

Various modifications of Theorem III may easily be secured. For example, in case we make the additional assumptions that the function $f(x, y)$ is bounded and is measurable in y for each x , then the set \mathfrak{E} may be replaced by the interval (a, b) . These additional assumptions are fulfilled in particular if f is bounded and Borel measurable on the square where it is defined. In this case the function $g(x, x)$ is Borel measurable on (a, b) . As another modification we may substitute for the square $a \leq x \leq b, a \leq y \leq b$, a bounded measurable set $\mathfrak{E}_0 \mathfrak{E}_0$, consisting of those points of the plane having x and y each in a linear measurable set \mathfrak{E}_0 . Then the integral is understood to be taken over those points of the interval (a, x) contained in \mathfrak{E}_0 .

HARVARD UNIVERSITY

A GENERAL THEORY OF REPRESENTATION OF FINITE OPERATIONS AND RELATIONS*

BY B. A. BERNSTEIN

Let $a \bmod n$ denote the least positive residue modulo n of an integer a , i. e., the least positive integer obtained from a by rejecting multiples of n . Consider the polynomials modulo a prime p

$$(1) \quad a_0 + a_1 x + \cdots + a_{p-1} x^{p-1}, \bmod p,$$

$$(2) \quad f_0(x) + f_1(x)y + \cdots + f_{p-1}(x)y^{p-1}, \bmod p,$$

where in (1) a_i are least positive p -residues and x ranges over the complete system of least positive p -residues, and where (2) is a polynomial modulo p in y whose coefficients $f_i(x)$ are modular polynomials in x of form (1). In a previous paper† I developed a theory of representation of abstract

* Presented to the Society, San Francisco Section, October 25, 1924.

† PROCEEDINGS OF THE INTERNATIONAL MATHEMATICAL CONGRESS, TORONTO, 1924.

binary operations and dyadic relations in a finite class of elements, in which theory the polynomials (2) entered fundamentally. I now wish to note the fact that this theory can be extended to finite operations and relations in general.

An m -ary operation O in a class K is a rule which determines for every ordered set of m K -elements x_1, x_2, \dots, x_m what K -element $O(x_1, x_2, \dots, x_m)$, if any, corresponds to the set. If K is finite, such a rule may always be given by an m -dimensional operation table or, when $m > 1$, by n tables each of $m-1$ dimensions. An m -adic relation R in K is a rule which states for every ordered set of m K -elements x_1, x_2, \dots, x_m whether or not these elements should be associated together in a proposition $R(x_1, x_2, \dots, x_m)$. When K is finite, such a rule may always be given by an m -dimensional relation table or by n tables each of $m-1$ dimensions ($m > 1$), in which the fact that $R(x_1, x_2, \dots, x_m)$ holds may be indicated by “+” and that it does not hold by “-”.* The function fundamental in the representation of finite m -ary operations and m -adic relations in general is the modular polynomial $f(x_1, x_2, \dots, x_m)$ of the form

$$(3) \quad f_0 + f_1 x_m + \dots + f_{p-1} x_m^{p-1}, \text{ mod } p,$$

where p is prime and the coefficients f_i are polynomials modulo p in the $m-1$ arguments x_1, x_2, \dots, x_{m-1} . Noting that when the K -elements are n in number they may be labeled $0, 1, \dots, n-1$, we may state the general theory by the propositions A, B, C following.

PROPOSITION A. Given an arbitrary set of least positive n -residues

$$(4) \quad e_0, e_1, \dots, e_{n-1};$$

if and only if n is prime, a function $f(x)$ of form (1) can always be obtained such that

$$(5) \quad f(0) = e_0, f(1) = e_1, \dots, f(n-1) = e_{n-1},$$

namely (1) in which (modulo n)

* This “±” notation has been used by H. M. Sheffer.

$$(6) \quad a_0 = e_0, a_1 = \frac{\begin{vmatrix} e_1 - e_0 & 1 & \dots & 1 \\ e_2 - e_0 & 2^2 & \dots & 2^{n-1} \\ \dots & \dots & \dots & \dots \\ e_{n-1} - e_0 & (n-1)^2 & \dots & (n-1)^{n-1} \end{vmatrix}}{\begin{vmatrix} 1 & 1 & \dots & 1 \\ 2 & 2^2 & \dots & 2^{n-1} \\ \dots & \dots & \dots & \dots \\ n-1 & (n-1)^2 & \dots & (n-1)^{n-1} \end{vmatrix}},$$

$$\dots, a_{n-1} = \frac{\begin{vmatrix} 1 & 1 & \dots & e_1 - e_0 \\ 2 & 2^2 & \dots & e_2 - e_0 \\ \dots & \dots & \dots & \dots \\ n-1 & (n-1)^2 & \dots & e_{n-1} - e_0 \end{vmatrix}}{\begin{vmatrix} 1 & 1 & \dots & 1 \\ 2 & 2^2 & \dots & 2^{n-1} \\ \dots & \dots & \dots & \dots \\ n-1 & (n-1)^2 & \dots & (n-1)^{n-1} \end{vmatrix}}.$$

PROPOSITION B. Given any m -dimensional operation table for the K -elements $0, 1, \dots, n-1$; a function equivalent to this table may be found having the form

$$(7) \quad f + 0/\varphi,$$

where f and φ are modular polynomials of form (3), with the x 's ranging over the K -elements.

PROPOSITION C. Given any m -dimensional relation table for the K -elements $0, 1, \dots, n-1$; an equation equivalent to this table may be found having the form

$$(8) \quad f = 0,$$

where f is a modular polynomial of form (3), with the x 's ranging over the K -elements.

For the proof of Proposition A the reader is referred to the paper cited above.

The second term of (7) is designed to care for operations that do not satisfy the conditions of closure. To see the

truth of Proposition B, consider several cases. (i) If n is prime and the given operation satisfies the condition of closure, function (7) is the polynomial of form (3) obtained from the given table by repeated application of Proposition A. (ii) If n is prime and the given operation does not satisfy the closure condition, consider the table got from the given table by assigning K -elements to the sequences x_1, x_2, \dots, x_m , to which no K -element corresponds; consider also the table got from the given table by assigning $\mathbf{0}$ to each sequence to which no K -element corresponds and a K -element not $\mathbf{0}$ to any other sequence. The polynomials (3) equivalent to the derived tables will be respectively the f and φ of (7). (iii) If n is composite, consider any operation table for a prime number $p(>n)$ of elements which will give the original table when the x 's range over the n elements of K ; the function equivalent to this table, with the x 's ranging over the K -elements, will be the required function (7).

To see that Proposition C is true, consider any operation table got from the given relation table by changing each "+" to $\mathbf{0}$ and each "-" to some K -element not $\mathbf{0}$; the function equivalent to this operation table will be the f of (8).

Our theory of representation shows that any finite mathematical system, quantitative or non-quantitative, can be represented arithmetically (and geometrically). The theory also makes clear the nature of operations and relations, and it brings out the fact that an m -ary operation is the same as an $(m+1)$ -adic relation, and m -adic relation the same as one or more $(m-1)$ -ary operations ($m > 1$).*

UNIVERSITY OF CALIFORNIA

* For other applications and for various illustrations, see the above cited paper. See also this BULLETIN, vol. 30 (1924), p. 24, and AMERICAN JOURNAL, vol. 46 (1924), p. 110.