SOME REMARKS ON SET THEORY

P. ERDÖS

The present note contains a few disconnected remarks on the theory of sets.

It is well known that the addition of ordinal numbers does not satisfy the the law of commutativity, for example, $1+\omega\neq\omega+1$. Let now n be a finite number. Denote by $f(n)$ the maximum number of different ordinals we can obtain by adding in all possible ways n ordinals. We prove the following theorem.

THEOREM I. *We have*

$$f(n) = \max_{k\leqq n-1} (k2^{k-1} + 1)f(n - k). \tag{1}$$

In fact, $f(2)=2$, $f(3)=5$, $f(4)=13$, $f(5)=33$, $f(6)=81$, $f(7)=193$, $f(8)=449$, $f(9)=1089$, $f(10)=2673$, $f(11)=6561$, $f(12)=15633$, $f(13)=37249$, $f(14)=88209$, $f(15)=216153$, $\cdots$, *and for* $x\geqq 3$, $f(5x+1)=81^x$, $f(5x+2)=193\cdot 81^{x-1}$, $f(5x+3)=193^2 81^{x-2}$, $f(5x+4)=193^3 81^{x-3}$, $f(5x+5)=33\cdot 81^x$. *Thus for* $n\geqq 21$

$$f(n) = 81f(n - 5). \tag{2}$$

Let there be given n ordinals $\alpha_1, \alpha_2, \cdots, \alpha_n$. It is well known that every ordinal can be written uniquely as the sum of indecomposable ordinals. (An ordinal is said to be indecomposable if it is not the sum of two smaller ordinals.) Denote by $\phi(\alpha)$ the largest of these indecomposable ordinals belonging to α. ($\phi(\alpha)$ may have a coefficient c in the decomposition of α.) Put $\gamma=\min_{i\leqq n}\phi(\alpha_i)$, and assume that there are k α's with $\phi(\alpha_i)=\gamma$. Denote these α's by $\alpha_1, \alpha_2, \cdots, \alpha_k$. If in the sum $\alpha_{i_1}+\alpha_{i_2}+\cdots+\alpha_{i_n}$, $i_1, i_2, \cdots, i_n$ a permutation of $1, 2, \cdots, n$, none of the α_i, $i\leqq k$ appear at the end, they get absorbed in the following summands, and we get exactly $f(n-k)$ different sums. Assume next that exactly r of the α_i's, $r\leqq k$, appear at the end of $\alpha_{i_1}+\alpha_{i_2}+\cdots+\alpha_{i_n}$. Put

$$\alpha_i = 2^i\gamma + \delta_i,\ \delta_i < \gamma,\ \delta_i \neq \delta_j, \qquad \text{for } i, j \leqq k. \tag{3}$$

We then have

$$\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_n} = \beta + (2^{i_n} + 2^{i_{n-1}} + \cdots + 2^{i_{n-r+1}})\gamma + \delta_{i_n} \tag{4}$$

where $\beta\geqq\omega\gamma$. (All the δ's except δ_{i_n} get absorbed.) Now $2^{i_n}+2^{i_{n-1}}+\cdots+2^{i_{n-r+1}}$ can be chosen in $C_{k,r}$ ways and δ_{i_n} in r ways. Thus

Received by the editors November 2, 1948.

the number of sums is $rC_{k,r}f(n-k)$. (The $k-r$ α's with $\phi(\alpha)=\gamma$ not appearing at the end get absorbed.) Summing for r, we obtain

$$(5)\qquad f(n) \geqq \left[1 + \sum_{r=1}^{k} rC_{k,r}\right] f(n-k) = (k2^{k-1}+1)f(n-k).$$

Hence clearly

$$(6)\qquad f(n) = \max_{k \leqq n-1} (k2^{k-1}+1)f(n-k)$$

(since it clearly follows from our proof that our choice of the α's gives the maximum number of different summands). This proves (1).

We obtain from (1) by a simple computation that for $n \leqq 20$ the value of $f(n)$ is given by Theorem I. The rest of Theorem I is easily proved by induction, we have to use that $(k2^{k-1}+1)^{1/k}$ (k integer) increases for $k \leqq 5$ and decreases for $k \geqq 5$. We suppress the details since they can easily be given and depend only on numerical estimates. Thus the proof of Theorem I is complete.

Mr. Spanier remarked that the number of different products one can obtain from n ordinals is $n!$. It suffices to choose $\alpha_1 = \omega+1$, $\alpha_2 = \omega+2, \cdots, \alpha_n = \omega+n$. A simple computation shows that

$$\alpha_{i_1}\cdot\alpha_{i_2}\cdots\alpha_{i_n} = \omega^n + i_n\omega^{n-1} + \cdots + i_1$$

where $i_1, i_2, \cdots, i_n$ is any permutation of $1, 2, \cdots, n$.

Let X be a set of power m. Letters $a, b, \cdots$ denote subsets of X; $A, B, \cdots$, sets of subsets of X. A and B are defined (by Lusin) to be orthogonal if for any $a \in A$, $b \in B$, $a \cap b$ has power less than m. The orthogonal sets are said to be separable if there exist c and d with $c \cap d$ empty and such that for every $a \in A$, $b \in B$, $a \subset c \cup a'$, $b \subset d \cup b'$, where the power of a' and b' is less than m.

Lusin[1] proves with the aid of the axiom of choice that if $m = \aleph_0$ there exists two orthogonal sets which are not separable. We shall give a very simple proof of this result for all m, which for $m = \aleph_0$ will be independent of the axiom of choice.

Let A consist of m disjoint sets of power m and B consist of all the sets which intersect the sets of A in not more than one point. Clearly A and B are orthogonal, but they clearly are not separable, for every set c which intersects all the sets of A contains a set of B. For $m = \aleph_0$ this proof is independent of the axiom of choice, but in the general case the equality $m^2 = m$ is used and this is equivalent to the axiom of choice.[2]

[1] C. R. (Doklady) Acad. Sci. URSS. vol. 40 (1943) pp. 175–178.

[2] Tarski, Fund. Math. vol. 7, pp. 147–154.

Lusin[1] also proves that if both A and B contain only countably many sets, then they are separable. His proof generalizes to the case when m is a regular number and both A and B contain only m sets. We give the proof only for the sake of completeness.

Suppose A consists of the sets $\{a_\alpha\}$ and B of the sets $\{b_\alpha\}$. Put

$$c = \bigcup_\alpha \Big(a_\alpha - \sum_{\beta \leqq \alpha} b_\beta\Big), \qquad d = \bigcup_\alpha \Big(b_\alpha - \sum_{\beta \lneqq \alpha} a_\beta\Big).$$

Clearly c and d separate A and B.

The proof breaks down if m is singular. We shall give an example which shows that the theorem is not always true for singular m. Put

$$m = \aleph_0 + 2^{\aleph_0} + 2^{2^{\aleph_0}} + \cdots .$$

Let A consist of countably many disjoint sets a_i of power m. Write $a_i = n_0^{(i)} + n_1^{(i)} + \cdots$ where card $(n_0^{(i)}) = \aleph_0$, card $(n_1^{(i)}) = \aleph_1, \cdots$ (card a denotes the cardinal number of a) and $n_k^{(i)} \cap n_l^{(i)} = 0$. B consists of all the sets b of the form $\bigcup_i n_{f(i)}^{(i)}$ where $f(i)$ is any function of i (clearly card $B = 2^{\aleph_0} < m$). A and B are clearly orthogonal, but a simple argument shows that they are not separable.

If n is the smallest cardinal number cofinal to m and A and B contain not more than n sets, then it is easy to see that if A and B are orthogonal, they are also separable.

The orthogonal sets A and B are said to be complete (Lusin) if we can add no set either to A or to B without destroying orthogonality, that is, if X is the set of integers and A consists of all the subsets containing only a finite number of even numbers and B of all sets containing only finitely many odd numbers.

A and B are called k-orthogonal if for any $a \in A$ and $b \in B$, card $(a \cap b) < \aleph_k$. k-completeness can be defined in the obvious way. We shall prove the following theorem.

THEOREM II. *The cardinal number N of the k-complete orthogonal pairs equals*

$$N = 2^{m^{\aleph_k}}.$$

We shall assume the generalized continuum hypothesis $2^{\aleph_k} = \aleph_{k+1}$. Tarski[3] proved (by using the generalized hypothesis of the continuum) that there exist $m^{\aleph_k}$ subsets of X(card $X = m$) such that the intersection of any two has power less than $\aleph_k$. Denote such a set of subsets by C. Split C in an arbitrary way into the union of two sets of subsets A' and B'. This can clearly be done in $2^{m^{\aleph_k}}$ ways. Clearly

[3] Ibid. vol. 12, pp. 186–206 and vol. 14, pp. 205–216.

A' and B' are k-orthogonal. It immediately follows from the axiom of choice that they can be extended to the k-complete orthogonal pair A and B, and a simple argument shows that to different A' and B' correspond different A and B. This shows that

$$N \geqq 2^{m^{\aleph_k}}.$$

Let now A' be any set of subsets of X. There clearly exists a maximal set of subsets of X, B say, which is k-orthogonal to A'. We shall prove that there exists a subset A'' of A' of power $\leqq m^{\aleph_k}$ which determines the same set B. Consider all the subsets of power $\aleph_k$ of the sets $a \in A'$. The power of these sets is clearly not greater than $m^{\aleph_k}$. To each of these sets select an arbitrary $a_\alpha \in A'$ which contains it, and let the sets of A'' be all these a_α. Clearly if B is k-orthogonal to A'' then it is also k-orthogonal to A' (and vice versa), which completes the proof of our statement. But then a simple argument shows that the number of complete k-orthogonal pairs is not greater than

$$(2^m)^{m^{\aleph_k}} = 2^{m^{\aleph_k}}$$

which completes the proof of Theorem II. In the second part of our proof we clearly did not use the continuum hypothesis.

It follows from Theorem II that the number of complete orthogonal pairs is 2^{2^m}. The number of complete orthogonal and separable pairs is clearly only 2^m, which again shows that there are orthogonal pairs which are not separable.

Without using the continuum hypothesis it seems to be very hard to prove that the number of complete orthogonal pairs is greater than 2^m. But if $m=\aleph_0$ this is quite easy, since it is well known that there exist $2^{\aleph_0}$ sets of integers such that the intersection of any two is finite. It suffices to let a_α consist of the integers $2^n+[n^\alpha]$ where α is an arbitrary positive real number.

THEOREM III. *Let S be any infinite subset of k-dimensional Euclidean space.* Card $S=m$. *Then there exists a subset S_1 of S,* card $S_1=m$, *such that all the distances between any two points of S_1 are different.*

REMARK. We are not going to assume the continuum hypothesis. In fact the proof will be complicated only because we cannot exclude the possibility that m is singular.

We use induction with respect to the dimension k. We slightly strengthen the statement of our theorem. In fact we prove: Let the set S (card $S=m$) be situated on n ($n<m$) k-dimensional hyperplanes or hyperspheres. Then there exists a subset S_1 of S, card $S_1=m$, such that all the distances between any two points of S_1 are different.

First we prove this for $k=1$. Put $S=L+C$, where L is the subset of S situated on lines and C the subset situated on circles. Assume first card $L=m$. Denote by M_L the set of lines containing L. By assumption card $M_L \leqq n < m$. Let L_1 be a subset of L, such that any line bisecting the distance between any two points of L_1 is not in M_L, and L_1 is maximal with respect to this property (it clearly follows from the axiom of choice that such an L_1 exists, possibly it is empty). We prove card $L_1=m$. For if not assume that card $L_1=r<m$, then by definition of L_1, to every point x of $L-L_1$ there exists a point y of L_1 such that the perpendicular bisector of x and y is a line of M_L. But a point y of L_1 and a line l of M_L uniquely determines a point x of $L-L_1$ such that the perpendicular bisector of the segment $[x, y]$ is l. But since card $L_1<m$ and card $M_L<m$ this would imply that $L-L_1 \leqq m$, and hence card $L<m$, which is not true. Thus we prove that card $L_1 =m$. Let now L_2 be a maximal subset of L_1 with the property that all distances between points of L_2 are different. Let card $L_2=t$. If $t<m$, then all the points of L_1-L_2 must lie on t circles or lines. But this is impossible since the lines cannot coincide with any of the lines of M_L, therefore any of these lines can intersect any line of M_L in at most one point. Therefore each of these lines can contain at most card M_L points of L_1-L_2, and each of the circles can contain also at most card M_L points of L_1-L_2. But this would mean that card $(L_1-L_2) \leqq t \cdot$card $M_L<m$ which is not the case. Thus $t=m$, which completes the case card $L=m$. Assume next card $C=m$. Denote by M_c the set of circles containing C, put card $M_C=r<m$, denote further by O the set of centers of the circles of M_{C_1}, and consider the set $C-O$. Denote by C_1 a maximal subset of $C-O$ with the property that all distances between points of C_1 are different. Then it is easy to see that card $C_1=m$, which completes the proof in case $k=1$.

Assume now that our theorem is true for $k-1$, and we shall prove it for k. Suppose then that S lies on $n<m$ k-dimensional hyperplanes and hyperspheres. By the same argument as used in the previous pages we can find n $(k-1)$-dimensional hyperplanes and hyperspheres which contain m points of S, and by the induction hypothesis this completes the proof of Theorem III. In case m is a regular number it is easy to give a very much simpler proof.

Assume that m is regular and that S is a set of power m in k-dimensional Euclidean space. Then we can select a subset S_1 of S of power m such that for $r=1, 2, \cdots, k$ the volume of any two r-dimensional nondegenerate simplices is different. The proof is similar to the case for $r=1$. If m is singular this result is false. Take $m=\aleph_\omega$, and denote by $l_1, l_2, \cdots$ a countable set of parallel lines. Let l_k contain $\aleph_k$ points of S. Clearly any subset S_1 of S of power $\aleph_1$ contains two nondegenerate triangles of the same area.

If the set S is in Hilbert space our theorems of the previous pages do not generalize. In fact Oxtoby and I constructed a set of power $\aleph_1$, such that the distance between any two points is rational. We do not give the construction here. At present we cannot decide whether there exists in Hilbert space such a set of power c. (Added in proof: Kakutani and I found a simple example of such a set.)

One can ask the following question: Is it possible to split the n-dimensional Euclidean space into countably many disjoint sets, such that in each set any two distances between any two points should be different. For $n=1$ this is known,[4] and I do not know the answer for $n>1$.

The problems we just considered have some interest also for finite sets. Let there be given n points (n finite) on a line. Then we can select $c \cdot n^{1/3}$ points among them, such that all the distances are different. It is probable that $c \cdot n^{1/3}$ can be replaced by $c \cdot n^{1/2}$. If the n points are in k-dimensional space, we can select $c \cdot n^{1/f(k)}$ points among them such that all the distances are different. I do not know the exact value of $f(k)$.

Dénes König's[5] book on graphs contains the following theorem: Let G be a graph of order m (m is an infinite cardinal) and any two vertices are connected by less than n edges, and we assume $n<m$. Then G is the product of linear factors. Let us first explain the terminology: The order of a point is the cardinal number of edges of its star (the star of a vertex is the collection of edges incident with it). A graph is said to be of order m, if every vertex of it has order m. Let Ω_k be the initial number belonging to the cardinal number m. G is the product of linear factors if we can make correspond to each edge of G an ordinal number $\beta<\Omega_k$, such that the star of every vertex contains one and only one edge to which the ordinal β, $\beta=1, 2, \cdots$, corresponds. König[5] raises the question whether the condition "connected by less than n edges, and $n<m$" can be replaced by "connected by less than m edges." The proof given in his book shows that the answer is affirmative in case m is a regular number. We shall show that the answer is negative for singular numbers. Let the vertices of G be the points $\{a_i\}$, $i=1, 2, \cdots$, and $\{b_\alpha\}$, $\alpha<\Omega_1$. The vertices a_i and a_j, $i<j$, are connected by $\aleph_j$ edges, and b_α and a_i are connected by $\aleph_i$ edges. Clearly G is of order $\aleph_\omega$ and any two vertices are con-

[4] P. Erdös and S. Kakutani, Bull. Amer. Math. Soc. vol. 49 (1943) pp. 457–460.

[5] *Theorie der endlichen und unendlichen Graphen*, pp. 220–223.

nected by less than $\aleph_\omega$ edges. Nevertheless G is not the product of linear factors, in fact G has no linear factor at all. (A linear factor is a subgraph of order 1 containing all the vertices of G.) Clearly any linear factor would have all the b's as vertices, but then at least one a would have to have order $\aleph_1$, which is impossible; this contradiction proves our assertion. It would be easy to construct an analogous counterexample for every other singular number.

Now we prove the following theorem.

THEOREM IV. *Let G be a graph of order m, where every vertex is connected (by an edge) to at least m different vertices. Then G is the product of linear factors.*

REMARK. This theorem is clearly a generalization of the theorem given in König's book.[5] My original proof was very complicated. Hajós found the following very much simpler proof:

Let Ω_k be the initial number belonging to m, $\{a_\alpha\}$, $\alpha<\Omega_k$, be the vertices of G and $\{e_\beta\}$, $\beta<\Omega_k$, the edges of G. We construct the factors of G by transfinite induction. Let $0<\gamma<\Omega_k$, and suppose that for every $\delta<\gamma$ we have already found a linear factor. Then we construct the γth linear factor as follows: Let e_ρ be the edge of smallest index which has not been used in any of the previous linear factors (in other words every $e_{\rho'}$, with $\rho'<\rho$, occurs in some previous linear factor). Let then e_ρ be the first edge of our γth linear factor. We construct the γth factor by transfinite induction. Suppose we have already constructed a subgraph $G_\gamma(\alpha)$ of order 1 of G containing e_ρ and also all the vertices of index less than α of G. Clearly $G_\gamma(\alpha)$ has less than m vertices. By our assumption a_α is connected to at least m different vertices. Thus it is connected to m different vertices not in $G_\gamma(\alpha)$. In the factors of index less than γ we clearly used less than m (in fact card γ) edges all emanating from a_α. Thus there remains an unused edge of G which connects a_α to a vertex not in $G_\gamma(\alpha)$, this edge will be in our γth factor. This construction gives our γth factor for every $\gamma<\Omega_k$ and clearly by construction every edge of G occurs in one of the factors once and only once, q.e.d. This proves Theorem IV.

The following problem is due to Turán[6] (oral communication):

Let card $S=c$, to every $a\in S$ there corresponds a finite subset $f(a)$ of S. We assume that a is not contained in $f(a)$. Two elements a and b

[6] The problem was originally raised by Turán in connection with a problem on interpolation and solved by G. Grünwald in case card $S=\aleph_0$. For the literature of the problem see, for example, P. Erdös, *Some set-theoretical properties of graphs*, Universidad Nacional de Tucuman Revista 1942, also footnote 7.

are called independent if $a\notin f(b)$ and $b\notin f(a)$. A subset S' of S is said to be independent if any two elements of it are independent or if $S'\cap f(S')$ is empty. Turán's question was: does there always exist an infinite independent set? G. Grünwald showed that the answer is affirmative. Later Lázár showed that there exists an independent set of power c. Sierpinski and Ruzievicz raised the following general question: Let S be a set of power m, and let $n<m$, an arbitrary cardinal number. To every $a\in S$ there corresponds a subset $f(a)$ of S satisfying $a\notin f(a)$ and $f(a)<n$. Does there always exist an independent set S' with card $S'=m$? This has been proved if m is a regular number, or if m is the countable sum of smaller cardinals.[7] We shall prove, assuming the generalized continuum hypothesis, that the answer is always affirmative (Theorem V).

If we replace the condition card $(f(a))<n<m$ by card $(f(a))<m$, then in general we do not even have two independent points. Let Ω_k be the initial number belonging to m, and α_ξ the set of ordinals less than Ω_k. Define $f(\alpha_\xi)$ as the collection of all $\beta<\alpha_\xi$. Clearly no two elements are independent.

First I give a very simple proof of Theorem V in case m is a regular number. This proof is due to D. Lázár, and has been communicated to me orally. Assume that the theorem is false, that is, the power of every independent set is less than m. Let S_1 be a complete set of independent elements, that is, $S_1\cap f(S_1)$ is empty and if $a\notin S_1$, then $(a\cup S_1)\cap f(a\cup S_1)$ is not empty. Consider $S-S_1-f(S_1)$, and let S_2 be a maximal independent subset of it, and consider $S-S_1-S_2-f(S_1)-f(S_2)$. Continue this process for all ordinals $\alpha<\Omega_l$, where Ω_l is the initial number belonging to $n=\aleph_l$. Since m is a regular number, the power of $\bigcup_\alpha(S_\alpha\cup f(S_\alpha))$ is less than m. Thus the set $S-\bigcup_\alpha(S_\alpha\cup f(S_\alpha))$ is not empty. Let a be an element of this set. Because of the maximal property of the sets S_α, $f(a)$ must intersect each of the S_α's (by our construction $a\notin f(S_\alpha)$, thus the last statement is a consequence of the fact that a and S_α are not independent). But this would mean that card $(f(a))\geqq n$, an evident contradiction. Clearly this proof also works if m is singular but is not the sum of n smaller cardinal numbers.

Now we prove our main theorem. Let card $S=m$, m singular. Put $S=\bigcup_\alpha S_\alpha$, $\alpha<\Omega_r$. Card $(S_\alpha)=m_\alpha$, $m_\alpha>m_\beta$ for $\alpha>\beta$. Let Ω_k be the initial number belonging to m and Ω_r the smallest ordinal number cofinal to Ω_k. We can clearly assume that each m_α is regular (every singular number is the sum of fewer, smaller regular numbers). Also

[7] Sophie Piccard, Fund. Math. vol. 29, pp. 5–9. See also Comptes Rendus des Séances de la Société des Sciences et des Léttres de Varsovie vol. 30 (1937).

we can assume that $m_1 > n^{\aleph_r}$ and $m_1 > \text{card } (\Omega_r)$. By the theorem proved in the previous pages, there exists for every S_α a set $S'_\alpha \subset S_\alpha$, such that $S'_\alpha \cap f(S'_\alpha)$ is empty and card $(S'_\alpha) = m_\alpha$. Omit for $\beta > \alpha$ all the elements of $f(S'_\alpha)$ from S'_β. Thus we get the sets S''_α of power m_α, such that

$$f(S''_\alpha) \cap \left(\bigcup_{\beta \geqq \alpha} S''_\beta \right) = 0 \qquad \text{(0 stands for the empty set).} \tag{7}$$

We want to construct sets $S'''_\alpha \subset S''_\alpha$ of power m_α which further satisfy

$$f(S'''_\alpha) \cap \left(\bigcup_{\beta < \alpha} S'''_\beta \right) = 0. \tag{8}$$

But then clearly

$$f\left(\bigcup_\alpha S'''_\alpha \right) \cap \left(\bigcup_\alpha S'''_\alpha \right) = 0. \tag{9}$$

Thus the set $\bigcup_\alpha S'''_\alpha$ is independent and clearly of power m. Thus we only have to construct S'''_α. We shall use transfinite induction. Let as before Ω_l be the initial number belonging to n and let N be any set with card $N \geqq n^{\aleph_r}$. We construct a ramification system belonging to N as follows: Consider the disjoint sets

$$\begin{gathered} N^{(\Omega_r)}_{i_1, \cdots, i_j, \cdots} i_j < \Omega_l, \ j < \Omega_r; \\ N = \bigcup_{i_1, \cdots, i_j, \cdots} N^{(\Omega_r)}_{i_1 \cdots}; \text{ card } (N^{(\Omega_r)}_{i_1 \cdots}) = \text{card } N. \end{gathered} \tag{10}$$

Clearly there are $n^{\aleph_r} \leqq N$ such sets, thus since $N^2 = N$ this is clearly possible. The sets (10) will be the Ω_rth (and last) column of the ramification system. The sets of the kth, $1 \leqq k < \Omega_r$, column we define as follows: $(i_1, i_2, \cdots, i_j, \cdots$ again run through the ordinals less than Ω_l and $j < k)$

$$N^{(k)}_{i_1 \cdots i_j \cdots} = \bigcup_{i_k \cdots} N^{(\Omega_r)}_{i_1 \cdots i_j \cdots i_k \cdots}, \tag{11}$$

this means that $N^{(k)}_{i_1} \cdots$ is the union of all the sets of (10) whose indices agree with it for $j < k$. (The 0th column $N^{(1)}$ is N.) We will denote this ramification system by $R(N)$.

Consider now $R(S''_1)$. Let a be any element of S''_2. Since card $(f(a)) < n$ there must exist an $(S''_1)^{(2)}_i$ (that is, a set of the first column of $R(S''_1)$) such that $f(a) \cap S''_1)^{(2)}_i = 0$. Now since m_2 (card $S''_2 = m_2$) is regular (thus not the sum of n sets of power $< m_2$) there exists a set

$S''_{2'} \subset S''_2$ with card $S''_{2'} = m_2$ and an index $i^{(1)}_{(1)} < \Omega_l$ so that

$$f(S''_{2'}) \cap (S''_{1'})^{(2)}_{i_1^{(1)}} = 0.$$

Consider now $R(S''_{2'})$. Let a be any element of S''_3. As before there exists a set $S''_{3'} \subset S''_3$ with card $S''_{3'} = m_3$ and

$$f(S''_{3'}) \cap (S''_{1'})^{(3)}_{i_1^{(1)}, i_2^{(1)}} = 0, \qquad f(S''_{3'}) \cap (S''_{2'})^{(2)}_{i_1^{(2)}} = 0,$$

where $i_1^{(1)}$, $i_2^{(1)}$, $i_1^{(2)}$ are less than Ω_l. Again we construct $R(S''_{3'})$, and so on. Assume we have already completed this construction for all ordinals $\beta < \alpha < \Omega_r$. This means that there exists for all ordinals $\gamma < \alpha$ sets $S''_{\gamma'}$, with card $S''_{\gamma'} = m_\gamma$ and so that for all $\delta < \gamma$ we have

$$f(S''_{\gamma'}) \cap (S''_{\delta'})^{(k)}_{i_1^{(\delta)}, \cdots} = 0, \qquad (S''_1 = S''_{1'})$$

where $i_1^{(\delta)} \cdots$ are ordinals less than Ω_l and $k = 1 + (\gamma - \delta)$. Now we construct the αth step as follows: Let a be any element of S''_α. Since card $(f(a)) < n$, there exists for every $\beta < \alpha$ an index $i^{(\beta)} < \Omega_l$ such that

$$f(a) \cap (S''_{\beta'})^{(k)}_{i_1^{(\beta)}, \cdots, i_{k-1}^{(\beta)}} = 0, \qquad k = 1 + (\alpha - \beta).$$

The number of possible choices for all the $i^{(\beta)}$, $\beta < \alpha$, does not exceed

$$n^{\aleph_r} < m_\alpha,$$

since the generalized continuum hypothesis was assumed to be true (it is clear from the generalized continuum hypothesis that $a^b \leqq \max (a^+, b^+)$ where a^+ is the cardinal number immediately following a). Thus since m_α is regular there exists a set $S''_{\alpha'}$ of power m_α such that for all $\beta < \alpha$

$$f(S''_{\alpha'}) \cap (S''_{\beta'})^{(k)}_{i_1^{(\beta)}, \cdots, i_{k-1}^{(\beta)}} = 0, \qquad k = 1 + (\alpha - \beta).$$

Now we construct our ramification system $R(S''_{\alpha'})$. We continue this construction for every ordinal $\delta < \Omega_r$. Thus we obtain the sets

$$(S''_{\delta'})^{(\Omega_r)}_{i_1^{(\delta)}, \cdots} = D_\delta, \qquad \delta = 1, 2, \cdots ; \delta < \Omega_r. \tag{12}$$

The sets (12) all occur in the last (that is, Ω_rth) column of their ramification system. By construction they satisfy

$$f(D_{\delta_1}) \cap D_{\delta_2} = 0 \qquad \text{for } \delta_2 < \delta_1 < \Omega_r.$$

Thus we can put

$$D_\delta = S'''_\alpha$$

and this completes the proof of Theorem V.

In the first paper on this subject Lázár[8] proved (without assuming the continuum hypothesis) that Theorem V holds if $f(a)$ is finite and card $S=c$. In fact his proof gives that S is the union of $\aleph_0$ independent sets. One can ask the question what happens in the general case? It is easy to see that if $f(a)$ is finite and has not more than k elements and S is also finite, then S is the union of $2k+1$ independent sets, and $2k+1$ is best possible. By a method of König[9] it is easy to see that this also holds if S is countable. I conjectured that it is true for all sets S. Clearly this would be a consequence of the following result: Let G be a graph. Assume that all finite subgraphs of G are the union of r independent sets. (Two points are independent if they are not connected. A set of vertices is independent if any two of them are independent, and a graph G' is said to be the sum of r independent sets if the vertices of the graph can be split into r independent sets.) Then G is the union of r independent sets. De Bruijn recently proved this conjecture (written communication). In general perhaps the following result holds: Let card $(f(a))<n$. Then S is the sum of n independent sets (n is an infinite cardinal number).

Let S be any set of real numbers. We define S_k to be the set of all numbers

$$\sum_{r=1}^{k} c_r a_r, \qquad c_r \text{ rational}, \quad a_r \in S.$$

Let H be a Hamel basis. It has been remarked[10] that the sets H_k cannot all be measurable. Indeed since $\bigcup_k H_k$ is the set of all real numbers, they cannot all have measure 0. Suppose that H_k has nonzero measure. If the inner measure of H_k would be positive, then by a well known theorem of Steinhaus[11] there would exist a δ such that if $|x|<\delta$, $x=a-b$, $a\in H_k$, $b\in H_k$. But then H_{2k} contains the set of all real numbers, which is clearly impossible.

Sierpinski[12] proved that there exist Hamel bases which are nonmeasurable and also Hamel bases of measure 0. We shall prove that for every k there exists a Hamel basis such that H_k has measure 0 but H_{k+1} is nonmeasurable.

Let $0\leqq A_1<A_2<\cdots$ be an infinite sequence of integers, such that every integer is the sum of $k+1$ A's, and the number of A's not ex-

[8] Compositio Math. vol. 3 (1936) p. 304.

[9] *Theorie der endlichen und unendlichen Graphen*, pp. 81–85.

[10] This remark is probably due to Sierpinski, but I do not remember for sure.

[11] Fund. Math. vol. 1, pp. 93–104.

[12] Ibid. vol. 1, pp. 105–111.

ceeding n is less than $c_1 n^{1/k+1}$. We shall prove the existence of such sequences later. Denote by B the set of real numbers in $(0, 1)$, which admit the representation:

$$\sum_{j=2}^{\infty} \frac{A_i}{j!}, \qquad \text{with } A_i < j \text{ an arbitrary term of } \{A_n\}.$$

First we prove that B_k has measure 0. It clearly suffices to prove that $\sum_{r=1}^{k} c_r b_r$ where the c's are fixed integers and $b_r \in B$ has measure 0. Let $x \in B_k$ be arbitrary. We have

$$x = \sum_{r=1}^{k} \sum_{j=2}^{\infty} c_r \frac{A_{i_j}(r)}{j!} = \sum_{j=2}^{\infty} \frac{u_j}{j!}, \qquad 0 \leqq A_{i_j}(r) < j,$$

where $|u_j| < c_2 \cdot j$ and we have, for u_j less than $c', j^{k/k+1}$ choices. Consider all the numbers

$$\sum_{k=2}^{n} \frac{u_k}{k!}.$$

The number of these numbers is less than $c'^n (n!)^{k/k+1}$. Consider all the intervals whose centers are all these points and whose length equals $4c_2/n!$. It follows from $|u_j| < c_2 j$ that all the $\sum_{k=2}^{\infty} u_k/k!$ are in the interior of these intervals, that is, the whole set $\sum_{r=1}^{k} c_k b_r$, $b_r \in B$, is covered by them. The sum of the length of these intervals is $< 4c(c'^n / n!^{1/k+1}) = o(1)$, which proves that B_k has measure 0.

Now we construct a Hamel basis $H \subset B$, with H_{k+1} nonmeasurable. First we construct a set $L \subset B$ such that L is rationally independent (that is, any finite subset of L is rationally independent) and L_{k+1} is nonmeasurable. Let $M = A_1 + A_2 + \cdots + A_{k+1}$. It is well known (and easy to see) that the real numbers z, $0 \leqq z \leqq 1$, in whose representation $z = \sum_{j=2}^{\infty} u_j/j!$, $0 \leqq u_j < j$, we have infinitely often $u_j = M$, have measure 1. Denote this set of real numbers by I_M. Let $\{F_\alpha\}$, $\alpha < \Omega_c$, be the collection of all the perfect subsets of I_M (Ω_c is the initial number of c). Suppose we have already constructed a set $L^{(\beta)}$ of power less than c, which is rationally independent and such that $L_{k+1}^{(\beta)}$ intersects all the F_α with $\alpha < \beta$. Let $z \notin F_\beta$, $z \notin \bigcup_j L_j^{(\beta)}$. Such a z exists since the power of $\bigcup_j L_j^{(\beta)}$ is less than c. Consider the equation

$$z = x_1 + x_2 + \cdots + x_{k+1}, \quad x_i \in B, \quad z = \sum_{j=2}^{\infty} \frac{u_j}{j!},$$

$$x_i = \sum_{j=2}^{\infty} \frac{A_j^{(i)}}{j!}, \qquad 0 \leqq u_j, A_j^{(i)} < j.$$

This equation is solvable. Also clearly we have c choices for x_1, c choices for x_2 after we have chosen x_1, and so on. Finally we have c choices for x_k after we have chosen $x_1, x_2, \cdots, x_{k-1}$. The proof of these statements is immediate, since $u_j = \sum_{i=1}^{k+1} A_j^{(i)}$ is solvable and since, in the representation of z, $M = A_1 + \cdots + A_{k+1}$ occurs infinitely often, say $u_{j_1} = u_{j_2} = \cdots = M$. We can clearly interchange the j_1th, j_2th, $\cdots$ digits of the x's (those digits are $A_1, A_2, \cdots, A_{k+1}$) and thus obtain the required c solutions. Thus we can clearly choose x_i, $i \leqq k$, so that the set consisting of $L^{(\beta)}$, the x_i, $i \leqq k$, and z should be rationally independent. But then the set consisting of $L^{(\beta)}$ and the x_i, $i \leqq k+1$, is also rationally independent. This set we denote by $L^{(\beta+1)}$. Clearly $L_{k+1}^{(\beta+1)}$ intersects F_β, and the power of $L^{(\beta+1)}$ is less than c. Put now $L = \bigcup_{\beta < \Omega_c} L^{(\beta)}$. Clearly L_{k+1} intersects all perfect subsets of I_M, thus can not have measure 0 (I_M has measure 1), but since L is rationally independent, L_{k+1} can not have positive inner measure (as was shown before). Thus L_{k+1} is nonmeasurable. Now since B_{k+1} clearly consists of all real numbers, we can find a Hamel basis $H \subset B$ which contains L. Clearly H_{k+1} is also nonmeasurable and $H_k \subset B_k$ has measure 0, which completes the proof.

We now have to construct our sequence A_i with the required properties: Denote by T_r, $0 \leqq r < k+1$, the sequence of integers of the form $\sum_{j=0}^{n} \epsilon_j 2^j$, $n = 1, 2, \cdots$, $\epsilon_j = 0$ or 1, and all the ϵ_j are 0 except possibly for those with $j \equiv r \pmod{(k+1)}$. Consider now the sequence $\bigcup_r T_r$, this sequence clearly has the required properties.[13]

Let S be a set of power greater than $\aleph_0$ but smaller then the first strongly inaccessible cardinal number ($> \aleph_0$). It is well known that no countably additive two-valued measure can exist for the subsets of S, so that elements have measure 0 and the whole set S has measure 1. Ulam now raised the question (oral communication): What is the smallest cardinal number n so that there should exist n two-valued measures defined for the subsets of S (elements of S having measure 0 and S having measure 1, in each of them) with the property that each subset of S is measurable in at least one of these measures? Ulam proved that $n \geqq \aleph_0$. Alaoglu and I proved $n \geqq \aleph_1$. I now present our proof.

Suppose the result is false. Then there exist countably many measures $M_1, M_2, \cdots$ so that each subset of S is measurable for at least one of these measures. Split the set S into the union of $\aleph_1$ sets each nonmeasurable in M_1.[14] Clearly only countably many can have positive measure in any M_k, thus there must exist two of them, S_1 and

[13] This example is due to Stöhr, Math. Zeit. vol. 42, pp. 739–743.

[14] S. M. Ulam, Fund. Math. vol. 16 (1930) p. 142.

S_1' say, which are both nonmeasurable in M_1 and whose union does not have positive measure in any M_k. Split now $S-S_1-S_1'$ into the union of $\aleph_1$ disjoint sets each nonmeasurable in M_2. Denote these sets by $U_1, U_2, \cdots, U_\xi, \cdots$. It is easy to see that among the sets $S_1+S_1'+U_\xi$ there are only countably many of positive measure in any M_k. Thus there exist two of them, S_2 and S_2' say, such that $S_1+S_1'+S_2+S_2'$ does not have positive measure for any M_k. Consider now the set $S-S_1-S_1'-S_2-S_2'$, and repeat the same operation. We can clearly repeat this operation for any k, and the set $\bigcup_i S_i$ will be nonmeasurable for any M_k, since it contains S_k but is disjoint to S_k'. We cannot decide the question whether $n>\aleph_1$. It seems probable that n is greater than the power of S.

Some simple remarks about ordinal numbers: (1) A sequence of ordinals (not necessarily countable) $\beta_i<\Omega_k$ is said to be rarified if $\lim \beta_{i+1}-\beta_i=\Omega_k$, also every bounded sequence is said to be rarified (that is, a sequence for which $\lim \beta_i=\Omega_k$). Sierpinski[15] remarked that the ordinals $\alpha<\Omega_1$ are the sum of $\aleph_0$ but not of a finite number of rarified sequences. Assume that Ω_k has an immediate predecessor. Then the ordinals $\alpha<\Omega_k$ are the sum of Ω_{k-1} but not fewer rarified sequences. If Ω_k does not have an immediate predecessor and Ω_l is the smallest ordinal cofinal with it, then the ordinals $\alpha<\Omega_k$ are the sum of Ω_l but not fewer rarified sequences. If Ω_k is weakly inaccessible, that is, $\Omega_k=\Omega_l$, then the ordinals $\alpha<\Omega_k$ are not the sum of fewer than Ω_k rarified sequences, or the weakly inaccessible numbers are the only ones which are not the sum of fewer rarified sequences.

Similarly we can define a sequence $\beta_i<\Omega_k$ to be r-rarified if $\lim \beta_{i+1}-\beta_i=\Omega_r$. Then the ordinals $\alpha<\Omega_k$ are the sum of $\min(\Omega_r, \Omega_l)$ but not fewer r-rarified sequences.

(2) Dushnik[16] proved the following theorem: Let m be a regular number, Ω_k the initial number belonging to it. Let $f(\alpha)$, $\alpha<\Omega_k$, be such that for all α, $f(\alpha)<\alpha$. Then there exists an ordinal β such that the equation $f(\alpha)=\beta$ has m solutions. For singular numbers the theorem is false. The following generalization holds: Assume that Ω_k is not cofinal to ω. Then there exists an ordinal β and a sequence α_i cofinal with Ω_k such that $f(\alpha_i)\leqq\beta$. For regular numbers one immediately obtains from this Dushnik's theorem. If Ω_k is cofinal to ω, the analogous result clearly does not hold. Dushnik's proof would easily give a proof of this theorem (oral communication) but perhaps the following proof is of some interest: Suppose the theorem is false. Then to every β there exists a $\phi(\beta)<\Omega_k$ such that for $\delta\geqq\phi(\beta)$, $f(\delta)>\beta$.

[15] Revista de Sciencias (Lima) vol. 41 (1939) pp. 289–296.

[16] Bull. Amer. Math. Soc. vol. 37 (1931) pp. 860–862.

Consider now

$$\gamma = \phi(1) + \phi(\phi(1)) + \cdots .$$

Clearly $\gamma < \Omega_k$ since Ω_k is not cofinal with ω. But then from the definition of γ, $f(\gamma) \geqq \gamma$, an evident contradiction; this completes the proof.

UNIVERSITY OF MICHIGAN

ON A PROBLEM OF G. BIRKHOFF

TADASI NAKAYAMA AND JUNJI HASHIMOTO

In his book *Lattice theory*, G. Birkhoff proposed to prove that the representation of a finite partially ordered system as the product of indecomposable factors is unique within pairwise isomorphism of factors.[1] The present short note is to show that this is not the case in general. A simple counterexample, and indeed one of the simplest, perhaps, can be constructed as follows:

Let X be the lattice $\{0, 1\}$ of two elements 0, 1 $(0<1)$, for instance, and A be the partially ordered system

$$I + X + X^2 + X^3 + X^4 + X^5,$$

where I resp. X^i stands for the one-lattice resp. the direct product of i copies of X, and where $+$ means direct summation. The finite partially ordered system A may be expressed also by $f(X)$ with the polynomial $f(x) = 1+x+x^2+x^3+x^4+x^5$. Since every X^i has the up to isomorphism unique decomposition into indecomposable factors, $X^i = XX \cdots X$ (i factors), one sees easily that direct decompositions of A are, in the sense of isomorphism, in 1-1 correspondence with factorizations of polynomial $f(x) = 1+x+x^2+x^3+x^4+x^5$ into factors with non-negative rational integral coefficients. But our $f(x)$ has two distinct decompositions into factors which are irreducible in the prescribed sense, namely

$$f(x) = (1 + x)(1 + x^2 + x^4) = (1 + x^3)(1 + x + x^2).$$

Two direct decompositions

$$A = (I + X)(I + X^2 + X^4) = (I + X^3)(I + X + X^2)$$

Received by the editors October 28, 1948.

[1] G. Birkhoff, *Lattice theory*, Amer. Math. Soc. Colloquium Publications, vol. 25, New York, 1940, Problem 8.