma $(A+B) \times (A+B) \backsim c$. Hence by axiom V b the pair class of $A + B$ is represented by a set, and, since $A \times B \subseteq (A+B) \times (A+B)$, we have by V a that $A \times B$ is also represented by a set.

Thus we have generally that the pair class of classes represented by sets is itself represented by a set. We may therefore define the *pair set* $a \times b$ of sets a, b, in the same way that we did before on the basis of the pair class axiom.

At the same time we obtain, for every infinite set a, the one-to-one correspondence $a \times a \backsim a$. Hence by the Bernstein theorem, for every infinite set a and every non-empty set b which is not of higher power than a, $a \times b \backsim a$, and $b \times a \backsim a$.

A further one-to-one correspondence obtainable here concerns the *class of mappings* of a set b into the class represented by a set a. If A is the class represented by a, this class of mappings is $A^{[b]}$; we shall denote it also by $a^{[b]}$.

From the obvious fact that for any set a there exists a one-to-one correspondence between a and a subclass of $2^{[a]}$, it follows readily that for every set b,

$$(a^{[b]} \backsim (2^{[a]})^{[b]}) \vee (a^{[b]} \prec (2^{[a]})^{[b]}).$$

Now by one of the formal laws stated in §11,

$$(2^{[a]})^{[b]} \backsim 2^{[a \times b]};$$

and combining this with the result just obtained concerning the power of the pair set $a \times b$, we have that, if a is not empty and not of higher power than b, and b is infinite, then

$$(a^{[b]} \backsim 2^{[b]}) \vee (a^{[b]} \prec 2^{[b]}).$$

Hence by the Bernstein theorem it follows that, if a is a set with at least two elements, b is an infinite set, and a is not of higher power than b, then $a^{[b]} \sim 2^{[b]}$. In particular, for every infinite set a, we have $a^{[a]} \sim 2^{[a]}$, and thus also the class of subsets of a is of equal power with the class of mappings of a into the class represented by a.—

We can also further apply the result concerning the existence of the pair set to the *general definition of the product of ordinals*, analogously to the way in which we have introduced the sum of arbitrary ordinals by using the existence of the set-sum of arbitrary sets. For this purpose we consider, for arbitrary ordinals a, b, a special well-ordering of the pair set $a \times b$, namely the class of those pairs of elements of $a \times b$ which have one of the three forms:

$\langle q, q\rangle$ with $q \in a \times b$;

$\langle\langle m, r\rangle, \langle n, r\rangle\rangle$ with $m \in n$, $n \in a$, and $r \in b$;

$\langle\langle m, r\rangle, \langle n, s\rangle\rangle$ with $m \in a$, $n \in a$, $r \in s$, and $s \in b$.

By the theorem of adapted numeration, this well-ordering of $a \times b$ is associated with a numeration of $a \times b$, and we define the domain of this numeration to be the *product* $a \cdot b$ of a and b.

Thus the relation $a \cdot b = c$ among the ordinals a, b, c is defined to mean that there exists a numeration of the pair set $a \times b$ having the domain c and satisfying the condition that, if the element $\langle m, r\rangle$ of $a \times b$ is assigned to a lower ordinal than that to which the element $\langle n, s\rangle$ is assigned, then either $r \in s$, or $r = s$ and $m \in n$. And by the preceding argument it follows that there is always a unique numeration of $a \times b$ with the required properties.

From this it is seen that the relation $a \cdot b = c$ can be formulated by a constitutive expression, so that there exists a function assigning to every pair of ordinals $\langle a, b\rangle$ the value $a \cdot b$, and for every ordinal a there exists a function assigning to every ordinal b the value $a \cdot b$.

As further consequences of the definition of the product, we have, for arbitrary ordinals a, b, c:

$$0 \cdot b = 0, \qquad a \cdot 0 = 0, \qquad a \cdot 1 = a, \qquad a \neq 0 \;\&\; b \neq 0 \rightarrow a \cdot b \neq 0;$$

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad \text{and hence } a \cdot b' = a \cdot b + a;$$

$$a \neq 0 \;\&\; b \in c \rightarrow a \cdot b \in a \cdot c;$$

also if $a \neq 0$ and l is any limiting number, the product $a \cdot l$ is the limit of the ascending l-sequence assigning to every element n of l the value $a \cdot n$.

Using the preceding results, we prove by transfinite induction that the equation,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$

is valid for arbitrary ordinals a, b, c.

As to the cardinal number of the product of ordinals a, b, it follows from our result concerning the cardinal number of the pair set that, if at least one of the ordinals a, b is infinite, and neither is 0, then the cardinal number of $a \cdot b$ is identical with the cardinal number of a or the cardinal number of b, whichever is higher, and thus also identical with the cardinal number of $a + b$. —

We now go on to apply our results concerning the existence of the pair set, and its cardinal number, as we intended, to the proof of a theorem of transfinite recursion.

15. Transfinite recursion. Remarks on formal algebra. As we saw in §13, there is possible in the strengthened system of general set theory an easy derivation of a theorem of transfinite recursion from the general recursion theorem. The sum theorem, which was required for this, is not available in general set theory, based on the axioms I–IV, V a, b alone. But we do have a certain substitute for it. In fact we shall prove, in general set theory, the following *sum lemma*:

If p is an infinite ordinal, and if s is a sequence such that, for every element n of its domain k, the cardinal number of $s(n)$ is not higher than that of $p+n$, then the sum of the members of s is represented by a set whose cardinal number is not higher than that of $p+k$.

Proof. From the hypotheses it follows that the cardinal number of any member of s is at most as high as the cardinal number c of $p+k$. As a consequence of the axiom of choice and axiom V b, there exists a sequence f, with the domain k, which assigns to every element n of k a functional set representing a one-to-one correspondence between $s(n)$ and its cardinal number,which last is a subset of c. And by the class theorem there exists the class R of pairs $\langle\langle n, r\rangle, \langle n, t\rangle\rangle$ such that $n \epsilon k$, $r \epsilon s(n)$, and $t = (f(n))(r)$. This class R is evidently a one-to-one correspondence. Its converse domain B is a subclass of the pair set $k \times c$, hence by V a is represented by a set, and by V b (applied to the converse class of R) the domain A of R is also represented by a set. Moreover the class of pairs $\langle\langle n, r\rangle, r\rangle$ such that $\langle n, r\rangle \eta A$ is a function having the domain A, which is represented by a set, hence by the theorem of replacement the converse domain is represented by a set. This converse domain is, however, identical with the sum S of the members of s. Therefore S is represented by a set.

By the axiom of choice, S is of equal power with a subclass of A. Since $A \sim B$, we have that S is not of higher power than B. But B is a subclass of $k \times c$, and consequently the cardinal number of the set representing S is not higher than the cardinal number of the pair set $k \times c$. Since c is the cardinal number of $p+k$, and p is infinite, the cardinal number of $k \times c$ is not higher than c.

Thus we do have the existence of a set which represents the sum of the members of s and whose cardinal number is not higher than the cardinal number of $p+k$.

Remark. From the sum lemma we can infer in particular that every infinite cardinal than which there is a next lower cardinal is an irreducible limiting number.

In fact if c is an infinite cardinal and p the next lower cardinal, then the cardinal number of an element of c cannot be higher than p. Therefore any ascending sequence of elements of c whose domain k is an element of c has, in consequence of the sum lemma, a limit whose cardinal number is not higher than that of $p+k$. But $p+k \sim p$. Therefore c cannot be the limit of an ascending sequence of ordinals with a domain lower than c, or in other words, c is irreducible.

On the other hand it can easily be shown that every irreducible limiting number is a cardinal.

Now by means of the sum lemma we prove the following *restricted theorem of transfinite recursion*:

If a and b are ordinals, b is infinite, and P is a function which assigns to every pair of ordinals $\langle n, c\rangle$ an ordinal whose cardinal number is not higher than that of $(b+c)+n$, then there exists a function K which assigns to every ordinal an ordinal in such a way that: (1) $K(0) = a$; (2) $K(n') = P(\langle n, K(n)\rangle)$ for every ordinal n; (3) for every limiting number l, $K(l)$ represents the sum of the members of the l-segment of K. Moreover, upon the conditions (1), (2), (3) on K, the value $K(n)$ for an ordinal n is uniquely determined by n, a, and P, and the cardinal number of $K(n)$ is not higher than that of $(a+b)+n$.

Proof. By the class theorem there exists a function F assigning to every sequence of ordinals an ordinal in such a way that for the 0-sequence its value is a, for a k'-sequence s its value is $P(\langle k, s(k)\rangle)$, for a sequence whose domain is a limiting number and the sum of whose members is represented by a set c its value is c, and for all other sequences of ordinals its value is 0. Then by the general recursion theorem there exists a function K whose domain is the class of all ordinals and which assigns to every ordinal n the value of F for the n-segment of K. Obviously K satisfies conditions (1) and (2). Using the class theorem again, let C be the class of ordinals n for which the cardinal number of $K(n)$ is not higher than that of $(a+b)+n$. We show by transfinite induction that every ordinal belongs to C. First obviously $0\eta C$. Further, by the given condition on P we have $n\eta C \rightarrow n'\eta C$, since, because b is infinite, the cardinal number of $(b+((a+b)+n))+n$ is the highest of the cardinals a, b, n and therefore identical with the cardinal number of $(a+b)+n'$. Thirdly, if l is a limiting number and every element of l belongs to C, then, where s is the l-segment of K, we have that for every element n of l the cardinal number of $s(n)$ is not higher than that of $(a+b)+n$; also $a+b$ is infinite; hence by the sum lemma the sum of the members of s is represented by a set c whose cardinal number is not higher than that of $(a+b)+l$; consequently $F(s) = c$, $K(l) = c$, and the cardinal number of $K(l)$ is not higher than that of $(a+b)+l$. So in fact for every limiting number l we have $(x)(x\epsilon l \rightarrow x\eta C) \rightarrow l\eta C$. Thus the three premisses required for the proof by transfinite induction that every ordinal belongs to C are satisfied. Hence it follows that for every ordinal n the cardinal number of $K(n)$ is not higher than that of $(a+b)+n$; also—on account of the sum lemma—that for every limiting number l, $K(l)$ represents the sum of the members of the l-segment of K, i.e., that K also satisfies condition (3).

It remains only to prove that if H is a function assigning to every ordinal an ordinal in such a way that conditions (1), (2), (3) are satisfied, then for every ordinal n, $H(n) = K(n)$. But this follows obviously by transfinite induction.

This (restricted) theorem of transfinite recursion—whose proof is now complete—affords a general method of introducing functions of ordinals. An instance of this method is the *extension of our former definition of* a^b, given for finite ordinals, *to arbitrary ordinals*.

Of course an extension of this definition is required only in case that there exist infinite ordinals, and we have to deal, therefore, only with this case. We apply our theorem of transfinite recursion, taking for a the ordinal 1, for P the function assigning to every pair of ordinals $\langle n, c\rangle$ the ordinal $c \cdot m$, where m is a fixed ordinal, and for b the lowest infinite ordinal or m according as m is finite or infinite. The required condition on P is satisfied, since the cardinal number of $c \cdot m$ is not higher than that of $b+c$. Thus we infer the existence of a function K, uniquely determined for a given m, which has the following properties: the domain of K is the class of all ordinals; $K(0) = 1$; for every ordinal n, $K(n') = K(n) \cdot m$; and for every limiting number l, $K(l)$ represents the sum of the members of the l-segment of K.

Denoting the value $K(n)$, which depends also on the parameter m, by m^n, we have, for arbitrary ordinals m, n:

$$m^0 = 1, \qquad\qquad m^{n'} = m^n \cdot m.$$

Moreover, for every limiting number l, m^l is the lowest of those ordinals which are at least as high as every one of the ordinals m^n for $n \epsilon l$ and m fixed.

For an ordinal m higher than 1 it follows by transfinite induction that, for all ordinals a, b,

$$a \,\epsilon\, b \rightarrow m^a \,\epsilon\, m^b,$$

so that for any limiting number l the class of pairs $\langle n, m^n\rangle$, such that $n \epsilon l$, is represented by an ascending sequence of ordinals, and the limit of this sequence is m^l.

Moreover by transfinite induction, in virtue of the properties of the sum and product of ordinals, the following equations result, for arbitrary ordinals a, b, m:

$$1^a = 1, \qquad (m^a) \cdot (m^b) = m^{(a+b)}, \qquad (m^a)^b = m^{(a \cdot b)}.$$

And it can also be shown that the class of triplets of ordinals $\langle\langle a, b\rangle, c\rangle$, such that $a^b = c$, exists.

Remark. The general definition of m^n for ordinals m, n, by transfinite recursion, refers to the general definition of the product of ordinals. We have defined the product of arbitrary ordinals m, n by means of a well-ordering of the pair set $m \times n$. But we could as well have extended our definition of the product of finite ordinals to arbitrary ordinals m, n by applying the restricted theorem of transfinite recursion (upon the assumption that there exist infinite ordinals) to the case that m is a fixed ordinal, the ordinal a of the theorem is 0, the function P is the class of pairs $\langle\langle n, c\rangle, c+m\rangle$ with n and c ordinals, and b is the lowest infinite ordinal or m according as m is finite or infinite. The correctness of this procedure is due to the circumstance that in our proof of the restricted theorem of transfinite recursion no reference is made to the concept of the product of arbitrary ordinals.

As regards the concept of the sum of arbitrary ordinals, it has to be observed that the references to it in the sum lemma and in the restricted theorem of transfinite recursion could be avoided. In fact the occurrences of the sum of arbitrary ordinals in these theorems have to do only with the cardinal number of a sum $a+b$ of ordinals a, b of which one at least is infinite. But this cardinal number is "the maximum of the cardinal numbers of a and b," i.e., it is the cardinal number of a or the cardinal number of b according as a is higher than b or not. Thus the use of the sum of arbitrary ordinals can be eliminated from the formulation and the proofs of these two theorems. And it is then also possible, as is easily seen, to base the general definition of the sum of ordinals upon the restricted theorem of transfinite recursion.

Now having established the general basis for the development of transfinite arithmetic within our general set theory, we do not enter into further details. Comparing our method for the foundation of the theory of transfinite numbers, as it is brought about by the restricted axiomatic basis of our general set theory, with the usual method, we see that the difference lies chiefly in a changed order of treatment, certain considerations relating to the notion of power coming in at an earlier place under our method.

From the developments of Parts IV and V, taken altogether, it will appear that the axioms I–IV, V a, b constitute a sufficient axiomatic basis for general set theory. On the other hand we shall show in Part VI, by a method of von Neumann, that the axioms V c and V d cannot be derived as theorems from I–IV, V a, b, and in fact even that each of V c and V d is independent of all the other axioms I–VII, provided that the axioms I–VI are consistent. In particular the independence of V d will be proved in the stronger form that the axioms I-IV, V a, b, c, VI, VII are compatible with the additional assumption that every set is either finite or enumerable.

As a supplement to our survey of classical arithmetic which we have made on the basis of our axiomatic system, we insert at this point a brief *discussion of formal algebras*, which could have been made already at the end of §6.

Formal algebras can be treated within our axiomatic system on the basis of the axioms I-III, V a, or else of I-III, VII—either set being, as we have seen, sufficient for number theory and the theory of finite sets. Let us give here a few indications as to the first steps (in regard to which there is of course a certain amount of arbitrariness).

In formal algebras we have to deal with polynomials formed out of variables and coefficients by means of addition and multiplication. The coefficients are elements of a ring, i.e., of a class C for whose elements addition, subtraction, and multiplication are defined in such a way that the usual laws of computation are valid. The identity element for the operation of addition in C we shall call "zero."

As representatives of the variables we take the sets which either belong to the converse domain of the iterator on ((0)) of the function assigning to every set p the value (p) or else have two elements of which one belongs to this same converse domain and the other is a finite ordinal. The sets of the latter kind, having two elements, are representatives of variables with numerical subscripts; e.g., (((0)), 1) and (((0)), 2) may be taken as representatives of the variables x_1 and x_2 respectively. By this means we have the possibility of formulating theorems in which a numerical subscript of a variable appears as a parameter. The representatives of the variables constitute a class, of which they are the elements, and which we shall call Ξ.

In order to define polynomials as sets of a certain kind, we first introduce the notion of a complex. By a *complex* we understand a functional set the domain of which is a finite subset of Ξ and every value of which is a finite ordinal different from 0. (The null set in particular is a complex, under this definition.) It is then easily seen that the class of all complexes exists.

The complexes are to be representatives of expressions like x^2y^3z, or $x_1^{k_1}x_2^{k_2} \cdots x_n^{k_n}$ where $k_1, k_2, \cdots, k_n$ are positive integers.

By the *algebraic product of a complex h and a complex k* we understand the functional set whose domain is the set-sum c of the domain a of h and the domain b of k and whose value for an element t of c is $h(t)+k(t)$, or $h(t)$, or $k(t)$, according as t is in both a and b, or in a alone, or in b alone. Obviously, under this definition the algebraic product of complexes is again a complex.

An ordered pair whose first member is a complex and whose second member is an element of C will be called a *monomial over C*, and its second member will be called the *coefficient of the monomial.*

Now we define a *polynomial over C* to be a finite functional set whose elements are monomials over C. It is then easily seen that the class of all polynomials over C exists.

In cases where, as below, the class C remains fixed we may speak simply of "monomials" and "polynomials," omitting the qualifying phrase "over C."

The null set is a particular polynomial.

A polynomial p is said to be *equal* to a polynomial q if it differs from q only by monomials whose coefficient is zero. This relation obviously has the properties of an equality.

Besides polynomials we also have to consider finite sequences of monomials. For every polynomial p there exists an n-sequence of monomials which is a numeration of p, n being the number attributable to p.

We proceed now to introduce the elementary operations on polynomials. First the algebraic sum of polynomials is to be defined in a manner analogous to our definition of the algebraic product of complexes. By the *algebraic sum* of a polynomial p and a polynomial q we understand the functional set whose domain is the set-sum of the domain a of p and the domain b of q and whose value for an element t of its domain is $p(t)$, or $q(t)$, or the element of C resulting from the addition of $p(t)$ and $q(t)$, according as t is in a alone, or in b alone, or in both a and b.

The algebraic sum of polynomials, as thus defined, is obviously also a polynomial. And the algebraic sum of a polynomial equal to p and a polynomial equal to q is equal to the algebraic sum of p and q. Further, in consequence of the condition that C is a ring, the commutative and associative laws are valid for the algebraic sum of polynomials.

In order to define the algebraic difference of polynomials we first note that, since C is a ring, there is for each element a of C a uniquely determined element of C whose addition to a yields zero; we shall call it *the opposite element to a.* In consequence of this there exists for every polynomial p a uniquely determined polynomial having the same domain as p and assigning to each element c of this domain the opposite element to $p(c)$; this polynomial we shall call *the opposite polynomial to p.* Then the *algebraic difference* of a polynomial p and a polynomial q can be defined simply as the algebraic sum of p and the opposite polynomial to q.

For the definition of the algebraic product of polynomials we proceed in the following way. First we define the algebraic product of a polynomial p by a monomial $\langle k, b\rangle$ to be the set of pairs $\langle l, c\rangle$ for which there is an element $\langle h, a\rangle$ of p such that l is the algebraic product of the complexes h and k, and c is the element of C resulting from the multiplication of a by b. Then the algebraic product of a polynomial by a monomial is a polynomial.

Next we define the algebraic product of a polynomial by a finite sequence of monomials. By the theorem of finite recursion, if p is a polynomial and s is an m-sequence of monomials, where m is a finite ordinal, there exists a function K assigning to every finite ordinal a polynomial in such a way that $K(0) = 0$, and for every ordinal n lower than m, $K(n')$ is the algebraic sum of the polynomial $K(n)$ and the algebraic product of p by the monomial $s(n)$, and for every finite ordinal n not lower than m, $K(n') = K(n)$. The value of this function K for the ordinal m is a polynomial which is uniquely determined by the polynomial p and the sequence s; we shall call it the algebraic product of p by s.

Then, using the class theorem, complete induction, and the commutative and associative laws for the algebraic sum of polynomials, we can show that, if p and q are polynomials, we have for every numeration s of q that the algebraic product of p by s (as just defined) is the same polynomial. I.e., the algebraic product of a polynomial p by a sequence of monomials which is a numeration of a polynomial q is uniquely determined by p and q. Hence we define this to be the *algebraic product* of the polynomial p by the polynomial q.

Under this definition, polynomials p and q have always a uniquely determined algebraic product, and the algebraic product of a polynomial equal to p by a polynomial equal to q is equal to the algebraic product of p by q.

Now it can be proved, for the algebraic sum, algebraic difference, and algebraic product of polynomials over C, in consequence of the foregoing definitions, that all the familiar laws of computation, corresponding to the laws of addition, subtraction, and multiplication in the ring C, are valid as laws of equality.[61]

This therefore provides a basis for the further development of formal algebras.

ZURICH

[61] In order to avoid distinguishing between equality and identity, we may introduce the notion of a proper polynomial, defining a polynomial over C to be a *proper polynomial* if every element of its converse domain is different from zero. As is easily seen, there is for every polynomial a uniquely determined proper polynomial equal to it, which is obtained from it by omitting the elements (monomials) with the coefficient zero. The class of proper polynomials exists. Then we may define the *proper algebraic sum* of proper polynomials p and q as the proper polynomial which is equal to the algebraic sum of p and q; and analogously the *proper algebraic difference* and the *proper algebraic product* of proper polynomials can be defined. With respect to the operations thus defined the class of proper polynomials constitutes a ring. (Added September 12, 1943.)