Acta Mathematica Academiae Scientiarum Hungaricae
Tomus 18 (3—4), 1967, pp. 321—328.

OPERATIONS WITH STRUCTURES

By
L. LOVÁSZ (Budapest)
(*Presented by* A. RÉNYI)

Introduction

We deal in this paper with (relational) structures $\langle H, R_1, \ldots, R_l\rangle$ with finitely many finitary relations over a set H. H is not necessarily non-empty. We shall consider only the case when $l=1$, i.e. structures of form $\langle H, R\rangle$ but our results extend without difficulty for the general case.

Our main concern will be in the direct product of finite structures (i.e. $\langle H, R\rangle$ with finite domain H). In [1] the question was discussed under what conditions it is true that any two direct factorizations of a structure have a common refinement. It was mentioned that if the structures A, B have this "refinement-property" then e.g. $A^2 \cong B^2$ implies $A \cong B$. We shall prove a general theorem from which it follows that for finite A, B the last implication always holds. On the other hand, it is easy to see that not all finite structures have the refinement-property (or the unique prime factorization-property).

The same is true with an arbitrary natural number n instead of 2. Further, if A, B, C are finite structures, and the relation of C is not irreflexiv (i.e. there is an element c in C such that $R(c, \ldots, c)$ holds, where R is the relation of C), then $AC \cong BC$ implies $A \cong B$. Our general result states that under certain conditions, a "polynomial" formed from structures assumes every value only once (up to isomorphism).

In § 1 we define the necessary notions, among them the (cardinal) sum and the (direct) product of two structures and a new operation on structures which will be called exponentiation. This operation has a remarkable resemblance to ordinary exponentiation in the domain of the natural numbers, when we bring it into contact with the sum and the product operation on structures. The relevant identities will be proved in § 2. In § § 1—2 we do not suppose that the structures are finite.

In § 3 we prove our main theorem from which the result mentioned above (concerning "polynomials" of structures) will follow easily. We mention that the operation of exponentiation is not indispensable in our arguments in § 3, i.e. the necessary notions derived from it could be introduced more directly. This will be pointed out on the due place. However, the "exponentiation" seems to us to be very natural in the present context and to be interesting also for its own sake.

§ 1. If N is a set we denote its cardinality by $|N|$. Let φ, ψ be mappings. By $\mathrm{Dom}\,\varphi$, $\mathrm{Rng}\,\varphi$ we denote the definition domain and the range of φ, respectively. The result of application of φ on $a \in \mathrm{Dom}\,\varphi$ is denoted by $a\varphi$. The product $\varphi\psi$ is defined if and only if $\mathrm{Rng}\,\varphi \subseteq \mathrm{Dom}\,\psi$. In this case $\mathrm{Dom}\,(\varphi\psi) = \mathrm{Dom}\,\varphi$ and $\varphi\psi$ is determined by the equation $a(\varphi\psi) = (a\varphi)\psi$ $(a \in \mathrm{Dom}\,\varphi = \mathrm{Dom}\,\varphi\psi)$. If φ is one-to-one then φ^{-1} is defined by $(a\varphi^{-1})\varphi = a$ $(a \in \mathrm{Rng}\,\varphi)$. We have in this case $\mathrm{Dom}\,\varphi^{-1} = \mathrm{Rng}\,\varphi$, $\mathrm{Rng}\,\varphi^{-1} = \mathrm{Dom}\,\varphi$. If $M \subseteq \mathrm{Dom}\,\varphi$ then $M\varphi = \{x\varphi : x \in M\}$.

Let k be a natural number, $k \geqq 1$. By a *k-dimensional structure* we mean a pair $\langle S, R\rangle$, where S is a set and $R \subseteq S^k$. S is the *domain* and R is the *relation* of $A=\langle S, R\rangle$. S and R are also denoted by $S(A)$ and $R(A)$ in dependence of A. The elements of A are the elements of $S(A)$. Obviously, for $k=2$, the 2-dimensional structures are the directed graphs without parallel edges. On the other hand, if $\mathscr{S}$ is an algebraic structure with domain S and finitary operations $m_1, \ldots, m_l$ then we can correspond to $\mathscr{S}$ the $k+l$ dimensional structure $\langle S, R\rangle$ where k is the maximum of the numbers k_i of places of m_i $(i=1, \ldots, l)$ and R is defined as the set of the $k+l$ tuples $\langle x_1, \ldots, x_k, m_1(x_1, \ldots, x_{k_1}), \ldots, m_l(x_1, \ldots, x_{k_l})\rangle$. What is important for us is that this correspondence is a one-to-one and is preserved under isomorphism and direct product. Hence our results in § 4 extend also to finite algebraic structures.

In what follows we consider structures of a fixed dimension k. By A, B, C, D, E, F, G (possibly with indices) we always mean structures.

If $S(A)=\emptyset$, $R(A)=\emptyset$ then we denote A by O. $A_p^{(k)}$ is the structure with the domain consisting of the natural numbers $1, 2, \ldots, p$ and with the identity relation; i.e. $(x_1, \ldots, x_k) \in R(A_p^{(k)})$ if and only if $x_1=\ldots=x_k$.

We denote the set of elements x of the structure such that $(x, \ldots, x) \in R(A)$ by $Q(A)$.

Let M, N be sets, $\varphi_1, \ldots, \varphi_k$ mappings of M into N (i.e. $\mathrm{Dom}\ \varphi_i = M$, $\mathrm{Rng}\ \varphi_i \subseteq N$). $[\varphi_1, \ldots, \varphi_k]$ denotes that mapping of M^k into N^k for which the image of $(x_1, \ldots, x_k) \in M^k$ is $(x_1\varphi_1, \ldots, x_k\varphi_k) \in N^k$.

If A is a structure and for the mapping φ we have $\mathrm{Dom}\ \varphi = S(A)$ then $B=A\varphi$ denotes the structure defined as follows. $S(A\varphi)=S(A)\varphi=\mathrm{Rng}\ \varphi$, $R(A\varphi)=$ $=\{(x_1, \ldots, x_k)[\varphi, \ldots, \varphi]: (x_1, \ldots, x_k) \in R(A)\}$. In this case we call φ a *homomorphism of A onto B*. If, in addition, φ is one-to-one, then φ is *isomorphism of A onto B*, and we write $A \cong B$. $H(A, B)$ will denote the set of all homomorphisms of A onto B.

Let $e=(x_1, \ldots, x_k)$, $f=(y_1, \ldots, y_k)$. Then $e \cdot f$ denotes $((x_1, y_1), \ldots, (x_k, y_k))$. Similarly, if $\langle x_1, x_2, \ldots\rangle, \langle y_1, y_2, \ldots\rangle$ are vectors of the same (finite or infinite) length then $\langle x_1, x_2, \ldots, \ldots\rangle \cdot \langle y_1, y_2, \ldots\rangle = \langle (x_1, y_1), (x_2, y_2), \ldots\rangle$.

Let A and B be structures. If $A' \cong A$ and $B' \cong B$, furthermore A' and B' have no element in common then the structure C defined by $S(C)=S(A') \cup S(B')$ and $R(C)=R(A') \cup R(B')$ is called a *(cardinal) sum* of A and B. Obviously, all cardinal sums of A and B are isomorphic. Therefore we may denote an arbitrary one of them by $A+B$ and this indeterminacy will not cause any difficulty. Certainly, in case $S(A) \cap S(B)=\emptyset$ we define $A+B$ by putting $A'=A$, $B'=B$ in the above construction. AB is the *direct product* of A and B, i.e. $S(AB)=S(A) \cdot S(B)$ (where for any sets M, N $M \cdot N$ means the cartesian product of M and N) and if $e \in S(A)^k$, $f \in S(B)^k$ then $e \cdot f \in R(A \cdot B)$ if and only if $e \in R(A)$ and $f \in R(B)$.

To define the exponentiation, we mean by A^B the structure for which $S(A^B)=$ $=S(A)^{S(B)}$ (i.e. the set of all mappings of $S(B)$ into $S(A)$) and if $\varphi_1, \ldots, \varphi_k \in S(A^B)$ then $(\varphi_1, \ldots, \varphi_k) \in R(A^B)$ is equivalent to $R(B)[\varphi_1, \ldots, \varphi_k] \subseteq R(A)$.

We remark that the following are identically true:

$$A+O \cong O+A \cong A, \quad A_p^{(k)} \cdot A \cong A \cdot A_p^{(k)} \cong A \cdot p = \underbrace{A}_{1} + \ldots + \underbrace{A}_{p},$$

$$A_1^{(k)} \cdot A \cong A \cdot A_1^{(k)} \cong A,$$

$$O \cdot A \cong A \cdot O \cong O, \quad A^{A_p^{(k)}} \cong A^p,$$

$$A^{A_1^{(k)}} \cong A, \quad (A_p^{(k)})^{A_q^{(k)}} \cong A_{pq}^{(k)},$$

$$(A_1^{(k)})^A \cong A_1^{(k)},$$

$$A^0 \cong A_1^{(k)}.$$

Concerning the product of structures we mention that every element of $S(AB)^k$ be written in the form ef with $e \in S(A)^k$, $f \in S(B)^k$ in a unique way. B is called *ubstructure* of A and we write $B \subseteqq A$ if $S(B) \subseteqq S(A)$ and $R(B) \subseteqq R(A)$. This ion is more general then the usual notion of substructure, namely, in the case the latter we require $R(B) = R(A) \cap S(B)^k$.

In § 3 the expression $Q(A^B)$ will play a central role. It is seen that $Q(A^B)$ ısists of all $\varphi \in S(A)^{S(B)}$ for which $B\varphi \subseteqq A$. Therefore we might call the elements $Q(A^B)$ *homomorphisms of B into A*. $F(B, A)$ will denote the elements of $Q(A^B)$ ich are one-to-one mappings. Similarly, the elements of $F(B, A)$ can be called morphisms of B into A.

Finally, we call a structure *connected* if it cannot be split up into a sum of two uctures neither of which is 0. In case $k = 2$ this is the notion of the graph-theoretic nnectedness. If φ is a mapping of $S(A)$ and A is connected, then obviously so $A\varphi$.

§ 2. We enumerate the basic identities for the addition, the multiplication d the exponentiation of structures.

(2. 1) The following are identically true:

1. 1)	$A+B \cong B+A$	(2. 1. 2)	$(A+B)+C \cong A+(B+C)$
1. 3)	$AB \cong BA$	(2. 1. 4)	$(AB)C \cong A(BC)$
1. 5)	$A(B+C) \cong AB+AC$	(2. 1. 6)	$A^{B+C} \cong A^B \cdot A^C$
1. 7)	$(AB)^C \cong A^C B^C$	(2. 1. 8)	$A^{BC} \cong (A^B)^C$.

The relations including only the addition and multiplication are well known, we confine ourselves to the proof of (2. 1. 6)—(2. 1. 8).

PROOF OF (2. 1. 6). We may suppose that B and C have no element in common. $\varphi \in S(A^{B+C})$ then we can associate with φ the pair (σ, τ) in a one-to-one way such at $\sigma \in S(A^B)$, $\tau \in S(A^C)$ and $x\varphi = x\sigma$ if $x \in S(B)$ and $x\varphi = x\tau$ if $x \in S(C)$. Obviously, e pairs (σ, τ) associated to all $\varphi \in S(A^{B+C})$ exhaust the set $S(A^B \cdot A^C)$. With this rrespondence, the mapping ψ defined by $\varphi\psi = (\sigma, \tau)$ is an isomorphism of A^{B+C} to $A^B \cdot A^C$. To show this, let $\varphi_1, \ldots, \varphi_k \in S(A^{B+C})$, $\varphi_i\psi = (\sigma_i, \tau_i)$ $(i = 1, \ldots, k)$. this case

$$R(B+C)[\varphi_1, \ldots, \varphi_k] =$$

$$= R(B)[\varphi_1, \ldots, \varphi_k] \cup R(C)[\varphi_1, \ldots, \varphi_k] = R(B)[\sigma_1, \ldots, \sigma_k] \cup R(C)[\tau_1, \ldots, \tau_k].$$

ıerefore $R(B+C)[\varphi_1, \ldots, \varphi_k] \subseteqq R(A)$ if and only if $R(B)[\sigma_1, \ldots, \sigma_k] \subseteqq R(A)$ ıd $R(C)[\tau_1, \ldots, \tau_k] \subseteqq R(A)$. Hence we have $(\varphi_1, \ldots, \varphi_k) \in R(A^{B+C})$ if and only if ı, ..., $\sigma_k) \in R(A^B)$ and $(\tau_1, \ldots, \tau_k) \in R(A^C)$, i.e. if $((\sigma_1, \tau_1), \ldots, (\sigma_k, \tau_k)) = (\varphi_1, \ldots,$, $\varphi_k)[\psi, \ldots, \psi] \in R(A^C \cdot B^C)$. Q.e.d.

(2. 1. 7) If $\varphi \in S(AB)^{S(C)}$ then we can associate with φ in a one-to-one way the pair (σ, τ) $(\sigma \in S(A^C), \tau \in S(B^C))$ such that for every $y \in S(C)$ $y \cdot \varphi = (y\sigma, y\tau)$. The mapping ψ defined by $\varphi\psi = (\sigma, \tau)$ is one-to-one and maps $S((AB)^C)$ onto $S(A^C B^C)$. We show that ψ is an isomorphism. Let $\varphi_1, \ldots, \varphi_k \in S((AB)^C)$ and $\varphi_i\psi = (\sigma_i, \tau_i)$ $(i = 1, \ldots, k)$. If e is any element of $S(C)^k$ then

$$e[\varphi_1, \ldots, \varphi_k] = e[\sigma_1, \ldots, \sigma_k] \cdot e[\tau_1, \ldots, \tau_k]. \tag{1}$$

$(\varphi_1, \ldots, \varphi_k) \in R((AB)^C)$ if and only if the expression on left hand side of (1) is an element of $R(AB)$ for any $e \in R(C)$, i.e., by (1), if for any $e \in R(C)$ we have $e[\sigma_1, \ldots, \ldots, \sigma_k] \in R(A)$ and $e[\tau_1, \ldots, \tau_k] \in R(B)$. The last condition is equivalent to saying that $(\sigma_1, \ldots, \sigma_k) \in R(A^C)$ and $(\tau_1, \ldots, \tau_k) \in R(B^C)$, or in other words that $(\varphi_1, \ldots, \varphi_k) \cdot [\psi, \ldots, \psi] = ((\sigma_1, \tau_1), \ldots, (\sigma_k, \tau_k)) \in R(A^C B^C)$. Our proof is complete.

(2. 1. 8) First we prove that for any $\xi \in S(A^{BC})$ there is exactly one $\varphi \in S((A^B)^C)$ and conversely, for any $\varphi \in S((A^B)^C)$ there is exactly one $\xi \in S(A^{BC})$ such that

$$(x, y)\xi = x(y\varphi) \tag{2}$$

is true for any $x \in S(B)$ and $y \in S(C)$. The unicity in both directions and the existence of the appropriate ξ for given φ are obvious. It remains to show that for any appropriate ξ there exists a φ. Let $y \in S(C)$. Let τ_y be the mapping of $S(B)$ into $S(A)$ satisfying $x\tau_y = (x, y)\xi$ for any $x \in S(B)$. Then the mapping φ defined by $y\varphi = \tau_y$ is the required one.

We prove that the mapping ψ, defined by $\xi = \varphi\psi$, where $\varphi \in S((A^B)^C)$ $\xi \in S(A^{BC})$ and (2) holds, is an isomorphism. Indeed

$$(\varphi_1, \ldots, \varphi_k) \in R((A^B)^C)$$

if and only if for any $e \in R(C)$

$$e[\varphi_1, \ldots, \varphi_k] \in R(A^B).$$

This is equivalent to that for every $e \in R(C), f \in R(B)$

$$f[e[\varphi_1, \ldots, \varphi_k]] \in R(A). \tag{3}$$

Applying (2) for the components of the vector standing on the left hand side of the last formula, we obtain

$$f[e[\varphi_1, \ldots, \varphi_k]] = (f \cdot e)[\varphi_1\psi, \ldots, \varphi_k\psi].$$

This means that the assertion that (3) holds for every $e \in R(C), f \in R(B)$ is the same as

$$(\varphi_1\psi, \ldots, \varphi_k\psi) = (\varphi_1, \ldots, \varphi_k)[\psi, \ldots, \psi] \in R(A^{BC})$$

what was to be proved.

We have finished the verification of (2. 1).

We close this section with three simple remarks.

(2. 2) If D is connected and $S(A)$, $S(B)$ are disjoint then we have $Q((A+B)^D) = Q(A^D) \cup Q(B^D)$. The $\supset$ inclusion is obvious. Conversely, if $\varphi \in Q((A+B)^D)$ then $D\varphi$ is a connected substructure of $A+B$, therefore $D\varphi \subseteq A$ or $D\varphi \subseteq B$.

(2. 3) $Q(AB) = Q(A)Q(B)$.

(2. 4) If $Q(A)$ is non empty, then so is $Q(A^B)$. Indeed, if $x \in Q(A)$ then the mapping of $S(B)$ which maps every element of B into x is an element of $Q(A^B)$.

§ 3. In this section we deal with finite structures. The operations $A\varphi$, $A+B$, $A \cdot B$, A^B applied to finite A, B give again finite structures. Furthermore, the following are obviously true:

(3. 1) A finite structure has finitely many different substructures.

(3. 2) Every finite structure can be written uniquely as the sum of connected substructures.

(3. 3) If both of two structures are isomorphic to a substructure of the other, then the two structures are isomorphic to each other.

(3. 4) If φ is a mapping of $S(D)$ then $|S(D\varphi)| \leqq |S(D)|$ and here equality holds if and only if φ is one-to-one.

(3. 5) If $\varphi \in H(G, G)$ i.e. φ is a homomorphism of G onto itself, then φ is an isomorphism of G onto G, i.e. an automorphism of G.

Our main aim is to prove the following theorem.

(3. 6) THEOREM. *With every finite structure A we can associate an infinite vector $\langle A \rangle$ of type ω whose components are natural numbers and the following are satisfied:*

(i) $\langle A+B \rangle = \langle A \rangle + \langle B \rangle$,

(ii) $\langle AB \rangle = \langle A \rangle \cdot \langle B \rangle$,

(iii) *If $Q(A)$ is non-empty, then all components of $\langle A \rangle$ are non-zero.*

(iv) $\langle A \rangle = \langle B \rangle$ *if and only if* $A \cong B$.

Let us select a series $D_1, D_2, \ldots$ of connected finite structures such that for $i \neq j$ D_i is not isomorphic to D_j but every connected finite structure is isomorphic to one of $D_1, D_2, \ldots$. Then we can make the following addition to (3. 6):

For the i-th component of $\langle A \rangle$ we can take $|Q(A^{D_i})|$.

PROOF. The statements (i), (ii), (iii) assert that

$$|Q((A+B)^{D_i})| = |Q(A^{D_i})| + |Q(B^{D_i})|;$$

$$|Q((AB)^{D_i})| = |Q(A^{D_i})|\,|Q(B^{D_i})|;$$

and if $|Q(A)| > 0$ then $|Q(A^{D_i})| > 0$. These follow from (2. 2), (2. 1. 7), (2. 3), (2. 4) directly.

We remark that (ii) could be shown more directly, without the notion of exponentiation but using the alternative characterization of $Q(A^D)$ given at the end of § 1 as a definition.

Obviously, $A \cong B$ implies $\langle A \rangle = \langle B \rangle$. Therefore it suffices to prove the following:

If for every connected D

$$|Q(A^D)| = |Q(B^D)|, \tag{4}$$

then $A \cong B$.

Suppose that for every connected D (4) holds. Let C be an arbitrary structure. By (3. 2) we have $C = C_1 + \ldots + C_r$ where $C_1, \ldots, C_r$ are connected. Using (2. 1. 6) and (2. 3)

$$|Q(A^C)| = |Q(A^{C_1})| \ldots |Q(A^{C_r})| = |Q(B^{C_1})| \ldots |Q(B^{C_r})| = |Q(B^C)|,$$

i.e. (4) holds for arbitrary (not necessarily connected) structures. Therefore it is sufficient to show that

If for every D

$$|Q(A^D)| = |Q(B^D)| \tag{5}$$

then $A \sim B$.

Suppose that (5) holds for every D. By (3. 3) it is sufficient to prove that A and B are isomorphic to a substructure of the other, i.e. that $|F(A, B)|>0$ and $|F(B, A)|>0$.

This will follow from $|F(A, B)| = |F(A, A)|$ and $|F(B, A)| = |F(B, B)|$. More generally we shall show that $|F(D, A)| = |F(D, B)|$ for every D.

Let $G_1, G_2, G_3, \ldots$ be a sequence of finite structures such that no two of them are isomorphic, and every finite structure is isomorphic to a G_i.

I. First we deduce the following formula

$$|Q(A^D)| = \sum_i \frac{|H(D, G_i)|}{|H(G_i, G_i)|} |F(G_i, A)|. \tag{6}$$

By (3. 1), the sum on the right hand side of the formula contains only finitely many members different from 0. If φ is a mapping of $S(D)$, then $D\varphi$ is isomorphic to exactly one G_i. Let Q_i be the subset of $Q(A^D)$ consisting of those φ for which $D\varphi \cong G_i$. Then obviously $|Q(A^D)| = \sum_i |Q_i|$. Hence (6) will follow from

$$|Q_i| = \frac{|H(D, G_i)|}{|H(G_i, G_i)|} |F(G_i, A)|. \tag{7}$$

For any $\varphi \in Q_i$ we consider the set X_φ of all pairs (ξ, ψ) such that $\xi \in H(D, G_i)$, $\psi \in F(G_i, A)$ and $\varphi = \xi\psi$. We show that (a) for any φ there are exactly $|H(G_i, G_i)|$ elements in X_φ and (b) for different mappings φ_1, φ_2 $X_{\varphi_1} \cap X_{\varphi_2} = \emptyset$, and finally, (c) every pair (ξ, ψ) with $\xi \in H(D, G_i)$ and $\psi \in F(G_i, A)$ is an element of an X_φ for some $\varphi \in Q_i$. (b) and (c) are trivial. We deal with (a). For $\varphi \in Q_i$ X_φ is non-empty since by $D\varphi \cong G_i$ there is an isomorphism ψ with $D\varphi = G_i\psi$, consequently $\psi \in F(G_i, A)$, and if we put $\xi = \varphi \cdot \psi^{-1} \in H(D, G_i)$ then $\varphi = \xi\psi$.

On the other hand, let $\varphi = \xi\psi$, $\xi \in H(D, G_i)$, $\psi \in F(G_i, A)$. If $\alpha \in H(G_i, G_i)$ then by (3. 5) we can write $\varphi = (\xi\alpha)\,(\alpha^{-1}\psi)$ and here we have $\xi\alpha \in H(D, G_i)$, $\alpha^{-1}\psi \in F(G_i, A)$. Consequently, with $(\xi, \psi) \in X_\varphi$ we have also $(\xi\alpha, \alpha^{-1}\psi) \in X_\varphi$ for all $\alpha \in H(G_i, G_i)$.

For different $\alpha_1, \alpha_2 \in H(G_i, G_i)$ $\xi\alpha_1 \neq \xi\alpha_2$ is clearly true, using $\operatorname{Rng} \xi = G_i$. Therefore the set $X'_\varphi = \{(\xi\alpha, \alpha^{-1}\psi) : \alpha \in H(G_i, G_i)\}$ is a subset of X_φ and has the cardinality $|H(G_i, G_i)|$. To complete our proof it is sufficient to show $X_\varphi \subseteq X'_\varphi$. Let $\varphi = \xi\psi = \xi'\psi'$ where $\xi' \in H(D, G_i)$ and $\psi' \in F(G_i, A)$. Then $\alpha = \psi\psi'^{-1}$ is defined and $\alpha \in H(G_i, G_i)$, furthermore $\xi' = \xi\alpha$ and $\psi' = \alpha^{-1}\psi$. Therefore we have really $X_\varphi \subseteq X'_\varphi$ and thus $X_\varphi = X'_\varphi$. We have completed the proof of the assertion (a).

To sum up our considerations, (a), (b), (c) show that the sets X_φ for different $\varphi \in Q_i$ form a partition of a set with the cardinality $|H(D, G_i)|\,|F(G_i, A)|$ into disjoint subsets, furthermore all X_φ have the same cardinality $|H(G_i, G_i)|$. This gives (7), and as mentioned above, also (6).

Suppose now that $|Q(A^D)| = |Q(B^D)|$ for every D.

II. We prove by induction on $|S(D)|$ that $|F(D, A)| = |F(D, B)|$. For $|S(D)| = 0$ this is obvious, for $|S(D)| = 1$ we have $|F(D, A)| = |Q(A^D)| = |Q(B^D)| = |F(D, B)|$.

Suppose that our assertion is true for any D' such that $|S(D')|<|S(D)|$. By (3. 4), (6) can be written in the form

$$|Q(A^D)| = |F(D, A)| + \sum_{\substack{i \\ |S(G_i)|<|S(D)|}} \frac{|H(D, G_i)|}{|H(G_i, G_i)|} |F(G_i, A)|.$$

Therefore

$$|F(D, A)| - |F(D, B)| = \sum_{\substack{i \\ |S(G_i)|<|S(D)|}} \frac{|H(D, G_i)|}{|H(G_i, G_i)|} (|F(G_i, B)| - |F(G_i, A)|)$$

and by the induction hypothesis the right hand side is equal to 0, thus $|F(D, A)| = |F(D, B)|$.

By the remarks given above we have finished the proof of (3. 6).

§ 4. We prove the result mentioned in the introduction.

(4. 1) THEOREM. *If $C_0, \ldots, C_n$ are finite structures and $|Q(C_1 + \ldots + C_n)|>0$ then for the "polynomial" $f(A)=C_0+C_1A+\ldots+C_nA^n$ we have that $f(A)\cong f(B)$ implies $A\cong B$ (A, B are finite structures).*

Taking $C_0=\ldots=C_{n-1}=0$, $C_n=A_1^{(k)}$ we get

(4. 2) If A and B are finite structures and $A^n\cong B^n$ then $A\cong B$.

Taking $n=1$, $C_0=0$ we obtain

(4. 3) If A, B, C are finite structures and $Q(C)$ is non-empty then $AC\cong BC$ implies $A\cong B$.

PROOF OF (4. 1). Let $f(A)\cong f(B)$. We have by (3. 6) $\langle f(A)\rangle=\langle f(B)\rangle$. We introduce the notations $\langle A\rangle=\langle a_1, \ldots\rangle$, $\langle B\rangle=\langle b_1, \ldots\rangle$, $\langle C_i\rangle=\langle c_{i1}, \ldots\rangle$. Then by (3. 6)

$$c_{0j}+c_{1j}a_j+\ldots+c_{nj}a_j^n = c_{0j}+c_{1j}b_j+\ldots+c_{nj}b_j^n \tag{9}$$

for every $j=1, 2, \ldots$. There is an i ($i=1, \ldots, n$) such that $|Q(C_i)|>0$. This implies $c_{ij}>0$ for every $j=1, 2, \ldots$ by (3. 6). Therefore the function $c_{0j}+c_{1j}t+\ldots+c_{nj}t^n$ is strictly monotonic and thus (9) gives that $a_j=b_j$ for every $j=1, 2, \ldots$.

This means $\langle A\rangle=\langle B\rangle$ and by (3. 6) $A\cong B$, q.e.d.

We note that the condition $|Q(C_1+\ldots+C_n)|>0$ cannot be left out from (4. 1). Let namely $k=2$, $S(C)=\{x, y\}$, $R(C)=\{(x, y), (y, x)\}$, $f(A)=CA$. In this case $C\cdot A_2^{(2)}\cong C\cdot C$ but $C\ncong A_2^{(2)}$. However, I do not know whether this condition can be weakened.

Since the identical mapping of $S(D)$ is always an element of $\varphi(D^D)$ therefore if $AD\cong BD$ then we have $A^DD^D\cong B^DD^D$ and (4. 3) $A^D\cong B^D$. Therefore we can infer from the last example that $(A_2^{(k)})^C\cong C^C$ i.e. the exponentiation does not have an inverse in general.

Finally, we note that the structure $A_2^{(k)}\cdot C\cong C\cdot C$ defined above has two irreducible direct factorizations which are essentially different. The unique prime-factorization property appears not even in case $|Q(A)|>0$ (see [2], [3]).

(Received 8 July 1966)

References

[1] C. C. CHANG, B. JÓNSSON, A TARSKI, Refinement properties for relational structures, *Fund. Math.*, **55** (1964), pp. 249–281.

[2[B. JÓNSSON, Unique factorization problem for finite relational structures, *Colloquium Math.*, **14** (1966), pp. 1—32.

[3] F. B. THOMPSON, Some contributions to abstract algebra and metamathematics, Doctoral dissertation, Berkeley 1951.