

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**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

3. PROOF OF THEOREM

Put $e_0 = 1$ and let $(e_i)_{i < \kappa}$ (κ some cardinal) be an extension of $e_0, e_1, \dots, e_p$ 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 $(\sum a_i e_i)(\sum b_j e_j) = \sum c_k e_k$ 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

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

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

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 $\alpha_1, \dots, \alpha_{2s} \in K$ and canonical representations

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

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 $F[\alpha_1, \dots, \alpha_{2s}]$.

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

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

lie in $F[\alpha_1, \dots, \alpha_{2s-2}, c, c']$ where $\alpha_1, \dots, \alpha_{2s-2} \in K$ 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 $\sum_{j=1}^p d_{ij} e_j$, $1 \leq i \leq m$, in $(\Omega, E \cup K)$ with s counting M/D . By the Lemma there exist $\alpha_1, \dots, \alpha_{2s} \in K$ and canonical representations

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

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

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

Multiplying out the left hand side and comparing the coefficients of each e_k on both sides (recall that $e_0, e_1, \dots$, are independent over K) we obtain, by using (5), a system $\mathcal{S}$ 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 $\mathcal{S}$ has a unique solution, and hence $d_{ij}, c_i \in F(\alpha_1, \dots, \alpha_{2s})$, by linear algebra. Since D has degree of transcendence t over F we obtain $2s \geq t$, i.e. $s \geq \left\lceil \frac{t}{2} \right\rceil$.

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