NIM MULTIPLICATION [*)]

by

H.W. LENSTRA, Jr.

-:-:-:-

General reference : J.H. Conway, "On numbers and games" (abbreviated "ONAG"), Academic Press 1976, Ch. 6 and 11.

1.- Games and sets

The games we shall consider have three characteristics. First, they are played by two players, who move alternately according to certain rules. Secondly, we require that in any game it happens, after a finite number of moves, that the player whose turn it is has no legal move ; and thirdly, we adopt the convention that this player then is the loser. Of the several possible ways to formalize this concept the following is probably the simplest.

Definition.- A game is a set.

A few words of explanation may be in order. If a,b are two positions in a game, then we say that b is an option of a if, according to the rules of the game, it is legal to move from a to b ; it is assumed that this only depends on a and b , and not on whose turn it is. We identify each position with the set of its options, and each game with its initial position ; whence the definition. Notice that an element of a game, or of a position, is itself a position ; hence all sets we are considering

[*)] Research supported by the Netherlands Organisation for the Advancement of Pure Research (Z.W.O.).

have only sets as their elements, as is usual in axiomatic set theories.

Thus, playing a set S is done as follows. The first player chooses an element of S, say S'. Next the second player chooses an element, say S'', of S', whereafter the first player chooses an element of S''. The game continues in this way until one of the players - the loser! - has to choose an element from the empty set; the axiom of regularity (any non-empty set x contains an element disjoint from x) easily implies that this situation actually occurs after a finite number of moves.

Example. Let n be a natural number, i.e. a finite ordinal. If we adopt the usual definition of ordinal numbers, which implies that

$$\alpha = \{\beta : \beta \text{ is an ordinal } < \alpha\} \qquad \text{for every ordinal } \alpha,$$

then we have

$$n = \{0, 1, 2, \ldots, n-1\}.$$

The game n can be played with n counters; moving just means taking away an arbitrary non-empty subset of these counters. Notice that the first player has an easy win by taking all counters, if $n > 0$; if $n = 0$, the first player has no move and loses. The reader may wish to analyze the game $\mathbb{N} = \{n : n \text{ is a natural number}\}$ (including zero). ▲

Example. $\mathbb{C}$, the complex numbers. The following annotated game will make the rules clear.

	White	Black
1.	$3 - 2i$	$\{3_{\mathbb{R}}\}$
2.	$3_{\mathbb{R}}$	$(22/7)_{\mathbb{Q}}$
3.	$(-44_{\mathbb{Z}}, -14_{\mathbb{Z}})$?	$\{-44_{\mathbb{Z}}\}$
4.	$-44_{\mathbb{Z}}$	$(0_{\mathbb{N}}, 44_{\mathbb{N}})$!
5.	White resigns.	

Comment. 1. White selected a complex number. Black knows that $\mathbb{C} = \mathbb{R} \times \mathbb{R}$, by $a + bi = (a,b)$, and remembers Kuratowski's definition of an ordered pair:

$(x,y) = \{\{x\},\{x,y\}\}$. Thus Black must choose an element of $\{\{3_{\mathbb{R}}\}, \{3_{\mathbb{R}}, -2_{\mathbb{R}}\}\}$; The index $\mathbb{R}$ here, and later $\mathbb{Q}$, $\mathbb{Z}$ and $\mathbb{N}$, serve to distinguish between real numbers, rational numbers, integers and natural numbers usually denoted by the same symbol. Black's move leaves White a minimum of choice, but it is not the best one.

2. White has no choice. The "Dedekind cut" definition of $\mathbb{R}$ which the players agreed upon identifies a real number with the set of all strictly larger rational numbers; so Black's move is legal.

3. A rational number is an equivalence class of pairs of integers (a,b), with $b \neq 0$; here (a,b) represents the rational number a/b. The question mark denotes that White's move is a bad one.

4. The pair (a,b) of natural numbers represents the integer $a - b$. Black's move is the only winning one.

5. White resigns, since he can choose between $\{0_{\mathbb{N}}\}$ and $\{0_{\mathbb{N}}, 44_{\mathbb{N}}\}$. In both cases Black will reply by $0_{\mathbb{N}}$, which is the empty set.

2. Nim addition and multiplication.

The sum $J + K$ of two games is recursively defined by

$$J + K = \{j + K,\ J + k:\ \ j \in J,\ k \in K\},$$

the recursion being justified by the axiom of regularity. Informally, playing a sum of two games means selecting one of the component games, making any legal move in that game, and not touching the other one. The next player then also selects one of the component games - possibly the same, possibly not -, makes a legal move in it, and does not touch the other game. The game continues in this way until some player is unable to move in any of the two components; by our convention, this player has then lost.

Notice that $+$ is commutative and associative. We denote repeated sums by $J + K + \ldots + M$; they are played in a similar manner.

Example. NIM is played with a finite number of heaps of counters, the i-th heap counting n_i counters, say $(0 \leq i < t)$. A legal move is to decrease strictly the number of counters in any heap. Clearly, this is the game

$$n_0 + n_1 + \dots + n_{t-1}$$

with n_i as in section 1, and $+$ not to be confused with ordinary addition of natural numbers.

The analysis of NIM is well-known, and due to C.L. Bouton (Nim, a game with a complete mathematical theory, Ann. Math. 3 (1902), 35-39). Let the nim-sum $a \oplus b$ of two natural numbers a and b be obtained by writing them down in binary and then adding them without carrying; e.g. $5 \oplus 9 = (101)_2 \oplus (1001)_2 = (1100)_2 = 12$. Clearly, $(\mathbb{N}, \oplus)$ is an abelian group of exponent two. Bouton showed that a winning strategy for NIM consists of always moving to positions for which $n_0 \oplus n_1 \oplus \dots \oplus n_{t-1} = 0$; such a move is impossible if the position one has to move from already has this property, but this is only natural, as the opponent may be following the strategy.

It was noted by R.P. Sprague (Über mathematische Kampfspiele, Tôhoku Math. J. 41 (1935/6), 438-444) and P.M. Grundy (Mathematics and games, Eureka 2 (1939), 6-8) that the analysis applies to arbitrary sums, in the following manner.

Let the Grundy number $G(J)$ of a game J be recursively defined by

$$G(J) = \text{smallest ordinal not of the form } G(j), \text{ with } j \in J.$$

The reader who dislikes ordinals may restrict to bounded games, i.e. games J with the property that for some fixed $n \in \mathbb{N}$ no chain $x_n \in x_{n-1} \in \dots \in x_1 \in x_0 = J$ exists. For such games, and all their positions, the Grundy numbers are finite. Examples of bounded games are short games, i.e. finite sets all of whose elements are short ("hereditarily finite sets").

We have $G(\emptyset) = 0$, and more generally $G(n) = n$ if n is a natural number. Notice that

$$G(J) \neq 0 \Leftrightarrow \exists j \in J\colon G(j) = 0.$$

From this it follows recursively that the first player has a winning strategy in the game J if and only if $G(J) \neq 0$, and that, for such J, the choice of an element $j \in J$ is a winning move if and only if $G(j) = 0$. Thus to win a game one has to know the zeros of G. The result of Sprague and Grundy implies that the Grundy number of the sum of two games only depends on the Grundy numbers of the components:

Sum theorem. $G(J + K) = G(J) \oplus G(K)$.

Here $\oplus$ is defined for ordinals as for natural numbers: write each of the two ordinals to be nim-added as a strictly decreasing sum of ordinals of the form 2^{α}, delete the terms occurring in both expressions, and add the remaining terms in decreasing order. The class On of ordinal numbers with the operation $\oplus$ satisfies the group axioms, except that the underlying domain is no set. Following Conway, we say that $(\underline{\mathrm{On}}, \oplus)$ is a Group. The exponent is again two.

Exercise. Determine the unique winning move in the game $\mathbb{N} + \mathbb{Z} + \mathbb{Q} + \mathbb{R} + \mathbb{C}$, the conventions being as in section 1.

The proof of the sum theorem may be left to the reader. The essential property of $\oplus$ which one needs is that for any three ordinals α, β, γ with $\gamma < \alpha \oplus \beta$ there exists $\alpha' < \alpha$ with $\alpha' \oplus \beta = \gamma$ or $\beta' < \beta$ with $\alpha \oplus \beta' = \gamma$. Since for $\alpha' \neq \alpha$, $\beta' \neq \beta$ one certainly has $\alpha' \oplus \beta \neq \alpha \oplus \beta \neq \alpha \oplus \beta'$, it follows that

(2.1) $\alpha \oplus \beta$ is the smallest ordinal number different from all $\alpha' \oplus \beta$ with $\alpha' < \alpha$ and from all $\alpha \oplus \beta'$ with $\beta' < \beta$.

It was noticed by Conway that this property may in fact be taken as a recursive definition of $\oplus$. A charming feature of the definition is that no mention is made of the binary system; on the other hand, (2.1) cannot be taken as a basis for an efficient algorithm to calculate $\alpha \oplus \beta$.

As Conway remarks, $\oplus$ is in a sense the simplest addition making the ordinals into a Group. More precisely, if $*$ is any Group operation on the ordinals, then surely

$$\alpha * \beta \neq \alpha' * \beta \qquad \text{for all} \quad \alpha' \neq \alpha,$$
$$\alpha * \beta \neq \alpha * \beta' \qquad \text{for all} \quad \beta' \neq \beta.$$

Taking for $\alpha * \beta$ the smallest ordinal not forbidden by these rules, for $\alpha' < \alpha$ and $\beta' < \beta$ (since $\alpha' * \beta$, $\alpha * \beta'$ must "already exist") we obtain $* = \oplus$. It is remarkable that starting from the inequalities above we arrive in this way at a Group structure. Precisely the same thing happens for nim multiplication. The basic inequality to be used here expresses that we wish no zero-divisors, i.e.

$$(a - a').(b - b') \neq 0$$

for $a \neq a'$, $b \neq b'$, so

$$ab \neq a'b + ab' - a'b'.$$

For us, $+ = - = \oplus$, so we are led to the following definition of nim multiplication, due to Conway:

> $\alpha \circ \beta$ is the smallest ordinal number different from all ordinals $(\alpha' \circ \beta) \oplus (\alpha \circ \beta') \oplus (\alpha' \circ \beta')$, with $\alpha' < \alpha$, $\beta' < \beta$.

For example, if $\alpha = 0$, then no $\alpha' < \alpha$ exists, so there are no forbidden elements; hence $0 \circ \beta = 0$ for all β. In a similar way one proves that $1 \circ \beta = \beta$ for all β.

Conway's amazing result is:

THEOREM- The class On of ordinal numbers, with addition $\oplus$ and multiplication $\circ$, is an algebraically closed Field of characteristic 2.

This field is denoted by $\underline{On}_2$.

In the next section we shall see which role the nim product plays in the analysis of games. In section 4 the subfield $\mathbb{N}$ of $\underline{On}_2$ will be considered, and section 5 is devoted to the nim-algebra of transfinite ordinals.

3. Coin turning games.

It is not difficult to define a multiplication of games such that the multiplicative analogue of the sum theorem holds: if we put

$$J \times K = \{(j \times K) + (J \times k) + (j \times k): \ j \in J, \ k \in K\}$$

then one easily checks that

$$G(J \times K) = G(J) \circ G(K)$$

for all games J, K. Unlike sums, however, products do not naturally turn up in the analysis of games, and it is in fact hard to see how a product lends itself to practical play. For example, consider the game $n \times m$, with n, m natural numbers. After t moves the position will be of the form

$$(3.1) \qquad (a_1 \times b_1) + (a_2 \times b_2) + \ldots + (a_{2t+1} \times b_{2t+1}),$$

with all a_i, b_i natural numbers. A legal move is to replace one of the terms, $(a \times b)$ (say), by three terms $(a' \times b) + (a \times b') + (a' \times b')$, with $a' < a$, $b' < b$. Conway, in his game "Diminishing rectangles", represents the position (3.1) by $2t + 1$ rectangular cards placed on a table, the i-th card measuring a_i inches in one direction and b_i in the other. Cards with $a_i = 0$ or $b_i = 0$ are naturally invisible, which corresponds to $\emptyset \times J = J \times \emptyset = \emptyset$ for all games J. Conway assumes that the players have an indefinitely large stock of cards and a pair of scissors at their disposal; for a description of the ritual, see ONAG, p. 132.

A more playable version of the same game is obtained if we observe that, for any two fixed natural numbers a and b, the number of times $(a \times b)$ occurs as a term in (3.1) is only relevant modulo two, as far as the Grundy number is concerned. This is an immediate consequence of the sum theorem and the fact that $\underline{On}_2$ has characteristic 2. Thus we may restrict attention to positions

$$(3.2) \qquad (a_1 \times b_1) + (a_2 \times b_2) + \ldots + (a_u \times b_u)$$

in which all pairs (a_i, b_i) are distinct. Moving now means <u>first</u> to replace one of the terms $(a \times b)$ by three terms $(a' \times b) + (a \times b') + (a' \times b')$, with $a' < a$, $b' < b$, and *next* to remove terms occurring twice.

We represent the position (3.2) by a rectangular array of coins, with those coins showing heads occupying positions $(a_1, b_1), \ldots, (a_u, b_u)$, the coordinates numbering from zero. A legal move clearly consists of turning the coins at the four corners of a rectangle with horizontal and vertical sides, subject to the condition that the top right-hand coin goes from heads to tails.

This is an example of a *coin turning game*. As we have seen, the Grundy number of a position is the nim sum, over all the heads, of the nim product of the two coordinates. The corresponding one-dimensional game is played with a *row* of coins, a legal move being to turn two coins, of which the right-most goes from heads to tails. This game is easily seen to be a disguise of NIM; so the two-dimensional version might be called NIM × NIM.

Generally, a coin turning game is specified by a partially ordered set P, the *board*, and a set $\mathcal{T}$ of finite subsets of P, the *turning sets*. It is required that there are no infinite strictly decreasing chains in P, and that each element of $\mathcal{T}$ has precisely one maximal element. In a typical position of the game, the board is covered with coins, with only finitely many coins showing heads. A legal move consists of turning the coins occupying a turning set, subject to the condition that the coin occupying the maximal element of the turning set goes from heads to tails. More formally, a position is determined by a finite subset A of P, and a legal move is to replace A by its symmetric difference with some element T of $\mathcal{T}$, subject to the condition that the maximal element of T is contained in A. As usual, two players move alternately, and if no legal move in possible - this is bound to happen after finitely many turns - the last player is the winner.

In the coin turning game specified by P and $\mathcal{T}$, let $A_{P,\mathcal{T}}$ denote the position determined by the finite subset A of P. It is easily checked that

(3.3) $$G(A_{P,\mathfrak{J}}) = \sum_{a\in A} G(\{a\}_{P,\mathfrak{J}})$$

(Σ denotes nim summation), and that $G(\{a\}_{P,\mathfrak{J}})$ is the smallest ordinal distinct from all ordinals $\Sigma_{t\in T,\ t\neq a}\ G(\{t\}_{P,\mathfrak{J}})$, with T ranging over all elements of $\mathfrak{J}$ which have a as their maximal element.

If P_1, $\mathfrak{J}_1$ and P_2, $\mathfrak{J}_2$ specify coin turning games, then the product of these games is specified by P, $\mathfrak{J}$, where P is the cartesian product of P_1 and P_2, and

$$\mathfrak{J} = \{T_1 \times T_2 \colon\ T_1 \in \mathfrak{J}_1,\ T_2 \in \mathfrak{J}_2\}.$$

The ordering on P is defined by

$$(a_1,a_2) \leq (b_1,b_2) \text{ if and only if } a_1 \leq b_1 \text{ in } P_1 \text{ and } a_2 \leq b_2 \text{ in } P_2.$$

It is easily seen that P and $\mathfrak{J}$ satisfy our requirements. The product theorem states that we have

$$G(\{(a,b)\}_{P,\mathfrak{J}}) = G(\{a\}_{P_1,\mathfrak{J}_1})\circ G(\{b\}_{P_2,\mathfrak{J}_2})$$

for all $(a,b) \in P$, hence

$$G(A_{P,\mathfrak{J}}) = \sum_{(a,b)\in A} (G(\{a\}_{P_1,\mathfrak{J}_1})\circ G(\{b\}_{P_2,\mathfrak{J}_2}))$$

for all finite $A \subset P$. The proofs may be left to the reader.

Any game J can be represented by a coin turning game: define $P(J)$, $\mathfrak{J}(J)$ by

$$P(J) = \{J\} \cup \bigcup_{j\in J} P(j) \quad \text{(the "set of all positions of J")},$$
$$\mathfrak{J}(J) = \{\{a,b\} \subset P(J)\colon\ a \in b\},$$

and impose on $P(J)$ the weakest partial ordering for which $a < b$ for all a, $b \in P(J)$ with $a \in b$. It can be checked that, in the game specified by $P(J)$ and $\mathfrak{J}(J)$, the position determined by the one-element subset $\{J\}$ of $P(J)$ is J itself:

$$\{J\}_{P(J),\mathfrak{J}(J)} = J.$$

Several examples of coin turning games are given in the forthcoming book by E.R. Berlekamp, J.H. Conway and R.K. Guy ("Winning Ways", Freeman, ≥ 1978).

We describe here a class of examples, invented by Conway, which has an interesting connection with coding theory.

Let d, n be natural numbers, satisfying $n \geq d \geq 1$. We choose $P = n = \{0, 1, \ldots, n-1\}$ with the natural ordering, and $\mathfrak{T} = \{T \subset P\colon\ 1 \leq \#T < d\}$. Thus, the coin turning game specified by P and $\mathfrak{T}$ is played with a row of n coins, and a legal move is to turn less than d coins, but at least one, the right-most going from heads to tails.

We identify the positions in this game with the elements of $\mathbb{F}_2{}^n$ (here $\mathbb{F}_2$ is the two-element field), the element $(a_i)_{i=0}^{n-1}$ of $\mathbb{F}_2{}^n$ corresponding to the subset $\{i \in P\colon\ a_i = 1\}$. By (3.3), the map $\mathbb{F}_2{}^n \to \mathbb{N}$ which maps each position to its Grundy number, is $\mathbb{F}_2$-linear; here $\mathbb{N}$ is an $\mathbb{F}_2$-vector space with nim addition. Therefore the subset $K \subset \mathbb{F}_2{}^n$ of positions with zero Grundy number is a linear subspace of $\mathbb{F}_2{}^n$. Recall that the positions with zero Grundy number are exactly those which one should move to in order to win.

We give an alternative description of these positions. Order $\mathbb{F}_2{}^n$ lexicographically, by $(a_i)_{i\in n} < (b_i)_{i\in n}$ if and only if there exists $j \in n$ with

$$a_j = 0, \quad b_j = 1, \quad a_i = b_i \quad \text{for all} \quad i \in n \quad \text{with} \quad i > j.$$

The <u>Hamming distance</u> δ on $\mathbb{F}_2{}^n$ is defined by

$$\delta((a_i)_{i\in n}, (b_i)_{i\in n}) = \#\{i \in n\colon\ a_i \neq b_i\}.$$

Now we construct a sequence of elements $c^{(0)}, c^{(1)}, \ldots, c^{(k-1)}$ of $\mathbb{F}_2{}^n$ in the following inductive manner:

$$\begin{aligned} c^{(i)} \quad & \text{is the least element} \quad x \in \mathbb{F}_2{}^n \quad \text{for which} \\ & \delta(c^{(j)}, x) \geq d \quad \text{for all} \quad j < i; \end{aligned}$$

if no such x exists then the construction stops, and we put $k = i$. Clearly, all elements of $C = \{c^{(0)}, c^{(1)}, \ldots, c^{(k-1)}\}$ have mutual Hamming distance at least d; in the language of coding theory, the subset C of $\mathbb{F}_2{}^n$ is a <u>code of word length</u> n <u>and distance</u> d over $\mathbb{F}_2{}^n$. Moreover, C is the lexicographically first such code, in an obvious sense.

Notice that $c^{(0)} = 0 \in \mathbb{F}_2^n$, and that

$$c^{(0)} < c^{(1)} < \ldots < c^{(k-1)}.$$

The definition of the $c^{(i)}$ makes it clear that in the game we are discussing it is illegal to move from $c^{(i)}$ to $c^{(j)}$, for any pair j, i, but that for every $x \in \mathbb{F}_2^n$ not appearing among the $c^{(i)}$ there exists a $c^{(j)} < x$ such that it is legal to move from x to $c^{(j)}$. These properties imply that the $c^{(i)}$ are exactly the positions one should move to in order to win, i.e.,

$$C = K.$$

It thus follows that the lexicographically first code of given word length and distance over $\mathbb{F}_2$ is linear. It is an amusing exercise to prove this directly.

Conway observed that for specific choices of d and n some well known codes appear.

$d = 1$. In this case, $C = \mathbb{F}_2^n$; the game is a very quick win for the second player.

$d = 2$. Here $C \subset \mathbb{F}_2^n$ is the "parity check code", consisting of all vectors with an even number of coordinates equal to one. The game is known as "She loves me, she loves me not".

$d = 3$. This game is a disguise of NIM. For $n = 2^m - 1$, for some $m \geq 2$, the code is the Hamming code; this is a perfect one error correcting binary code. Its dimension is $n - m$.

$d = 4$. Here we obtain, in dimension $n = 2^m$, the extended Hamming code, which is obtained from the Hamming code by adding a parity check bit in front. We leave the analysis of the game to the reader.

$d = 5$, $n = 17$. This yields the quadratic residue code with the prime 17, of dimension 9.

$d = 6$, $n = 18$. The same, extended by a parity check bit.

$d = 7$, $n = 23$. The code obtained here is the famous Golay code, a perfect binary three-error correcting code of word length 23 and dimension 12. $d = 8$, $n = 24$. The same, extended. The group of all permutations of the n coordinates of $\mathbb{F}_2{}^n$ mapping the code to itself is the Mathieu group M_{24}. It acts 5-fold transitively, and has order 24.23.22.21.20.48.

The reader easily checks that, for odd d, the passage from d, n to $d + 1$, $n + 1$ generally corresponds to adding a parity check bit in front of the code C.

4. Exercises with natural numbers.

The set $\mathbb{N}$ of natural numbers is a subfield of $\underline{On}_2$ which is isomorphic to the quadratic closure of $\mathbb{F}_2$. We recall Conway's more precise results. For proofs, see ONAG or section 5.

The quadratic closure of $\mathbb{F}_2$ may be described as

$$\mathbb{F}_2(x_0,x_1,x_2,\ldots)$$

where the x_i satisfy the equations

$$x_i{}^2 + x_i + \prod_{j<i} x_j = 0. \tag{4.1}$$

For each i we have

$$\mathbb{F}_2(x_0,x_1,\ldots,x_{i-1}) = \mathbb{F}_{2^{2^i}},$$

and x_i is quadratic over this field. It follows that any element of $\mathbb{F}_2(x_0,x_1,x_2,\ldots)$ can be written in a unique way as

$$\sum_{V\in\mathfrak{W}} \prod_{i\in V} x_i, \tag{4.2}$$

where $\mathfrak{W}$ is a finite set of finite subsets of $\mathbb{N}$.

Any natural number can be uniquely written as $\sum_{k\in W} 2^k$, with $W \subset \mathbb{N}$ finite. Writing each $k \in W$ as $\sum_{i\in V} 2^i$ for some finite $V \subset \mathbb{N}$ depending on k we see that every natural number has a unique representation

$$\sum_{V\in\mathfrak{W}} \prod_{i\in V} 2^{2^i}, \tag{4.3}$$

with $\mathfrak{W}$ as before.

Conway proved that there is a field isomorphism $(\mathbb{N},\oplus,\circ) \to \mathbb{F}_2(x_0,x_1,\ldots)$ mapping the element (4.3) to (4.2). In view of (4.1) we are thus able to nim-multiply any two natural numbers. For example, $77 = 2^{2^2}\cdot 2^{2^1} + 2^{2^1}\cdot 2^{2^0} + 2^{2^1} + 1$ maps to $x_2x_1 + x_1x_0 + x_1 + 1$, so $77\circ 77$ maps to

$$x_2^2x_1^2 + x_1^2x_0^2 + x_1^2 + 1$$

which by $x_2^2 = x_2 + x_1x_0$, $x_1^2 = x_1 + x_0$, $x_0^2 = x_0 + 1$ reduces to

$$x_2x_1 + x_2x_0 + x_1x_0 + x_1 + 1.$$

This is the image of $2^{2^2}\cdot 2^{2^1} + 2^{2^2}\cdot 2^{2^0} + 2^{2^1}\cdot 2^{2^0} + 2^{2^1} + 1 = 109$, so

$$77\circ 77 = 109.$$

The isomorphism implies that for each i the number $2^{2^i} = \{0, 1, 2, .., 2^{2^i}-1\}$ is a subfield of $\mathbb{N}$.

Exercise 1. From the definition of the nim product it is clear that $n\circ m \leq nm$, since the number of "forbidden values" is at most nm. For which pairs of natural numbers does equality hold?

Exercise 2. Prove that 2^{2^i} is a primitive root of the field $2^{2^{i+1}}$ if and only if $i = 0$ or 1.

Exercise 3. Prove that $x\circ\circ 3 = 2^{2^i}$ has three solutions in $\mathbb{N}$, for each $i \geq 2$. Here, of course, $x\circ\circ 3 = x\circ x\circ x$. Can the solutions be explicitly written down? (To the last question I have no satisfactory answer).

Exercise 4. Prove that the following algorithm to calculate the nim product of two natural numbers is correct.

Write each of the two numbers n, m to be nim-multiplied in the binary system:

$$n = \sum_k a_k 2^k, \qquad m = \sum_k b_k 2^k,$$

with all a_k, b_k equal to zero or one, and almost all to zero. For any natural number $k = \sum_{i\in V} 2^i$ ($V \subset \mathbb{N}$ finite) we define $k^* = \sum_{i\in V} 3^i$. Multiply the two polynomials $\sum_k a_k X^{k^*}$ and $\sum_k b_k X^{k^*}$ in $\mathbb{F}_2[X]$. Let the result be

$$f = \sum_{\ell} c_\ell X^\ell \in \mathbb{F}_2[X], \qquad c_\ell \in \{0, 1\} = \mathbb{F}_2 .$$

If now every ℓ with $c_\ell = 1$ is of the form k^*, then with $d_k = c_{k^*}$ we can write $f = \sum_k d_k X^{k^*}$, and the product of n and m is given by

$$n \circ m = \sum_k d_k 2^k$$

where $d_k \in \{0, 1\}$ is interpreted as an element of $\mathbb{N}$.

If however $c_\ell = 1$ for some ℓ not of the form k^*, then let h denote the largest such ℓ. The number h has a 2 in its ternary expansion, say at position j (i.e., corresponding to 3^j), with j minimal. Redefine f and c_ℓ by

$$f := f + X^h + X^{h-3^j} + X^{h-(3^{j+1}+1)/2} \qquad (\text{in } \mathbb{F}_2[X]),$$

$$f = \sum_{\ell} c_\ell X^\ell$$

and return to #.

Exercise 5. Prove that the following algorithm to determine the nim inverse $1/n$ of a non-zero natural number n terminates. If $n = 1$, put $1/n = 1$. If $n > 1$, then determine the largest natural number i with $n \geq 2^{2^i}$, put $a = [n/2^{2^i}]$ (greatest integer brackets), calculate $m = 1/(n\circ(n\oplus a))$ by recursion and put $1/n = (n\oplus a)\circ m$.

Exercise 6. Let q be a natural number which is a field, i.e. $q = 2^{2^n}$ for some n. Then $\{q^i:\ i \in \mathbb{N}\}$ is a q-basis for $\mathbb{N}$, and if we express the q-linear map $F: \mathbb{N} \to \mathbb{N}$ defined by

$$F(x) = x\circ\circ q$$

(repeated nim multiplication, cf. exercise 3) on this basis:

$$q^j \circ\circ q = \sum_{i\in\mathbb{N}} b_{ij} \circ q^i,$$

with $b_{ij} \in q$, $b_{ij} = 0$ for almost all i (for fixed j), the coefficients b_{ij} satisfy

$$b_{ij} = 0 \qquad \text{if } i > j,$$

$$b_{jj} = 1 \qquad \text{for all } j,$$

$b_{j\,j+1} = 1$ for all j,

$b_{j\,j+2}$ does not depend on j, only on q, and equals 0 or 1.

In particular

$$q \circ\circ q = q \oplus 1 = q + 1,$$
$$q^2 \circ\circ q = q^2 \oplus q \oplus \varepsilon = q^2 + q + \varepsilon$$

where $\varepsilon = b_{0\,2} \in \{0, 1\}$.

Exercise 7. For $q = 2, 4, 16, 256, 65536$ we have $\varepsilon = 0, 1, 1, 0, 0$ in the previous exercise, respectively. What is the general rule? (I know the answer).

Exercise 8. Let the $2^n \times 2^n$-matrices A_n, B_n over $\mathbb{F}_2$ be defined by

$$A_0 = (1), \qquad A_{n+1} = \begin{pmatrix} 0 & A_n^2 \\ A_n & A_n \end{pmatrix},$$
$$B_0 = (1), \qquad B_{n+1} = \begin{pmatrix} B_n & A_n B_n \\ 0 & B_n \end{pmatrix}.$$

Prove that if we put $q = 2$ in exercise 6 we have

$$B_n = (b_{ij})_{0 \le i,j < 2^n},$$

and that $A_n^2 B_n = B_n A_n$, for all $n \geq 0$. (See page 16 for the matrix B_5.)

Exercise 9. Let $q \in \mathbb{N}$ be a field. We extend the q-vector space structure on $\mathbb{N}$ to a module structure over the polynomial ring $q[X]$ by

$$X.n = n \circ\circ q \qquad \text{for } n \in \mathbb{N}.$$

Prove that for every $i \in \mathbb{N}$ the number q^i is a $q[X]$-submodule of $\mathbb{N}$, and that $\mathbb{N}$ has no other $q[X]$-submodules except itself.

Exercise 10. Let the natural numbers q, r be fields, with $q \leq r$, and let $x \in r$. Prove that the elements $\sigma(x)$, with σ ranging over the Galois group of r over q, constitute a q-basis of r if and only if $x \geq r/q$.

Exercise 11. Let n be a natural number which is a group, i. e. a power of 2. Prove that the sequence $(n \circ\circ q)_{q=2,\,4,\,16,\,\ldots}$, q ranging through the natural numbers which are fields, is monotonically non-increasing with limit n.

Exercise 12. Let $a, n \in \mathbb{N}$. Prove that

$$\mathop{\mathring{\prod}}_{i<2^n} (a \oplus i) = \sum_{j,\ j\oplus(n-j)=n} a\circ\circ(2^j).$$

Exercise 13. Let $n \in \mathbb{N}$. Prove that

$$\begin{aligned}\sum_{i<2^n} i\circ\circ j &= 0 \quad \text{if } 0 \le j < 2^n - 1,\\ &= 1 \quad \text{if } j = 2^n - 1.\end{aligned}$$

$$\begin{array}{cccccccccccccccccccccccccccccccc}
1&1&&1&&&1&&&&&&1&1&1&&&&&&&&&&&1&&1&&&&1 \\
&1&1&&&&1&1&&&&&&1&1&1&&&&&&&&&1&&1&&&&1& \\
&&1&1&&1&1&1&&&&&1&&1&&&&&&&&&&1&&&&1&1&1& \\
&&&1&1&&&1&&&&&1&1&1&1&&&&&&&&&1&1&&&&1&1&1 \\
&&&&1&1&&1&&&1&&1&1&&&&&&&&&&&1&1&1&&1&1&1& \\
&&&&&1&1&&&&1&1&&1&&&&&&&&&&&&1&1&1&&1&1&1 \\
&&&&&&1&1&&1&1&1&1&1&&1&&&&&&&&&1&&1&&1&&1& \\
&&&&&&&1&1&&&1&&1&1&&&&&&&&&&1&1&1&1&1&1&1&1 \\
&&&&&&&&1&1&&1&&&1&&&&&&1&1&1&&&1&&1&1&1&1&1 \\
&&&&&&&&&1&1&&&&1&1&&&&&&1&1&1&1&&1&&&1&&1 \\
&&&&&&&&&&1&1&&1&1&1&&&&&1&&1&&1&&&&&1&& \\
&&&&&&&&&&&1&1&&&1&&&&&1&1&1&1&1&1&&&1&&& \\
&&&&&&&&&&&&1&1&&1&&&1&&1&1&&&1&1&&&&&1& \\
&&&&&&&&&&&&&1&1&&&&1&1&&1&&&&1&&&&&1&1 \\
&&&&&&&&&&&&&&1&1&&1&1&1&1&1&&1&1&1&&1&&1&1&1 \\
&&&&&&&&&&&&&&&1&1&&&1&&1&1&&&1&1&&1&&&1 \\
&&&&&&&&&&&&&&&&1&1&&1&&&1&&&&&&1&1&1& \\
&&&&&&&&&&&&&&&&&1&1&&&&1&1&&&&&&1&1&1 \\
&&&&&&&&&&&&&&&&&&1&1&&1&1&1&&&&&1&&1& \\
&&&&&&&&&&&&&&&&&&&1&1&&&1&&&&&1&1&1&1 \\
&&&&&&&&&&&&&&&&&&&&1&1&&1&&&1&&1&1&& \\
&&&&&&&&&&&&&&&&&&&&&1&1&&&&1&1&&1&& \\
&&&&&&&&&&&&&&&&&&&&&&1&1&&1&1&1&1&1&&1 \\
&&&&&&&&&&&&&&&&&&&&&&&1&1&&&1&&1&1& \\
&&&&&&&&&&&&&&&&&&&&&&&&1&1&&1&&&1& \\
&&&&&&&&&&&&&&&&&&&&&&&&&1&1&&&&1&1 \\
&&&&&&&&&&&&&&&&&&&&&&&&&&1&1&&1&1&1 \\
&&&&&&&&&&&&&&&&&&&&&&&&&&&1&1&&&1 \\
&&&&&&&&&&&&&&&&&&&&&&&&&&&&1&1&&1 \\
&&&&&&&&&&&&&&&&&&&&&&&&&&&&&1&1& \\
&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&1&1 \\
&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&1
\end{array}$$

The matrix B_5 (see exercise 8). Zeros are not shown.

Exercise 14. Let $q \in \mathbb{N}$ be a field. Prove that the $(q+1)$-st nim-roots of unity different from 1 are the numbers

$$((x \circ x) \oplus q \oplus (q/2)) \mathbin{/\!\!^{\circ}} ((x \circ x) \oplus x \oplus (q/2)), \qquad 0 \leq x < q.$$

Here $\mathbin{/\!\!^{\circ}}$ denotes nim division.

Exercise 15. (S. Norton). Define $a \,\&\, b$, for natural numbers a and b, by

$a \,\&\, b$ = smallest natural number different from all numbers

$a' \,\&\, b$, with $a' < a$,

$a \,\&\, b'$, with $b' < b$,

$a'' \,\&\, b''$, with $a'' < a$, $b'' < b$, $a \,\&\, b'' = a'' \,\&\, b$.

Prove that $(\mathbb{N}, \&)$ is an abelian group of exponent three, and that $a \,\&\, b$ is obtained by writing a and b in the ternary system and adding without carrying.

Exercise 16. Is there a multiplication $*$ on $\mathbb{N}$, with a similar definition as $\circ$, such that $(\mathbb{N}, \&, *)$ is a field of characteristic three? And what about characteristics $5, 7, 11, \ldots, 0$? (I do not know).

5. Transfinite nim-algebra.

This section is devoted to the nim-algebraic properties of ordinals. For the ordinary arithmetic of ordinals to be used, see H. Bachmann, Transfinite Zahlen, Springer, Berlin etc., 1967^2. We denote by ω the least infinite ordinal, and we adopt the convention $\alpha = \{\beta\colon \beta \text{ is an ordinal} < \alpha\}$ for ordinals α; so $\omega = \mathbb{N}$. We call α a group, ring, etc., if it is one with respect to the nim operations.

The basis for all we shall say is formed by Conway's simplest extension theorems, which state that an ordinal α behaves algebraically in the simplest possible way with respect to the set α of smaller ordinals. More precisely, if $\alpha \geq 2$ then we have:

- if α is no group, then $\alpha = \beta \oplus \gamma$, where (β, γ) is any lexicographically least pair of elements of α with $\beta \oplus \gamma \notin \alpha$;

- if α is a group but no ring, then $\alpha = \beta \circ \gamma$, where (β, γ) is any lexicographically least pair of elements of α with $\beta \circ \gamma \notin \alpha$;
- if α is a ring but no field, then $\alpha = 1 \mathbin{\overset{\circ}{/}} \beta$, where β is the least non-zero element of α with $1 \mathbin{\overset{\circ}{/}} \beta \notin \alpha$;
- if α is a field but not perfect, then $\alpha \circ \alpha = \beta$, where β is the least element of α having no nim-square root in α;
- if α is a perfect field but not algebraically closed, then α is a zero of the lexicographically least polynomial with coefficients in α having no zero in α (in the lexicographic order, consider high degree coefficients first);
- if α is an algebraically closed field, then α is transcendental over α.

<u>Exercise</u>. Let α, β be fields, $\alpha < \beta$. Show that $\beta = \alpha^{\gamma}$ for some γ. Prove that if $\gamma = 4$, then also α^{2} is a field.

The foregoing results were used by Conway to show that $\omega^{\omega^{\omega}}$ is an algebraic closure of $2 = \{0, 1\}$, see ONAG, Ch. 6, th. 49. For a proof that in $\omega^{\omega^{\omega}}$ the nim operations can be performed effectively, if the ordinals are represented in Cantor normal form, see HWLJ, On the algebraic closure of two, Proc. Kon. Ned. Akad. Wet. <u>80</u> = Indag. Math. <u>39</u> (1977), 389-397. The reader is invited to solve the following problem, and to communicate the solution to me: is it true that

$$(\omega^{\omega^{13}}) \circ\circ 47 = \omega^{\omega^{7}} + 1\ ?$$

Let t be an ordinal which is an algebraically closed field, e.g. $t = \omega^{\omega^{\omega}}$. Then t is transcendental over t, so a t-basis for $t(t)$ is given by

$$B = \{t \circ\circ n : n \in \omega\} \cup \{(t \oplus \alpha) \circ\circ (-n) : \alpha \in t,\ n \in \omega,\ n \neq 0\}$$

("partial fraction expansions"). It can be deduced from the simplest extension theorems that

$$t \circ\circ n < t \circ\circ m \qquad \text{if } n, m \in \omega,\ n < m,$$

$$
\begin{array}{ll}
t\circ\circ n < (t\oplus\alpha)\circ\circ(-m) & \text{if } n,\ m\in\omega,\ m\neq 0,\ \alpha\in t,\\
(t\oplus\alpha)\circ\circ(-n) < (t\oplus\alpha)\circ\circ(-m) & \text{if } n,\ m\in\omega,\ 0<n<m,\ \alpha\in t,\\
(t\oplus\alpha)\circ\circ(-n) < (t\oplus\beta)\circ\circ(-m) & \text{if } n,\ m\in\omega,\ \neq 0,\ \alpha,\ \beta\in t,\ \alpha<\beta,
\end{array}
$$

and that, for α_b, $\beta_b \in t$, $\alpha_b = \beta_b = 0$ for almost all $b \in B$, we have

$$\sum_{b\in B} \alpha_b \circ b < \sum_{b\in B} \beta_b \circ b$$

if and only there exists $b' \in B$ with $\alpha_{b'} < \beta_{b'}$, $\alpha_b = \beta_b$ for all $b \in B$ with $b > b'$. So the well-ordering of $t(t)$ is lexicographic with respect to the t-basis B. Since B has order type $\omega.(1+t) = t$ (use the last exercise!) it follows that $t(t) = t^t$. In particular:

$$(\omega^{\omega^{\omega^{\omega}}},\ \oplus,\ \circ) \simeq \overline{\mathbb{F}}_2(t)\ .$$

The field $t(t)$ is made perfect by adjoining $t\circ\circ(1/2^n)$ for all $n \in \omega$. That yields a tower of ω quadratic extensions, so the perfect closure of t^t is $(t^t)^{2^\omega} = t^{t\omega}$, in particular

$$\omega^{\omega^{\omega^{\omega}+1}} \text{ is the perfect closure of } \omega^{\omega^{\omega^{\omega}}}\ .$$

Since algebraic extensions of perfect fields are perfect, the next nim-square root extraction will only take place after the next transcendental.

We prove:

THEOREM.-*If the ordinal* t *is an algebraically closed field, then the quadratic closure of* $t(t)$ *is*

$$\lim_{n\in\omega} \underbrace{t^{t^{\cdot^{\cdot^{\cdot^{t}}}}}}_{n\times},$$

in particular

$$\epsilon_0 = \lim_{n\in\omega} \underbrace{\omega^{\omega^{\cdot^{\cdot^{\cdot^{\omega}}}}}}_{n\times}$$

is isomorphic to the quadratic closure of $\overline{\mathbb{F}}_2(t)$.

We make some definitions. For an ordinal x, let $\wp(x) = x\circ x \oplus x$, and denote by x^* the smallest y with $\wp(y) = x$; the other y is then $x^* \oplus 1$.

Notice that $x^* \oplus y^* = (x \oplus y)^*$ for all x and y. If the ordinal u is a field, we put $\wp[u] = \{\wp(x): x \in u\}$; this is a nim-additive subgroup of u. The field u is quadratically closed if and only if u is perfect and $\wp[u] = u$, i.e. $x^* \in u$ for all $x \in u$. If u is perfect but not quadratically closed, then $u = x^*$ with x the smallest element of $u - \wp[u]$. Clearly, this x is also the smallest element of

$$L(u) = \{\lambda \in u\text{: there is no } \beta \in u \text{ such that } \lambda \oplus \wp(\beta) \text{ can be written as a finite nim sum of ordinals } < \lambda\}.$$

We notice that every $\lambda \in L(u)$ is a group, and that $L(u)$ represents a 2-basis for $u/\wp[u]$. One should think of $L(u)$ as "the list of elements λ for which λ^* must be adjoined". In the case $u = t(t) = t^t$ it is straightforward to verify that

$$L(t^t) = \{(t \circ\circ (2n+1)) \circ \lambda,\ ((t \oplus \alpha) \circ\circ (-2n-1)) \circ \lambda\text{:}\ \ n \in \omega,\ \alpha, \lambda \in t,\ \lambda \text{ a group}\}.$$

(Notice that $\wp[t] = t$.) The order type of $L(t^t)$ is $s.t$, where $2^s = t$.

If u/u' is algebraic and purely inseparable, then $L(u) = L(u')$, as one easily checks. Thus $L(t^{t\omega}) = L(t^t)$. The above theorem now follows from the following more general claim, in which an ϵ-number is an ordinal α with $2^\alpha = \alpha$.

Claim. Let the ordinal u be a perfect field, and let v be the order type of $L(u)$. Suppose that $v \neq 0$. Then the quadratic closure of u is u^ϵ, where ϵ is the smallest ϵ-number $> v$.

For $u = 2$ we find $v = 1$, $\epsilon = \omega$, so ω is the quadratic closure of 2, as asserted in section 4. The multiplication rules in ω can easily be deduced from the proof of the claim given below.

Proof of the claim. The quadratic closure w of u is an ascending union

$$u = u_0 \subset u_1 \subset u_2 \subset \ldots \subset u_\omega \subset u_{\omega+1} \subset \ldots \subset u_y = w$$

for some y to be determined, where the u_α are defined as follows: $u_{\lim \alpha} = \lim u_\alpha = \bigcup u_\alpha$ for a limit ordinal, and $u_{\alpha+1} = u_\alpha(u_\alpha) = u_\alpha^2$ with $u_\alpha = \lambda_\alpha^*$, where λ_α is the smallest element of $L(u_\alpha)$; if $L(u_\alpha) = \emptyset$ then $\alpha = y$ and we have reached the quadratic closure. Clearly, $u_\alpha = u^{2^\alpha}$ for all $\alpha \leq y$.

To determine y we investigate the lists $L(u_\alpha)$. It is straightforward to prove that

$$L(u_\delta) = \lim_{\alpha<\delta} L(u_\alpha) = \bigcup_{\alpha<\delta} \bigcap_{\beta\geq\alpha} L(u_\beta) = \bigcap_{\alpha<\delta} \bigcup_{\beta\geq\alpha} L(u_\beta)$$

$$\text{if } \delta \text{ is a limit ordinal,}$$

$$L(u_{\alpha+1}) = (L(u_\alpha) - \{\lambda_\alpha\}) \cup \{u_\alpha.\lambda : \lambda \in L(u_\alpha)\} \qquad \text{if } L(u_\alpha) \neq \emptyset.$$

It follows that if we put

$$M(\alpha) = \bigcup_{\beta\leq\alpha} L(u_\beta), \qquad \text{for } \alpha \leq y,$$

then $M(\alpha)$ is a beginning segment of $M(\alpha')$, for $\alpha < \alpha' \leq y$, and $L(u_\alpha)$ consists of all elements of $M(\alpha)$ except the first α ones. Consequently, if $f(\alpha)$ is the order type of $M(\alpha)$, then we have

$$f(0) = v,$$

$$f(\lim \alpha) = \lim f(\alpha),$$

$$f(\alpha + 1) = f(\alpha) + (-\alpha + f(\alpha)) \qquad \text{if } f(\alpha) > \alpha,$$

and y is the only α with $f(\alpha) = \alpha$. Notice that $f(\alpha) > \alpha$ for all $\alpha < y$, and that $f(\alpha) < f(\alpha')$ if $\alpha < \alpha' \leq y$.

Let first $1 \leq v < \omega$. Then one easily checks that $f(n) = -(2^n - n - 1) + v.2^n$ for all $n < \omega$, so $f(\omega) = \omega$, $y = \omega$, $w = u^{2^y} = u^\omega$, and since ω is the smallest ε-number $> v$ the claim follows.

Next assume that $v \geq \omega$. Then $f(n) = v.2^n$ for all $n < \omega$, so $f(\omega) = v.\omega \geq \omega.\omega > \omega$, hence $y > \omega$. From the definition of f it is clear that $f(\alpha) \leq v.2^\alpha$ whenever $f(\alpha)$ is defined, i.e. whenever $\alpha \leq y$. Let now ε denote the smallest ε-number $> v$. If $\varepsilon < y$ then $f(\varepsilon)$ is defined, and $f(\varepsilon) \leq v.2^\varepsilon = \varepsilon$ (cf. Bachmann, section 15), contradicting that $\varepsilon < y$. We conclude that $\varepsilon \geq y$. We prove below:

(5.1) $\quad \omega \leq \beta < \varepsilon \Rightarrow f(\beta)$ is defined and $\geq \beta + 2^\beta$.

It follows that every $\beta < \varepsilon$ is $\leq y$, so $\varepsilon \leq y$ since ε is a limit ordinal.

We conclude that $\epsilon = y$, and $w = u^{2^y} = u^{2^\epsilon} = u^\epsilon$, as required.

The proof of (5.1) is by induction on β. For $\beta = \omega$ we have $f(\beta) = v.\omega \geq \omega.\omega > \omega.2 = \omega + 2^\omega$, as required. Next, if $f(\beta) \geq \beta + 2^\beta$ then $f(\beta) > \beta$, so $f(\beta+1)$ is defined, and since $\beta \geq \omega$ implies $1 + 2^\beta = 2^\beta$ we have in fact $f(\beta+1) = f(\beta) + (-\beta + f(\beta)) \geq \beta + 2^\beta + 2^\beta = \beta + 1 + 2^\beta + 2^\beta = (\beta + 1) + 2^{\beta+1}$, as required. It remains to do the case of a limit ordinal. Let $\beta < \epsilon$ be a limit ordinal. Then $f(\beta) = \lim\limits_{\alpha<\beta} f(\alpha) \geq \lim\limits_{\alpha<\beta} (\alpha + 2^\alpha) = 2^\beta$. Now 2^β is a "γ-number", i.e. $\delta + 2^\beta = 2^\beta$ for all ordinals $\delta < 2^\beta$ (see Bachmann, section 15), so if $\beta < 2^\beta$ then $2^\beta = \beta + 2^\beta$ and $f(\beta) \geq \beta + 2^\beta$, as required. If however $\beta \geq 2^\beta$ then $\beta = 2^\beta$ and β is an ϵ-number. But ϵ is the smallest ϵ-number $> v$, and $\beta < \epsilon$, so we must have $\beta \leq v$. Since f is strictly increasing and $f(0) = v$, we have $f(\alpha) \geq v + \alpha$ for all α, in particular

$$f(\beta) \geq v + \beta \geq \beta + \beta = \beta + 2^\beta,$$

as required. This proves (5.1), the claim, and the theorem.

<u>Problem</u>. Can all field operations be performed effectively in the field ϵ_0, if all ordinals are written in Cantor normal form? Can all quadratic equations be solved effectively in ϵ_0? (The above proof seems to indicate two affirmative answers.)

<u>Exercise</u>. Prove that $\epsilon_0 \circ\circ 3 = \omega^{\omega^\omega}$.

<u>Exercise</u>. Prove that ϵ_1 (the least ϵ-number $> \epsilon_0$) is the quadratic closure of ϵ_0.

It is unknown which ordinal number is the algebraic closure of ϵ_0. We propose a conjecture. For ordinals $x; \alpha_0, \alpha_1, \alpha_2, \ldots$ (indices $\in \omega$), almost all 0, we define $f(x;\alpha_0,\alpha_1,\alpha_2,\ldots)$ as follows:

$$f(x;0,0,0,\ldots) = x + 1,$$

$$f(x;\alpha_0+1,\alpha_1,\alpha_2,\ldots) = f(f(x;\alpha_0,\alpha_1,\alpha_2,\ldots);0,\alpha_1,\alpha_2,\ldots)$$

(left iteration),

$$f(x;\underbrace{0,\ldots,0}_{k\times},\beta,\alpha_{k+1},\alpha_{k+2},\ldots) = \lim_{\alpha<\beta} f(x;\underbrace{0,\ldots,0}_{k\times},\alpha,\alpha_{k+1},\alpha_{k+2},\ldots)$$

if β is a limit ordinal, and $k \in \omega$,

$$f(x;\underbrace{0,\ldots,0}_{k\times},\alpha_k+1,\alpha_{k+1},\alpha_{k+2},\ldots) = \text{smallest } y > x \text{ for which}$$

$$f(0;\underbrace{0,\ldots,0}_{k-1\times},y,\alpha_k,\alpha_{k+1},\alpha_{k+2},\ldots) = y, \qquad \text{if } k \in \omega,\ k \geq 1.$$

The proof that the definition makes sense is left to the reader.

Conjecture. If the ordinal t is an algebraically closed field, then the algebraic closure of $t(t)$ equals $\lim_{n\in\omega} f(t;\underbrace{0,\ldots,0}_{n\times},1,0,0,\ldots)$.

The conjecture is based on the assumption that any polynomial is irreducible, except if one explicitly adjoined a zero of it. Clearly, the assumption is wrong, but it may well be "cofinal" with the true state of affairs.

Problem. Prove that the algebraic closure of $t(t)$ is at most its conjectured value. (This should be the easy part.)

Exercise. Prove that $f(x;\alpha,\beta,0,0,0,\ldots) = \omega^\beta+\alpha$ if $x < \omega^\beta$, and $= x+1+\alpha$ if $x \geq \omega^\beta$.

Exercise. Prove that $f(0;0,0,2,0,0,\ldots)$ is the least ordinal α with $\boxed{\alpha}_0 = \alpha$, in Conway's notation (ONAG, p. 63).

(Texte reçu le 16 mars 1978)

-:-:-:-

H.W. LENSTRA, Jr.
Mathematisch Instituut
Roetersstraat 15
1018 WB AMSTERDAM