

136

icm

Enfin, si  $a \neq b$  et si aucune des suites a et b n'est segment de l'autre, posons:

h(a,b)=1.

La fonction h(a,b) est évidemment un écart dans H, qui devient ainsi un espace semi-métrique.

Soit maintenant G un espace semi-métrique quelconque de puissance  $\mathfrak{m}$ . Nous pouvons donc poser  $G=\{p_\xi\}_{\xi<\omega_\tau}$ . Soit  $g(p_\eta,p_\xi)$  l'écart dans G. Posons:

(45) 
$$f(\eta,\zeta) = g(p_{\eta},p_{\zeta}) \quad \text{pour } \eta < \omega_{\tau} \text{ et } \zeta < \omega_{\tau}:$$

c'est donc un écart dans l'ensemble de tous les nombres ordinaux < m.

Nous définirons maintenant une suite transfinie  $\{a_{\lambda}\}_{\lambda<\omega_{\tau}}$  de nombres ordinaux  $<\omega_{\tau}$  comme il suit. Soit  $\lambda$  un nombre ordinal donné,  $1\leqslant \lambda<\omega_{\tau}$ . D'après la définition de l'ensemble  $\Phi_{\lambda}$  et vu que  $\Phi_{\lambda}$  est formé de fonctions  $f_{\xi}^{\lambda}$  où  $\xi<\omega_{\psi(\varphi_{\lambda})}$ , il existe un nombre ordinal  $a_{\lambda}<\omega_{\psi(\varphi_{\lambda})}$  tel qu'on a les formules (34). On aura donc pour tout nombre ordinal  $\lambda<\omega_{\tau}$  les formules (8) et (9). La suite (finie ou transfinie)  $\{a_{\xi}\}_{\xi\leqslant\lambda}$  est donc, pour tout  $\lambda<\omega_{\tau}$ , un point de H: désignons-le par  $q_{\lambda}$  et posons  $Q=\{q_{\lambda}\}_{\lambda<\omega_{\tau}}$ .

Soient maintenant  $\mu$  et  $v>\mu$  deux nombres ordinaux  $<\omega_r$ . On a donc  $q_{\mu}=\{\alpha_i\}_{i<\mu}$  et  $q_{\nu}=\{\alpha_i\}_{i<\nu}$ . D'après la définition de la fonction h, on a donc  $h(q_{\mu},q_{\nu})=f^{\nu}_{\alpha_{\nu}}(\mu,\nu)$ , donc, d'après (34) (vu que  $\mu<\nu$ ):

$$h(q_{\mu},q_{\nu})=f(\mu,\nu),$$

donc, d'après (45):

$$h(q_{\mu}, q_{\nu}) = g(p_{\mu}, p_{\nu})$$
 pour  $\mu < \nu < \omega_{\tau}$ ,

ce qui prouve que les ensembles Q et G sont congruents.

L'espace semi-métrique H est par conséquent un espace universel de puissance m, et il est ainsi établi qu'on peut remplacer dans le théorème 1 le mot "métrique" par le mot "semi-métrique". Pour démontrer qu'on peut le faire aussi dans le théorème 2, il ne faut que répéter la démonstration du théorème 2, en y remplaçant partout le mot "distance" par "écart". Or, les théorèmes 3, 4 et 5 modifiés résultent tout de suite des théorèmes 1 et 2 modifiés.

Le théorème 6 est ainsi démontré.

#### Axiom of choice for finite sets.

B

# Andrzej Mostowski (Kraków)

Accordingly to N. Lusin two cardinal numbers  $\mathfrak{m}$  and  $\mathfrak{n}$  may serve to a characterisation of every case in which we are using the axiom of choice. If we apply this axiom to the class K of (mutually disjoint) sets, then  $\mathfrak{m}$  denotes the cardinal number of K and  $\mathfrak{n}$  is the least cardinal number surpassing the cardinal numbers of all elements of  $K^1$ ).

In the present paper I shall study particular cases of the axiom of choice which arise by giving n a finite value, whereas m is left arbitrary. The problem will consist on the study of mutual dependence or independence between these particular cases of the axiom.

In order to formulate this problem more precisely I shall consider the following proposition:

[n] For every class K of sets with n elements there is a function  $\Phi_K$  (the "choice-function" for K) defined for all X from K and such that  $\Phi_K(X) \in X^2$ ).

 $Z=\{n_1,n_2,...,n_k\}$  being any finite set of positive integers, we denote by [Z] the logical product of k propositions  $[n_1],[n_2],...,[n_k]$ .

Our problem is now this: n being a positive integer and Z a finite set of such integers, what are the necessary and sufficient conditions under which the implication  $[Z] \rightarrow [n]$  holds true?

Proof of equivalency is exactly the same as proof of equivalency of theprinciple of choice and the axiom of choice in general case. See e. g. W. Sier piński, loc. cit., p. 141.

<sup>1)</sup> See W. Sierpiński, Zarys teorji mnogości (An outline of set-theory, polish), 3ª edition, 1928, p. 112.

<sup>&</sup>lt;sup>2</sup>) This proposition may be called "the principle of choice for sets of power n". It is equivalent with the following proposition ("the axiom of choice for sets of power n"): For every class K of disjoint sets with n elements there is a set Y such that the product  $X \cdot Y$  has exactly one element for any  $X \in K$ .

As I did not success to find a full solution, I shall give here only a sufficient condition and another (apparently weaker) necessary condition. In the final section I shall treat some particular cases for which the necessary condition becomes sufficient and yields thus the complete answer for the question.

My methods of proofs are chiefly based on group-theoretical concepts introduced to investigations of the above type by Fraenkel<sup>3</sup>).

In order to demonstrate the applicability of these methods, I shall sketch a proof of the implication  $[2] \rightarrow [4]$ .

Let us consider a set with 4 elements  $A = \{a_1, a_2, a_3, a_4\}$ , and let  $A^*$  be the set whose elements are all unordered pairs which can be built up of the elements of A:

$$A^* = \left\{ \langle a_1, a_2 \rangle, \ \langle a_1, a_3 \rangle, \ \langle a_1, a_4 \rangle, \ \langle a_2, a_3 \rangle, \ \langle a_2, a_4 \rangle, \ \langle a_3, a_4 \rangle \right\}.$$

The proposition [2] implies the existence of a choice-function  $\Phi$  for the class  $A^*$ . Hence  $\Phi(\langle x,y\rangle)$  is one of the elements x or y for  $x,y\in A$ . Let  $n_l$  be the number of those pairs  $\langle x,y\rangle\in A^*$  for which  $\Phi(\langle x,y\rangle)=a_l$ . We have then  $n_1+n_2+n_3+n_4=6$ , which proves that numbers  $n_1,n_2,n_3$  and  $n_4$  cannot be identical. Suppose that  $n_l$  is the smallest of them, and let B be the set of those  $a_l$  for which  $n_l=n_l$ . B has at least one and at most three elements. If B has one element, let  $\Psi(A)$  be its unique element. If B has three elements, let  $\Psi(A)$  be the unique element of A.—B. If B has two elements, let  $\Psi(A)=\Phi(B)$ . Hence  $\Psi(A)\in A$ , and we have a rule which permits to select a particular element from A.

We see that  $a_1, a_2, a_3$  and  $a_4$  are indiscernible in A or  $A^*$ : No permutation of  $a_1, a_2, a_3, a_4$  changes A nor  $A^*$ . This is not true for sets built up with the help of the choice function  $\phi$ , and the asymmetry carried by this function enables us the choice of an element of A.

No such asymmetry would be introduced if  $\phi$  were a choice-function for a class of sets of the power 3. This is the basis of the proof that the implication  $[3] \rightarrow [4]$  does not hold.

The above proof of the implication  $[2] \rightarrow [4]$  was given by Tarski.

I shall use the current notation of group-theory.  $S_n$  will denote the symmetric group of degree n (i. e., the group of all permutations of numbers 1,2,...,n). A subgroup G of  $S_n$  will be said to have no fixpoints, if for any  $i \leq n$  there is a  $\varphi \in G$  such that  $\varphi(i) \neq i$ . The index of the subgroup H of any group G will be denoted by Ind (G/H).

#### § 1. Sufficient conditions.

We shall need some auxiliary definitions and theorems.

1. Definition 1. A set A is said to be normal, if there are in A no such X and Y that for some  $T_1, T_2, ..., T_p$ 

$$(1) X \epsilon T_1 \epsilon T_2 \epsilon \dots \epsilon T_p \epsilon Y.$$

 $(p \text{ may be } = 0; (1) \text{ says then that } X \in Y)^4$ ).

Lemma 1. If A is any set, then:

either (i) there is exactly one element  $b \in A$  such that for some  $c_1, c_2, ..., c_p$   $(p \geqslant 0)$  every  $a \in A - \{b\}$  satisfies  $a \in c_1 \in c_2 \in ... \in c_p \in b$ 

or (ii) the class  $A^*$  of all differences  $A-\{a\}$  where a runs over A is normal.

Proof. Suppose that  $A^*$  is not normal, i. e., that there are  $a,b \in A$  such that for some  $T_1,T_2,...,T_p$ 

(1) 
$$A - \{b\} \in T_1 \in T_2 \in \dots \in T_p \in A - \{a\}.$$

Let us first consider the case p>0. If  $T_p$  were different from b, we would have  $T_p \in A - \{b\}$ , and (1) would give an impossible relation

$$A-\{b\} \in T_1 \in T_2 \in \dots \in T_p \in A-\{b\}.$$

Thus  $T_p=b$  and (1) shows that putting  $c_1=A-\{b\}$  and  $c_{l+1}=T_i$  (i=1,2,...,p-1), we have for every  $a \in A-\{b\}$ 

$$a \in c_1 \in c_2 \in \dots \in c_p \in b$$
.

Hence there is at least one  $b \in A$  for which (i) holds. If there were two, say  $b_1$  and  $b_2$ , we would have  $b_1 \in A - \{b_2\}$ ,  $b_2 \in A - \{b_1\}$ , and (i) would give

$$b_1 \in c_1 \in c_2 \in \ldots \in c_p \in b_2$$
,  $b_2 \in c_1' \in c_2' \in \ldots \in c_q' \in b_1$ 

against the so called axiom of foundation 5).

If p=0, (1) gives  $A-\{b\} \in A-\{a\}$ . It follows that  $A-\{b\}=b$ , because otherwise we would have  $A-\{b\} \in A-\{b\}$ . Thus  $a \in b$  for every  $a \in A-\{b\}$ . The end of the proof is the same as above.

From this lemma we easily obtain the following

<sup>3)</sup> A. Fraenkel, Journal of Symbolic Logic, 2, 1937, pp. 1-25.

<sup>4)</sup> It follows from this definition that every set whose elements are not sets is normal.

<sup>5)</sup> This axiom states that there is no sequence  $x_1, x_2, ...$  of sets such that  $x_{n+1} \in x_n$  for n=1,2,... See, e. g., E. Zermelo, Fund. Math. 16, 1930, p. 31.



Lemma 2. If there is a choice function for every class of normal sets with n elements, then [n] is true.

Proof. Let K be an arbitrary class of sets of the power n. Divide K in two parts  $K_1$  and  $K_2$ , including to  $K_1$  those  $A \in K$  for which the alternative (i) of lemma 1 holds and to  $K_2$  the remaining A's. Lemma 1 enables us to distinguish a particular element b in any set of the class  $K_1$ . The principle of choice is thus true for this class.

For every  $A \in K_2$  the class  $A^*$  of all differences  $A - \{a\}$  where a runs over A is a normal set with n elements. Accordingly to our supposition we may distinguish a particular element  $\Psi(A^*)$  of this class. Denoting by  $\Phi(A)$  the unique element of  $A - \Psi(A^*)$ , we have  $\Phi(A) \in A$ , what proves that  $\Phi$  is a choice-function for the class  $K_2$ .

Thus there are choice-functions for classes  $K_1$  and  $K_2$ , and consequently there is such a function for their sum, i. e., for the class K, q. e. d.

**2.** For every set X denote by P(X) the class of all subsets of X and put

$$P_0(X) = X$$
,  $P_{m+1}(X) = P\left(\sum_{k=0}^{m} P_k(X)\right)$ ,  $O(X) = P_0(X) + P_1(X) + P_2(X) + \dots$ 

The elements of O(X) will be called objects with the base X.

If  $T \in P_{q+1}(X) - \sum_{k=0}^{q} P_k(X)$ , we shall say that T is of degree q+1; if  $T \in P_0(X)$ , we say that the degree of T is 0.

**Lemma** 3. If T is an object with the base X of degree q+1, and  $U \in T$ , then  $U \in O(X)$  and the degree of U is  $\leq q$ .

Proof follows immediately from/definitions.

**Lemma 4.** If X is a normal set and  $T \in X$ , then no element of T belongs to O(X).

Proof. An easy induction shows that, if U is an object with the base X of degree q>0, there are  $r\leqslant q$  elements  $V_1,V_2,...,V_r$  such that  $V_1\in X$  and  $V_1\in V_2\in ...\in V_r\in U$ . Hence, if U were an element of T, we would have

$$V_1 \in V_2 \in \dots \in V_r \in U \in T$$
,  $V_1 \in X$  and  $T \in X$ ,

which is impossible, because X is a normal set. If U were of degree 0, we would have  $U \in T$  and  $U \in X$ ,  $T \in X$ , which is again impossible.

Two above lemmas enable us to characterize the objects with the normal base in the following way:

- (i) Objects of degree 0 are identical with the elements of X;
- (ii) Objects of degree q+1 are identical with sets of the objects of degree less than q+1, one at least of these objects having exactly the degree q  $^{6}$ ).

Easy proofs of these assumptions may be omitted here.

The characterisation given in (i) and (ii) is more preferable than the primitive one, because it makes possible proofs and definitions by induction. Indeed, from (i) and (ii) follows that in order to prove that every object with a normal base X has a given property P it is sufficient to show that  $1^{\circ}$  every element of X has this property and  $2^{\circ}$  if all elements of a set A have the property P, then A has this property too. Analogous remarks apply to definitions by induction.

It is well to note that (ii) is, in general, false for objects with a non normal base 7).

3. The set  $\{1,2,...,n\}$  of first n integers will, for brevity, be denoted by (n). A and B being any two sets of the same power, we denote by  $A \not\subset B$  the class of all one to one mappings of A on B. If A has n elements (n finite), then  $A \not\subset A$  is the group of all permutations of A, and is isomorph with  $S_n = (n) \not\subset (n)$ .  $(n) \not\subset A$  is the class of all one to one functions defined on (n) and taking on values from A. I shall use letters f, g, h, ... to denote functions of the class  $A \not\subset A$  and letters  $\varphi, \psi, \chi, ...$  to denote functions of the class  $(n) \not\subset (n)$ .

Let A and B be two normal sets of the same power and f a function of the class  $A \not\supseteq B$ . For any object X with the base A I shall define its image f(X) by induction on X:

- ...(i) if  $X \in A$ , f(X) denotes the value of f for the argument X;
- (ii) if f(Y) is defined for any element Y of X, then  $f(X) = F[Y \in X]$ , i.e. the set of all f(Y) such that  $Y \in X$ .

It follows easy that f(X) is an object with the base B.

7) Example:  $X = \{a, b, \{a, b\}\}\$ . The degree of  $\{a, b\}$  is 0, though it is a set of two objects of degree 0.

<sup>6)</sup> Our "objects of degree q" form the same as the q<sup>th</sup> layer ("Schicht") considered by Zermelo, loc. cit. 5), p. 36. The difference is only this, that we do not suppose that the lowest layer is built up from elements which are not sets.

. . .

By induction we show that, if A, B and C are normal sets of the same power, and if  $f \in A \supseteq B$ ,  $g \in B \supseteq C$  and  $X \in O(A)$ , then

$$f(g(X)) = fg(X);$$
  $f^{-1}(f(X)) = X;$   $1(X) = X^{8}.$ 

It follows at once from these formulas that the set of all functions  $f \in A \not\subset A$  for which f(X) = X, is a group. This group will be called the symmetry group of X and denoted by G(X).

**Lemma 5.** If A is a normal set and X,Y two objects with the base A, then the symmetry group of the ordered pair  $\langle X,Y \rangle$  9) is contained in G(X) and G(Y).

Proof. If  $f \in A \not\subset A$ , then  $f(\langle X, Y \rangle) = \langle f(X), f(Y) \rangle$ . Hence, if  $f(\langle X, Y \rangle) = \langle X, Y \rangle$ , we must have f(X) = X and f(Y) = Y, i. e., f belongs to G(X) and G(Y).

**Lemma 6.** If A and B are two normal sets of the same power,  $X \in O(A)$  and  $\varphi \in A \supseteq B$ , then the symmetry group of  $\varphi(X)$  is  $\varphi(G(X)\varphi^{-1})$ .

This follows from equivalences:

$$\begin{cases} f \, \epsilon \, G \big| \varphi(X) \big| \big\} = \big\{ f \, \varphi(X) = \varphi(X) \big\} = \{ \varphi^{-1} f \, \varphi(X) = X \} = \\ = \big\{ \varphi^{-1} f \, \varphi \, \epsilon \, G(X) \big\} = \big\{ f \, \epsilon \, \varphi \, G(X) \varphi^{-1} \big\}.$$

**4.** Let A be any normal set and a an element of A. The symmetry group of the object  $\langle A, a \rangle$  has of course a fixpoint a. Thus, if we are able to choose an element from a normal set A, we can also construct an object X with the base A whose symmetry group has at least one fixpoint. We shall now show that for finite A the converse theorem is true:

**Lemma 7.** There is a function  $\Theta(A,X)$  defined for finite normal sets A and  $X \in O(A)$  such that if the symmetry group of X has fixpoints, then  $\Theta(A,X)$  belongs to A.

Proof. Suppose that A has n elements. The set O((n)) of objects with the base (n) may, of course, be well ordered. Let

$$(1)$$
  $B_1, B_2, B_3, ...$ 

be a sequence formed of all elements of O((n)).

$$\langle A_1, A_2, ..., A_k \rangle = \langle A_1, \langle A_2, A_3, ..., A_k \rangle \rangle.$$

If  $X \in O(A)$  and G(X) has no fixpoints, we may define  $\Theta(A,X)$  quite arbitrary (e. g.  $\Theta(A,X)=A$ ). Suppose now that G(X) has fixpoints and let  $A^+$  be their set.

Consider the images  $\varphi^{-1}(X)$  where  $\varphi \in (n) \not\subset A$ . Since they are objects with the base (n), they must occur in the sequence (1). Let  $B_i$  be the first term of (1) of the form  $\varphi^{-1}(X)$  where  $\varphi \in (n) \not\subset A$ , and let E(A) be the class of all  $\varphi \in (n) \not\subset A$  such that  $\varphi^{-1}(X) = B_i$ . If  $\varphi, \psi \in E(A)$ , then  $\varphi^{-1}(X) = B_i = \psi^{-1}(X)$  and therefore  $\psi \varphi^{-1}(X) = X$ , i. e.,  $\psi \varphi^{-1}$  belongs to the symmetry group of X, which proves that  $\psi \varphi^{-1}(a) = a$  or  $\varphi^{-1}(a) = \psi^{-1}(a)$  for any  $a \in A^+$ . We thus see that to every fixpoint  $a \in A^+$  corresponds an integer  $n(a,A) = \varphi^{-1}(a)$  where  $\varphi$  is any function of E(A), and that this integer do not depend of the particular choice of the function  $\varphi$ . Now define  $\Theta(A,X)$  as this element a of  $A^+$  for which n(a,A) has the least possible value.

 $\Theta(A,X)$  is thus defined for every  $X \in O(A)$  and it fulfills the condition  $\Theta(A,X) \in A$  for all X such that G(X) has fixpoints.

5. In light of the foregoing theorem the problem of choice of an element from a finite normal set A reduces to the following: It is to construct a function  $\Omega(X)$  defined for all  $X \in O(A)$  and such that if the symmetry group of X has no fixpoints, then  $\Omega(X)$  is an object with the base A and the symmetry group of  $\Omega(X)$  is a proper subgroup of G(X).

Suppose, indeed, that such a function  $\Omega$  has been found. We may then choose an element of A in the following way: consider the sequence

$$A, \quad \Omega(A), \quad \Omega(\Omega(A)) = \Omega^2(A), \quad \Omega(\Omega^2(A)) = \Omega^3(A), \quad \dots$$

Since the symmetry group of  $\Omega^{k+1}(A)$  is a proper subgroup of  $G(\Omega^k(A))$  (under the supposition that  $G(\Omega^k(A))$  has no fixpoints) and since the number of all possible symmetry groups is finite, there must be a number k such that the symmetry group of  $\Omega^k(A)$  has at least one fixpoint. Putting  $a = \Theta(A, \Omega^k(X))$  we obtain an element of A.

In order to prove that (under suitable conditions) such a function  $\Omega$  exists, we shall introduce still one new concept;

**6.** Definition 2. Let A be a normal set, G a subgroup of  $A \not\subset A$  and X an object with the base A. We denote by  $R_G(X)$  the class of all objects of the form f(X) where f runs over G:  $R_G(X) = F_G(X) = F_G(X)$ .

<sup>\*)</sup> fg denotes the composed function fg(x)=f(g(x));  $f^{-1}$  is the function inverse to f, and 1 the identical function 1(x)=x.

<sup>\*)</sup> The ordered pair  $\langle A,B\rangle$  is defined as  $\{\{A\},\{A,B\}\}$ . Generally, we denote by  $\langle A_1,A_2,...,A_k\rangle$  the ordered k-tuplet defined by induction on k as follows:

Axiom of choice for finite sets

Lemma 8. If the symmetry group of X is a subgroup H of G, then:

- (i)  $R_G(X)$  has Ind (G/H) elements;
- (ii) the symmetry group of  $R_G(X)$  is G.

Proof. (i) Let

$$G = H + f_1 H + f_2 H + \dots$$

be a decomposition of G in co-sets with respect to H. We let correspond to a co-set fH the element f(X) of  $R_G(X)$ . This element depends of the co-set fH as a whole and not of the particular choice of f, because for  $h \in H$  we have fh(X) = f(h(X)) = f(X).

To every co-set is thus attributed an element of  $R_G(X)$ , and it is easy to see that every element of  $R_G(X)$  is attributed to one of the co-sets. This correspondence is in addition one to one, because f(X) = g(X) yields  $g^{-1}f(X) = X$ , i.e.,  $g^{-1}f \in H$  or  $f \in gH$ . The cardinal number of  $R_G(X)$  is hence the same as the number of co-sets.

- (ii)  $g\left(R_G(X)\right)$  is the set of all objects of the form gf(X) where f runs over G. If  $g \in G$ , the conditions  $f \in G$  and  $gf \in G$  say the same and  $g\left(R_G(X)\right) = R_G(X)$ . If, conversely, g is such that  $g\left(R_G(X)\right) = R_G(X)$ , then g(X) must be contained in  $R_G(X)$ , i.e., there must be a  $f \in G$  such that g(X) = f(X). It follows  $f^{-1}g(X) = X$ , i.e.,  $f^{-1}g \in H$  or  $g \in fH$ . Since fH is contained in G, we obtain finally  $g \in G$ . Hence G is the symmetry group of  $R_G(X)$ .
- 7. Definition 3. We shall say that a positive integer n and a finite set of such integers Z satisfy the condition (D) if every subgroup G of  $S_n$  without fixpoints contains a subgroup H such that there is a finite number r of (not necessarily different) proper subgroups  $K_1, K_2, ..., K_r$  of H such that the sum

Ind 
$$(H/K_1)$$
 + Ind  $(H/K_2)$  +...+ Ind  $(H/K_r)$ 

belongs to the set Z.

Using this definition we shall prove the following lemma concerning the existence of the function  $\Omega$  mentioned at the beginning of section 5:

**Lemma 9.** Let a positive integer n and a finite set of such integers  $Z = \{n_1, n_2, ..., n_k\}$  satisfy the condition (D), and suppose that the proposition [Z] holds true. Let K be a class of normal sets of the power n. Under these suppositions there is a function  $\Omega_K(A, X)$  defined for  $A \in K$  and  $X \in O(A)$ , and such that if the symmetry group G(X) of X has no fixpoints,  $\Omega_K(A, X)$  is an object with the base A whose symmetry group is a proper subgroup of G(X).

Proof. Suppose that  $A \in K$  and  $X \in O(A)$ . If G(X) has at least one fixpoint, we may define  $\Omega_K(A, X)$  as we please, e. g.  $\Omega_K(A, X) = A$ . Suppose now that G(X) has no fixpoints.

(a, Let

(1) 
$$\Gamma_1, \Gamma_2, \Gamma_3, \dots$$

be a (finite) sequence formed of all subgroups of  $S_n$  and let  $\Gamma(A,X)$  be the first term of this sequence which has the form  $\varphi^{-1}G(X)\varphi$  with  $\varphi \in (n) \subset A$ . Let E(A,X) be the subset of  $(n) \subset A$  containing all  $\varphi$ 's for which

$$\varphi^{-1}G(X)\varphi=\Gamma(A,X).$$

The group  $\Gamma(A,X)$  does not possess fixpoints, because the group  $G(X) = \varphi\Gamma(A,X)\varphi^{-1}$ , where  $\varphi \in E(A,X)$ , has none. In virtue of the condition (D) there is a group  $X \subset \Gamma(A,X)$  and a finite number r of (not necessarily different) proper subgroups  $K_1, K_2, ..., K_r$  of X such that the sum

Ind 
$$(X/K_1)$$
 + Ind  $(X/K_2)$  + ... + Ind  $(X/K_r)$ 

belongs to the set Z.

If there are many groups  $X, K_1, K_2, ..., K_r$  with this property, we choose them so that r has the least possible value and further that the groups  $X, K_1, K_2, ..., K_r$  occur as early as possible in the sequence (1).

The number r and groups  $X, K_1, K_2, ..., K_r$  being thus defined uniquely by A and X, we shall denote them by r(A, X) and  $X(A, X), K_1(A, X), K_2(A, X), ..., K_{r(A, X)}(A, X)$ .

Putting for i=1,2,...,r(A,X)

$$h_i(A,X) = \operatorname{Ind} \left( X(A,X) / K_i(A,X) \right)$$

and

$$q(A, X) = h_1(A, X) + h_2(A, X) + \ldots + h_{r(A, X)}(A, X),$$

we follow that q(A, X) is one of the numbers  $n_1, n_2, ..., n_k$  which form the set Z.

( $\beta$ ) Let  $C_m$  (m=1,2,...) be defined in the following way:

$$C_1 = (n) = \{1, 2, ..., n\}, \quad C_2 = \{C_2\}, \quad C_3 = \{C_2\}, ..., C_{m+1} = \{C_m\}, ...,$$

The symmetry group of  $C_m$  is the whole  $S_n$ .

I put for i=1,2,...,r(A,X):

$$a_i = \langle \langle 1, 2, ..., n \rangle, C_i \rangle, \qquad D_i(A, X) = R_{K_i(A, X)}(a_i).$$

Axiom of choice for finite sets

147

For every  $\varphi \in E(A,X)$  I put further

$$\begin{split} B_i(A,X,\varphi) &= \varphi \left( D_i(A,X) \right), \qquad T_i(A,X,\varphi) = R_{\varphi X(A,X)\varphi^{-1}} \left( B_i(A,X,\varphi) \right), \\ S(A,X,\varphi) &= \sum_{i=1}^{r(A,X)} T_i(A,X,\varphi), \quad M(A,X,\varphi) = R_{G(X)} \left( S(A,X,\varphi) \right). \end{split}$$

 $a_l$  is an object with the base (n) with the unit group as the symmetry group. Accordingly to lemma 8 (ii)  $D_l(A,X)$  has  $K_l(A,X)$  as its symmetry group. Using lemma 6 we follow that the symmetry group of  $B_l(A,X,\varphi)$  is  $\varphi K_l(A,X)\varphi^{-1}$ . Since this group is contained in  $\varphi X(A,X)\varphi^{-1}$ , we follow from lemma 8 (ii) that the symmetry group of  $T_l(A,X,\varphi)$  is  $\varphi X(A,X)\varphi^{-1}$  and further that  $T_l(A,X,\varphi)$  has

$$\operatorname{Ind}\left(\varphi X(A,X)\varphi^{-1}/\varphi K_i(A,X)\varphi^{-1}\right)=\operatorname{Ind}\left(X(A,X)/K_i(A,X)\right)=h_i(A,X)$$
 elements.

We now show that sets  $T_i(A, X, \varphi)$  and  $T_j(A, X, \varphi)$  are disjoint, if  $i \neq j$ . Indeed, any element of  $T_i(A, X, \varphi)$  has a form

$$\left| arphi \chi arphi^{-1} igl( B_i(A,X,arphi) igr) = arphi \chi arphi^{-1} igl( arphi igl( D_i(A,X) igr) igr) = arphi \chi igl( D_i(A,X) igr)$$

where  $\chi \in X(A,X)$ . If  $T_l(A,X,\varphi)$  and  $T_j(A,X,\varphi)$  were not disjoint, there would be in X(A,X) such  $\chi_1$  and  $\chi_2$  that  $\varphi \chi_1 \left( D_l(A,X) \right) = \varphi \chi_2 \left( D_j(A,X) \right)$ , i. e.,  $\chi_1 \left( D_l(A,X) \right) = \chi_2 \left( D_l(A,X) \right)$  or  $\chi_2^{-1} \chi_1 \left( D_l(A,X) \right) = D_j(A,X)$ . Since  $a_l \in D_l(A,X)$ , it would follow that  $\chi_2^{-1} \chi_1 (a_l) \in D_j(A,X)$ , i. e.,  $\chi_2^{-1} \chi_1 (a_l) = \varkappa (a_j)$  where  $\varkappa \in K_j(A,X)$ . Remembering the definition of  $a_l$  we would thus obtain  $\chi_2^{-1} \chi_1 (C_l) = \varkappa (C_j)$  or  $C_l = C_p$ , which is of course impossible.

Hence  $T_l(A, X, \varphi)$  and  $T_l(A, X, \varphi)$  are, in fact, disjoint.  $S(A, X, \varphi)$  has consequently

$$h_1(A,X) + h_2(A,X) + \ldots + h_{r(A,X)}(A,X) = q(A,X)$$

elements and the symmetry group of  $S(A,X,\varphi)$  is  $\varphi X(A,X)\varphi^{-1}$ . Since this group is contained in  $\varphi \Gamma(A,X)\varphi^{-1}=G(X)$ , it follows by lemma 8 (ii) that  $M(A,X,\varphi)$  has the whole group G(X) as its symmetry group. Every element of  $M(A,X,\varphi)$  has |q(A,X)| elements, because it has the form  $f(S(A,X,\varphi))$  where  $f \in G(X)$ .

 $(\gamma)$  We saw above that for every  $\varphi \in E(A, X)$  and every  $A \in K$  and  $X \in O(A)$ , if G(X) has no fixpoints, then  $M(A, X, \varphi)$  is a class of sets of the power q(A, X) where q(A, X) is one of the numbers  $n_i$  (i=1,2,...,k).

Let  $\Pi_l$  be the class of such pairs  $\langle A, X \rangle$  that  $A \in K$ ,  $X \in O(A)$ , G(X) has no fixpoints and  $q(A, X) = n_l$ , and let us consider the sum

$$Q_i = \sum_{\langle A, X \rangle \in \Pi_i} \sum_{\varphi \in E(A, X)} M(A, X, \varphi).$$

 $Q_i$  is a class of sets of the power  $n_i$ . Since  $n_i \, \epsilon \, Z$  and the proposition [Z] is true by our hypothesis, we follow that there is a function  $\Phi_i$  defined for  $V \, \epsilon \, Q_i$  and such that  $\Phi_i(V) \, \epsilon \, V$ .

It follows that [Z] implies the existence of a choice-function  $\Phi$  for the class  $Q = Q_1 + Q_2 + ... + Q_k$ . We put namely for  $V \in Q_i - (Q_1 + Q_2 + ... + Q_{i-1})$ 

$$\Phi(V) = \Phi_i(V)$$

and obtain a choice-function for the whole class Q.

It is well to remark that we do not use here the axiom of choice, since the number k of different  $Q_i$  is finite.

( $\delta$ ) We now give the definition of  $\Omega_{K}(A, X)$  for  $A \in K$ ,  $X \in O(A)$  under the supposition that G(X) has no fixpoints.

Let  $N(A,X,\varphi)$  be the class of all pairs  $\langle V,\Phi(V)\rangle$  where  $V\in M(A,X,\varphi)$  and  $\varphi\in E(A,X)$  and let P(A,X) be the class of all pairs  $\langle M(A,X,\varphi),N(A,X,\varphi)\rangle$  where  $\varphi$  runs over E(A,X). Finally we put

$$Y = \Omega_{\mathbf{K}}(A, X) = \langle P(A, X), X \rangle.$$

The construction of the function  $\Omega_{K}$  being thus finished, it remains to show that the symmetry group of Y is a proper subgroup of G(X).

Let  $A \in K$ ,  $X \in O(A)$  and let us suppose that G(X) has no fixpoints. A and X being fixed for all what follows, we shall omit them in our notations and write e. g.  $S(\varphi)$  instead of  $S(A, X, \varphi)$ .

(e) Lemma 5 shows, for the first, that the symmetry group of Y is contained in G(X).

Let  $\varphi$  be an element of E. Since  $S(\varphi) \in M(\varphi)$ , the pair  $\langle S(\varphi), \Phi(S(\varphi)) \rangle$  occurs in  $N(\varphi)$  and  $\Phi(S(\varphi)) \in S(\varphi)$ . It follows by the definition of  $S(\varphi)$  that there is a number  $i \leq n$  such that  $\Phi(S(\varphi)) \in T_i(\varphi)$ , i. e.,  $\Phi(S(\varphi))$  has the form  $\varphi \chi \varphi^{-1}(B_i(\varphi)) = \varphi \chi(D_i)$  where  $\chi \in K_i$ . The symmetry group of  $\Phi(S(\varphi))$  is therefore  $\varphi \chi K_i \chi^{-1} \varphi^{-1}$  since  $G(D_i) = K_i$  (compare lemma 6). The group  $K_i$  being a proper

subgroup of X, we follow that  $\chi K_l \chi^{-1}$  is a proper subgroup of  $\chi X \chi^{-1} = X$  and  $\varphi \chi K_l \chi^{-1} \varphi^{-1}$  is a proper subgroup of  $\varphi X \varphi^{-1}$ . Consequently there is a function f which belongs to  $\varphi X \varphi^{-1}$  and does not belong to  $\varphi \chi K_l \chi^{-1} \varphi^{-1}$ .

We shall show that f does not occur in the symmetry group of Y which will prove that  $G(Y) \neq G(X)$  (since  $\varphi X \varphi^{-1} \subset G(X)$ ).

(n) From the definition of f we obtain

(2) 
$$f(\Phi(S(\varphi))) \neq \Phi(S(\varphi)), \quad f(S(\varphi)) = S(\varphi),$$

because the symmetry groups of  $\Phi(S(\varphi))$  and  $S(\varphi)$  are respectively  $\varphi_{\chi}K_{i\chi^{-1}\varphi^{-1}}$  and  $\varphi_{\chi}X_{\varphi^{-1}}$ . It follows that  $f(\langle S(\varphi), \Phi(S(\varphi)) \rangle)$  does not occur in  $N(\varphi)$ . Indeed, otherwise we would have  $f(\langle S(\varphi), \Phi(S(\varphi)) \rangle) = \langle V, \Phi(V) \rangle$  where  $V \in M(\varphi)$  and consequently also  $V = S(\varphi)$  and  $f(\Phi(S(\varphi))) = \Phi(V) = \Phi(S(\varphi))$  against (2). This proves that

(3) 
$$f(N(\varphi)) \neq N(\varphi).$$

We shall show that  $f(\langle M(\varphi), N(\varphi) \rangle)$  does not occur in P. In fact, if  $f(\langle M(\varphi), N(\varphi) \rangle)$  were in P, there would be a  $\psi \in E$  such that  $f(\langle M(\varphi), N(\varphi) \rangle) = \langle M(\psi), N(\psi) \rangle$ , i. e.,

$$f(M(\varphi)) = M(\psi),$$

(5) 
$$f(N(\varphi)) = N(\psi).$$

But f occurs in G(X) and consequently  $f(M(\varphi)) = M(\varphi)$ , because the symmetry group of  $M(\varphi)$  is G(X). (4) yields thus  $M(\varphi) = M(\psi)$  which proves accordingly to the definition of  $N(\varphi)$  that  $N(\varphi) = N(\psi)$ . From (5) we obtain now  $f(N(\varphi)) = N(\varphi)$  against (3).

We have thus proved that  $f(\langle M(\varphi), N(\varphi) \rangle)$  does not occur in P and we follow that  $f(P) \neq P$ . Since f(X) = X, we obtain finally  $f(Y) \neq Y$ , q. e. d.

8. We may now formulate the main theorem of  $\S 1$ :

**Theorem I.** Condition (D) is sufficient for the implication  $[Z] \rightarrow [n]$ .

Proof. Accordingly to lemma 2 it is sufficient to prove that if the proposition [Z] holds true, then there is a choice function for every class K of normal sets of power n.

Let  $\Theta(A,X)$  be the function defined in lemma 7. As we saw in lemma 9, the proposition [Z] implies the existence of a function  $\Omega_{K}(A,X)$  defined for all  $A \in K$  and  $X \in O(A)$ , and such that if G(X) has no fixpoints, then  $\Omega_{K}(A,X) \in O(A)$ , and the symmetry group of  $\Omega_{K}(A,X)$  is a proper subgroup of G(X).

Let us define for every  $A \in K$  the sequence  $S_m(A)$  in the following way

$$S_1(A) = A$$
,  $S_{m+1}(A) = \Omega_K(A, S_m(A))$ .

There must be for every  $A \in K$  a number  $m < 2^{n!}$  such that the symmetry group of  $S_m(A)$  has no fixpoints. Otherwise groups  $G(S_m(A))$  would form a descending sequence

$$Gigl(S_1(A)igr)\supset Gigl(S_2(A)igr)\supset Gigl(S_3(A)igr)\supset \ldots \ ,$$
  
 $Gigl(S_1(A)igr)\ne Gigl(S_2(A)igr)\ne Gigl(S_3(A)igr)\ne \ldots \ .$ 

with at least  $2^{n!}$  terms, which is impossible since the number of different symmetry groups does not exceed  $2^{n!}$ —1.

Let m(A) be the least integer such that the symmetry group of  $S_{m(A)}(A)$  has fixpoints and put

$$\phi(A) = \Theta(A, S_{m(A)}(A)).$$

Accordingly to lemma 7, we then have  $\Phi(A) \in A$  for every  $A \in K$ . Hence  $\Phi$  is a choice function for K, q. e. d.

**9.** We shall now apply theorem I to obtain another sufficient condition for the implication  $[Z] \rightarrow [n]$ .

**Definition 4.** We shall say that a positive integer n and a finite set Z of such integers satisfy the condition (S) if for every decomposition

$$n = p_1 + p_2 + \ldots + p_s$$

of n into a sum of (not nesessarily different) primes there is in Z a number divisible by one at least of the primes  $p_i \colon r \cdot p_i \in Z$ .

**Theorem 11.** Condition (S) is sufficient for the implication  $[Z] \rightarrow [n]^{-0}$ .

Proof. It is sufficient to prove that (D) is a consequence of (S).

<sup>10)</sup> This result has been first obtained by Mrs. W. Szmielew by an entirely another method in a paper to appear in Fundamenta Mathematicae.

icm

Let us suppose that (S) is satisfied, and let G be a subgroup of  $S_n$  without fixpoints. Let  $A_1, A_2, ..., A_s$  be the domains of transitivity of G, and let  $n_i$  denote the number of elements of  $A_i$  (i=1,2,...,s). All these numbers are greater than 1, because G would otherwise have fixpoints. Let  $p_i$  be any prime factor of  $n_i$  (i=1,2,...,s).

The number  $n = n_1 + n_2 + ... + n_s$  may be decomposed into a sum of primes in the following manner:

$$n = \underbrace{p_1 + p_1 + \ldots + p_1}_{n_1/p_1 \text{ times}} + \underbrace{p_2 + p_2 + \ldots + p_2}_{n_2/p_2 \text{ times}} + \ldots + \underbrace{p_s + p_s + \ldots + p_s}_{n_s/p_s \text{ times}}.$$

In virtue of (S) there are thus numbers  $i \leq s$  and r such that  $r \cdot p_i \in Z$ . Every permutation  $\varphi \in G$  induces a permutation  $\varphi^*$  of the set  $A_i$ . All permutations  $\varphi^*$  thus obtained form a transitive permutation group  $G^*$  of degree  $n_i$  homomorph with G. It follows that the order of  $G^*$  is divisible by  $p_i^{-11}$ , and since the order of G is divisible by the order of  $G^*$ , we follow that the order of G is divisible by  $p_i$ .

Accordingly to the Cauchy's well-known theorem  $^{12})$  G must therefore contain a permutation  $\varphi$  of the order  $p_j.$  Putting

$$H = \{1, \varphi, \varphi^2, ..., \varphi^{p_i-1}\}, \qquad K_1 = K_2 = ... = K_r = \{1\}$$

we get a subgroup H of G and r proper subgroups of H such that the sum

$$\operatorname{Ind} (H/K_1) + \operatorname{Ind} (H/K_2) + \ldots + \operatorname{Ind} (H/K_r) = r \cdot p_i$$

belongs to Z. This proves that n and Z satisfy the condition (D).

### § 2. Necessary conditions.

10. In the foregoing section we studied conditions sufficient for the implication  $[Z] \rightarrow [n]$ . This section will be devoted to a study of the necessary ones. It will be well to point out an entirely different character of both problems: If we have to prove the sufficiency of a condition, say C, we must show that if this condition is satisfied, the proposition [n] follows from the axioms of set-theory and

the proposition [Z]. In the proof of necessity of C, however, we must show that if C is not satisfied, [n] is independent from the axioms of set-theory and from the proposition [Z]. We could say that proofs of sufficiency have a mathematical and proofs of necessity a meta-mathematical character.

We shall relate our meta-mathematical investigations to the axiomatic set-theory of Zermelo<sup>13</sup>) in the precise formulation due to Quine<sup>14</sup>). We may, if we wish, extend this system adding to it the axiom of substitution<sup>15</sup>).

11. We need the following group-theoretical definitions. If G is any group, we denote by  $G^{\infty}$  the set of all infinite sequences

$$\varphi = [\varphi_1, \varphi_2, \varphi_3, \ldots]$$

whose terms belong to G. Greek letters  $\varphi, \psi, \vartheta, ...$  will always denote elements of  $G^{\aleph_0}$ ;  $\varphi_p$  will denote the  $p^{\text{th}}$  term of the sequence  $\varphi$ .

 $G^{\aleph_0}$  will become a group if we define the product  $\varphi \psi$  through the formula  $\varphi \psi = [\varphi_1 \psi_1, \varphi_2 \psi_2, \varphi_3 \psi_3, \dots].$ 

 $G^{\omega}$  will denote the subgroup of  $G^{\aleph_0}$  containing such  $\varphi$ 's that almost all  $\varphi_n$  are equal to the unity of G (i. e.,  $\varphi_p = 1$  for all  $p \geqslant p_0$ ).

**Definition 5.** We shall say that a positive integer n and a finite set Z of such integers satisfy the condition (K) if for every subgroup G of  $S_n$  without fixpoints there is a group  $H \subset G^{\omega}$  and a finite number r of (not necessarily different) proper subgroups  $K_1, K_2, ..., K_r$  of H such that the sum

(1) Ind 
$$(H/K_1)$$
 + Ind  $(H/K_2)$  + ... + Ind  $(H/K_r)$ 

is contained in Z.

12. Our main result concerning necessary conditions is given by the following

**Theorem III.** Condition (K) is necessary for the implication  $[Z] \rightarrow [n]$ .

In order to prove this theorem let us suppose that n and Z do not satisfy the condition (K), i. e., that there is a group  $G \subset S_n$ 

<sup>&</sup>lt;sup>11</sup>) The order of a transitive permutation-group is always divisible by its degree. See e. g. A. Speiser, *Theorie der Gruppen von endlicher Ordnung*, 2<sup>nd</sup> edition, 1927, p. 112.

<sup>12)</sup> This is the special case of the Sylow's theorem. See Speiser, loc. cit., p. 64.

<sup>13)</sup> E. Zermelo, Math. Ann., 65, 1908, p. 261-281.

<sup>14)</sup> W. V. Quine, Journal of Symbolic Logic 1, 1936, pp. 45—57.

<sup>115)</sup> See A. Fraenkel, Einleitung in die Mengenlehre, 3d edition, 1928, p. 309.

without fixpoints such that for any subgroup H of  $G^{\omega}$  and any proper subgroup  $K_1, K_2, ..., K_r$  of H the sum (1) does not belong to Z.

We have to show that [n] is, under this supposition, independent from the axioms of set-theory and from the proposition [Z]. For this purpose we shall construct a model in which all axioms and the proposition [Z] are satisfied, but the proposition [n] is not satisfied. Speaking more precisely, we shall give a new meaning to the primitive concepts of set-theory

"
$$\epsilon$$
", "set", "individual" <sup>16</sup>)

such that all axioms and [Z] will become true propositions <sup>17</sup>), whereas [n] will become a false one <sup>18</sup>).

The new meaning of  $,\epsilon$  will be identical with the old one. In order to define the new meaning of two other primitive concepts we must introduce some definitions.

**13.** Let  $N_1 = \{1,2,3,...,n\}$ ,  $N_2 = \{n+1,n+2,...,2n\}$ , . . . ,  $N_k = \{(k-1)\,n+1,(k-1)\,n+2,...,kn\}$ , . . .

The sum  $N=N_1+N_2+N_3+\ldots$  is the set of all positive integers.

For any  $\pi$  of G numbers  $\pi(1), \pi(2), ..., \pi(n)$  are well defined and fill up the whole set  $N_1$ . Putting

$$\pi((k-1)n+j) = (k-1)n+\pi(j)$$
  $(1 \le j \le n, k=1,2,...),$ 

we extend the permutation  $\pi$  over the whole N. The extended  $\pi$  transforms every  $N_k$  (k=1,2,...) in itself.

Let  $\xi$  be any ordinal and let  $\varphi \in G^{\omega}$ . We shall define a set  $K_{\xi}$  and the meaning of  $\varphi(x)$  for  $x \in K_{\xi}$  by transfinite induction on  $\xi$ .

For  $\xi=0$  we put  $K_0=N$ ; the meaning of  $\varphi(x)$  for  $x \in K_0$  is defined by the assumption  $\varphi(x)=\varphi_{\epsilon}(x)$  for  $x \in N_k$  (k=1,2,...).

Assume that  $\xi>0$  and that for  $\eta<\xi$  sets  $K_\eta$  are already defined. Assume further that the meaning of  $\varphi(x)$  for  $x\in\sum_{\eta<\xi}K_\eta$  is defined too.

Let  $M_{\xi}$  be the class of all subsets of the sum  $\sum_{\eta < \xi} K_{\eta}$ :

$$M_{\xi} = P(\sum_{\eta < \xi} K_{\eta}).$$

For  $x \in M_{\xi} - \sum_{\eta < \xi} K_{\eta}$  define  $\varphi(x)$  as the set of all  $\varphi(y)$  where y is an element of x. This definition is exact, because from  $y \in x \in M_{\xi}$  follows  $y \in x \subset \sum_{\eta < \xi} K_{\eta}$  and  $\varphi(y)$  is defined. Finally define  $K_{\xi}$  as the subset of  $M_{\xi}$  containing every x for which the following invariance-condition is satisfied:

(2) there is an integer q such that if  $\varphi \in G^{\omega}$  and  $\varphi_1 = \varphi_2 = \varphi_3 = ... = \varphi_q = 1$ , then  $\varphi(x) = x$ .

The inductive definition for  $K_{\xi}$  and  $\varphi(x)$  is thus accomplished. The following lemma can be easily proved by induction:

Lemma 10. Following propositions hold:

(i) If  $x \in K_{\xi}$  and  $\varphi \in G^{\omega}$ , then  $\varphi(x) \in K_{\xi}$ ;

(ii) if  $x \in K_{\xi}$  and  $\varphi, \psi \in G^{\omega}$ , then  $\varphi(\psi(x)) = \varphi\psi(x)$  and  $\varphi^{-1}(\varphi(x)) = x$ ;

(iii) if  $x \in K_{\xi}$ ,  $\xi > 0$  and  $\{t \in x\} = \{\varphi(t) \in x\}$  for every t, then  $x = \varphi(x)$ .

It is further easy to show that  $K_{\xi} \subset K_{\eta}$  for  $\xi < \eta$  and that from  $y \in x \in K_{\xi}$  follows  $y \in K_{\xi}$ . The least property of  $K_{\xi}$  is called transitivity.

We may now define the new meaning of "sets" and "individuals". As individuals in the new sense we assume the elements of  $K_0$  and as sets in the new sense the elements of any  $K_{\xi}$  with  $\xi > 0$ .

14. Before going further we shall still introduce a convenient terminology <sup>19</sup>).

Let  $\Xi$  be any concept definable in terms of the primitive concepts  $,\epsilon$ , ,individual and ,set. If we replace these primitive concepts by their new meanings, we obtain a new concept  $\Xi^*$  which is, in general, different from  $\Xi$ . This new concept will be called  $,pseudo-\Xi^*$ . We can thus speak about  $,pseudo-inclusion^*$ ,  $,pseudo-product^*$  etc. Pseudo-individuals resp. pseudo-sets mean the same as individuals resp. sets in the new sense.

<sup>16) &</sup>quot;Individual" means here the same as "Urelement" in the Zermelo's system, i. e., an object which can be an element of a set, but which is not a set itself.

<sup>17)</sup> I. e., propositions which are consequences of axioms usually admitted in mathematics. We add to these axioms the axiom of choice. Accordingly to Gödel's famous result we do not introduce thereby any contradiction if it was not already contained in the primitive axioms. See K. Gödel, Proc. Nat. Acad. Sci., 25, 1939, pp. 220-224.

<sup>19)</sup> I.e., a proposition whose negation is true in the sense explained in footnote 17).

<sup>19)</sup> This terminology has been introduced by K. Gödel in his lectures at the University of Vienna in 1937.

If the pseudo-concept  $\Xi^*$  related to pseudo-sets or pseudo-individuals x,y,z,... coincides with the primitive concept  $\Xi$  related to x,y,z,..., we shall say that  $\Xi$  is an absolute concept. Examples thereof are given in the following

**Lemma 11.** Following concepts are absolute: (i) inclusion; (ii) product of two sets; (iii) the relation between two sets: their product has exactly k elements (k=0,1,2,3,...).

We have now to prove that we get true propositions if we replace in the axioms of set theory all concepts by the correspondent pseudo-concepts. It will be sufficient to outline this theorem for two axioms, since its detailed proof has been given elsewhere <sup>20</sup>).

**15.** One of the axioms states that if x is a set, there is another set y = P(x) (class of subsets of x) such that, for any t,  $t \in y$  if and only if t is a subset of x.

In order to show that this axiom remains valid for the new sense of the primitive concepts, we must show that if x is a pseudoset, there is another pseudo-set y such that if t is any pseudo-individual or pseudo-set, then  $t \in y$  if and only if t is pseudo-included in x.

Let us assume as y the class of those subsets of x which are pseudo-sets themselves. It is plain that if t is a pseudo-individual or a pseudo-set, then  $t \in y$  if and only if t is included or (what is by lemma 11 (i) the same) pseudo-included in x.

It remains to show that y is a pseudo-set. Assume that  $x \in K_{\xi}$ . Every subset of x being an element of  $M_{\xi+1}$ , we follow that  $y \in K_{\xi+1}$  and consequently  $y \in M_{\xi+2}$ .

By our hypothesis there is further a number q such that if  $\varphi \in G^{\omega}$  and  $\varphi_1 = \varphi_2 = \ldots = \varphi_q = 1$ , then  $\varphi(x) = x$ . Suppose that  $\varphi \in G^{\omega}$  and  $\varphi_1 = \varphi_2 = \ldots = \varphi_q = 1$ . If  $t \subset x$ , then  $\varphi(t) \subset \varphi(x) = x$  and vice versa. By lemma 10 (i)  $\varphi(t)$  is a pseudo set if and only if t is one. Thus  $\{t \in y\} = \{\varphi(t) \in y\}$ , i.e.,  $\varphi(y) = y$ , which proves that y satisfies the invariance-condition (2) and is consequently a pseudo-set  $^{21}$ ).

**16.** As the second axiom for which our theorem will be proved we choose the axiom of substitution. It states that if x is a set and  $\Xi(u,t)$  is any relation between sets or individuals t,u, and if there is for any  $u \in x$  exactly one t such that  $\Xi(u,t)$  holds, then there is a set y such that  $t \in y$  if and only if an  $u \in x$  exists for which the relation  $\Xi(u,t)$  holds.

In order to eliminate the concept of an "arbitrary relation"  $^{22}$ ) we admit only such  $\Xi$  which may be defined in terms of primitive relations:

(3)  $v \in w^{"}$ ,  $v \in w^{"}$ ,  $v \in w^{"}$ ,  $v \in w^{"}$ ,  $v \in w^{"}$ 

and of logical operations:

negation, conjunction and quantifiers (bounding sets or individuals)

It is well to remark that  $\Xi$ , which is involved in the formulation of our axiom, may depend upon another sets or individuals a, b, ..., h which play the rôle of parameters. y is then a function of x and of these parameters.

We shall need the following

Lemma 12  $^{23}$ ). Let  $\Xi(u,t,a,b,...,h)$  be a relation of the above type and let  $\Xi^*(u,t,a,b,...,h)$  be the corresponding pseudo-relation. Let further u,t,a,b,...,h be pseudo-sets or pseudo-individuals and  $\varphi \in G^\omega$ . Then

$$(4) \qquad \Xi^*(u,t,a,b,...,h) \equiv \Xi^*[\varphi(u),\varphi(t),\varphi(a),\varphi(b),...,\varphi(h)].$$

Proof. The lemma is of course true for the primitive relations (3). If it is true for relations  $\Xi$  and H, it is also true for relations

"non-
$$\Xi$$
" and " $\Xi$  and H".

It remains to prove that if (4) holds for a relation  $\Xi$ , it holds also for the relation

$$H(u,t,b,...,h) \equiv \sum_{a} \Xi(u,t,a,b,...,h).$$

<sup>&</sup>lt;sup>20</sup>) A. Mostowski, Fund. Math. 32, 1939, p. 221-252.

The relation y is the class of all sub-sets of x is not absolute in the sense introduced in 14. It follows that if we only know about a domain D of sets that it contains P(x) with every of its element x, we cannot still be sure that the axiom y for any set y there is the class of its sub-sets relativized to the domain y is valid. This is one point which y do not understand in the works of Fraenkel about the independence of the axiom of choice. See footnote and the litterature quoted in this paper.

<sup>22)</sup> If we wish to retain this concept, we must give to our system of axioms a larger logical basis (variables of the second type). The proofs of independence are still possible, but must be modified a little, because it is necessary to relativize to a model not only the primitive concepts of axiomatic system but also the logical concepts.

<sup>&</sup>lt;sup>22</sup>) This lemma is essentially due to A. Tarski and A. Lindenbaum, Ergebn. eines math. Kolloq., 7, 1934, pp. 15-22.

Axiom of choice for finite sets

157

Suppose that pseudo-individuals or pseudo-sets u, t, b, ..., h fulfill  $H^*(u, t, b, ..., h)$ . There is then a pseudo-set or a pseudo-individual a such that  $\Xi^*(u, t, a, b, ..., h)$  and hence by (4)

$$\equiv *(\varphi(u), \varphi(t), \varphi(a), \varphi(b), ..., \varphi(h)).$$

There is thus a pseudo-individual or a pseudo-set  $\alpha' = \varphi(a)$  such that  $\Xi^*(\varphi(u), \varphi(t), \alpha', \varphi(b), ..., \varphi(h))$ , i. e.  $H^*(\varphi(u), \varphi(t), \varphi(b), ..., \varphi(h))$ . This proves the implication

$$H^*(u,t,b,...,h) \to H^*(\varphi(u),\varphi(t),\varphi(b),...,\varphi(h)).$$

Replacing here  $\varphi$  by  $\varphi^{-1}$  and u,t,b,...,h resp. by  $\varphi(u),\varphi(t),\varphi(b),...,\varphi(h)$  we obtain the converse implication and lemma 12 is proved.

We pass now to the axiom of substitution. We have to show that if x is a pseudo-set, a,b,...,h are pseudo-sets or pseudo-individuals and  $\Xi(u,t,a,b,...,h)$  is a relation of the type described above such that for any  $u \in x$  there is exactly one pseudo-set or pseudo-individual t for which  $\Xi^*(u,t,a,b,...,h)$ , then there is a pseudo-set y such that

(5)  $t \in y$  if and only if there is an  $u \in x$  for which  $\Xi^*(u,t,a,b,...h)$ .

For  $u \in x$  denote by f(u) the unique t for which  $\Xi^*(u, t, a, b, ..., h)$ , and let y be the set of all f(u) where u runs over x. Since it is obvious that this y satisfies (5), we have only to show that y is a pseudo-set.

Suppose that  $x \in K_{\xi}$ . If  $u \in x$ , then f(u) is a pseudo-set or pseudo-individual and there are ordinals  $\eta$  such that  $f(u) \in K_{\eta}$ . Let  $\zeta(u)$  be the least such  $\eta$ , and let  $\zeta$  be the least ordinal exceeding all  $\zeta(u)$  with  $u \in x$ . Then  $f(u) \in K_{\xi}$  for every  $u \in x$ , i. e.,  $y \subset K_{\xi}$  or  $y \in M_{\xi+1}$ .

We now show that y satisfies the invariance-condition. Let q(x), q(a), ..., q(h) be numbers such that

(6) 
$$\varphi(x) = x, \quad \varphi(a) = a, \quad \dots, \quad \varphi(h) = h$$

for any  $\varphi \in G^{\omega}$  for which the first q(x), q(a), ..., q(h) terms  $\varphi_k$  are equal to 1. Let q be the greatest of the numbers q(x), q(a), ..., q(h). If  $\varphi$  is such that  $\varphi_1 = \varphi_2 = ... = \varphi_q = 1$ , we have equalities (6). I shall show that  $\varphi(y) = y$ . In fact

$$\{t \in y\} = \sum_{u} \{(u \in x) \cdot [\Xi^*(u,t,a,b,...,h)]\};$$

this is by lemma 12 equivalent to

$$\sum_{u} \{ (u \in \varphi(x)) \cdot [\Xi^*(u,\varphi(t),\varphi(a),\varphi(b),...,\varphi(h))] \}$$

or in virtue of (6) to

$$\textstyle \sum \{(u \in x) \, \cdot \, [\, \Xi^*(u, \varphi(t), a, b, ..., h)] \} \, \equiv \, \{\varphi(t) \in y\}.$$

Hence  $\{t \in y\} = \{\varphi(t) \in y\}$ , i. e.  $y = \varphi(y)$ , which proves that y is really a pseudo-set.

17. It is almost obvious that the proposition [n] will become false if we replace the primitive concepts by their new meanings. Indeed, since the axiom of choice for sets of power n is a consequence of [n] (comp. the footnote  $^2$ )), we follow that if [n] were true in our model, the axiom of choice for sets of the power n would be true too. In virtue of lemma 11 this would mean that for every pseudo-set x whose elements are disjoint sets of the power n, there is a pseudo-set y such that if  $z \in x$ , then  $y \cdot z$  has exactly one element. This consequence is false. The pseudo-set  $x = \{N_1, N_2, N_3, ...\}$  satisfies namely all hypothesies and there is no corresponding pseudo-set y, because if y has exactly one element  $a_k$  in common with  $N_k$  (k=1,2,...), then y does not satisfy the invariance-condition. In fact, let q be any integer. Since G has no fixpoints, there is a  $\pi \in G$  such that  $\pi(a_{g+1}) \neq a_{g+1}$ , and putting

$$arphi = [\underbrace{1,1,...,1}_{q ext{ times}},\pi,1,1,\ldots]$$

we obtain an element  $\varphi \in G^{\omega}$  such that  $\varphi_1 = \varphi_2 = ... = \varphi_q = 1$  and  $\varphi(y) = y$ . Hence y cannot be a pseudo-set.

**18.** In order to accomplish the proof of the theorem III we must still show that if  $z \in Z$ , the proposition [z] remains valid in the model. In view of lemma 11 and footnote  $^2$ ) this means that for every pseudo-set X whose elements are disjoint sets of the power z, there is a pseudo-set Y such that if  $P \in X$ , the product  $Y \cdot P$  has exactly one element.

Suppose that X is a pseudo-set

$$(7) X \in K_{\xi},$$

that every element of X has z elements and that  $U \cdot V = 0$  if  $U \neq V$  and  $U, V \in X$ .

It follows from (7) that there is a positive integer q such that  $\varphi(X) = X$  for any  $\varphi \in G^{\omega}$  for which  $\varphi_1 = \varphi_2 = \dots = \varphi_q = 1$ . Let  $\Gamma$  be a subgroup of  $G^{\omega}$  consisting of all  $\varphi$ 's for which  $\varphi_1 = \varphi_2 = \dots = \varphi_q = 1$ .

For  $U,V\in X$  we write  $U\sim V$  if there is a  $\varphi\in \Gamma$  such that  $\varphi(U)=V$ . Since this relation is of course reflexive, symmetric and transitive, it induces a decomposition

$$X = \sum_{R \in \Delta} R$$

of X into the classes of abstraction  $R \in \Delta$  of  $\sim$ . Thus  $\Delta$  is the family of all classes of abstraction and the relation  $\sim$  holds between two elements U,V of X if and only if they belong to the same summand R of (8).

Applying the axiom of choice (see footnote <sup>17</sup>) I select from every  $R \in \Delta$  a particular element and call it  $E_R$ . Hence

(9) 
$$E_R \in R \subset X \text{ for } R \in \Delta$$

and consequently

(10) 
$$E_R$$
 has  $z$  elements.

Let  $H_R$  be the subgroup of  $\Gamma$  containing all  $\varphi$ 's such that  $\varphi(E_R) = E_R$  and let us write  $U \approx V$  if  $U, V \in E_R$  and if there is a  $\varphi \in H_R$  such that  $\varphi(U) = V$ . We may again decompose  $E_R$  into a sum of classes of abstraction of  $\approx$ :

(11) 
$$E_R = S_1 + S_2 + \ldots + S_r.$$

The number r of these classes (which will, in general, be different for different R) is finite in virtue of (10).

Using again the axiom of choice, I select from every  $S_i$  a particular element  $T_i$  and denote by  $K_i$  the group of those  $\varphi \in H_R$  for which  $\varphi(T_i) = T_i^{24}$ .

I shall show that  $S_j$  has exactly Ind  $(H_R/K_j)$  elements. Indeed, let

(12) 
$$H_R = K_j + \vartheta K_j + \vartheta K_j + \dots + \vartheta K_j$$

be the decomposition of  $H_R$  into co-sets. Elements

(13) 
$$T_{j}, \quad \overset{1}{\vartheta}(T_{j}), \quad \overset{2}{\vartheta}(T_{j}) \quad , \dots, \quad \overset{p}{\vartheta}(T_{j})$$

are all contained in  $S_j$ , because the relation  $\approx$  holds between them and  $T_j$ . They are all different, because from  $\partial(T_j) = \partial(T_j)$  would follow  $\partial^{-1}\partial(T_j) = T_j$  or  $\partial^{-1}\partial \in K_j$ , i. e.,  $\partial \in \partial K_j$ . Hence  $S_j$  has at least  $p+1=\operatorname{Ind}(H_R/K_j)$  elements. On the other hand, if  $U \in S_j$ , there must be a  $\varphi \in H_R$  such that  $\varphi(T_j) = U$ . Hence  $\varphi$  belongs to one of the summands  $\partial K_j$  of (12). Hence  $\varphi = \partial \psi$ , where  $\psi \in K_j$ , and consequently  $U = \partial(\psi(T_j)) = \partial(T_j)$ . We follow that  $S_j$  has no elements different from the elements (13), i. e.,  $S_j$  has exactly  $p+1=\operatorname{Ind}(H_R/K_j)$  elements.

Formulas (10) and (11) yield now

$$z = \text{Ind } (H_R/K_1) + \text{Ind } (H_R/K_2) + \ldots + \text{Ind } (H_R/K_r),$$

and since  $z \in Z$ , we follow from the hypothesis made at the beginning of 12 that one at least  $K_I$  is equal to  $H_R$ . This means that in every  $E_R$  there is at least one U such that  $\varphi(U) = U$  for every  $\varphi \in H_R$ . Using still once more the axiom of choice, I select from every  $E_R$  one such U and I call it  $U_R$ . For every  $R \in \Delta$  we have therefore

$$(14) U_R \in E_R,$$

(15) 
$$\varphi(U_R) = U_R \quad \text{for} \quad \varphi \in H_R.$$

Define now  $Q_R$  as the set of all  $\varphi(U_R)$  where  $\varphi \in \Gamma$  and put

$$Y = \sum_{R \in \Delta} Q_R$$
.

We shall show that this Y has desired properties.

For the first, Y is a pseudo-set. Indeed, from (7), (9) and (14) we follow that  $U_R \in K_{\xi}$  (transitivity of  $K_{\xi}$ ). Hence,  $Q_R \subset K_{\xi}$  by lemma 10 (i) and consequently  $Y \subset K_{\xi}$  or  $Y \in M_{\xi+1}$ . If  $\psi \in \Gamma$ , then  $\psi(Q_R) = Q_R$ , because  $\psi(Q_R)$  is the set of all  $\psi \varphi(U_R)$  where  $\psi \in \Gamma$ , and the conditions  $\psi \varphi \in \Gamma$  and  $\psi \in \Gamma$  are equivalent. From this we follow that  $\psi(Y) = Y$ . Y satisfies thus the invariance-condition, i. e., it is a pseudo-set.

It remains to show that if  $P \in X$ , then  $P \cdot Y$  has exactly one element.

Suppose that  $P \in X$ . There must be a summand R of the decomposition (8) such that  $P \in R$ , i. e.,  $P \sim E_R$ . Consequently there is a  $\varphi \in \Gamma$  such that  $\varphi(E_R) = P$ . Since  $U_R \in E_R$ , we have  $\varphi(U_R) \in \varphi(E_R) = P$ ; on the other side  $\varphi(U_R) \in Y$  by definition. This proves that  $P \cdot Y$  contains at least one element  $\varphi(U_R)$ .

<sup>&</sup>lt;sup>24</sup>) K<sub>j</sub> is, in general, not self-conjugate.

We shall now show that this element is unique, i. e., that if  $W \in P \cdot Y$ , then  $W = \varphi(U_R)$ .

Suppose that  $W \in P \cdot Y$ . Since  $W \in Y$ , there is a  $S \in \Delta$  such that  $W \in Q_S$  and it follows that W has the form  $\psi(U_S)$  where  $\psi \in \Gamma$ . Since  $W \in P = \varphi(E_R)$ , we have  $\psi(U_S) \in \varphi(E_R)$  or

(16) 
$$\varphi^{-1}\psi(U_S) \in E_R.$$

On the other side  $\varphi^{-1}\psi(U_S) \in \varphi^{-1}\psi(E_S)$  by (14). The sets  $E_R$ and  $\psi^{-1}\psi(E_S)$  are therefore not disjoint. Being both elements of X they must be disjoint or equal. Consequently  $\varphi^{-1}\psi(E_S) = E_R$ , which proves that  $E_R \sim E_S$ . But  $E_R \in R$ ,  $E_S \in S$  and the relation  $\sim$  holds never between two elements of different classes of abstraction. It follows thus R = S and (16) gives  $\psi(U_R) \in \varphi(E_R)$ . But  $\psi(U_R) \in \psi(E_R)$ by (14);  $\varphi(E_R)$  and  $\psi(E_R)$  have therefore an element in common and since they are both elements of X, they must be identical. This gives  $\psi(E_R) = \varphi(E_R)$  or  $\varphi^{-1}\psi(E_R) = E_R$ , i. e.,  $\varphi^{-1}\psi \in H_R$ . By (15) we obtain now  $\varphi^{-1}\psi(U_R) = U_R$ , i. e.,  $\psi(U_R) = \varphi(U_R)$  or  $W = \varphi(U_R)$ . Every  $W \in P \cdot Y$  is therefore identical with  $\varphi(U_R)$ , i. e.,  $P \cdot Y$  has exactly one element.

The proof of theorem III is thus accomplished.

19. We shall now draw some consequences of theorem III.

**Definition** 6. We shall say that a positive integer n and finite set Z of such integers satisfy the condition (M) if for any decomposition of n into a sum of primes

$$(1) n = p_1 + p_2 + \ldots + p_s$$

there are s non negative integers  $q_1, q_2, ..., q_s$  such that the sum  $p_1q_1+p_2q_2+\ldots+p_sq_s$  is contained in Z.

Theorem IV. Condition (M) is necessary for the implication  $[Z] \rightarrow [n].$ 

Proof. It suffices to prove that (M) is a consequence of (K). Let us suppose that n and Z satisfy the condition (K), and let (1)be a decomposition of n into a sum of primes. Let  $\varphi$  be the permutation

$$(1,2,...,p_1)(p_1+1,p_1+2,...,p_1+p_2) \dots \dots (p_1+p_2+...+p_{s-1}+1,p_1+p_2+...+p_{s-1}+2,...,n),$$

and let G be the cyclic group composed of all powers of  $\varphi$ . The order h of G is equal to the product of all different p's.

Since G has, of course, no fixpoints, then there is accordingly to (K) a subgroup H of  $G^{\omega}$  and a finite number r of proper subgroups  $K_1, K_2, \dots, K_r$  of H such that the sum

Ind 
$$(H/K_1)$$
 + Ind  $(H/K_2)$  + ... + Ind  $(H/K_r)$ 

is contained in Z. It follows in particular that the indexes Ind  $(H/K_i)$ are all finite.

In order to prove the theorem IV it is now sufficient to show that if  $K \subset H \subset G^{\omega}$  and if Ind (H/K) is finite and greater than 1. then Ind (H/K) is divisible by one of the primes  $p_1, p_2, ..., p_s$ .

Let

(2) 
$$H = K + \varphi^{(1)}K + \varphi^{(2)}K + \dots + \varphi^{(p)}K$$

be the decomposition of H in co-sets of K  $(p+1=\operatorname{Ind}(H/K))$ . Every  $\varphi^{(i)}$  is a sequence  $[\varphi_1^{(i)}, \varphi_2^{(i)}, \varphi_3^{(i)}, \ldots]$  where almost all  $\varphi_i^{(i)}$  are equal to the unit 1 of G.

Suppose that  $\varphi_i^{(j)} = 1$  for j > q, and let q be the greatest of the numbers  $q_1, q_2, ..., q_n$ . Let  $H^*$  be the subgroup of H containing all such  $\varphi$ 's that  $\varphi_{g+1} = \varphi_{g+2} = ... = 1$  and let  $K^*$  be the common part of  $H^*$  and K. It follows that  $\varphi^{(1)}, \varphi^{(2)}, ..., \varphi^{(p)}$  are contained in  $H^*$ . We shall show that the decomposition of  $H^*$  into co-sets with respect to  $K^*$  is

(3) 
$$H^* = K^* + \varphi^{(1)}K^* + \varphi^{(2)}K^* + \dots + \varphi^{(p)}K^*.$$

Indeed, if  $\varphi \in H^*$ , then  $\varphi \in H$ , and there is an  $i \leq p$  such that  $\varphi \in \varphi^{(i)}K$  or  $\varphi = \varphi^{(i)}\psi$ , where  $\psi \in K$ . It follows that  $\varphi_{\iota} = \varphi^{(i)}\psi_{\iota}$ for k=1,2,... and since  $\varphi_k=\varphi_k^{(j)}=1$  for k>q, we have also  $\psi_k=1$ for k>q, i. e.,  $\psi \in H^*$ . Hence  $\psi \in K^*$ , and we follow from  $\varphi=\varphi^{(l)}\psi$ that  $\varphi \in \varphi^{(i)}K^*$ .  $H^*$  is therefore the sum of co-sets

$$K^*, \varphi^{(1)}K^*, \varphi^{(2)}K^*, \ldots, \varphi^{(p)}K^*,$$

and these co-sets are disjoint, because they are contained in the corresponding co-sets K,  $\varphi^{(1)}K$ ,  $\varphi^{(2)}K$ , ...,  $\varphi^{(p)}K$ .

Formula (3) is thus proved and we have

(4) Ind 
$$(H^*/K^*) = p+1 = \text{Ind } (H/K)$$
.

 $H^*$  and  $K^*$  may be treated as subgroups of the direct product  $G \times G \times ... \times G = G^q$  of order  $h^q$ . Ind  $(H^*/K^*)$  is thus a divisor of  $h^q$ , i. e., it must be divisible by one at least  $p_i$ . By (4) we follow that Ind (H/K) is also divisible by one at least  $p_i$ , q. e. d. 11 Fundamenta Mathematicae, T. XXXIII.

**20.** Theorem V. If  $[Z] \rightarrow [n]$  and if m is the greatest of the numbers occurring in Z, then  $n < 8m^2$ .

This theorem states that, for given Z, there is only a finite number of n such that  $[Z] \rightarrow [n]$ .

Proof. Suppose that  $[Z] \rightarrow [n]$  and  $n \ge 8m^2$ . By the so called Bertrand's postulate <sup>25</sup>) there are primes p,q such that

$$(1) m$$

By the elements of the Theory of numbers there are further integers  $\mu, \nu$  such that  $p\mu+q\nu=1$ . Putting  $\xi=\mu n$ ,  $\eta=\nu n$  we obtain

$$(2) p\xi + q\eta = n.$$

I shall show that there are non-negative  $\xi, \eta$  for which (2) holds. Indeed, if e.g.  $\xi > 0$  and  $\eta < 0$ , we denote by  $\lambda$  the least positive integer for which  $\eta + \lambda p \geqslant 0$  and we have obviously  $0 \leqslant \eta + \lambda p < p$ . If  $\xi - \lambda q$  were  $\leqslant 0$ , we would have by (1)

$$n = p(\xi - \lambda q) + q(\eta + \lambda p) \leqslant q(\eta + \lambda p) < pq \leqslant 8m^2$$

against the hypothesis. Therefore  $\xi - \lambda q \geqslant 0$ , and integers  $\xi' = \xi - \lambda q$ ,  $\eta' = \eta + \lambda p$  are both non-negative and satisfy (2).

Let  $\xi$  and  $\eta$  be any non-negative solutions of (2). n may then be decomposed into a sum of primes

$$n = \underbrace{p + p + \ldots + p}_{\xi \text{ times}} + \underbrace{q + q + \ldots + q}_{\eta \text{ tim s}}.$$

Since  $[Z] \rightarrow [n]$ , the condition (M) must be satisfied. It follows that for some non-negative integers  $\varkappa_1, \varkappa_2, ..., \varkappa_{\hat{\xi}}, \lambda_1, \lambda_2, ..., \lambda_n$  the sum

$$\varkappa_1 p + \varkappa_2 p + \ldots + \varkappa_{\varepsilon} p + \lambda_1 q + \lambda_2 q + \ldots + \lambda_n q$$

is contained in Z. This sum must hence be not greater than m, which is of course impossible, because p and q both exceed m.

### § 3. Some particular cases.

**21.** The first particular case we shall consider is that of Z having the form  $\{1,2,...,m\}=(m)$ . The proposition [Z], which we shall, for brevity, denote by [m]!, represents then the principle of choice for sets of at most m elements.

**Theorem VI.** Condition (M) is necessary and sufficient for the implication  $\lceil m \rceil! \rightarrow \lceil n \rceil^{26}$ .

Proof. Necessity follows from theorem IV. In virtue of theorems II it remains to show that the condition (M) for  $Z = \{1, 2, ..., m\}$  implies the condition (S).

Let us suppose that (M) is satisfied and let be  $n=p_1+p_2+...+p_s$  where  $p_1,p_2,...,p_s$  are primes. By (M) there are  $q_1,q_2,...,q_s$  such that  $p_1q_1+p_2q_2+...+p_sq_s$  belongs to Z, i. e.,

$$0 < p_1q_1 + p_2q_2 + \ldots + p_sq_s \leqslant m.$$

It follows immediately that for an  $i \leq s$  we have  $p_i \leq m$ , i. e.,  $p_i \in Z$ . Hence the condition (S) is satisfied, q. e. d.

**22.** Let us denote by  $\mu(n)$  the greatest prime p such that n is expressible as a sum of primes not less than p.

It is easy to see that condition (M) for  $Z=\{1,2,...,m\}$  says the same as  $m \ge \mu(n)$ . We may hence express theorem VI by the equivalence

(1) 
$$([m]! \rightarrow [n]) \equiv (m \geqslant \mu(n)).$$

The following table gives values of  $\mu(n)$  for lowest n:

We note the following properties of  $\mu(n)$ :

(2) 
$$\frac{1}{2}\sqrt{\frac{n}{2}} < \mu(n) \leqslant n \qquad \text{(follows from theorem V);}$$

(3)  $\mu(n)$  is always prime;  $\mu(n)=n$  if and only if n is prime;

(4) if 
$$n \neq 2$$
 and  $n \neq 4$ , then  $\mu(n) > 2$ ,

Proof of (4): for  $n \le 32$  the values of  $\mu(n)$  are given in the able. For n > 32 the left side of (1) exceeds 2.

From (4) and (1) we obtain immediately

<sup>&</sup>lt;sup>25)</sup> Proof of this theorem may be found, e. g., in Serret's Cours d'Algèbre Supérieure, 2<sup>nd</sup> edition, 1854, pp. 587-600.

<sup>&</sup>lt;sup>26</sup>) The proof of sufficiency has been given by Mrs. W. Szmielew; comp. foot-note <sup>10</sup>).

**Theorem VII.** Implication [2] $\rightarrow$ [n] holds if and only if n=2 or n=4.

Another consequence of (1) and (3) is

**Theorem VIII.**  $[m]! \rightarrow [n]!$  if and only if there is no prime p between m and n.

Proof. If m and if <math>p is prime, then  $\mu(n) \ge p$  by (2) and (3) and consequently even the implication  $[m]! \to [p]$  cannot be true. If, on the other side, there is no prime between m and n, we have  $\mu(x) \le m$  for  $x \le n$  and all implications  $[m]! \to [x]$   $(x \le n)$  are true, i. e.,  $[m]! \to [n]!$ .

#### 23. We shall now prove

**Theorem IX.** Condition (M) is necessary and sufficient for the implication  $[Z] \rightarrow [n]$  in the following cases:

(i) n is prime; (ii) n < 15; (iii) n = 16, 18.

The proof is based on some lemmas.

**Lemma 13.**  $[nk] \rightarrow [k]$  for every positive integers n and k.

An easy proof will be omitted here.

**Lemma 14.** If A has m elements and B n elements,  $A \cdot B = 0$ , and if we know to realize the proposition [km+ln] where k and l are non-negative integers not both 0, then we may choose an element from A+B.

Proof. Consider the set  $A^*$  of ordered pairs  $\langle i,a \rangle$  where  $a \in A$  and i=1,2,...,k, and the set  $B^*$  of ordered pairs  $\langle j,b \rangle$  where  $b \in B$  and j=1,2,...,l. The sum  $A^*+B^*$  has km+ln elements, and we can by the hypothesis select a particular element p of  $A^*+B^*$ . p is an ordered pair whose second member belongs to A+B and may be taken as selected element of A+B.

**Lemma 15** <sup>27</sup>). If p is a prime, A has  $n \cdot p$  elements (n=2,3,4,...), and if we know to realize the proposition [p], then we can define effectively a decomposition  $A=A_1+A_2$  into a sum of two disjoint non-empty sets.

Proof. Let  $\overline{A}$  be the class of subsets of A having exactly p elements. From every  $X \in \overline{A}$  we can by supposition choose an element  $X^*$ . For  $a \in A$  denote by  $n_a$  the number of  $X \in \overline{A}$  such that  $X^* = a$ . Hence, the sum of all  $n_a$  is equal to the number of elements.

ments of  $\overline{A}$ , i. e., to  $\binom{n \cdot p}{p}$ . Since this number is not divisible by p and the number  $n \cdot p$  of all  $n_a$  is divisible by p, we follow that not all  $n_a$  can be identical. Hence, denoting by  $A_1$  the set of those  $a \in A$  for which  $n_a$  has the lowest possible value and putting  $A_2 = A - A_1$ , we obtain the desired decomposition.

**Lemma 16.** If p is a prime, A has n p elements (n=2,3,...), and if we know to realize the proposition  $[n \cdot p-1]$ , then we can define effectively a decomposition  $A=A_1+A_2+...+A_r$  into a sum of a finite number of disjoint sets of the power >1.

Proof. Accordingly to the hypothesis, to every  $a \in A$  corresponds an element f(a) choosen from the set  $A - \{a\}$ . We have thus a function f(a) defined for  $a \in A$  and such that  $f(a) \neq a$ .

If the set of values of f coincides with A, then f is a permutation of A and can be decomposed into cycles. In every cycle there is more than one element, because  $f(a) \neq a$ . If the number of cycles is greater than 1, they define a decomposition of A of the desired type. If f is a single cycle, we consider  $f^p$  instead of f and obtain a permutation for which the number of cycles is p>1, and in every cycle there is n>1 elements.

If f is not a permutation, we denote by  $A_1$  the set of values of f. Sets  $A_1$  and  $A-A_1$  are both non-empty and we have a decomposition  $A=A_1+(A-A_1)$ . It is already of desired type, if  $A-A_1$  has more than 1 element  $(A_1$  has never one element, because  $f(a) \neq a$ ). In this exceptional case we have  $A-A_1=\{a\}$  and may put  $A=(A_1-\{f(a)\})+\{a,f(a)\}$ .

24. We pass now to the proof of theorem IX.

Suppose that n and Z satisfy the condition (M) and that [Z] is true.

If n is prime, Z must contain a number of the form  $n \cdot k$  and we follow by lemma 13 that [n] is true.

If n=4, Z must contain at least one number of the form 2i. Using lemma 13 we get the proposition [2] and, by theorem VII, the proposition [4].

If n=6, Z must contain at least one number of the form 2i and at least one number of the form 3j. Lemma 13 yields propositions [2] and [3], i. e., the proposition [3]! from which we obtain [6] by theorem VI.

<sup>&</sup>lt;sup>27</sup>) This lemma and its proof are due to A. Tarski.

Let us suppose that n=8 and that A has 8 elements. Z contains in this case numbers of the form 2k and 3l+5m; we have thus propositions [2] and [3l+5m] at our disposal.

Accordingly to lemma 15 we decompose A into a sum  $A=A_1+A_2$  of two non-empty disjoint sets. The notation can be arranged so that  $A_2$  has at least as much elements as  $A_1$ .  $A_1$  can therefore have 1, 2, 3 or 4 elements. In the first case we take the unique element of  $A_1$  as the distinguished element of A. In the second case we can select an element from  $A_1$  in virtue of [2]. In the third case we may choose an element from  $A=A_1+A_2$  using lemma 14. In the last case we choose an element a from  $A_1$  and an element b from  $A_2$  using the proposition [4], which is, as we already know, the consequence of [2]. We obtain thus a decomposition  $A=\{a,b\}+(A-\{a,b\})$  and we may apply the same reasoning as in the first or second case. Hence we can always choose an element from A.

Cases n=10, n=12 and n=18 may be treated in similar manner as n=8. For n=10 Z must contain numbers of the form 2i, 5j, 3k+7l, for n=12 numbers of the form 2i, 5j, 5k+7l and for n=18 numbers of the form 2i, 3j, 5k+13l, 7p+11q.

Treating the case n=18, it is well to remember that [6], [8] and [9] are consequences of [2] and [3] (see theorem VI).

A little more complex are cases n=9, 14 and 16.

Consider first the case n=9. Z contains then numbers of the form 3k and 2l+7m; we have thus propositions [3] and [2l+7m] at our disposal. Let A be a set with 9 elements. Using lemma 15 we decompose A into a sum  $A=A_1+A_2$  of two disjoint non-empty sets and suppose the notation to be arranged so that  $A_2$  has more elements than  $A_1$ .  $A_1$  may therefore have 1, 2, 3 or 4 elements. In the first and third case we can immediately choose an element from  $A_1$ . In the second case we choose an element from the sum  $A=A_1+A_2$  using lemma 14. In the last case we apply lemma 16 to  $A_1$  and obtain a decomposition of  $A_1$  into a sum of a finite number of disjoint sets of the power >1. Since  $A_1$  has 4 elements, only the decomposition  $A_1=A'+A''$  into a sum two of sets of the power 2 is possible. Accordingly to lemma 14 decompositions

$$A = A' + (A'' + A_2)$$
 and  $A = A'' + (A' + A_2)$ 

define two elements a, b of A. We have thus

$$A = \{a,b\} + (A - \{a,b\})$$

and may proceed further as in the first or second case.

For n=9 the theorem is thus proved.

If n=14, Z must contain numbers of the form 2i, 7j and 3k+11l. Remarking that 3k+11l=3(k+2l)+5l, we follow that [8] is a consequence of [Z]. Hence we have at our disposal propositions [2], [7], [8] and [3k+11l].

Suppose that A has 14 elements. As in the foregoing cases, we decompose A into a sum  $A = A_1 + A_2$  of two non-empty disjoint sets and suppose again that  $A_2$  has at least as many elements as  $A_1$ . The number  $\nu$  of elements of  $A_1$  may therefore be equal to 1, 2, 3, 4, 5, 6 or 7.

In cases  $\nu=1,2,3,4,7$  we can choose an element from A without difficulty.

If v=6 we decompose  $A_1$  into a sum  $A_1=A'+A''$  of two disjoint non-empty sets using lemma 15 and proposition [2]. If one of the sets A',A'' has 1 or 2 elements, the choice of an element from this set is already possible. If A' and A'' have both 3 elements, we consider the decompositions

$$A = A' + (A'' + A_2),$$
  $A = A'' + (A' + A_2).$ 

to which correspond two well-defined elements a, b of A in view of lemma 14 and of proposition [3k+11l]. Hence

$$A = \{a,b\} + (A - \{a,b\})$$

and we are in the same situation as for  $\nu=2$ .

It remains the case  $\nu=5$ .  $A_2$  has then 9 elements and we may apply lemma 16 to the set  $A_2$  obtaining a decomposition

$$(1) A_2 = B_1 + B_2 + \ldots + B_q$$

into a sum of disjoint sets of the power >1. Let us denote by  $b_l$  the number of elements of  $B_l$  (i=1,2,...,q) and by b the least of these numbers.

If not all  $b_i$  are equal to b, we may decompose  $A_2$  into a sum of disjoint non-empty sets

$$A_2 = A_2' + A_2'',$$

taking as  $A'_2$  the sum of those  $B_i$  for which  $b_i=b$  and as  $A''_2$  the sum of the remaining  $B_i$ . Arranging now the notation so that  $A'_2$  has less elements than  $A''_2$ , we obtain the decomposition

$$A = A_2' + (A_1 + A_2'')$$

# A. Mostowski.

in which  $A_2$  has 2, 3 or 4 elements and return so to cases  $\nu=2,3$  or 4 discussed previously.

If all  $b_i$  are equal to b, then b=3, q=3 and (1) takes the form  $A_2=B_1+B_2+B_3$  where  $B_1,B_2$  and  $B_3$  have 3 elements. Consider the decompositions:

$$A = B_1 + (B_2 + B_3 + A_1),$$
  
 $A = B_2 + (B_3 + B_1 + A_1),$   
 $A = B_3 + (B_1 + B_2 + A_1),$ 

to which correspond 3 elements a, b, c of A in virtue of lemma 14 and of proposition [3k+11l]. We write now down the decomposition

$$A = \{a, b, c\} + (A - \{a, b, c\})$$

and return so to cases v=1,2,3 in which we can already accomplish the choice.

Case n=14 is thus discussed in full.

168

In case n=16 the reasoning is the same as for n=14. Z contains in this case numbers of the form 2i, 3j+13k and 5k+11l.

Theorem IX is thus proved completely.

Results of this section suggest a supposition that condition (M) is in every case sufficient for the implication  $[Z] \rightarrow [n]$ . I was not able to solve this question even in the case n=15 and  $Z=\{3,5,13\}$ .



# Sur les fonctions de plusieurs variables

Par

### Wacław Sierpiński (Warszawa).

Le but de cette Note est de démontrer que les fonctions de plusieurs variables où toutes les valeurs des variables, ainsi que celles des fonctions, appartiennent à un ensemble fixe quelconque se réduisent par superpositions aux fonctions de deux variables. Plus précisément

Soient: E un ensemble donné, m un nombre naturel,  $F_m$  la famille de toutes les fonctions de m variables  $f(x_1, x_2, ..., x_m)$  définies pour  $x_i \in E$  où i=1,2,...,m (autrement dit: définies dans le produit cartésien  $E^m$ ) et ne prenant que des valeurs appartenant à E. Soit S la famille de toutes les fonctions de  $F_2+F_3+...$  qui sont des superpositions d'un nombre fini de fonctions de la famille  $F_2$ . S est donc la plus petite famille de fonctions qui contient  $F_2$  et telle que si les fonctions  $f(x_1,x_2,...,x_m)$  et  $g(x_{m+1},x_{m+2},...,x_{m+n})$  appartiennent à S et si la fonction h(x,y) appartient à  $F_2$ , la fonction

$$h(t(x_1,x_2,...,x_m),g(x_{m+1},x_{m+2},...,x_{m+n}))$$

appartient à S, de même que les fonctions qu'on en obtient en échangeant ou en identifiant entre elles certaines de variables  $x_1, x_2, \dots, x_{m+n}$ .

Notre théorème équivaut ainsi à la formule

$$(1) F_m \subset S pour m=2,3,...$$

Nous allons démontrer la formule (1) séparément pour E fini et E infini. Pour E infini, notre démonstration fera usage de l'axiome du choix; or, pour E fini, elle est plus compliquée que pour E infini.

Soit donc E un ensemble fini contenant au moins deux éléments distincts. Je démontre d'abord deux lemmes.