3. Proof of Theorem

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **26 (1980)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.04.2024**

3. Proof of Theorem

Put $e_o = 1$ and let $(e_i)_{i<\kappa}$ (κ some cardinal) be an extension of $e_0, e_1, ..., e_p$ to an F-base of E. By linear disjointness, $(e_i)_{i<\kappa}$ is also a K-base of the K-algebra $K[E]$. Since for $i, j < \kappa$ $e_i e_j = \sum_k g_{ijk} e_k$ for suitable $g_{ijk} \in F$ we have:

(5) If $(\Sigma a_i e_i)(\Sigma b_j e_j) = \Sigma c_k e_k$ where $a_i, b_j, c_k \in K$
(and the sums are finite of course) then

$$c_k = \sum_{i,j} a_i b_j g_{ijk} \in F[\{a_i\} \cup \{b_j\}],$$

Any element $r \in KE$, the quotient field of $K[E]$, can be written in the form

$$r = \frac{\Sigma a_i e_i}{\Sigma b_j e_j} + c$$

where $a_i, b_j, c \in K$, not all $b_j = 0$. Such a representation of r will be called a canonical representation, and the a_i's and b_j's are the coefficients of the given representation. Note that the canonical representation is not unique.

Lemma. *If $r_1, ..., r_n$ is the sequence of results of some computation in $(\Omega, E \cup K)$ using s M/D that count then there are $2s$ elements $\alpha_1, ..., \alpha_{2s} \in K$ such that each $r_\nu \neq u$, $1 \leqslant \nu \leqslant n$, has a canonical representation all of whose coefficients are in $F[\alpha_1, ..., \alpha_{2s}]$.*

The proof is by induction on n. The case $n = 0$ being trivial assume $n > 0$.

If $r_n \in E \cup K$ then obviously r_n has a canonical representation with coefficients in F, so the claim follows from the induction hypothesis. The same applies if $r_n = u$.

Next assume that $r_n \in \Omega$ is the result of a non-counting operation, i.e. $r_n = r_\mu \pm r_\nu$ for some $\mu, \nu < n$ or r_n is the result of a M/D where one of the factors or the denominator is a $g \in F$. Let us consider the case $r_n = r_\mu + r_\nu$, the other cases are similar. Choose $\alpha_1, ..., \alpha_{2s} \in K$ and canonical representations

$$r_\mu = \frac{A}{B} + c, \qquad r_\nu = \frac{A'}{B'} + c'$$

according to the induction hypothesis. Then, by (5), the coefficients of the canonical representation

$$r_n = \frac{AB' + A'B}{BB'} + (c + c')$$

also lie in $F[\alpha_1, ..., \alpha_{2s}]$.

Finally let $r_n = r_\mu \cdot r_\nu$ ($r_n = r_\mu / r_\nu$ resp.), $r_n \in \Omega$. Then, again by (5), the coefficients of the representation

$$r_n = \frac{(A + cB)(A' + c'B')}{BB'} \qquad \left(r_n = \frac{(A + cB)\, B'}{(A' + cB')B} \text{ resp.} \right)$$

lie in $F[\alpha_1, ..., \alpha_{2s-2}, c, c']$ where $\alpha_1, ..., \alpha_{2s-2} \in K$ are provided by induction hypothesis. Putting $\alpha_{2s-1} = c$, $\alpha_{2s} = c'$ completes the induction.

Proof of Theorem 1. Assume that π computes the elements $\sum_{j=1}^{p} d_{ij}\, e_j$, $1 \leqslant i \leqslant m$, in $(\Omega, E \cup K)$ with s counting M/D. By the Lemma there exist $\alpha_1, ..., \alpha_{2s} \in K$ and canonical representations

$$\sum_{j=1}^{p} d_{ij}\, e_j = \frac{\sum_k a_{ik}\, e_k}{\sum_q b_{iq}\, e_q} + c_i\,, \quad 1 \leqslant i \leqslant m\,, \tag{6}$$

with coefficients $a_{ik}, b_{iq} \in F[\alpha_1, ..., \alpha_{2s}]$. Now fix i. Multiplying (6) by the denominator gives

$$\Big(\sum_q b_{iq}\, e_q\Big)\Big(-c_i e_0 + \sum_j d_{ij}\, e_j\Big) = \sum_k a_{ik}\, e_k\,. \tag{7}$$

Multiplying out the left hand side and comparing the coefficients of each e_k on both sides (recall that $e_0, e_1, ...,$ are independent over K) we obtain, by using (5), a system $\mathscr{S}$ of linear equations for the d_{ij}'s and c_i whose coefficients are F-linear forms of the b_{iq}'s. Now the equation (7) clearly determines the element $-c_i\, e_0 + \sum_j d_{ij}\, e_j$ uniquely. Since the e_j are K-linear independent it follows that $\mathscr{S}$ has a unique solution, and hence d_{ij}, $c_i \in F(\alpha_1, ..., \alpha_{2s})$, by linear algebra. Since D has degree of transcendence t over F we obtain $2s \geqslant t$, i.e. $s \geqslant \left\lceil \frac{t}{2} \right\rceil$.

Remark. The method for handling divisions was proposed by Volker Strassen and we kindly thank him for this.