ON THE ALGEBRAIC CLOSURE OF TWO

BY

H. W. LENSTRA, Jr.

(Communicated by Prof. J. H. van Lint at the meeting of January 29, 1977)

INTRODUCTION

J. H. Conway [4] discovered that the Class **On** of all ordinal numbers is turned into an algebraically closed Field $\mathbf{On}_2$ of characteristic two by the following inductive definitions of addition and multiplication:

$\alpha+\beta$ is the least ordinal distinct from all ordinals $\alpha'+\beta$ and $\alpha+\beta'$,
$\alpha\beta$ is the least ordinal distinct from all ordinals $(\alpha'\beta+\alpha\beta')+\alpha'\beta'$.

In each case, α' and β' range over all ordinals smaller than α and β, respectively. Conway has shown, inter alia, that a suitable beginning segment of $\mathbf{On}_2$ is an algebraic closure of the two-element subfield $\{0, 1\}$, cf. section 1. The purpose of this paper is to prove that, in this beginning segment, the field operations can be performed in an effective manner.

Following Conway we distinguish the ordinary ordinal operations from those in $\mathbf{On}_2$ by the use of square brackets [ ] – that is, all sums, products and powers appearing inside square brackets are meant in the sense of classical ordinal arithmetic, cf. Bachmann [2], and all others represent operations in $\mathbf{On}_2$. A single decimal digit between square brackets refers to the bibliography at the end of this paper. We denote by ω the least infinite ordinal, and we identify each ordinal number with the set of all previous ones. In particular, $2=\{0, 1\}$.

1. THE FIELD $[\omega^{\omega^\omega}]$

Every ordinal number has a unique expression

$$(1.1) \qquad [2^{\alpha_0}+2^{\alpha_1}+\ldots+2^{\alpha_{n-1}}], \text{ with } n\in\omega,\ \alpha_0>\alpha_1>\ldots>\alpha_{[n-1]},$$

and Conway proved that in this situation we have

$$(1.2) \qquad [2^{\alpha_0}+2^{\alpha_1}+\ldots+2^{\alpha_{n-1}}]=[2^{\alpha_0}]+[2^{\alpha_1}]+\ldots+[2^{\alpha_{n-1}}].$$

Since $\beta+\beta=0$ for every ordinal β this leads to the following addition rule: write each of the two ordinals to be added in the form (1.1), delete the terms occurring in both expressions, and [add] the remaining terms in decreasing order. Expressed differently: write the ordinals down in "binary" and then "add" without carrying.

Unfortunately, no such simple rule exists for multiplication. Below we

restrict ourselves to the ordinals $<[\omega^{\omega^\omega}]$, which, as Conway proves, form an algebraic closure of 2. In order to describe his results it is convenient to introduce some notation.

Let $q=[p^n]$ be a prime [power], with p prime and $n\in\omega$, $n\neq 0$, and let k denote the number of primes less than p (so $k=0$ if $p=2$, $k=1$ if $p=3$, etc.). Then we put

$$\varkappa_q=[2^{\omega^k\cdot p^{n-1}}]. \tag{1.3}$$

Notice that for two prime [powers] $q=[p^n]$ and $q'=[p'^{n'}]$ we have $\varkappa_q<\varkappa_{q'}$ if and only if $p<p'$ or $p=p'$, $n<n'$.

By the distributive law and (1.2), we are able to multiply two ordinals $<[\omega^{\omega^\omega}]$ if we know how to compute a product $[2^\alpha]\cdot[2^\beta]$, with $\alpha,\beta<[\omega^\omega]$. Each of α, β can be expressed as

$$[\omega^t\cdot n_t+\omega^{t-1}\cdot n_{t-1}+\ldots+\omega\cdot n_1+n_0],\quad \text{with } t,\ n_k\in\omega. \tag{1.4}$$

Writing n_k in base p, where p is the $[k+1]$-st prime number:

$$n_k=[\sum_j p^j\cdot m(j,k)],\quad 0\leqslant m(j,k)<p,$$

we see that any [power] of 2 belonging to $[\omega^{\omega^\omega}]$ has a unique expression as a decreasing product

$$[\prod_q \varkappa_q{}^{m(q)}]$$

with

$0\leqslant m(q)<p$ if q is a [power] of the prime p,

$m(q)=0$ for all but finitely many q.

Conway's results about $[\omega^{\omega^\omega}]$ now give rise to two multiplication rules. The first is, that in the situation just described we have

$$[\prod_q \varkappa_q{}^{m(q)}]=\prod_q \varkappa_q{}^{m(q)}.$$

Notice the analogy with (1.2). But this rule does not enable us to compute all products, since it may happen that $[m(q)+m'(q)]\geqslant p$ for some q. Thus it remains to specify the ordinals $(\varkappa_q)^p$. This is done by the second multiplication rule:

$$(\varkappa_{[2^n]})^2=\varkappa_{[2^n]}+\prod_{1\leqslant i<n}\varkappa_{[2^i]}, \tag{1.5}$$

$$(\varkappa_{[p^n]})^p=\varkappa_{[p^{n-1}]}\quad (p \text{ an odd prime},\ n\geqslant 2), \tag{1.6}$$

$$(\varkappa_p)^p=\alpha_p\quad (p \text{ an odd prime}), \tag{1.7}$$

where α_p is the smallest ordinal $<\varkappa_p$ which cannot be written as β^p, with $\beta<\varkappa_p$. For proofs of these statements we refer to [4].

The only obscure quantities here are the ordinals α_p. In section 3 we show that they can be effectively determined. It follows that multiplication

in $[\omega^{\omega^\omega}]$ can be performed effectively, if the ordinals are written as in (1.1) with exponents expressed in the form (1.4). The same holds for division, since every non-zero element of $[\omega^{\omega^\omega}]$ has finite multiplicative order. We leave it to the reader to deduce from (2.1) and (3.5) that the set of zeros of any one-variable polynomial with coefficients in $[\omega^{\omega^\omega}]$ can be determined effectively.

The proper beginning segments of $[\omega^{\omega^\omega}]$ which are at the same time subfields are precisely the ordinals $\varkappa_q$:

$$\varkappa_2 \subset \varkappa_4 \subset \varkappa_8 \subset \ldots \subset \varkappa_3 \subset \varkappa_9 \subset \ldots \subset \varkappa_5 \subset \ldots \subset [\omega^{\omega^\omega}].$$

Here $\varkappa_2$ is the prime field $\{0, 1\}$, and each $\varkappa_{[2^{n+1}]}$ $(n \in \omega,\ n \geqslant 1)$ arises from the preceding field $\varkappa_{[2^n]}$ by adjunction of the element $\varkappa_{[2^n]}$ which satisfies the Artin-Schreier equation (1.5) of degree 2. Further, if p is an odd prime, then $\varkappa_p$ is the union of the preceding fields, and each $\varkappa_{[p^{n+1}]}$ $(n \in \omega,\ n \geqslant 1)$ arises from the field $\varkappa_{[p^n]}$ by adjunction of the element $\varkappa_{[p^n]}$, which satisfies a Kummer equation (1.6), (1.7) of degree p. This leads to the following algebraic description of the fields $\varkappa_q$.

(1.8) PROPOSITION: For $\alpha \in [\omega^{\omega^\omega}]$, let the *degree* $d(\alpha)$ of α be the degree of the irreducible polynomial of α over 2. Then if $q = [p^n]$, p prime, $n \in \omega$, $n \geqslant 1$, we have

$$\varkappa_q = \{\alpha \in [\omega^{\omega^\omega}]: \text{ every prime dividing } d(\alpha) \text{ is } \leqslant p, \text{ and } q \text{ does not divide } d(\alpha)\}.$$

2. THE NUMBERS $\varkappa_h$

From (1.8) it is clear that $\varkappa_q$ is the smallest element of $[\omega^{\omega^\omega}]$ with a degree which is divisible by q, for any prime [power] q. Hence no confusion arises if we define

$$\varkappa_h = \min \{\alpha \in [\omega^{\omega^\omega}]: d(\alpha) \text{ is divisible by } h\}$$

for any $h \in \omega$, $h \neq 0$. Clearly, $\varkappa_1 = 0$. We show that each $\varkappa_h$ is a finite sum of terms $\varkappa_q$.

(2.1) THEOREM: Let $h \in \omega$, $h > 1$. Put

$$p = \text{smallest prime number dividing } h,$$
$$q = \text{highest [power] of } p \text{ dividing } h,$$
$$g = [h/q].$$

Then

$$\varkappa_h = \varkappa_g \text{ if } q \text{ divides } d(\varkappa_g),$$
$$\varkappa_h = \varkappa_g + \varkappa_q = [\varkappa_g + \varkappa_q] \text{ otherwise.}$$

(2.2) COROLLARY: For each $h \in \omega$, $h \neq 0$, there exists a unique finite set $Q(h)$ of prime [powers] for which

$$\varkappa_h = \sum_{q \in Q(h)} \varkappa_q.$$

Every $q \in Q(h)$ divides h and is relatively prime to $[h/q]$. Further, if $h > 1$ and p is the largest prime dividing h, then the highest [power] of p dividing h belongs to $Q(h)$.

PROOF: Corollary (2.2) follows from (2.1) by an obvious induction; for the uniqueness of $Q(h)$, cf. (1.2).

The proof of (2.1) is by induction on the number of different primes dividing h. If $h = q$ then $g = 1$ and the assertion is clear. Generally, since g divides h we have

$$\varkappa_h \geqslant \varkappa_g. \tag{2.3}$$

We shall also need

$$\varkappa_g + \alpha = [\varkappa_g + \alpha] \text{ for all } \alpha < \varkappa_q. \tag{2.4}$$

To see this, notice that the inductive hypothesis implies that $\varkappa_g$ is a finite sum of terms $\varkappa_{q'}$, each one of which is larger than $\varkappa_q$. The relation (2.4) then follows from (1.2).

In the first case, q divides $d(\varkappa_g)$. Since $d(\varkappa_g)$ is also divisible by g, it is divisible by h, so $\varkappa_g \geqslant \varkappa_h$, and (2.3) shows that $\varkappa_h = \varkappa_g$, as required.

Before treating the second case we prove a lemma.

(2.5) LEMMA: Let $\beta, \gamma \in [\omega^{\omega^\omega}]$. Then any prime [power] dividing $d(\beta)$ but not dividing $d(\gamma)$ divides $d(\beta + \gamma)$.

PROOF OF (2.5): From $\beta \in 2(\gamma, \beta + \gamma)$ we see that $d(\beta)$ divides the least common multiple of $d(\gamma)$ and $d(\beta + \gamma)$. The lemma follows.

Continuing the proof of (2.1), suppose that q does not divide $d(\varkappa_g)$. Since q does divide $d(\varkappa_q)$ it follows from (2.5) that q divides $d(\varkappa_g + \varkappa_q)$.

From (1.8) we see that every prime dividing $d(\varkappa_q)$ is $\leqslant p$. But every prime dividing g is $> p$. Therefore g and $d(\varkappa_q)$ are relatively prime. Also, g divides $d(\varkappa_g)$. Applying lemma (2.5) to the prime [powers] dividing g we conclude that $d(\varkappa_g + \varkappa_q)$ is divisible by g. Combined with the result of the previous paragraph this implies that $d(\varkappa_g + \varkappa_q)$ is divisible by h, so

$$\varkappa_h \leqslant \varkappa_g + \varkappa_q.$$

By (2.3) and (2.4), this means that

$$[\varkappa_g + 0] \leqslant \varkappa_h \leqslant [\varkappa_g + \varkappa_q].$$

This is only possible if $\varkappa_h = [\varkappa_g + \alpha]$ for some $\alpha < \varkappa_q$. Then $\alpha = \varkappa_h + \varkappa_g$ by (2.4), and (2.5) yields $q | d(\alpha)$. This implies $\alpha \geqslant \varkappa_q$ and the proof is finished.

3. THE NUMBERS α_p

For an odd prime number p, we define $f(p)=d(\zeta_p)$, where $\zeta_p \in [\omega^{\omega^\omega}]$ denotes a primitive p-th root of unity. Equivalently,

$$f(p) = \min \{h \in \omega : h \neq 0, \text{ and } p \text{ divides } [2^h - 1]\}.$$

Obviously $f(p)$ is a divisor of $[p-1]$.

(3.1) THEOREM: Let p be an odd prime number. Then there exist $m, m' \in \omega$ such that

$$\alpha_p = [\varkappa_{f(p)} + m] = \varkappa_{f(p)} + m'.$$

The number m is called the *excess* of α_p over $\varkappa_{f(p)}$.

PROOF: Since α_p is no p-th power in the field $\varkappa_p$, the p-th power map $2(\alpha_p) \to 2(\alpha_p)$ is not surjective. Consequently, it is not injective, so $\zeta_p \in 2(\alpha_p)$. This implies that $d(\alpha_p)$ is divisible by $d(\zeta_p) = f(p)$, and we find

$$\alpha_p \geqslant \varkappa_{f(p)}. \tag{3.2}$$

Conversely, since $d(\varkappa_{f(p)})$ is divisible by $f(p)$, we have $\zeta_p \in 2(\varkappa_{f(p)})$, so the p-th power map $2(\varkappa_{f(p)}) \to 2(\varkappa_{f(p)})$ is not injective. Therefore some element $\beta \in 2(\varkappa_{f(p)})$ is not a p-th power in $2(\varkappa_{f(p)})$. Since no subextension of $2(\varkappa_{f(p)}) \subset \varkappa_p$ has degree p over $2(\varkappa_{f(p)})$, it follows that β is still not a p-th power in $\varkappa_p$. But by lemma (3.4), stated and proved below, we can write β as a product of elements of the form $\varkappa_{f(p)} + m$, $m \in \omega$. It follows that there exists $m_0 \in \omega$ such that the element $\varkappa_{f(p)} + m_0$ of $\varkappa_p$ has no p-th root in $\varkappa_p$. We conclude

$$\alpha_p \leqslant \varkappa_{f(p)} + m_0. \tag{3.3}$$

By (1.2) we can write

$$\varkappa_{f(p)} = \lambda + m_1, \quad m_1 \in \omega,$$

in such a way that λ has the property

$$\lambda + m = [\lambda + m] \text{ for all } m \in \omega.$$

Then with $m_2 = m_1 + m_0$ we get from (3.2) and (3.3):

$$[\lambda + m_1] \leqslant \alpha_p \leqslant [\lambda + m_2].$$

This implies $\alpha_p = [\lambda + m_1 + m]$ for some $m \in \omega$, so

$$\begin{aligned} \alpha_p &= [[\lambda + m_1] + m] = [\varkappa_{f(p)} + m], \\ \alpha_p &= [\lambda + [m_1 + m]] = \lambda + [m_1 + m] = \\ &= \varkappa_{f(p)} + m_1 + [m_1 + m] = \varkappa_{f(p)} + m', \end{aligned}$$

where $m' = m_1 + [m_1 + m]$. This proves (3.1), modulo the following lemma.

(3.4) LEMMA: Let $\varkappa$ be any element of $[\omega^{\omega^\omega}]$. Then the multiplicative group of the field $\omega(\varkappa)$ is generated by the elements $\varkappa+m$, $m\in\omega$.

PROOF: Let $F=\sum_{i\in k} f_i X^i$ be the irreducible polynomial of $\varkappa$ over ω, and let $\beta=\sum_{j\in l} g_j \varkappa^j$ be any non-zero element of $\omega(\varkappa)$. Denote the finite subfield of ω generated by the coefficients f_i, g_j by μ. Then the polynomials $G=\sum_{j\in l} g_j X^j$ and F are relatively prime in the polynomial ring $\mu[X]$. Hence Kornblum-Artin's analogue of Dirichlet's theorem on primes in arithmetic progressions, cf. [1], p. 94, asserts, that for every sufficiently large $t\in\omega$ there exists an irreducible polynomial $H\in\mu[X]$ of degree t, which has leading coefficient 1 and belongs to the residue class (G mod F). The latter condition clearly means $H(\varkappa)=\beta$. If we choose t to be a [power] of 2 then H decomposes completely over the field $\varkappa_3=\omega$:

$$H=\prod_{i\in t}(X+m_i) \qquad (m_i\in\omega)$$

and substituting $\varkappa$ for X we get

$$\beta=\prod_{i\in t}(\varkappa+m_i).$$

This proves lemma (3.4).

(3.5) THEOREM: For every odd prime number p the number α_p can be effectively determined.

PROOF: Inductively, assume that for all odd primes $r<p$ the numbers α_r can be determined effectively. Then in the field $\varkappa_p$ all field operations can be performed effectively. In particular, for any non-zero $\beta\in\varkappa_p$ the multiplicative order $\mathrm{ord}(\beta)$ of β can be calculated, and the same is true for the degree $d(\beta)$:

$$d(\beta)=\min\{h\in\omega\colon h\neq 0, \text{ and } \mathrm{ord}(\beta) \text{ divides } [2^h-1]\}.$$

Thus, using theorem (2.1), one can determine the element $\varkappa_{f(p)}$ of $\varkappa_p$. It remains, by theorem (3.1), to find the smallest $m\in\omega$ such that $[\varkappa_{f(p)}+m]$ is no p-th power in $\varkappa_p$. But, by an argument in the proof of (3.1), an element β of $\varkappa_p$ is a p-th power in $\varkappa_p$ if and only if it is a p-th power in $2(\beta)$, which in turn is equivalent to the condition

$$\beta^{[(2^{d(\beta)}-1)/p]}=1 \text{ if } p \text{ divides } [2^{d(\beta)}-1]. \tag{3.6}$$

Hence, if one tries $\beta=[\varkappa_{f(p)}+m]$ for $m=0, 1, 2, \ldots$ in succession, then α_p is the first β for which (3.6) fails. This proves (3.5).

4. EXAMPLES

Table (4.1) gives, for each odd prime number $p\leqslant 43$, the value of $f(p)$, the elements of $Q(f(p))$ (cf. (2.2)), the excess of α_p over $\varkappa_{f(p)}$ (cf. (3.1)) and the value of α_p.

TABLE (4.1)

p	$f(p)$	$Q(f(p))$	excess	α_p
3	2	2	0	2
5	4	4	0	4
7	3	3	1	$[2^\omega]+1$
11	10	5	1	$[2\omega^2]+1$
13	12	3, 4	0	$[2^\omega]+4$
17	8	8	0	16
19	18	9	4	$[2^{\omega\cdot 3}]+4$
23	11	11	1	$[2\omega^4]+1$
29	28	7, 4	0	$[2\omega^3]+4$
31	5	5	1	$[2\omega^2]+1$
37	36	9, 4	0	$[2^{\omega\cdot 3}]+4$
41	20	5	1	$[2\omega^2]+1$
43	14	7	1	$[2\omega^3]+1$

The table provides examples for the following rules:

(4.2) if p is a Fermat prime, then the excess is 0 and $\alpha_p=[p-1]$;
(4.3) if $Q(f(p))=\{q\}$, q odd, then the excess is $\geqslant 1$;
(4.4) if $f(p)=[2\cdot 3^k]$ for some $k\in\omega$, $k>0$, then the excess is $\geqslant 4$.

We leave the reader the pleasure of finding the proofs.

An effective upper bound for the excess can be derived from a result of Carlitz [3]. I do not know whether the excess is absolutely bounded.

The set $Q(f(p))$ can be arbitrarily large:

(4.5) PROPOSITION: For any $t\in\omega$, $t>0$, there exists an odd prime number p for which $Q(f(p))$ has precisely t elements.

(4.6) LEMMA: For every $h\in\omega$, $h\notin\{0, 1, 6\}$, there exists an odd prime p for which $f(p)=h$.

PROOF OF (4.6): See [1], pp. 387–390.

PROOF OF (4.5): Choose, for every $j\in t$, a prime $q(j)$ with $f(q(j))=[3^{j+1}]$, using (4.6). Then $\alpha_{q(j)}=\varkappa_{[3^{j+1}]}+m_j$ and $d(\alpha_{q(j)})=[2^{n_j}\cdot 3^{j+1}]$ for certain m_j, $n_j\in\omega$. Next choose a prime p with $f(p)=[\prod_{j\in t} q(j)]$. Then (2.1) easily implies $\varkappa_{f(p)}=\sum_{j\in t}\varkappa_{q(j)}$, so $Q(f(p))=\{q(j): j\in t\}$. This proves (4.5).

Mathematisch Instituut,
Universiteit van Amsterdam

REFERENCES

1. Artin, E. – Collected papers, Reading, Addison Wesley (1965).
2. Bachmann, H. – Transfinite Zahlen, Berlin, Springer (1955).
3. Carlitz, L. – Distribution of primitive roots in a finite field, Quart. J. Math. Oxford (2), 4, 4–10 (1953).
4. Conway, J. H. – On numbers and games, London, Academic Press (1976).