COLLOQUIUM MATHEMATICUM

VOL. XXXVI 1976 FASC. 1

THREE PROBLEMS OF S. M. ULAM WITH SOLUTIONS AND GENERALIZATIONS

BY

G. S. STOLLER (BROOKLYN, NEW YORK)

In [3], S. M. Ulam proposes many problems. Here I shall solve three of these problems and propose some generalizations. The first is a problem on what Ulam calls Peano mappings, the second is a problem on sets and cardinality, and the third is a question on product-automorphisms (which will be defined later on).

On p. 32 of his book [3], S. M. Ulam states the following problem:

4. A problem on Peano mappings

Let R be the set of positive rational integers with the usual operations $a+b = s(a, b)$ and $a\cdot b = m(a, b)$. Every one-to-one (Peano) mapping $c = p(a, b)$ on $R\times R$ to all of R may serve to associate with $s(a, b)$ and $m(a, b)$ two functions σ and μ on R to R by the definitions $\sigma(c) = \sigma(p(a, b)) = s(a, b)$, and $\mu(c) = \mu(p(a, b)) = m(a, b)$. Does there exist a Peano mapping $p(a, b)$ such that "addition commutes with multiplication" in the sense that $\sigma(\mu(c)) = \mu(\sigma(c))$ for all c of R? To illustrate, we note that the well-known Peano mapping $c = p(a, b) = 2^{a-1}(2b-1)$ fails. For, $\sigma(\mu(14)) = \sigma(\mu(2^{2-1}\cdot[2\cdot 4-1])) = \sigma(8) = \sigma(2^{4-1}\cdot[2\cdot 1-1]) = 5$, while $\mu(\sigma(14)) = \mu(\sigma(2^{2-1}\cdot[2\cdot 4-1])) = \mu(6) = \mu(2^{2-1}\cdot[2\cdot 2-1]) = 4$.

This problem is solved in [1] by violating the finiteness of the number of factorizations of a positive integer into two positive integers. The equality $\mu(n) = \mu(2n-3)$ is obtained and is applied to the sequence given by $a_1 = 4$ and $a_{k+1} = 2a_k - 3$. (Any value may be chosen for a_1 as long as it is greater than 3.)

We shall present a proof here which is essentially the same as the proof given in [2] and depends on violating the one-to-oneness of the function p. This method of proof may also be more applicable to generalizations of this problem.

It is easily shown that a function p having the properties stated in the problem cannot exist.

Suppose that such a function p exists. We evaluate $p^{-1}(4)$, $p^{-1}(5)$, and $p^{-1}(6)$; a contradiction can then be obtained by investigating $\sigma\{\mu[p(2, 3)]\}$ and $\mu\{\sigma[p(2, 3)]\}$.

We get $p^{-1}(4) = (2, 2)$, $p^{-1}(5) \epsilon \{(1, 4), (4, 1)\}$, $p^{-1}(6) \epsilon \{(1, 5), (5, 1)\}$.

The function p is surjective (onto), so there exist a and b in R such that $p(a, b) = 4$. Hence

$$\begin{aligned} a+b &= \sigma[p(a, b)] = \sigma(4) = \sigma(2\cdot 2) \\ &= \sigma\{\mu[p(2, 2)]\} = \mu\{\sigma[p(2, 2)]\} \\ &= \mu(2+2) = \mu(4) = \mu[p(a, b)] \\ &= ab \end{aligned}$$

and the only solution in positive integers of $a+b = ab$ is $(a, b) = (2, 2)$. So $p(2, 2) = 4$ and $\sigma(4) = 4 = \mu(4)$.

Now we evaluate $p^{-1}(5)$ and $p^{-1}(6)$. First of all, $\sigma\{\mu[p(1, 4)]\} = \sigma(1\cdot 4) = \sigma(4) = 4$, and $\mu\{\sigma[p(1, 4)]\} = \mu(1+4) = \mu(5)$, so we get $\mu(5) = 4$.

Say $(a', b') = p^{-1}(5)$, then $4 = \mu(5) = \mu[p(a', b')] = a'b'$, which has $\{(1, 4), (2, 2), (4, 1)\}$ as the set of all positive integer solutions. But $p(2, 2) = 4$, so we are left with $(a', b') \epsilon \{(1, 4), (4, 1)\}$. Thus $5 = \sigma[p(a', b')] = \sigma(5)$.

Secondly, we have $\sigma\{\mu[p(1, 5)]\} = \sigma(1\cdot 5) = \sigma(5) = 5$ and $\mu\{\sigma[p(1, 5)]\} = \mu(1+5) = \mu(6)$, so we get $\mu(6) = 5$. As with $p^{-1}(5)$, we see that $p^{-1}(6) \epsilon \{(1, 5), (5, 1)\}$, whence $\sigma(6) = 6$.

Finally, we get the desired contradiction by comparing $\sigma\{\mu[p(2, 3)]\}$ with $\mu\{\sigma[p(2, 3)]\}$. Indeed, $\sigma\{\mu[p(2, 3)]\} = \sigma(2\cdot 3) = \sigma(6) = 6$, but $\mu\{\sigma[p(2, 3)]\} = \mu(2+3) = \mu(5) = 4 \neq 6$.

Therefore, a function p as described in the problem cannot exist.

Note. The solution given to the problem does not require that p be surjective, only that certain integers be in the image of p and certain ordered pairs be in the domain of p. This suggests the following generalization of the problem (using the notation of the problem):

Let S be a subset of R and let q be an injection (one-one map) of S into $R \times R$. Define functions σ and μ that map S into R by $\sigma(c) = s[q(c)]$ and $\mu(c) = m[q(c)]$. Do there exist such a set S and such a function q satisfying:

(i) $S \supseteq \sigma(S)$ and $S \supseteq \mu(S)$,

(ii) $\mu[\sigma(c)] = \sigma[\mu(c)]$ for all c in S,

(iii) S is infinite?

The solution presented earlier says that there is no such set S and function q satisfying (i) and (ii) if we have $4 \epsilon S$, $\{(1, 4), (4, 1)\} \cap q(S) \neq \emptyset$, $\{(1, 5), (5, 1)\} \cap q(S) \neq \emptyset$, $\{(2, 3), (3, 2)\} \cap q(S) \neq \emptyset$.

Observe that the generalization above is a generalization of the function p (although we use $q = p^{-1}$). Generalizations of the set R to the positive rationals, positive reals, or other fully ordered domains, can be stated.

On page 15 of [3] the following problem appears:

> Let A and B be infinite sets which admit a transfinite sequence of point transformations $t_\xi(a) \in B$, $a \in A$, with the properties: (1) $t_\xi(X) \cdot t_\xi(Y) = 0$ for $X \subset A$, $Y \subset A$, and some ξ implies $t_\eta(X) \cdot t_\eta(Y) = 0$ for all $\eta > \xi$; (2) for every infinite subset $X \subset A$ there exists a ξ such that $t_\xi(X)$ contains at least two distinct points; (3) $X \cdot Y = 0$ for finite X, Y implies existence of η such that $t_\eta(X) \cdot t_\eta(Y) = 0$.
>
> Is the power of A necessarily less than or equal to that of B?

We shall soon see that:

(I) Condition (2) is redundant.

(II) An upper bound on the power of A dependent upon the powers of other sets mentioned in the problem will be given.

(III) The power of A can be greater than the power of B.

(I) Condition (2) follows from condition (3).

Let X be an infinite subset of A and pick any two distinct elements of X, say x_1 and x_2. Clearly, both $\{x_1\}$ and $\{x_2\}$ are finite, and satisfy $\{x_1\} \cap \{x_2\} = \emptyset$. By (3) there exists an η such that $t_\eta(\{x_1\}) \cap t_\eta(\{x_2\}) = \emptyset$. This is just $\{t_\eta(x_1)\} \cap \{t_\eta(x_2)\} = \emptyset$ which is equivalent to $t_\eta(x_1) \neq t_\eta(x_2)$, hence $t_\eta(X)$ contains at least two distinct elements. Note that we only needed $|X| > 1$.

(II) Let I be the index set for the sequence of point transformations. Condition (3) implies $|A| \leqslant |B|^{|I|}$.

Define the function T: $A \to B^I$ by $T(a) = \langle t_\eta(a) \colon \eta \in I \rangle$ for all a in A. Clearly, T is a monomorphism of A into B^I by condition (3) (see solution of (I)). Therefore

$$|A| \leqslant |B^I| = |B|^{|I|}.$$

(III) The power of A can be greater than the power of B. In the example that I will present, A and B will be familiar sets; A will be the continuum and B will be the subset of the rationals that consists of elements of the form $k/2^n$, where k is an integer and n is a natural number.

Let $\mathcal{N}$ be the natural numbers with the usual ordering. We shall use $\mathcal{N}$ as the index set for the point transformations and to construct B. Let Z be the set of integers and let [ ] be the familiar "greatest integer" function. Finally, let A be the real numbers, $B_n = \{k/2^n \colon k \in Z\}$ for all $n \in \mathcal{N}$, and $B = \bigcup \{B_n \colon n \in \mathcal{N}\} = \{k/2^n \colon k \in Z \;\&\; n \in \mathcal{N}\}$. Define the sequence $\{t_n \colon n \in N\}$ of maps of A into B by $t_n(a) = [2^n a]/2^n$.

A few simple observations and a very elementary lemma will aid us in verifying that conditions (1) and (3) hold. For all $n \in \mathcal{N}$, the image of t_n is B_n. For all m and n in $\mathcal{N}$, if $m < n$, then $B_n \supset B_m$. Each t_n is a monotonically increasing function and satisfies $t_n[t_n(z)] = t_n(z)$ (i.e. t_n is a projection). B is dense in A.

LEMMA. *Let* X *and* Y *be subsets of* A *and let* $n \in \mathcal{N}$.

$t_n(X) \cap t_n(Y) = \emptyset$ *if and only if one of the following conditions holds*:

(i) $X = \emptyset$,

(ii) $Y = \emptyset$,

(iii) *each pair of elements, one from* X *the other from* Y, *is separated by an element of* B_n. (*I.e., if* x *in* X *and* y *in* Y *satisfy* $x < y$ ($y < x$), *then there is a* b *in* B_n *such that* $x < b \leqslant y$ ($y < b \leqslant x$).)

Proof. Necessity. Each of conditions (i) and (ii) clearly implies that $t_n(X) \cap t_n(Y) = \emptyset$.

Say (iii) holds and suppose that $t_n(X) \cap t_n(Y)$ is non-null. Then there exist $x \in X$ and $y \in Y$ such that $t_n(x) = t_n(y)$. Without loss of generality we may assume that $x < y$. By hypothesis, there exists b in B_n that lies between x and y (i.e. $x < b \leqslant y$); then by the definition of t_n and its monotonicity we have $t_n(x) < t_n(b) \leqslant t_n(y)$, which contradicts our supposition that $t_n(x) = t_n(y)$. Consequently, our supposition was false, and so $t_n(X) \cap t_n(Y) = \emptyset$.

Sufficiency. Say (i) and (ii) do not hold. We must show that (iii) holds.

Both X and Y are non-empty; pick any x in X and y in Y. Without loss of generality we may assume that $x < y$ since the case $y < x$ is handled identically.

The function t_n is monotonic, whence $t_n(x) \leqslant t_n(y)$. This must be a strict inequality since $t_n(X) \cap t_n(Y) = \emptyset$ (by hypothesis). From the definition of t_n we see that $t_n(z) \leqslant z$ and $t_n[t_n(z)] = t_n(z)$. So $t_n(x) < t_n(y) \leqslant y$ and $t_n(x) < x$.

Compare x with $t_n(y)$. The inequality $t_n(y) \leqslant x$ is impossible since this would imply $t_n(y) = t_n[t_n(y)] \leqslant t_n(x)$ contradicting $t_n(x) < t_n(y)$. Thus $x < t_n(y)$, whence $t_n(y)$ can be chosen as the element of B_n separating the pair of elements x and y, q.e.d.

Condition (1) of Ulam's problem can now be demonstrated. We have $t_m(X) \cap t_m(Y) = \emptyset$. Pick any n in the index set ($\mathcal{N}$) satisfying $m < n$. By the lemma, one of the following holds: $X = \emptyset$, or $Y = \emptyset$, or the elements of X are pairwise separated from the elements of Y by elements of B_m. This last statement can have B_m replaced by B_n since $B_n \supset B_m$, whence the "if" portion of the lemma yields $t_n(X) \cap t_n(Y) = \emptyset$.

Condition (3) is easily established. If $X = \emptyset$ or $Y = \emptyset$, then the stated result clearly holds. So assume that X and Y are finite non-null sets. Note that B is dense in A and $X \cap Y = \emptyset$, so for any x in X and y in Y there exists an element of B that separates them. Select one such element for this pair and call it $b(x, y)$. Both X and Y are finite, so $\{b(x, y) \colon x \in X \;\&\; y \in Y\}$ is finite. Hence there exists n in $\mathcal{N}$ such that

$$B_n \supset \{b(x, y) \colon x \in X \;\&\; y \in Y\}.$$

Therefore $t_n(X) \cap t_n(Y) = \emptyset$ by the lemma.

Finally, page 5 of [3] has the following development arriving at the problem "Does there exist, for every n, a set having exactly n product-automorphisms?"

3. *Product-isomorphisms and some generalizations*

The direct product $A \times B$ of two sets A and B is the set of all ordered pairs (a, b) with a in A and b in B. Analogously the product ΠA_i is the set of all sequences $\{a_1, a_2, \ldots\}$ with a_i in A_i. In case all $A_i = A$ and $i = 1, \ldots, n$, we shall write $\Pi A_i = A^n$.

Two subsets A and B of a product E^2 are said to be product-isomorphic in case there exists a one-one transformation $f(x)$ on E to all of E such that the resulting transformation

$$(x, y) \rightarrow (f(x), f(y))$$

of E^2 to itself takes A into all of B. The relation of product-isomorphism is reflexive, symmetric, and transitive, and thus constitutes an equivalence relation on subsets of E^2 which divides the class of all such subsets into mutually disjoint subclasses of sets, product-isomorphic among themselves.

The first questions that arise in connection with this relation concern enumeration properties. It is obvious that sets of different cardinal numbers cannot be product-isomorphic. (...)

A product-isomorphism of a subset A with itself is called a product-automorphism. The number of product-automorphisms of a subset A of E^2, different on A, is in general 2^c when E has power c; this is true, for example, when $A = E^2$. One easily constructs examples of sets A which have only a finite number of product-automorphisms, in particular, some which admit only the identity as such an automorphism. Does there exist, for every n, a set having exactly n product-automorphisms?

We swiftly see that, for every $n > 0$, there exist sets E and A such that A has exactly n product-automorphisms. Let E be the group of integers modulo n and put

$$A = \{(k, k+1) \colon k \in E\}.$$

It is easy to check that $f(k)$ determines the values of $f(k+1)$ and $f(k-1)$ as $f(k)+1$ and $f(k)-1$, respectively. By mathematical induction, the value of $f(0)$ determines the function f everywhere. Also, $f(0)$ can be any element of E and $|E| = n$. Thus A has exactly n product-automorphisms.

In general, it is trivial to show that the product-automorphisms form a group under the operation of function composition. For the particular example given above, the product-automorphisms formed a cyclic group of order n.

Another question that can be asked is:

Can every group be realized as the group of product-automorphisms of a set A that is a subset of E^2?

Letting E be the group of integers and taking A as above, we see that the infinite cyclic group can be realized as the group of product-automorphisms of a set.

REFERENCES

[1] И. Бровкин и Я. Габович, *Об отображениях Пеано*, Colloquium Mathematicum 15 (1966), p. 199.
[2] В. В. Ермаков, *Об одной задаче Улама*, Математические заметки 12 (1972), p. 155-156; English translation in Mathematical Notes 12 (1972), p. 528-529.
[3] S. M. Ulam, *A collection of mathematical problems*, Interscience Publishers Inc., New York 1960.

Reçu par la Rédaction le 1. 3. 1974;
en version modifiée le 25. 7. 1975