ANNALES
POLONICI MATHEMATICI
XXII (1969)

A representation theorem for $(X_1-1)(X_2-1)\ldots(X_n-1)$ and its applications

by D. Ž. Djoković (Waterloo, Canada)

1. Introduction. The representation which we shall establish is given by formula (1). The proof is constructive. For instance, if $n = 2$ we obtain by this method the following representation:

$$2(X-1)(Y-1) = (XY-1)^2 - Y^2(X-1)^2 - 2X(Y-1)^2 + (Y-1)^2 .$$

We apply representation (1) to the difference operator and obtain an analogous representation of the iterated difference operator. Finally we apply this result to the difference functional equation

$$\underset{u}{\Delta^n} f(x) = 0$$

and obtain the generalizations of some recent results of McKiernan [2].

In this paper, by definition, a *monomial* in the indeterminates $X_1, \ldots, X_n$ is any expression of the form

$$X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n} ,$$

where $i_1, i_2, \ldots, i_n$ are non-negative integers. Note that there is no scalar coefficient in this expression.

2. Representation theorem.

THEOREM 1. *Let $R[X_1, \ldots, X_n]$ be the polynomial ring over a commutative ring R with unity* 1. *Then there exists a non-negative integer s such that the polynomial*

$$(n!)^{2^s} \prod_{i=1}^{n} (X_i - 1)$$

belongs to the ideal I generated by the polynomials

$$(X_{i_1} X_{i_2} \ldots X_{i_k} - 1)^n \qquad (1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n) .$$

In other words we have a representation

$$(1)\qquad (n!)^{2^s}\prod_{i=1}^{n}(X_i-1)=\sum_{1\leqslant i_1<\ldots<i_k\leqslant n}P_{i_1\ldots i_k}(X_{i_1}X_{i_2}\ldots X_{i_k}-1)^n$$

where $P_{i_1\ldots i_k}\in R[X_1,\ldots,X_n]$.

For the proof we need the following

LEMMA 1. *If* $X_1,\ldots,X_n$ *are elements of a commutative ring with unity* 1, *then we have the identities*

$$(2)\qquad \sum_{k=1}^{n}(-1)^k\sum_{1\leqslant i_1<i_2<\ldots<i_k\leqslant n}(X_{i_1}X_{i_2}\ldots X_{i_k}-1)^n = \sum_{m=1}^{n}(-1)^m\binom{n}{m}\prod_{i=1}^{n}(X_i^m-1)\,,$$

and

$$(3)\qquad \sum_{k=1}^{n}(-1)^k\sum_{1\leqslant i_1<i_2<\ldots<i_k\leqslant n}(X_{i_1}X_{i_2}\ldots X_{i_k}+1)^n = -2^n+(-1)^n\sum_{m=1}^{n}\binom{n}{m}\prod_{i=1}^{n}(X_i^m-1)\,.$$

Proof. Let us perform all multiplications on both sides of (2) and (3). By inspection we conclude that all these four sides contain only the monomials of the form

$$(4)\qquad (X_{i_1}X_{i_2}\ldots X_{i_k})^m\,,$$

where $1\leqslant i_1<i_2<\ldots<i_k\leqslant n$ and $0\leqslant m\leqslant n$. If $m>0$ the coefficient of monomial (4) on both sides of (2) is equal to

$$(-1)^k(-1)^{n-m}\binom{n}{m}\,,$$

and the corresponding coefficient on both sides of (3) is equal to

$$(-1)^k\binom{n}{m}\,.$$

It remains to verify the equality of constant terms in (2) and (3). By this what we already proved we know that the difference of the left-hand side and the right-hand side in (2) and also in (3) is a constant. In order to prove that these constants are zero it is sufficient to verify (2) and (3) for some particular values of $X_1,\ldots,X_n$. It is convenient to take

$X_1 = X_2 = \ldots = X_n = 1$. Then in (2) both sides vanish and (3) reduces to the identity

$$2^n \sum_{k=1}^{n} (-1)^k \binom{n}{k} = -2^n .$$

Proof of Theorem 1. Let P be the polynomial which is equal to both sides of identity (2). Identity (2) implies that $P \in I$ and also that P is divisible by $(X_1-1)(X_2-1)\ldots(X_n-1)$. We have

$$P = Q \prod_{i=1}^{n} (X_i-1) , \tag{5}$$

where

$$Q = \sum_{m=1}^{n} (-1)^m \binom{n}{m} \prod_{i=1}^{n} \left(\sum_{r=0}^{m-1} X_i^r \right) .$$

From this formula we obtain

$$Q(1, \ldots, 1) = \sum_{m=1}^{n} (-1)^m \binom{n}{m} m^n = (-1)^n n! , \tag{6}$$

where we made use of a well-known identity (cf., for instance [1], Chapter II, § 12, Exercise 16). Let us introduce the new indeterminates $Y_i = X_i-1$, $i = 1, \ldots, n$. From (5) and (6) we infer that

$$P = (-1)^n Y_1 Y_2 \ldots Y_n (n! - Q') ,$$

where Q' is a polynomial in $Y_1, \ldots, Y_n$ with zero constant term. Multiplying both sides by

$$S = \prod_{r=0}^{s-1} [(n!)^{2^r} + (Q')^{2^r}]$$

we obtain

$$(-1)^n SP = Y_1 Y_2 \ldots Y_n [(n!)^{2^s} - (Q')^{2^s}] .$$

It follows that

$$(n!)^{2^s} Y_1 Y_2 \ldots Y_n = (-1)^n SP + Y_1 Y_2 \ldots Y_n (Q')^{2^s} . \tag{7}$$

Since Q' has zero constant term we can choose s so large that every term in the expansion of

$$(Q')^{2^s}$$

is divisible by at least one of the polynomials Y_i^{n-1}, $i = 1, \ldots, n$.

Since $P \in I$ and obviously $Y_i^n \in I$ for all i, formula (7) implies that also $(n!)^{2^r} Y_1 Y_2 \dots Y_n \in I$. This is equivalent to (1). The proof is completed.

8. Applications to difference operator. Let A be an abelian semigroup and M an abelian group, both written additively. We shall denote the set of all mappings $f\colon A \to M$ by M^A. We define the shift operator

$$\underset{u}{E}\colon M^A \to M^A \qquad (u \in A)$$

as follows: the image of $f \in M^A$ under $\underset{u}{E}$ is the mapping $\underset{u}{E} f \in M^A$ which is defined by

$$(\underset{u}{E} f)(x) = f(x+u) \quad \text{for all } x \in A\,. \tag{8}$$

The identity operator $1\colon M^A \to M^A$ maps each $f \in M^A$ onto itself. The zero operator $0\colon M^A \to M^A$ maps each $f \in M^A$ onto the zero function $0 \in M^A$ which is defined by $0(x) = 0$ for all $x \in A$. The zero on the right-hand side of the last equation is, of course, the neutral element of M. The context will always make clear in what sense we use the symbols 1 and 0.

If m and m_i are integers and $u_i \in A$, we define the operator

$$E = m \cdot 1 + \sum m_i \cdot \underset{u_i}{E} \tag{9}$$

by equality

$$(Ef)(x) = mf(x) + \sum m_i f(x+u_i)$$

which holds for all $x \in A$ and all $f \in M^A$. If

$$E' = m' \cdot 1 + \sum m_i' \cdot \underset{u_i'}{E}\,, \qquad E'' = m'' \cdot 1 + \sum m_j'' \cdot \underset{u_j''}{E}\,,$$

are two operators of form (9) we define their sum $E'+E''$, and their product $E'E''$ in a natural way:

$$E' + E'' = (m' + m'') \cdot 1 + \sum m_i' \cdot \underset{u_i'}{E} + \sum m_j'' \cdot \underset{u_j''}{E}\,,$$

$$E'E'' = m'm'' \cdot 1 + \sum_i m''m_i' \cdot \underset{u_i'}{E} + \sum_j m'm_j'' \cdot \underset{u_j''}{E} + \sum_{i,j} m_i'm_j'' \cdot \underset{u_i'}{E}\,\underset{u_j''}{E}\,.$$

One can easily check that, with respect to these operations of addition and multiplication, the set of all operators of form (9) has the structure

of a commutative ring with unity 1. In the sequel we denote this ring by E. If A has neutral element 0, then we can strike out the term $m \cdot 1$ in (9) since in that case $\underset{0}{E} = 1$.

The difference operator $\underset{u}{\Delta}$ $(u \in A)$ is defined by

$$\underset{u}{\Delta} \overset{\text{df}}{=} \underset{u}{E} - 1 .$$

We recall that E is commutative and in particular we have

$$\underset{u}{E}\,\underset{u}{\Delta} = \underset{u}{\Delta}\,\underset{u}{E}, \qquad \underset{u}{\Delta}\,\underset{v}{\Delta} = \underset{v}{\Delta}\,\underset{u}{\Delta} . \tag{10}$$

We define the powers of an operator $E \in E$ in usual way: $E^0 = 1$, $E^k = EE^{k-1}$ for $k \geqslant 1$.

THEOREM 2. *Let A be an abelian semigroup and $t_1, \ldots, t_n \in A$. Then we have a representation*

$$(n!)^{2^s} \underset{t_1}{\Delta}\,\underset{t_2}{\Delta} \ldots \underset{t_n}{\Delta} = \sum_k m_k \cdot \underset{u_k}{E}\,\underset{v_k}{\Delta^n}, \tag{11}$$

where $s \geqslant 0$ and m_k are integers and $u_k, v_k \in A$ depend on $t_1, \ldots, t_n$.

Proof. Let R be the ring of integers and let $P(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$. Further, let us define the mapping of $R[X_1, \ldots, X_n]$ into E which maps

$$P(X_1, \ldots, X_n) \to P(\underset{t_1}{E}, \ldots, \underset{t_n}{E}) .$$

This mapping is a ring homomorphism. By applying this homomorphism, representation (1) gives rise to representation (11).

An example. The formula from the introduction gives rise to the following representation

$$2\,\underset{u}{\Delta}\,\underset{v}{\Delta} = \underset{u+v}{\Delta^2} - \underset{2u}{E}\,\underset{u}{\Delta^2} - 2\,\underset{u}{E}\,\underset{v}{\Delta^2} + \underset{v}{\Delta^2} .$$

COROLLARY 1. *Let A be an abelian semigroup and M an abelian group satisfying the condition: $(n!)\,\omega = 0$ $(\omega \in M)$ implies $\omega = 0$. Then the equations*

$$\underset{u}{\Delta^n} f = 0 \quad \textit{for all } u \in A \tag{12}$$

and

$$\underset{t_1}{\Delta}\,\underset{t_2}{\Delta} \ldots \underset{t_n}{\Delta} f = 0 \quad \textit{for all } t_i \in A , \tag{13}$$

are equivalent to each other.

Proof. (13) implies (12) by putting $t_1 = \ldots = t_n = u$. (12) implies (13) by force of representation (11).

4. A functional equation. Let A, M have the same meaning as in the preceding section. A function f_n: $A^n \to M$ is said to be *additive in the first variable* if

$$f_n(x_1' + x_1'', x_2, \ldots, x_n) = f_n(x_1', x_2, \ldots, x_n) + f_n(x_1'', x_2, \ldots, x_n)$$

holds for all $x_1', x_1'', x_2, \ldots, x_n \in A$. Similarly we can define additivity in other variables. We say that f_n is *symmetric* if

$$f_n(x_1, x_2, \ldots, x_n) = f_n(x_{i_1}, x_{i_2}, \ldots, x_{i_n})$$

holds for all $x_1, \ldots, x_n \in A$ and for all permutations $i_1, i_2, \ldots, i_n$ of the sequence $1, 2, \ldots, n$.

We define the diagonalization f_n^* of f_n to be the mapping $A \to M$ defined by

$$f_n^*(x) = f_n(x, x, \ldots, x) \quad \text{for all } x \in A .$$

LEMMA 2. *If f_n: $A^n \to M$ is symmetric and additive in each variable, then*

$$\underset{u_1 u_2}{\Delta\Delta} \ldots \underset{u_p}{\Delta} f_n^* = \begin{cases} 0 & \text{if } p > n , \\ n! f_n(u_1, \ldots, u_n) & \text{if } p = n . \end{cases} \tag{14}$$

Here 0 denotes the zero mapping which maps each $x \in A$ onto $0 \in M$, and $n!f_n(u_1, \ldots, u_n)$ denotes the constant mapping which maps each $x \in A$ onto $n!f_n(u_1, \ldots, u_n) \in M$.

Proof. (i) Let first $p > n$.

If $n = 1$, then $f_1^* = f_1$ and we have

$$\begin{aligned} (\underset{u_1 u_2}{\Delta\Delta} f_1^*)(x) &= \big((\underset{u_1+u_2}{E} - \underset{u_1}{E} - \underset{u_2}{E} + 1) f_1^*\big)(x) \\ &= f_1^*(x + u_1 + u_2) - f_1^*(x + u_1) - f_1^*(x + u_2) + f_1^*(x) \\ &= f_1(x + u_1 + u_2) - f_1(x + u_1) - f_1(x + u_2) + f_1(x) . \end{aligned}$$

By additivity property of f_1 the right-hand side reduces to zero. This proves the first part of (14) for $n = 1$.

Now we use induction. We assume that the first part of (14) is true for smaller values of n. We define $f_{n,k,u}$: $A^k \to M$ by

$$f_{n,k,u}(x_1, \ldots, x_k) \overset{\text{df}}{=} f_n(x_1, \ldots, x_k, u, \ldots, u) .$$

Making use of the symmetry and additivity properties of f_n we find that

$$\begin{aligned}(\underset{u_p}{\Delta} f_n^*)(x) &= f_n^*(x+u_p) - f_n^*(x) \\ &= f_n(x+u_p, \ldots, x+u_p) - f_n(x, \ldots, x) \\ &= \sum_{k=0}^{n-1} \binom{n}{k} f_n(\underbrace{x, \ldots, x}_{k}, \underbrace{u_p, \ldots, u_p}_{n-k}) \\ &= \sum_{k=0}^{n-1} \binom{n}{k} f_{n,k,u_p}^*(x) \,.\end{aligned}$$

Since this holds for each $x \in A$ we get

$$\underset{u_p}{\Delta} f_n^* = \sum_{k=0}^{n-1} \binom{n}{k} f_{n,k,u_p}^* \,. \tag{15}$$

By induction hypothesis

$$\underset{u_1}{\Delta}\,\underset{u_2}{\Delta} \ldots \underset{u_{p-1}}{\Delta} f_{n,k,u_p}^* = 0 \tag{16}$$

for each $k = 0, 1, \ldots, n-1$. Applying the operator

$$\underset{u_1}{\Delta}\,\underset{u_2}{\Delta} \ldots \underset{u_{p-1}}{\Delta}$$

on both sides of (15) and using (16) we obtain

$$\underset{u_1}{\Delta}\,\underset{u_2}{\Delta} \ldots \underset{u_p}{\Delta} f_n^* = 0 \,.$$

(ii) Now, let $p = n$.

If $n = 1$ we get

$$(\underset{u_1}{\Delta} f_1^*)(x) = (\underset{u_1}{\Delta} f_1)(x) = f_1(x+u_1) - f_1(x) = f_1(u_1) \,.$$

Hence $\underset{u_1}{\Delta} f_1^*$ is a constant function which maps each $x \in A$ onto $f_1(u_1)$, i.e., the second part of (14) is true for $n = 1$. Assume that the assertion of the second part of (14) is true for smaller values of n. Formula (15) is applicable in this case also:

$$\underset{u_n}{\Delta} f_n^* = \sum_{k=0}^{n-1} \binom{n}{k} f_{n,k,u_n}^* \,.$$

Applying the operator

$$\underset{u_1}{\Delta}\,\underset{u_2}{\Delta} \ldots \underset{u_{n-1}}{\Delta}$$

on both sides and using the result proved in (i) we get

$$\underset{u_1}{\Delta}\underset{u_2}{\Delta}\dots\underset{u_n}{\Delta} f_n^* = n\underset{u_1}{\Delta}\underset{u_2}{\Delta}\dots\underset{u_{n-1}}{\Delta} f_{n,n-1,u_n}^* . \tag{17}$$

By induction hypothesis

$$\begin{aligned}\underset{u_1}{\Delta}\underset{u_2}{\Delta}\dots\underset{u_{n-1}}{\Delta} f_{n,n-1,u_n}^* &= (n-1)!f_{n,n-1,u_n}(u_1, \dots, u_{n-1}) \\ &= (n-1)!f_n(u_1, \dots, u_n) .\end{aligned} \tag{18}$$

From (17) and (18) we deduce

$$\underset{u_1}{\Delta}\underset{u_2}{\Delta}\dots\underset{u_n}{\Delta} f_n^* = n!f_n(u_1, \dots, u_n) .$$

Now, we can prove the following

THEOREM 3. *Let A be an abelian semigroup and M an abelian group satisfying the condition: for each $a \in M$ the equation $(n!)\omega = a$ has unique solution $\omega = a/(n!)$. If $f: A \to M$ satisfies the functional equation*

$$\underset{u}{\Delta}^{n+1} f = 0 \quad \text{for all } u \in A , \tag{19}$$

then

$$f = \sum_{k=0}^{n} g_k^* , \tag{20}$$

where g_0^* is a constant mapping and $g_k: A^k \to M$ are symmetric and additive in each variable.

Conversely, any function having form (20) *satisfies the functional equation* (19).

Proof. The second assertion of the theorem follows immediately from Lemma 2. Let us assume that f satisfies (19). By Corollary 1 equation (19) implies that

$$\underset{u_1}{\Delta}\underset{u_2}{\Delta}\dots\underset{u_{n+1}}{\Delta} f = 0 \tag{21}$$

for all $u_1, \dots, u_{n+1} \in A$. It follows that the function

$$\underset{u_1}{\Delta}\underset{u_2}{\Delta}\dots\underset{u_n}{\Delta} f$$

is a constant function. Let us define the function $g_n: A^n \to M$ by

$$g_n(u_1, \dots, u_n) = \frac{1}{n!}\left(\underset{u_1}{\Delta}\underset{u_2}{\Delta}\dots\underset{u_n}{\Delta} f\right)(x) . \tag{22}$$

We remind again that the right-hand side is independent of $x \in A$.

The function g_n is symmetric since by (10) the difference operators commute each to other. We shall prove that g_n is also additive in each

variable. By symmetry, it is sufficient to prove that g_n is additive in the first variable. We have

$$\begin{aligned}(n!)[g_n(u_1'+u_1'', u_2, \ldots, u_n)-g_n(u_1', u_2, \ldots, u_n)-g_n(u_1'', u_2, \ldots, u_n)] \\ &= (\underset{u_1'+u_2'' u_2 \quad u_n}{\Delta \Delta \ldots \Delta} f)(x)-(\underset{u_1' u_2 \quad u_n}{\Delta \Delta \ldots \Delta} f)(x)-(\underset{u_1'' u_2 \quad u_n}{\Delta \Delta \ldots \Delta} f)(x) \\ &= \Big((\underset{u_1'+u_1'' \quad u_1' \quad u_1'' u_2 \quad u_n}{\Delta \quad -\Delta -\Delta}) \Delta \ldots \Delta f\Big)(x) \\ &= (\underset{u_1' u_1'' u_2 \quad u_n}{\Delta \Delta \Delta \ldots \Delta} f)(x)\,.\end{aligned}$$

The last expression is zero by force of (21). Hence, g_n is additive in each variable.

The theorem is evidently true for $n = 0$. Now let $n \geqslant 1$ and assume that the theorem is true for smaller values of n. Introducing the function $h = f - g_n^*$ we get

$$\underset{u}{\Delta^n} h = \underset{u}{\Delta^n} f - \underset{u}{\Delta^n} g_n^*\,.$$

Since by Lemma 2

$$\underset{u}{\Delta^n} g_n^* = n!\, g_n^*(u)$$

and by (22)

$$n!\, g_n^*(u) = \underset{u}{\Delta^n} f\,,$$

we get

$$\underset{u}{\Delta^n} h = 0 \quad \text{for all } u \in A\,.$$

By inductive hypothesis

$$h = \sum_{k=0}^{n-1} g_k^*\,,$$

where $g_k\colon A^k \to M$ are symmetric and additive in each variable. Finally, we obtain

$$f = h + g_n^* = \sum_{k=0}^{n} g_k^*\,.$$

The proof is finished.

COROLLARY 2. *The equation*

$$\underset{u}{\Delta^n} f = g(u) \quad \textit{for all } u \in A \tag{23}$$

has a solution in $f \in M^A$ *if and only if there exist* $g_n\colon A^n \to M$ *which is symmetric and additive in each variable and such that* $g = n!\, g_n^*$. *The general solution of* (23) *is then* $f = g_n^* + h$, *where* h *is the general solution of* $\underset{u}{\Delta^n} h = 0$.

Proof. (23) implies that $\Delta_u^{n+1} f = 0$. By Theorem 4

$$f = \sum_{k=0}^{n} g_k^* .$$

By Lemma 2: $\Delta_u^n f = n! g_n^*(u)$. Hence, $g = n! g_n^*$.

Conversely, if $g = n! g_n^*$, then $f = g_n^*$ is a solution of (23) by force of Lemma 2.

COROLLARY 3. *A necessary and sufficient condition that* $f: A \to M$ *has the form* $f = g_n^*$, *where* $g_n: A^n \to M$ *is symmetric and additive in each variable is that*

$$\Delta_u^n f = n! f(u) \quad \text{for all } u \in A . \tag{24}$$

Proof. If $f = g_n^*$, then Lemma 2 implies (24). Conversely, if (24) holds, then $f = g_n^*$ by Corollary 2.

Remarks 1. Corollary 1 of Theorem 2 for the case when A is also an abelian group was proved earlier by Van der Lijn [3].

2. If $A = M =$ real numbers and if we additionally assume that the function f in (19) is measurable, then formula (22) implies that g_n is also measurable. In that case the additive property of g_n implies that $g_n(x_1, \ldots, x_n) = c x_1 x_2 \ldots x_n$ consequently $g_n^*(x) = c x^n$. Hence, f is a polynomial of degree $\leqslant n$.

References

[1] W. Feller, *An introduction to probability theory and its applications*, vol. I, second edition.

[2] M. A. McKiernan, *On vanishing n-th ordered differences and Hamel basis*, Ann. Polon. Math. 19 (1967), pp. 331-336.

[3] G. Van der Lijn, *La définition fonctionnelle des polynômes dans les groupes abeliens*, Fund. Math. 33 (1939), pp. 42-50.

Reçu par la Rédaction le 3. 5. 1968