On a question of Kertész

By HANNA NEUMANN (Manchester)

During a recent visit to Debrecen I learnt from A. KERTÉSZ of a way of constructing semigroups from groups. If G is a given group, written multiplicatively, define a new operation $x \circ y$ on the elements of G, setting $x \circ y = f(x, y)$, where $f(x, y)$ is one of the following five types of function: a constant a, x, y, xay, or yax. In each case the new operation is associative; moreover the elements of G form a group G_1 under the operation $x \circ y = xay$, a group G_2 under the operation $x \circ y = yax$. G_1 is an isomorphic image of G under the mapping $x \to xa^{-1}$, similarly G_2 is an anti-isomorphic image of G under the same mapping. A. KERTÉSZ conjectured that the five functions he found are in fact the only functions defining associative operations. In this note I give a proof of KERTÉSZ' conjecture.

§ 1. Preliminaries

The function $f(x, y)$ defined on the group G is a word in the variables x and y and constant elements of G; that is, it is a product of powers x^{α_i}, y^{β_i}, possibly separated from each other by various constants $a, b, \dots$. We assume the word to be *reduced*, that is, no two adjacent letters represent elements inverse to each other in G. Words in three variables will be used as well. Our remarks naturally extend to these *mutatis mutandis*.

The number $m = \Sigma|\alpha_i|$ is called the *x-length* of $f(x, y)$, and the number $n = \Sigma|\beta_i|$ is called the *y-length* of $f(x, y)$.

We consider the x-length and y-length of a power of f. If k is a positive integer, cancellations will in general take place between neighbouring factors of the power f^k. To exhibit these, we write $f(x, y)$ in the form

$$f(x, y) = r^{-1}(x, y)s(x, y)r(x, y),$$

where we may assume that the first and last letters of s are not inverse to each other, and that no cancellation takes place between r^{-1} and s, and between s and r. Then

$$f^k(x, y) = r^{-1}(x, y)s^k(x, y)r(x, y)$$

is reduced as written. If, therefore, m_1 and n_1 denote respectively the x-length and the y-length of $s(x, y)$, one has for the x-length μ and the y-length ν of $f^k(x, y)$ the relations

(1.1) $$\mu = m + (k-1)m_1 \quad \text{and} \quad \nu = n + (k-1)n_1.$$

We extend this result to a more general situation: Let $w(u, v)$ be a word in the variables u, v and constants; again $w(u, v)$ is assumed reduced. If the u-length of $w(u, v)$ is k, then

(1.2) *the x-length μ and the y-length ν of $w(f(x, y), v)$ are subject to the inegualities*

$$m + (k-1)m_1 \leqq \mu \leqq km \quad \textit{and} \quad n + (k-1)n_1 \leqq \nu \leqq kn.$$

Similar inequalities obtain, of course, when $f(x, y)$ is substituted for v in $w(u, v)$.

The truth of these inequalities becomes evident, if one considers first the extreme cases leading to the least and greatest possible values for μ or ν. The least value is taken (as a direct application (1.1)) when u occurs only once in $w(u, v)$, and then in the form $u^{\pm k}$. The greatest value is taken when $w(u, v)$ contains the power $u^{\pm 1}$ in k separate places.

Finally we note the following simple fact:

(1.3) *If $x \circ y = f(x, y)$ is an associative operation, then so is $x * y = f(y, x)$.*

For associativity of $x \circ y$ means

$$f(f(x, y), z) = f(x, f(y, z)) \quad \text{for all} \quad x, y, z;$$

therefore in particular also

$$f(f(z, y), x) = f(z, f(y, x)) \quad \text{for all} \quad x, y, z,$$

and this is just the relation expressing associativity of $x * y$.

§ 2. The Theorem

We can now formulate the theorem on associative operations on groups:

(2.1) Theorem. *Let $f(x, y)$ be a reduced word in x, y and certain constants out of the group G. If the operation $x \circ y = f(x, y)$ is associative, then*

$$f(x, y) = a,\ x,\ y,\ xay, \quad \textit{or} \quad yax,$$

where a is an arbitrary constant.

PROOF. We write as before $f(x, y) = r^{-1}(x, y)s(x, y)r(x, y)$, where m and m_1 are the x-lengths of f and s respectively, therefore $m_1 \leqq m$; and n and n are the y-lengths of f and s respectively, therefore $n_1 \leqq n$.

Consider now the expression $f(f(x,y),z)$. Let its x-length be μ, and its z-length be ν_1; then (1.2) — with $k=m$ — shows that $\mu_1 \geqq m+(m-1)m_1$. Also, clearly, $\nu_1=n$.

Next consider the x-length μ_2 and the z-length ν_2 of $f(x,f(y,z))$. Obviously $\mu_2=m$; and, using the analogon to (1.2) for substitution for the second variable, one sees that $\nu_2 \geqq n+(n-1)n_1$.

But the assumption that the operation $x \circ y = f(x,y)$ is associative gives us the identity $f(f(x,y),z)=f(x,f(y,z))$. Therefore $\mu_1=\mu_2$ and $\nu_1=\nu_2$, and so

$$m \geqq m+(m-1)m_1 \quad \text{and} \quad n \geqq n+(n-1)n_1.$$

Using $0 \leqq m_1 \leqq m$ and $0 \leqq n_1 \leqq n$, we obtain

(2.2) *either* $m_1=0$ *or* $m_1=m=1$, *and either* $n_1=0$ *or* $n_1=n=1$.

It follows:

(2.3) *The function $f(x,y)$ has one of the following forms:*

$r^{-1}(x,y)\,a r(x,y)$ *where* $a \neq 1$, $r^{-1}(y) a x^{\varepsilon} b r(y)$, $r^{-1}(x) a y^{\varepsilon} b r(x)$, $a x^{\varepsilon_1} b y^{\varepsilon_2} c$, *or* $a y^{\varepsilon_2} b x^{\varepsilon_1} c$, *where* $\varepsilon, \varepsilon_1, \varepsilon_2$ *have the values* $+1$ *or* -1.

Because of (1.3), we need now only consider the first, second, and fourth of these possibilities.

(i) When $f=r^{-1}(x,y) a r(x,y)$, then

$$f(f(x,y),z)=r^{-1}(f(x,y),z)\,a r(f(x,y),z),$$

and

$$f(x,f(y,z))=r^{-1}(x,f(y,z))\,a r(x,f(y,z)).$$

With the same notation as before, $\nu_1=n$ and $\mu_2=m$ are again obvious. Applying (1.2) — with $m_1=0$ — to $r(f(x,y),z)$ we see that $r(f(x,y),z)$ has x-length at least m. Since the constant $a \neq 1$ prevents cancellation between r^{-1} and r, it follows that $f(f(x,y),z)$ has x-length at least $2m$; that is, in the previous notation, $\mu_1 \geqq 2m$. Similarly one obtains $\nu_2 \geqq 2n$. But again $\mu_1=\mu_2$ and $\nu_1=\nu_2$, because of the associativity. Therefore $m \geqq 2m$ and $n \geqq 2n$, and so $m=n=0$. It follows that $r(x,y)$, and therefore $f(x,y)$, is constant.

(ii) When $f=r^{-1}(y) a x^{\varepsilon} b r(y)$, then

$$f(f(x,y),z)=r^{-1}(z) a [r^{-1}(y) a x^{\varepsilon} b r(y)]^{\varepsilon} b r(z),$$

and

$$f(x,f(y,z))=r^{-1}(f(y,z)) a x^{\varepsilon} b r(f(y,z)).$$

As $\varepsilon=\pm 1$, $f(f(x,y),z)$ contains x^{ε^2} and no other power of x, while $f(x,f(y,z))$ contains precisely x^{ε}, the identity of the two expressions implies therefore $\varepsilon^2=\varepsilon$, $\varepsilon=1$.

Further one has again $\nu_1 = n$; and (1. 2) shows that $r(f(y,z))$ has z-length at least n, so that $\nu_2 \geqq 2n$; therefore $n \geqq 2n$ holds again. Thus $n = 0$, which means that $r(y)$ is constant, and so $f(x,y)$ has the form $f(x,y) = a_1 x b_1$. Using the associativity once again, one deduces without difficulty that $a_1 = b_1 = 1$.

The remark (1. 3) now shows that this case of (2. 3) leads to $f(x,y) = x$ and $f(x,y) = y$ as the only possibilities.

(iii) When, finally, $f = a x^{\varepsilon_1} b y^{\varepsilon_2} c$, then

$$f(f(x,y),z) = a[a x^{\varepsilon_1} b y^{\varepsilon_2} c]^{\varepsilon_1} b z^{\varepsilon_2} c,$$

and

$$f(x, f(y,z)) = a x^{\varepsilon_1} b [a y^{\varepsilon_1} b z^{\varepsilon_2} c]^{\varepsilon_2} c.$$

Comparing the exponents of x and z in these two expressions, one gets again $\varepsilon_1 = \varepsilon_2 = 1$; and the identity of the expressions then leads to $a^2 = a$, $c^2 = c$, and therefore $a = c = 1$. Using (1. 3) once more one obtains from this case the possibilities $f(x,y) = xby$ and $f(x,y) = ybx$, and no others.

This completes the proof of the theorem.

(Received November 2, 1959.)