

ROOTS AND FACTORS OF ORDINALS

PHILIP W. CARRUTH

1. **Introduction.** An ordinal X is termed a *root* of an ordinal A of index B if $X^B = A$. In §2 of this paper we employ the Cantor normal form¹ of an ordinal and make extensive use of a result of Sherman's, [3, Theorem 2.1], to determine necessary and sufficient conditions for one ordinal to be a root of another. By means of these conditions it is shown that the set of roots of an ordinal is a closed set (that is, it contains the least upper bound of each subset of it), and thus that two ordinals either have no root in common or a greatest common root. Also an immediate consequence of these conditions is the known result [1, p. 191, (13), Theorem] that an ordinal has an infinite number of roots if and only if it is indecomposable.² We also give necessary and sufficient conditions for an ordinal to have a greatest root less than itself.

In §3, we use results of Jacobsthal [1 and 2] to prove a theorem of which the fact that the set of left factors of an ordinal is closed (proved by other methods in [3] and [6]) and our result in §2 that the set of roots of an ordinal is closed are simple corollaries. Although the proof in this section is shorter than that in §2, the method used in §2 has the advantage of giving additional information concerning the roots of an ordinal, and it further demonstrates the usefulness of the Cantor normal form as a tool in investigations of this sort.

§4 is concerned with the decomposition of an ordinal into the product of prime factors. An ordinal is *prime* if it is not the product of two ordinals less than itself. It is known [1, p. 183, (17), Theorem] that an ordinal is prime if and only if it is one of the following: a prime integer, one greater than a transfinite indecomposable ordinal, an indecomposable power of ω . An ordinal can be written as the product of a finite number of prime factors, but this representation is not always unique. Sieczka [4] and Jacobsthal [1, p. 184, Theorem]

Presented to the Society, October 30, 1948; received by the editors October 21, 1948 and, in revised form, May 28, 1949.

¹ See [5] for information concerning the Cantor normal form and arithmetic operations with ordinals. Henceforth in this paper, whenever an ordinal is written as the sum of powers of ω , it will be assumed that the summation is the Cantor normal form. Numbers in brackets refer to the bibliography at the end of the paper.

² Throughout this paper, the term *indecomposable* will mean *indecomposable with respect to the operation of addition*.

showed that every ordinal has a unique prime factorization provided that certain additional conditions are satisfied by the factorization. We give some alternative additional conditions that insure the uniqueness of the prime factorization. The prime factorization satisfying these conditions has the possible advantage of using the minimum number of factors.

2. Powers and roots of ordinals. Throughout this section we let $A = \sum_{i=0}^s \omega^{\alpha(i)} a_i > 0$, $\alpha(0) = \sum_{i=0}^r \omega^{\gamma(i)} c_i$ or 0 , $X = \sum_{i=0}^m \omega^{\beta(i)} b_i > 1$, and $B = \sigma + n \geq 1$, where σ is a limit ordinal or 0 and n is a non-negative integer.

We shall define three types of ordinals A . The definitions will be so made that an ordinal will have a root less than itself if and only if it is of at least one of the three types. The division of such ordinals into types is strictly formal and is only necessary so that the statements of theorems concerning conditions for one ordinal to be a root of another will not become overly involved.

A is of *type I* if:

1. $s = 0$.
2. a_0 is an integral power, greater than the first, of an integer greater than 1, and/or $\alpha(0) > 0$.

A is of *type II* if $s < 0$ and if there exist an integer j , $0 \leq j \leq r$, and a factor p_j of c_j such that:³

1. $j > 0$ and/or $p_j > c_j$.
2. $(\omega^{\gamma(j)} p_j + \sum_{i=j+1}^r \omega^{\gamma(i)} c_i) (\sum_{i=0}^{j-1} \omega^{-\gamma(i)+\gamma(i)} c_i + c_j/p_j - 1) < \alpha(s)$.

It is noted that the integer j described for type II is not unique; namely, let $A = \omega^{\omega^2+2} + \omega^{\omega^2+1}$. Then j could be either 0 (in which case p_j could be taken to be 1) or 1 (in which case p_j could be taken to be 2).

A is of *type III* if $s > 0$, and if there exist integers j , $0 \leq j \leq r$, and m and n such that:

1. $j > 0$ and/or $m < s$.
2. $mn = s$.
3. $\alpha(km) = \sum_{i=0}^{j-1} \omega^{\gamma(i)} c_i + \omega^{\gamma(i)} c_{j,k} + \sum_{i=j+1}^r \omega^{\gamma(i)} c_i$ for $0 \leq k \leq n - 1$ ($c_{j,0} = c_j$).
4. $c_{j,k}/(n-k) = p_j$ is an integer for $0 \leq k \leq n - 1$.
5. $\alpha(s) = \sum_{i=0}^{j-1} \omega^{\gamma(i)} c_i$.
6. If $m > 1$, $-\alpha(km) + \alpha([k-1]m+i) = -\alpha(hm) + \alpha([h-1]m+i)$ for $1 \leq k, h \leq n$ and $1 \leq i \leq m - 1$.

³ Throughout this paper, whenever the upper limit of summation for the Cantor normal form of an ordinal is less than the lower limit, it is to be understood that the ordinal is 0.

- 7. If $n > 1$, $a_0 a_k = a_{km}$ for $1 \leq k \leq n - 1$.
- 8. If $m > 1$, $a_{km+i} = a_{hm+i}$ for $0 \leq k, h \leq n - 1$ and $1 \leq i \leq m - 1$.

$$A = \omega^{\omega^2+\omega 2} 2 + \omega^{\omega^2+\omega+2} 3 + \omega^{\omega^2+\omega} 10 + \omega^{\omega^2+2} 3 + \omega^{\omega^2} 5$$

is an example of an ordinal of type III. In this case $j = 1$, $m = 2$, and $n = 2$.

Condition (5) for type III implies that the integer j described for that type is unique. However, m and n are not uniquely determined; namely let $A = \omega^4 + \omega^3 + \omega^2 + \omega + 1$. Then $j = 0$ and both m and n could be 2 or m could be 1 and n could be 4.

It is noted that A could be of both types II and III; namely, let $A = \omega^{\omega^2+\omega+1} + \omega^{\omega^2+\omega}$. On the other hand, $A = \omega^{\omega+1} + \omega^\omega$ is of type III but not of type II; $A = \omega^4 + \omega^3$ is of type II but not of type III.

THEOREM 1. *Let B be greater than 1, and let $X^B = A$. Then A is of at least one of the types I, II, and III. Specifically:*

- 1. If $m = 0$ and/or $B = \sigma$, then A is of type I.⁴
- 2. If $m > 0$, $n > 0$, and $\beta(m) > 0$, then A is of type II.
- 3. If $m > 0$, $n > 0$, and $\beta(m) = 0$, then A is of type III.

PROOF OF (1). (1) is easily verified if X and B are integers. If X is an integer and $B \geq \omega$, then $X^{\sigma+n} = (X^\omega)^\mu X^n = \omega^\mu X^n$, where $\omega\mu = \sigma$. (It is easily verified that ω is a left factor of every limit ordinal.)

If $X \geq \omega$, $m = 0$, and $n > 0$, then $(\omega^{\beta(0)} b_0)^B = \omega^{\beta(0)B} b_0$ is of type I.

If $X \geq \omega$ and $B = \sigma$, then $(\sum_{i=0}^m \omega^{\beta(i)} b_i)^B = \omega^{\beta(0)\sigma}$ is of type I.

PROOF OF (2). In the proof of (2) and in further proofs we shall make use of [3, Theorem 2.1] which states that a necessary and sufficient condition that an ordinal Y be a left factor of an ordinal $D = \sum_{i=0}^k \omega^{\delta(i)} d_i$ is that either $0 < Y < \omega^{\delta(k)}$ or $Y = \omega^{\delta(j)} e_j + \sum_{i=j+1}^k \omega^{\delta(i)} d_i$, where e_j is a factor of d_j and $0 \leq j \leq k$.

$$\begin{aligned} X^B &= \omega^{\beta(0)B} b_0 + \omega^{\beta(0)(B-1)+\beta(1)} b_1 + \dots + \omega^{\beta(0)(B-1)+\beta(m)} b_m \\ &= \sum_{i=0}^m \omega^{\alpha(i)} a_i. \end{aligned}$$

Hence $\alpha(0) = \beta(0)B$. Since $n \neq 0$, it follows from [3, Theorem 2.1] that there exist an integer j , $0 \leq j \leq r$, and a factor p_j of c_j such that $\beta(0) = \omega^{\gamma(j)} p_j + \sum_{i=j+1}^r \omega^{\gamma(i)} c_i$. The proof of [3, Theorem 2.1] implies that $B = \sum_{i=0}^{j-1} \omega^{-\gamma(i)+\gamma(i)} c_i + c_j/p_j$. Since $B > 1$, $j > 0$ and/or $p_j < c_j$. The fact that $\alpha(s) = \beta(0)(B - 1) + \beta(s)$ implies that $\alpha(s) > \beta(0)(B - 1)$. Therefore condition (2) for type II is satisfied.

PROOF OF (3).

⁴ See also [1, p. 190, Corollary 1].

$$\begin{aligned}
 X^B &= \omega^{\beta(0)B}b_0 + \omega^{\beta(0)(B-1)+\beta(1)}b_1 + \dots \\
 &+ \omega^{\beta(0)(B-1)+\beta(m-1)}b_{m-1} \\
 &+ \omega^{\beta(0)(B-1)}b_0b_m + \omega^{\beta(0)(B-2)+\beta(1)}b_1 + \dots \\
 &+ \omega^{\beta(0)(B-2)+\beta(m-1)}b_{m-1} + \dots \\
 &+ \omega^{\beta(0)(\sigma+1)}b_0b_m + \omega^{\beta(0)\sigma+\beta(1)}b_1 + \dots \\
 &+ \omega^{\beta(0)\sigma+\beta(m-1)}b_{m-1} + \omega^{\beta(0)\sigma}b_m \\
 &= \sum_{i=0}^s \omega^{\alpha(i)}a_i.
 \end{aligned}$$

It is apparent that $mn = s$. Since $\beta(0)B = \alpha(0)$ and $n \neq 0$, [3, Theorem 2.1] implies that there are an integer j , $0 \leq j \leq r$, and a factor p_j of c_j such that $\beta(0) = \omega^{\gamma(j)}p_j + \sum_{i=j+1}^r \omega^{\gamma(i)}c_i$. It can be verified now that $B = \sum_{i=0}^{j-1} \omega^{-\gamma(i)+\gamma(i)}c_i + n$. Since $B > 1$, $j > 0$ and/or $m < s$.

$\beta(0)(B-k) = \alpha(km)$ for $0 \leq k \leq n$. Therefore $\alpha(km) = \sum_{i=0}^{j-1} \omega^{\gamma(i)}c_i + \omega^{\gamma(i)}c_{j,k} + \sum_{i=j+1}^r \omega^{\gamma(i)}c_i$ and $c_{j,k} = p_j(n-k)$ for $0 \leq k \leq n-1$.

$\beta(0)\sigma = \alpha(s) = \sum_{i=0}^{j-1} \omega^{\gamma(i)}c_i$, as can be verified by direct computation.

Since $\alpha([k-1]m+i) = \alpha(km) + \beta(i)$ for $1 \leq k \leq n$ and $1 \leq i \leq m-1$, if $m > 1$, it is seen that condition (6) for type III is satisfied. Conditions (7) and (8) are easily verified to be satisfied.

THEOREM 2. *Let A be of type I. Then X is a root of A if and only if one of the following conditions is satisfied:*

1. $X^n = a_0$, where n is a non-negative integer, and $X < \omega$.
2. $0 < \beta(0) < \omega^{\gamma(r)}$, if $a_0 = 1$.
3. $\beta(0) > 0$, $m = 0$, $b_0 = a_0$, $\beta(0) = \omega^{\gamma(j)}p_j + \sum_{i=j+1}^r \omega^{\gamma(i)}c_i$, where p_j is a factor of c_j and $0 \leq j \leq r$.

If (1) is satisfied, the index $B = \sum_{i=0}^r \omega^{1+\gamma(i)}c_i + n$. If (2) is satisfied, $B = \sum_{i=0}^r \omega^{-\tau+\gamma(i)}c_i$, where τ is the degree of $\beta(0)$ (that is, the greatest ordinal that appears as an exponent of ω in the Cantor normal form of $\beta(0)$). If (3) is satisfied, $B = \sum_{i=0}^{j-1} \omega^{-\gamma(i)+\gamma(i)}c_i + c_j/p_j$.

PROOF. Assume that (1), (2), or (3) is satisfied. Then using the corresponding value given for B , one can verify by direct computation that $X^B = A$.

Now assume that $X^B = A$ and that $B \neq 1$. (If $B = 1$, (1) or (3) is seen to hold.) The proof of (1) of Theorem 1 implies that if X is an integer, (1) must be satisfied.

If $\beta(0) > 0$, then the proof of (1) of Theorem 1 implies that either $a_0 = 1$ and $\beta(0)$ is a left factor of $\alpha(0)$ leaving a quotient that is a limit ordinal or that $m = 0$, $a_0 = b_0$, and $\beta(0)$ is a left factor of $\alpha(0)$

leaving a quotient that is not a limit ordinal. In the first case, [3, Theorem 2.1] implies that $0 < \beta(0) < \omega^{\gamma(r)}$. In the second case, this theorem implies that $\beta(0) = \omega^{\gamma(j)}p_j + \sum_{i=j+1}^r \omega^{\gamma(i)}c_i$, where p_j is a factor of c_j and $0 \leq j \leq r$.

THEOREM 3. *Let A be of type II but not of type III. Then X is a root of A if and only if $X = A$ or the following conditions are satisfied:*

1. $m = s$, $b_i = a_i$ for $0 \leq i \leq s$.
 2. $\beta(0) = \omega^{\gamma(j)}p_j + \sum_{i=j+1}^r \omega^{\gamma(i)}c_i$, where j and p_j satisfy the requirements for the integers j and p_j described for type II.
 3. $\beta(k) = -\beta(0)(\sum_{i=0}^{j-1} \omega^{-\gamma(i)+\gamma(i)}c_i + c_j/p_j - 1) + \alpha(k)$ for $0 < k \leq m$.
- If (1), (2), and (3) are satisfied, then the index $B = \sum_{i=0}^{j-1} \omega^{-\gamma(i)+\gamma(i)}c_i + c_j/p_j$.

PROOF. Assume that (1), (2), and (3) are all satisfied. Then using the value given for B , one can verify by direct computation that $X^B = A$.

Now assume that $X^B = A$ and that $B \neq 1$. Then by Theorem 1, X is a limit ordinal and $m > 0$. By the proof of (2) of Theorem 1, it is seen that (1) is satisfied and that $\beta(0)$ is a left factor of $\alpha(0)$ leaving a quotient that is not a limit ordinal. Hence [3, Theorem 2.1] implies that $\beta(0) = \omega^{\gamma(j)}p_j + \sum_{i=j+1}^r \omega^{\gamma(i)}c_i$, where p_j is a factor of c_j and $0 \leq j \leq r$, and that B has the value as stated in our theorem. Since $B > 1$, $j > 0$ and/or $p_j < c_j$. The proof of (2) of Theorem 1 also implies that $\beta(0)(B - 1) + \beta(i) = \alpha(i)$ for $0 < i \leq m$. Thus (2) and (3) of our theorem are seen to be satisfied.

THEOREM 4. *Let A be of type III but not of type II. Then X is a root of A if and only if $X = A$ or the following conditions are satisfied:*

1. $s = mn$, where m satisfies the requirements for the integer m described for type III.
 2. $\beta(0) = \omega^{\gamma(j)}p_j + \sum_{i=j+1}^r \omega^{\gamma(i)}c_i$, where j is the unique integer satisfying the requirements for the integer j described for type III.
 3. $p_j = c_{j,k}/(n - k)$ for $0 \leq k \leq n - 1$.
 4. If $m > 1$, $\beta(i) = -\alpha(km) + \alpha([k - 1]m + i)$ for $1 \leq k \leq n$ and $1 \leq i \leq m - 1$.
 5. $\beta(m) = 0$.
 6. $b_0 = a_0$, $b_m = a_n$, and if $n > 1$, $b_0b_m = a_{km}$ for $1 \leq k \leq n - 1$.
 7. If $m > 1$, $b_i = a_{km+i}$ for $0 \leq k \leq n - 1$ and $1 \leq i \leq m - 1$.
- If X satisfies these seven conditions, the index $B = \sum_{i=0}^{j-1} \omega^{-\gamma(i)+\gamma(i)}c_i + n$.

PROOF. Assume that the conditions (1) through (7) are satisfied. Using the value given for B , one can compute X^B . The normal form

for X^B will be that stated in the proof of (3) of Theorem 1. (2) and (3) of this theorem together imply that $\beta(0)(B-k) = \alpha(km)$ for $0 \leq k \leq n$. This fact together with (4) implies that if $m > 1$, $\beta(0)(B-k) + \beta(i) = \alpha([k-1]m+i)$ for $1 \leq k \leq n$ and $1 \leq i \leq m-1$. (6) and (7) now are sufficient to show that $X^B = A$.

Now assume that $X^B = A$ and that $B \neq 1$. Then by Theorem 1, $m > 0$, $\beta(m) = 0$, and B is not a limit ordinal. From the proof of (3) of Theorem 1 it is seen that $s = mn$, and $\beta(0)B = \alpha(0)$. Hence [3, Theorem 2.1] implies that $\beta(0) = \omega^{\gamma(i)}p_j + \sum_{i=j+1}^r \omega^{\gamma(i)}c_i$, where p_j is a factor of c_j and $0 \leq j \leq r$, and that $B = \sum_{i=0}^{j-1} \omega^{-\gamma(i)+\gamma(i)}c_i + n$. Since $B > 1$, $j > 0$, and/or $m < s$. Since $\beta(0)(B-k) = \alpha(km)$ for $0 \leq k \leq n-1$, by direct computation it is observed that $\alpha(km) = \sum_{i=0}^{j-1} \omega^{\gamma(i)}c_i + \omega^{\gamma(i)}c_{j,k} + \sum_{i=j+1}^r \omega^{\gamma(i)}c_i$ for these values of k , where $c_{j,k} = p_j(n-k)$. Since $\beta(0)(B-n) = \alpha(s)$, direct computation shows that j is the unique integer described for type III.

The proof of (3) of Theorem 1 implies that if $m > 1$, $\beta(i) = -\alpha(km) + \alpha([k-1]m+i)$ for $1 \leq k \leq n$ and $1 \leq i \leq m-1$, and also that (6) and (7) must hold. These facts together imply that m satisfies the requirements of the integer m described for type III.

THEOREM 5. *Let A be of both types II and III. Then X is a root of A if and only if one of the following three conditions is satisfied:*

1. $X = A$.
2. X satisfies conditions (1), (2), and (3) of Theorem 3.
3. X satisfies conditions (1) through (7) of Theorem 4.

THEOREM 6. *An ordinal has a root less than itself if and only if it is of at least one of the types I, II, and III.*

PROOF. This is an immediate consequence of Theorems 1 through 5.

THEOREM 7. *The set of roots of an ordinal is closed.*

PROOF. Let S be the set of roots of A . If A is of type I and $\alpha(0) = 0$, then S consists of a finite number of integers.

If A is of type I, $\alpha(0) > 0$, $a_0 > 1$, then S consists of a finite number of integers and of a finite number of ordinals that are greater than or equal to ω , since in $\sum_{i=0}^r \omega^{\gamma(i)}c_i$ there is only a finite number of coefficients, and each coefficient has only a finite set of factors.

If A is of type I, $\alpha(0) > 0$, and $a_0 = 1$, then S consists of all ordinals greater than 1 and less than or equal to ω raised to the power $\omega^{\gamma(r)}$ and of at most a finite number of ordinals greater than ω raised to the power $\omega^{\gamma(r)}$.

If A is of type II or of type III, S consists of a finite number of

ordinals greater than ω .

COROLLARY 1. *The set of roots of an ordinal is infinite if and only if the ordinal is indecomposable.⁵*

PROOF. This is an immediate consequence of the proof of Theorem 7 and the fact that the set of indecomposable ordinals is just the set of powers of ω .

COROLLARY 2. *A has a greatest root less than itself if and only if it is of types I, II, or III and is not equal to an indecomposable power of ω .*

PROOF. This follows immediately from Theorem 6 and the proof of Theorem 7.

THEOREM 8. *Two ordinals have no common root or a greatest common root.*

PROOF. This follows directly from Theorem 7, since the intersection (if not void) of the two sets of roots of two given ordinals will contain its least upper bound, which will be therefore the greatest common root of the two ordinals.

3. Ordinal functions. We begin this section by giving a few definitions and results from [1] and [2]. Following Jacobsthal [1], we let β_0 be a fixed ordinal and we let correspond to each ordinal $\alpha \geq \beta_0$ an ordinal $w(\alpha)$ having the property that if $\alpha > \alpha' \geq \beta_0$, then $w(\alpha) > w(\alpha')$. Now let ξ_0 and η_0 be two fixed ordinals. We let correspond to each pair of ordinals $\xi \geq \xi_0$, $\eta \geq \eta_0$ an ordinal $g(\xi, \eta)$ having the property that $g(\xi, \eta) > \xi$. Jacobsthal proved [1, Theorem II] that corresponding to given functions $w(\alpha)$ and $g(\xi, \eta)$ there is a fixed ordinal λ and a function $f(\alpha, \beta)$ defined for $\alpha \geq \lambda$, $\beta \geq 1$ with the properties:

1. $f(\alpha, 1) = w(\alpha)$.
2. $f(\alpha, \beta + 1) = g(f(\alpha, \beta), \alpha)$.
3. $f(\alpha, \bar{\beta}) = \lim_{\beta} f(\alpha, \beta)$, if $\bar{\beta}$ is a limit ordinal and β on the right side of equation (3) runs through all ordinals $\beta < \bar{\beta} = \lim \beta$.

The function g is called the *stem function* of f . A function defined as f is called a *C-function*. Throughout this section, $w(\alpha)$ will denote a function defined as is the function $w(\alpha)$ of [1, Theorem II], f will denote the corresponding *C-function*, and g will denote the stem function of f . Whenever the symbol $f(\alpha, \beta)$ is used, it will be assumed that $\beta \geq 1$ and that $\alpha \geq \lambda$, where λ is the ordinal λ described in [1, Theorem II]. It also will be assumed that g satisfies the following

⁵ See also [1, p. 191, (13), Theorem].

condition:

CONDITION A. If $\xi \geq \xi' \geq \xi_0$ and $\eta > \eta' \geq \eta_0$, then $g(\xi, \eta) > g(\xi', \eta')$ and $g(\xi, \eta') \geq g(\xi', \eta)$.

THEOREM 9. Let $f(\alpha, 1) \equiv \alpha$, and let $g = f_1$ be a C-function satisfying the condition $f_1(f_1(\alpha, \beta), \gamma) = f_1(\alpha, f_1(\beta, \gamma))$. Then for fixed γ , the set of all solutions α of the equation $f(\alpha, \beta) = \gamma$ is either vacuous or closed.

PROOF. Let Z be the set of all solutions α of the equation $f(\alpha, \beta) = \gamma$, and let Z_1 be any subset of Z . We assume that Z_1 is not vacuous. Let δ be the smallest ordinal that is greater than or equal to every ordinal in Z_1 . Suppose that δ is not in Z .

Let σ be the smallest ordinal satisfying the equation $f(\alpha, \sigma) = \gamma$, for α in Z_1 . Let τ be the smallest ordinal in Z_1 satisfying the equation $f(\tau, \sigma) = \gamma$.

[1, Theorem III] states that if $\beta > \beta'$, then $f(\alpha, \beta) > f(\alpha, \beta')$ and therefore that if $f(\alpha, \beta) > f(\alpha, \beta')$, then $\beta > \beta'$. [1, Theorem VII] states that if $\alpha \geq \alpha'$, then $f(\alpha, \beta) \geq f(\alpha', \beta)$, and if $f(\alpha, \beta) = f(\alpha', \beta)$ for $\alpha > \alpha'$, then β is a limit ordinal. Consequently it is seen that for $\alpha > \tau$ in Z_1 , $f(\alpha, \sigma) = \gamma$. Since according to our supposition there is no greatest element in Z_1 , [1, Theorem VII] also implies that σ is a limit ordinal.

Jacobsthal proved in [2, Theorem VIII] that under the hypotheses of our theorem, if σ is a fixed limit ordinal, then the set of all ordinals α satisfying the equation $f(\alpha, \sigma) = \gamma$ has a limit α_1 , and the equation $f(\alpha_1, \sigma) = \gamma$ has a solution σ_1 . According to our supposition $\alpha_1 \neq \delta$. Hence $\delta < \alpha_1$, and there exist two ordinals, α' and α'' , such that $\alpha' < \delta < \alpha''$ and such that $f(\alpha', \sigma) = f(\alpha'', \sigma) = \gamma$. But then it follows from [1, Theorem VII] that $f(\delta, \sigma) = \gamma$. This gives us a contradiction to our supposition.

The following corollary has been proved elsewhere by other methods [6, Theorem] and [3, Corollary 2.4].

COROLLARY 1. *The set of left factors of an ordinal is closed.*

PROOF. Let $g(\alpha, \beta) = f_1(\alpha, \beta) = \alpha + \beta$, and let $f(\alpha, \beta) = \alpha\beta$.

COROLLARY 2. *The set of roots of an ordinal is closed.*

PROOF. Let $g(\alpha, \beta) = f_1(\alpha, \beta) = \alpha\beta$, and let $f(\alpha, \beta) = \alpha^\beta$.

We prove another result of which [6, Lemma] is a corollary.

THEOREM 10. Let f satisfy the condition $g(f(\alpha, \beta), f(\alpha, n)) = f(\alpha, \beta + n)$ for finite n . Let σ be a fixed ordinal and τ a fixed limit ordinal. If ρ is a solution of the equation $g(\delta, \rho) = f(\sigma, \tau)$ and if $\delta < f(\sigma, \tau)$, then $\rho \geq f(\sigma, \omega)$.

PROOF. [1, Theorem VI] states that if β is given and if α is an ordinal such that $w(\alpha) \leq \beta$, then there is a unique ordinal ξ such that $f(\alpha, \xi + 1) > \beta \geq f(\alpha, \xi)$. This implies that since τ is a limit ordinal, there exists an ordinal $\mu < \tau$ such that $f(\sigma, \mu) > \delta$. Hence $f(\sigma, \tau) \leq g(f(\sigma, \mu), \rho)$ by Condition A.

Suppose that $\rho < f(\sigma, \omega)$. Then [1, Theorem VI] implies that there is an integer n such that $\rho < f(\sigma, n)$. Therefore $f(\sigma, \tau) < g(f(\sigma, \mu), f(\sigma, n)) = f(\sigma, \mu + n)$ by hypothesis and Condition A. Since $\mu + n < \tau$ [1, Theorem III] implies that this is a contradiction.

COROLLARY 1. *Let $f(\alpha, 1) \equiv \alpha$, and let g satisfy the two conditions, $g(g(\alpha, \beta), \gamma) = g(\alpha, g(\beta, \gamma))$ and $g(\alpha, \lim \beta) = \lim_{\beta} g(\alpha, \beta)$. Let σ be a fixed ordinal and τ a fixed limit ordinal. If ρ is a solution of the equation $g(\delta, \rho) = f(\sigma, \tau)$ and if $\delta < f(\sigma, \tau)$, then $\rho \geq f(\sigma, \omega)$.*

PROOF. This is an immediate consequence of [2, Theorem VI], which states that under the hypotheses of the corollary, it follows that $g(f(\alpha, \beta), f(\alpha, \gamma)) = f(\alpha, \beta + \gamma)$.

COROLLARY 2. *Let ρ be a remainder greater than 0 of $\sigma\tau$, where τ is a limit ordinal. Then $\rho \geq \sigma\omega$.*

COROLLARY 3. *Let ρ be a right factor greater than 1 of σ^τ , where τ is a limit ordinal. Then $\rho \geq \sigma^\omega$.*

4. **Prime factorization.** We revert to the notation of §2. We also let $\tau(b)$ stand for the number of prime factors in the unique prime factorization of the integer $b > 1$. We let $\tau(1) = 0$.

THEOREM 11. *An ordinal can be decomposed uniquely into a product of a finite number of prime factors if and only if it is not a limit ordinal. If A is not a limit ordinal, the number of prime factors in the unique decomposition of A is $s + \sum_{i=0}^s \tau(a_i)$.*

PROOF. If A is a limit ordinal, then $A = \omega R = 2\omega R$, and so the decomposition can not be unique.

Now assume that $\alpha(s) = 0$ and that $s > 0$. If $a_s = 1$, [3, Theorem 2.1] and [1, p. 183, (17), Theorem] imply that the only prime left factor of A is $\omega^{\alpha(s-1)} + 1$. In this case the quotient is $\sum_{i=0}^{s-2} \omega^{-\alpha(s-1) + \alpha(i)} a_i + a_{s-1}$.

If $a_s > 1$, [3, Theorem 2.1] implies that the only prime left factors of A are the prime integral factors of a_s . If p is a prime factor of a_s , then $A = p(\sum_{i=0}^{s-1} \omega^{\alpha(i)} a_i + a_s/p)$.

Since the quotient in each case again is not a limit ordinal and since prime factorization of integers is unique, a simple induction argument

shows that the prime factorization of A is unique. It is easily seen that the number of prime factors is $s + \sum_{i=0}^s \tau(a_i)$.

LEMMA. *Let an ordinal greater than 1 be indecomposable and not prime. Then it can be decomposed uniquely into the product, P_1P_2 , of two prime factors if the following additional condition is imposed: $QP_2 < P_1P_2$ for every prime ordinal Q that is less than P_1 .*

PROOF. Let A be greater than 1, indecomposable, and not prime. Then the proof of [3, Theorem 2.1] implies that A can be decomposed into the product, Q_1Q_2 , of two prime factors only if Q_2 is equal to ω raised to the power $\omega^{\gamma(r)}$. Let $Q_1 = \omega^\mu$ or $\omega^\mu + 1$. Then Q_1Q_2 is equal to ω raised to the power $\mu + \omega^{\gamma(r)}$. $Q_1Q_2 = A$ if and only if $\mu + \omega^{\gamma(r)} = \sum_{i=0}^r \omega^{\gamma(i)}c_i$; that is, $\mu = \delta + \eta$, where $\delta = \sum_{i=0}^{r-1} \omega^{\gamma(i)}c_i + \omega^{\gamma(r)}(c_r - 1)$, and $0 \leq \eta < \omega^{\gamma(r)}$. Hence our lemma is proved. In fact, P_2 is equal to ω raised to the power $\omega^{\gamma(r)}$, and $P_1 = \omega^\delta$ if δ is indecomposable, and $P_1 = \omega^\delta + 1$ if δ is decomposable.

THEOREM 12. *A can be factored uniquely into the product, $P_1P_2 \cdots$, of a finite number of prime ordinals if the following conditions are imposed:*

1. *The number, $\tau(A)$, of prime factors is the minimum into the product of which A can be decomposed.*
2. *If P_2 is a limit ordinal, then $QP_2 < P_1P_2$ for every prime ordinal Q that is less than P_1 .*

If A is not a limit ordinal, $\tau(A) = s + \sum_{i=0}^s \tau(a_i)$. If $\alpha(s)$ is greater than 0 and indecomposable, $\tau(A) = s + 1 + \sum_{i=0}^s \tau(a_i)$. If $\alpha(s)$ is decomposable, $\tau(A) = s + 2 + \sum_{i=0}^s \tau(a_i)$.

PROOF. If A is not a limit ordinal, the results follow from Theorem 11 and its proof.

Now let $\alpha(s)$ be greater than 0. By [3, Theorem 2.1], the only possible prime left factors of A are those prime ordinals less than or equal to $\omega^{\alpha(s)}$. If Q_1 is a prime left factor of A and if $A = Q_1B$, then $B = \sum_{i=0}^s \omega^{\beta(i)}a_i$, where $\beta(s) \geq 0$. Hence in order to factor A into the product of a finite number of prime factors, A must be factored as $Q_1 \cdots Q_n \sum_{i=0}^s \omega^{\phi(i)}a_i$, where $\phi(s) = 0$ and n is a positive integer, and $Q_1 \cdots Q_n = \omega^{\alpha(s)}$. To factor A into the product of the minimum number of prime factors, n must be made a minimum.

If $\alpha(s)$ is indecomposable, n will equal 1 if and only if we take Q_1 equal to $\omega^{\alpha(s)}$. Then $A = \omega^{\alpha(s)} \sum_{i=0}^s \omega^{-\alpha(s) + \alpha(i)}a_i = \omega^{\alpha(s)}C$. Since, by Theorem 11, C has a unique prime factorization, the factorization of A satisfying the required conditions is unique, and $\tau(A) = s + 1 + \sum_{i=0}^s \tau(a_i)$.

Now let $\alpha(s)$ be decomposable. Then $\omega^{\alpha(s)}$ is not prime, and so $n > 1$. Our lemma and Theorem 11 imply that A can be factored uniquely into the product, $P_1 P_2 \cdots$, of $s+2 + \sum_{i=0}^s \tau(a_i)$ prime factors, where P_2 is a limit ordinal, with the condition that QP_2 be less than $P_1 P_2$ for every prime ordinal Q that is less than P_1 .

COROLLARY. *A can be factored uniquely into the product of a finite number of prime ordinals with the single restriction that the number of prime factors be the minimum into the product of which A can be decomposed if and only if one of the following conditions is satisfied:*

1. $\alpha(s) = 0$; that is, A is not a limit ordinal.
2. $\alpha(s)$ is indecomposable; that is, $A = DE$, where D is an indecomposable power of ω , and E is not a limit ordinal.
3. $\alpha(s)$ is one greater than a decomposable ordinal; that is $A = D\omega E$, where D is a decomposable power of ω , and E is not a limit ordinal.

PROOF. This follows from Theorem 11 and the proof of our lemma and Theorem 12. In the case where $\alpha(s)$ is decomposable, the proof of the lemma implies that $\omega^{\alpha(s)}$ can be factored uniquely into the product of two prime factors with no further restriction, if and only if $\omega^{\alpha(s)} = (\omega^\rho + 1)\omega = \omega^{\rho+1}$, where ρ is decomposable.

BIBLIOGRAPHY

1. E. Jacobsthal, *Über den Aufbau der transfiniten Arithmetik*, Math. Ann. vol. 66 (1909) pp. 145–194.
2. ———, *Zur Arithmetik der transfiniten Zahlen*, Math. Ann. vol. 67 (1909) pp. 130–144.
3. S. Sherman, *Some new properties of transfinite ordinals*, Bull. Amer. Math. Soc. vol. 47 (1941) pp. 111–116.
4. F. Siczka, *Sur l'unicité de la décomposition de nombres ordinaux en facteurs irréductibles*, Fund. Math. vol. 5 (1924) pp. 172–175.
5. W. Sierpiński, *Leçons sur les nombres transfinis*, Paris, 1928.
6. ———, *A property of ordinal numbers*, Bull. Calcutta Math. Soc. vol. 20 (1930) pp. 21–22.

SWARTHMORE COLLEGE