ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

338

ON BASIC GROUPS FOR THE SET OF FUNCTIONS OVER A FINITE DOMAIN

BY

ARTO SALOMAA

HELSINKI 1963
SUOMALAINEN TIEDEAKATEMIA

https://doi.org/10.5186/aasfm.1964.338

Communicated 13 September 1963 by P. J. MYRBERG and K. INKERI

KESKUSKIRJAPAINO
HELSINKI 1963

On basic groups for the set of functions over a finite domain

1. *Results.* Let $\mathfrak{E}_n$ be the set of functions whose variables, finite in number, range over a fixed finite set

$$N = \{1, 2, \ldots, n\}, n \geqq 2$$

and whose values are elements of N. If $\mathfrak{F} \subset \mathfrak{E}_n$ we denote by $\overline{\mathfrak{F}}$ the closure of $\mathfrak{F}$ under composition. $\mathfrak{F}$ is said to be *complete* if $\overline{\mathfrak{F}} = \mathfrak{E}_n$.[1])

Every complete set contains a function satisfying *Słupecki conditions*, i.e. depending essentially on at least two variables and assuming all n values. We say that a subset $\mathfrak{F}$ of $\mathfrak{E}_n$ is a *basic set* for $\mathfrak{E}_n$ if $\mathfrak{F}$ is not complete but the addition to $\mathfrak{F}$ of any function satisfying Słupecki conditions yields a complete set. If a basic set is a group with respect to composition it is termed a *basic group* for $\mathfrak{E}_n$.

It is shown in [1, pp. 72—76] that all 1-place functions belonging to $\mathfrak{E}_n$ form a basic set $\mathfrak{F}_1$ for $\mathfrak{E}_n$, provided $n \geqq 3$. This result has been strengthened to concern various subsets of $\mathfrak{F}_1$ which are closed under composition. It is shown in [1] that the subset of $\mathfrak{F}_1$ consisting of all 1-place functions other than permutations is a basic set for $\mathfrak{E}_n$, provided $n \geqq 3$.

On the other hand, it is shown in [2] that the symmetric group of degree n is a basic group for $\mathfrak{E}_n$.[2]) Furthermore, according to [3], the alternating group of degree n is a basic group for $\mathfrak{E}_n$. (Obviously, the latter result implies the former.) These results are valid for all values of $n \geqq 5$. Counter-examples presented in [2] show that they are not valid for $n = 2, 3, 4$.

In this paper, we shall study the problem whether it is still possible to reduce basic groups, i.e. whether the alternating group can be replaced by a smaller group of degree n, provided $n \geqq 5$. In proofs of completeness criteria for subsets of $\mathfrak{E}_n$, the essential fact concerning groups is the degree of transitivity. Therefore, it is natural to ask whether the alternating group can be replaced by an arbitrary group of degree n with some lower limitation on the degree of transitivity.

---

[1]) For a detailed discussion, cf. [1, pp. 56—58]. Throughout this paper, n means the number of elements in the set N.

[2]) In fact, a slight modification in the proof of the theorem in [2] will yield this result.

It is clear that an arbitrary doubly transitive group is not basic for $\mathfrak{E}_n$. Counter-examples are found, for instance, by considering prime values of n and linear groups. A triply transitive group is basic for $\mathfrak{E}_n$ if n is not a power of 2. A quadruply transitive group is always basic for $\mathfrak{E}_n$ (provided the condition $n \geqq 5$ is satisfied). These results are due to the following theorem which we shall prove in section 2.

Theorem. *Every quadruply transitive group of degree n is a basic group for $\mathfrak{E}_n$, provided $n \geqq 5$. If, in addition, $n \neq 2^r$ then every triply transitive group of degree n is a basic group for $\mathfrak{E}_n$.*

It is a consequence of this theorem that if a quadruply transitive group of degree n is contained in the closure of a function $f \in \mathfrak{E}_n$ (i.e. if f *generates* a quadruply transitive group) then the unit set of f is complete.[1]) The same statement holds true for triply transitive groups of degree n, provided $n \neq 2^r, r \geqq 3$. It is very likely that the statement holds true for arbitrary triply transitive groups, perhaps even for arbitrary doubly transitive groups if $n \geqq 3$.

In section 3, we consider the exceptional cases in our theorem: $n = 2^r$, $r \geqq 3$. We construct a triply transitive group of degree 2^r which is not a basic group for $\mathfrak{E}_{2^r}$. Such a counter-example is provided by the holomorph of an Abelian group of order 2^r and type $(1, 1, \ldots, 1)$.

2. *Proofs.* To prove our theorem, we shall first establish several lemmas. We shall use the terms *genus* and *type* (of 1-place functions belonging to $\mathfrak{E}_n$) as defined in [3]. Assume that G_i, $i = 1, \ldots, k$, are non-empty subsets of N. Then, for any function $f(x_1, \ldots, x_k) \in \mathfrak{E}_n$, we denote by $f(G_1, \ldots, G_k)$ the set of values assumed by f when, for $i = 1, \ldots, k$, the variable x_i is restricted to the set G_i.

Lemmas 1 and 2 are the same as lemmas 1.1 and 1.3 in [3]. Therefore, we omit their proofs.

Lemma 1. *Assume that $n \geqq 3$ and $f(x_1, \ldots, x_k)$ satisfies Słupecki conditions. Then for any j, $3 \leqq j \leqq n$, there are sets G_i, $i = 1, \ldots, k$, each consisting of a most $j - 1$ elements such that $f(G_1, \ldots, G_k)$ contains at least j elements.*

Lemma 2. *The set of functions of type $[b_1, b_2, b_3, \ldots, b_t]$ where $1 < t < n$ generates every function of type $[b_1 + b_2, b_3, \ldots, b_t]$.*

Lemma 3. *Assume that $n \geqq 4$ and $\mathfrak{F} \subset \mathfrak{E}_n$ contains a triply transitive group $\mathfrak{G}$ (of degree n) and a function $f(x_1, \ldots, x_k)$ satisfying Słupecki conditions. Then $\mathfrak{F}$ generates a function of genus 2 and all functions of genus 1.*

---

1) This means that f is a so-called *Sheffer function*. The result is valid for $n \geq 4$ because, according to [3], it is valid for $n = 4$.

Proof. I. We shall first prove that $\mathfrak{F}$ generates a function $g(x)$ whose genus γ satisfies $1 < \gamma < n$.

By lemma 1, there are numbers $a_1, \ldots, a_k$ such that

$$f(G_1, \ldots, G_k) = N \tag{1}$$

where $G_i = N - \{a_i\}$, for $i = 1, \ldots, k$. By (1), there are numbers $a_i', i = 1, \ldots, k$, such that

$$f(a_1', \ldots, a_k') = f(a_1, \ldots, a_k)$$

and $a_i' \neq a_i$, for $i = 1, \ldots, k$. We choose from $\mathfrak{G}$ k permutations $p_i(x), i = 1, \ldots, k$, such that $p_i(1) = a_i$ and $p_i(2) = a_i'$. The choice is possible because $\mathfrak{G}$ is doubly transitive. Then the function

$$f(p_1(x), \ldots, p_k(x)) \tag{2}$$

is of genus smaller than n. If it is of genus greater than 1 we have found a function $g(x)$ as required.

We, therefore, assume that the function (2) is of genus 1. Hence, $\mathfrak{F}$ generates all functions of genus 1, i.e. all constants. Using lemma 1, we choose sets $H_i, i = 1, \ldots, k$, such that each H_i consists of two (not necessarily distinct) elements b_i and b_i' and $f(H_1, \ldots, H_k)$ contains at least three distinct elements b, b' and b''. By a suitable renumbering of the variables, this choice can be made in such a way that

$$f(b_1, b_2, \ldots, b_k) = b , \tag{3}$$

$$f(b_1', b_2, \ldots, b_k) = b' \tag{4}$$

and

$$f(b_1', b_2', \ldots, b_k') = b'' . \tag{5}$$

Consider the 1-place function

$$g_1(x) = f(x, b_2, \ldots, b_k)$$

which is generated by $\mathfrak{F}$. If $g_1(x)$ does not assume the value b'' we may choose $g(x) = g_1(x)$. Suppose

$$g_1(c_1) = b'' . \tag{6}$$

Then necessarily $c_1 \neq b_1, b_1'$. Choose numbers c_2 and $c_{3,i}, i = 2, \ldots, k$, such that $c_2 \neq b_1, b_1', c_1$ and $c_{3,i} \neq b_i, b_i'$ if $b_i \neq b_i'$ but $c_{3,i} = b_i$ if $b_i = b_i'$. The choice is possible because $n \geqq 4$.

Assume that

$$f(c_2, c_{3,2}, \ldots, c_{3,k}) = b'' . \tag{7}$$

Let $q_i(x)$, $i = 1, \ldots, k$, be constants in $\bar{\mathfrak{F}}$ or permutations in $\mathfrak{G}$, defined as follows. The function $q_1(x)$ is a permutation such that $q_1(1) = c_2$, $q_1(2) = b_1$ and $q_1(3) = b_1'$. Let $2 \leqq i \leqq k$ and $b_i \neq b_i'$. Then $q_i(x)$ is a permutation such that $q_i(1) = c_{3,i}$, $q_i(2) = b_i$ and $q_i(3) = b_i'$. Let $2 \leqq i \leqq k$ and $b_i = b_i'$. Then $q_i(x) = b_i$. By (3), (5) and (7), we may choose

$$g(x) = f(q_1(x), \ldots, q_k(x)) .$$

Assume that

$$f(c_2, c_{3,2}, \ldots, c_{3,k}) \neq b'' . \tag{8}$$

Let $q_1'(x)$ be a permutation in $\mathfrak{G}$ such that $q_1'(1) = c_2$, $q_1'(2) = c_1$ and $q_1'(3) = b_1'$. By (5), (6) and (8), we may choose

$$g(x) = f(q_1'(x), q_2(x), \ldots, q_k(x)) .$$

Thus, in all cases, $\mathfrak{F}$ generates a function $g(x)$ whose genus γ satisfies $1 < \gamma < n$.

II. Assume that $\gamma > 2$. We shall now prove that $\mathfrak{F}$ generates a function $h(x)$ whose genus γ_1 satisfies $2 \leqq \gamma_1 < \gamma$. By repeating the argument, we may conclude that $\mathfrak{F}$ generates a function of genus 2.

Let u be a value assumed by $g(x)$ at least twice and let v and w be any other distinct values of $g(x)$. Hence, there are distinct numbers u_1, u_2 and v_1 such that

$$g(u_1) = g(u_2) = u \quad \text{and} \quad g(v_1) = v .$$

Choose from $\mathfrak{G}$ a permutation $p(x)$ such that $p(u) = u_1$, $p(w) = u_2$ and $p(v) = v_1$. Then the function

$$h(x) = gpg(x)$$

is of genus γ_1 where $2 \leqq \gamma_1 < \gamma$.

We have, thus, shown that $\mathfrak{F}$ generates a function $h_1(x)$ of genus 2. Let $h_1(d_1) = h_1(d_2) = d$, $d_1 \neq d_2$, and $h_1(d_3) = d'$, $d' \neq d$. To complete the proof of lemma 3, we choose from $\mathfrak{G}$ a permutation $q(x)$ such that $q(d) = d_1$ and $q(d') = d_2$. Then $h_1qh_1(x) = d$. Thus, $\mathfrak{F}$ generates the constant d. Because $\mathfrak{F}$ contains a transitive group, we may conclude that $\mathfrak{F}$ generates all constants. Hence, lemma 3 follows.

Lemma 4. *Assume that* $n \geqq 3$[1]) *and* $\mathfrak{F} \subset \mathfrak{E}_n$ *contains a triply transitive group* $\mathfrak{G}$ *(of degree* n*), a function* $f(x_1, \ldots, x_k)$ *satisfying Słupecki conditions and a function* $g(x)$ *of type* $[n-1, 1]$. *Then* $\mathfrak{F}$ *is complete.*

[1]) For the proof of our theorem, it obviously suffices to consider the cases $n > 4$. A sharper formulation is given to some of the lemmas because their proofs remain unaltered. On the other hand, lemmas 4 and 5 may be considered as completeness criteria for subsets of $\mathfrak{E}_n$, $n \geqq 3$.

Proof. Obviously, any function of type $[n-1,1]$ may be expressed in the form $p_1 g p_2(x)$ where $p_1(x)$ and $p_2(x)$ are permutations belonging to $\mathfrak{G}$. In fact, p_2 may be chosen from any transitive subgroup of $\mathfrak{G}$ and p_1 may be chosen from any doubly transitive subgroup of $\mathfrak{G}$. Thus, $\mathfrak{F}$ generates all functions of type $[n-1,1]$.

We shall now make the following hypothesis of induction: $\mathfrak{F}$ generates all functions of type

(9) $$[n-i\,,\underbrace{1\,,\ldots\,,1}_{i \text{ terms}}]$$

where $1 \leqq i < n-2$. We shall prove that this implies that $\mathfrak{F}$ generates all functions of type

(10) $$[n-(i+1)\,,\underbrace{1\,,\ldots\,,1}_{i+1 \text{ terms}}]\,.$$

We choose numbers b_i and b_i', $i = 1\,,\ldots\,,k$, as in the proof of lemma 3 such that the equations (3) — (5) hold, for some distinct numbers b, b' and b''.

Let $h(x)$ be an arbitrary function of type (10). We have to show that $h(x) \in \overline{\mathfrak{F}}$.

The function $h(x)$ assumes $i+2$ distinct values. Let α_1 be the value assumed by $h(x)$ $n-(i+1)$ times and let U consist of all numbers y such that $h(y) = \alpha_1$. Hence, the cardinality of U (denoted by card(U)) is at least 2. Finally, let the other values assumed by $h(x)$ be $\alpha_2\,,\ldots\,,\alpha_{i+2}$ and let u_ν be numbers such that $h(u_\nu) = \alpha_\nu$, for $\nu = 2\,,\ldots\,,i+2$.

We choose from $\mathfrak{G}$ a permutation $p(x)$ such that $p(b') = \alpha_1$, $p(b) = \alpha_2$ and $p(b'') = \alpha_3$ and denote

(11) $$f_1(x_1\,,\ldots\,,x_k) = p(f(x_1\,,\ldots\,,x_k))\,.$$

Clearly, $f_1(x_1\,,\ldots\,,x_k)$ satisfies Słupecki conditions. Therefore, it is possible to choose numbers α_ν^μ, $\mu = 1\,,\ldots\,,i-1, \nu = 1\,,\ldots\,,k$, such that f_1 applied to the μ^{th} row vector of the matrix

$$\left\| \begin{matrix} \alpha_1^1 & \ldots\, \alpha_k^1 \\ \vdots & \vdots \\ \alpha_1^{i-1} & \ldots\, \alpha_k^{i-1} \end{matrix} \right\|$$

yields the value $\alpha_{\mu+3}$, for any $\mu = 1\,,\ldots\,,i-1$.

We now consider auxiliary functions $h_i(x), i = 1\,,\ldots\,,k$, defined by the following table:

	$h_1(x)$	$h_2(x)$	$\ldots$	$h_k(x)$
$x \in U$	b_1'	b_2		b_k
$x = u_2$	b_1	b_2		b_k
$x = u_3$	b_1'	b_2'		b_k'
$x = u_4$	$\overset{1}{\alpha}_1$	$\overset{1}{\alpha}_2$		$\overset{1}{\alpha}_k$
.				
.				
.				
$x = u_{i+2}$	$\overset{i-1}{\alpha}_1$	$\overset{i-1}{\alpha}_2$		$\overset{i-1}{\alpha}_k$

It follows from our inductive assumption concerning functions of type (9) and lemma 2 that every function assuming some value at least $n - i$ times is generated by $\mathfrak{F}$. Because the functions $h_i(x)$ satisfy this condition, we may conclude that $h_i(x) \in \overline{\mathfrak{F}}$, for $i = 1, \ldots, k$.

It is a consequence of (11) and the choice of the functions $h_i(x)$ that

$$h(x) = f_1(h_1(x), \ldots, h_k(x)) .$$

Thus, we have shown that all functions of type (10) are generated by $\mathfrak{F}$.

We conclude, by induction, that all functions of type

$$[2, \underbrace{1, \ldots, 1}_{n-2 \text{ terms}}] \tag{12}$$

are generated by $\mathfrak{F}$. By lemma 2, the set of functions of type (12) generates the subset of $\mathfrak{E}_n$ consisting of all 1-place functions other than permutations. By the criterion mentioned in section 1, we may conclude that $\mathfrak{F}$ is complete.

Lemma 5. *Assume that* $n \geqq 3$ *and* $\mathfrak{F} \subset \mathfrak{E}_n$ *contains a triply transitive group* $\mathfrak{G}$ *(of degree* n*), a function* $f(x_1, \ldots, x_k)$ *satisfying Slupecki conditions and a function* $g(x)$ *of type* $[n - a, a]$ *where* $a \neq \frac{n}{2}$. *Then* $\mathfrak{F}$ *is complete.*

Proof. If $n = 3$ or $n = 4$ the assumptions of lemmas 4 and 5 are equivalent. Therefore, we assume that $n \geqq 5$. We shall show that $\mathfrak{F}$ generates a function of type $[n - 1, 1]$. This implies, by lemma 4, that $\mathfrak{F}$ is complete.

By the hypothesis, $n - a \neq a$. We assume that the notation is chosen in such a way that $n - a > a$. If $a = 1$ the proof is completed. We, therefore, assume that $a \geqq 2$. We shall show that $\mathfrak{F}$ generates a function $g_1(x)$ of type $[n - a_1, a_1]$ where $1 \leqq a_1 < a$. By repeating the argument, we conclude that $\mathfrak{F}$ generates a function of type $[n - 1, 1]$.

Let E_1 and E_2 be disjoint subsets of N such that $\mathrm{card}(E_1) = n - a$, $\mathrm{card}(E_2) = a \geqq 2$ and $g(x)$ assumes a constant value both in E_1 and in E_2. Because $\mathfrak{F}$ contains a doubly transitive group it generates every function assuming a constant value both in E_1 and in E_2.

We choose from $\mathfrak{G}$ a permutation $p(x)$ mapping some element of E_2 into itself and some other element of E_2 into E_1. Consider the sets

$$(13) \qquad \begin{aligned} V_1 &= E_1 \cap p(E_1)\,, \quad V_2 = E_2 \cap p(E_1)\,, \\ V_3 &= E_2 \cap p(E_2)\,, \quad V_4 = E_1 \cap p(E_2)\,. \end{aligned}$$

The union of the sets (13) equals N. On the other hand, by the choice of the permutation p,

$$(14) \qquad 1 \leqq \mathrm{card}\,(V_i) < \mathrm{card}\,(E_2) = a\,, \quad \text{for} \quad i = 2\,,3\,,4\,.$$

Furthermore, $1 \leqq \mathrm{card}\,(V_1)$. The sets (13) are not of the same cardinality. For if $\mathrm{card}\,(V_1) = \mathrm{card}\,(V_2)$ and $\mathrm{card}\,(V_3) = \mathrm{card}\,(V_4)$ we obtain

$$\mathrm{card}\,(V_1) = \tfrac{1}{2}\,\mathrm{card}\,(E_1) > \tfrac{1}{2}\,\mathrm{card}\,(E_2) = \mathrm{card}\,(V_3)\,.$$

Let b_i and b_i', $i = 1\,,\ldots,k$, be the same numbers as in the proof of lemma 3. Thus, equations (3) — (5) hold, for some distinct numbers b, b' and b''. Choose arbitrary elements $v_i \in V_i$, $i = 1, 2, 3,$ and a permutation $p'(x) \in \mathfrak{G}$ such that $p'(b) = v_1, p'(b') = v_2$ and $p'(b'') = v_3$.

The following auxiliary functions $h_i(x)$ are generated by $\mathfrak{F}$:

$$h_i(E_1) = \{b_i\}\,,\; h_i(E_2) = \{b_i'\}\,, \quad i = 1\,,\ldots,k\,.$$

(Some of the functions $h_i(x)$ may be constants which are generated by $\mathfrak{F}$, according to lemma 3.) Let

$$\bar{g}(x) = p'(f(h_1(x)\,, h_2p^{-1}(x)\,,\ldots,h_kp^{-1}(x)))\,.$$

It follows from the definitions of the functions involved that

$$(15) \qquad \bar{g}(x) = v_i\,, \quad \text{for} \quad x \in V_i\,, \quad i = 1\,,2\,,3\,.$$

Furthermore, $\bar{g}(x)$ assumes a constant value v', for $x \in V_4$.

Suppose $v' \notin V_4$. Then $\bar{g}^2(x)$ is a function of genus 3 and type $[t_1, t_2, t_3]$ where at least one of the numbers t, say t_3, satisfies $1 \leqq t_3 < a$. This is due to (14) and the fact that $v' \in V_1 \cup V_2 \cup V_3$. Let the values assumed by $\bar{g}^2(x)$ be u_1, u_2 and u_3 where u_1 is assumed at least twice and u_3 exactly t_3 times. Choose numbers u_1^1, u_1^2 and u_3^1 such that $\bar{g}^2(u_1^1) = \bar{g}^2(u_1^2) = u_1$ and $\bar{g}^2(u_3^1) = u_3$. Furthermore, choose a permutation $p_1(x) \in \mathfrak{G}$ mapping the ordered triple (u_1, u_2, u_3) into the ordered triple (u_1^1, u_1^2, u_3^1). Then we may choose

$$g_1(x) = \bar{g}^2p_1\bar{g}^2(x)\,.$$

Clearly $g_1(x)$ is of type $[n - t_3, t_3]$ where $1 \leqq t_3 < a$.

Thus, we may assume that $v' = v_4 \in V_4$. The equations (15) may be written in the form

(16) $$\bar{g}(x) = v_i\,, \quad \text{for} \quad x \in V_i\,, \quad i = 1\,,2\,,3\,,4\,.$$

We say that a quadruple $(\zeta_1, \zeta_2, \zeta_3, \zeta_4)$ is a *permissible set of representatives* for the numbers v_i if there is a permutation in $\mathfrak{G}$ mapping v_i into ζ_i, $i = 1, 2, 3, 4$. Assume that the elements of some permissible set of representatives are contained in exactly three sets V_i and let $p_\zeta(x)$ be the corresponding permutation. Then the function $\bar{g}p_\zeta\bar{g}(x)$ is of type $[t_1, t_2, t_3]$ where $1 \leqq t_3 < a$. Proceeding as above, we obtain a function $g_1(x)$ as required. We may, therefore, assume that there is no permissible set of representatives whose elements are contained in exactly three sets V_i.

We shall now make use of the fact established above that the sets (13) are not of the same cardinality. If $\alpha(i)$ is a permutation of the numbers 1, 2, 3, 4 such that

$$\text{card}\,(V_{\alpha(1)}) \geqq \text{card}\,(V_{\alpha(2)}) \geqq \text{card}\,(V_{\alpha(3)}) \geqq \text{card}\,(V_{\alpha(4)})$$

then necessarily

(17) $$\text{card}\,(V_{\alpha(1)}) > \text{card}\,(V_{\alpha(4)})\,.$$

Furthermore, by (14),

(18) $$1 \leqq \text{card}\,(V_{\alpha(i)}) < \text{card}\,(E_2) = a\,, \quad \text{for} \quad i = 2\,,3\,,4\,.$$

Let $V_{\alpha(1)} = \{v^1_{\alpha(1)}\,, \ldots\,, v^\beta_{\alpha(1)}\}$. Consider the numbers v_i in the equations (16). Choose from $\mathfrak{G}$ β permutations $q_i(x)$, $i = 1\,, \ldots\,, \beta$, such that

$$q_i(v_{\alpha(1)}) = v_{\alpha(2)}\,,\; q_i(v_{\alpha(2)}) = v^i_{\alpha(1)}\,,\;\; q_i(v_{\alpha(3)}) = v_{\alpha(3)}\,.$$

Then, for all $i, q_i(v_{\alpha(4)}) \in V_{\alpha(4)}$ because, otherwise, we would obtain a permissible set of representatives whose elements are contained in exactly three sets V_i.

By (17), this implies that, for some μ and ν, $\mu \neq \nu$,

$$q_\mu(v_{\alpha(4)}) = q_\nu(v_{\alpha(4)}) = v^*_{\alpha(4)} \in V_{\alpha(4)}\,.$$

We have, thus, constructed the following two permissible sets of representatives which differ by one element only

(19) $$(v_{\alpha(2)}\,, v^\mu_{\alpha(1)}\,, v_{\alpha(3)}\,, v^*_{\alpha(4)})\,;\,(v_{\alpha(2)}\,, v^\nu_{\alpha(1)}\,, v_{\alpha(3)}\,, v^*_{\alpha(4)})\,.$$

We now choose from $\mathfrak{G}$ a permutation $q'(x)$ such that

$$q'(v^\mu_{\alpha(1)}) = v_{\alpha(2)}\,,\, q'(v^\nu_{\alpha(1)}) = v_{\alpha(3)}\,,\, q'(v_{\alpha(3)}) = v_{\alpha(1)}\,.$$

Consider the values

(20) $$q'(v_{\alpha(2)}) \quad \text{and} \quad q'(v^*_{\alpha(4)})\,.$$

Because the sets (19) are permissible and q' obviously maps a permissible set into a permissible set, the values (20) are both contained in the set $V_{\alpha(1)}$. Otherwise, we would obtain a permissible set of representatives whose elements are contained in exactly three sets V_i.

We may now choose

$$g_1(x) = \bar{g}q'q_\mu\bar{g}(x) \, .$$

The function $g_1(x)$ assumes the value $v_{\alpha(2)}$, for $x \in V_{\alpha(2)}$, and the value $v_{\alpha(1)}$, otherwise. By (18), it is of type $[n - a_1, a_1]$ where $1 \leqq a_1 < a$. This completes the proof of lemma 5.

Proof of the theorem. We assume first that $n \geqq 5, n \neq 2^r$ and $\mathfrak{G}$ is a triply transitive group of degree n. Let $f(x_1, \ldots, x_k)$ be an arbitrary function satisfying Słupecki conditions. To show that $\mathfrak{G}$ is basic for $\mathfrak{C}_n$, we prove that the set $\mathfrak{F}$ consisting of $\mathfrak{G}$ and f is complete.

By lemma 3, $\mathfrak{F}$ generates a function $g(x)$ of genus 2. This implies, by lemma 5, that $\mathfrak{F}$ is complete, provided $g(x)$ is not of type

$$[\tfrac{1}{2}n \, , \tfrac{1}{2}n] \, . \tag{21}$$

We assume that $g(x)$ is of type (21) and that E_1 and E_2 are disjoint subsets of N such that $\text{card}\,(E_1) = \text{card}\,(E_2) = \frac{1}{2}n$ and $g(x)$ assumes a constant value both in E_1 and in E_2. We shall now proceed as in the proof of lemma 5.

We form the sets $V_i, i = 1, 2, 3, 4,$ and obtain a function $\bar{g}(x)$ satisfying the equations (16). (Otherwise, we would obtain a function of genus 2 and not of type (21) which would complete the proof.) Furthermore, we may assume that the sets V_i are of the same cardinality because, otherwise, we could use the inequality (17) as in the proof of lemma 5. Thus, the set N is divided into subsets as follows:

N			
E_1		E_2	
V_1	V_4	V_2	V_3

We now form a new partition of N into V-sets by choosing from $\mathfrak{G}$ a permutation $\bar{p}(x)$ which maps some element of V_1 into itself and some other element of V_1 into V_3 and denoting

$$V_1^1 = E_1 \cap \bar{p}(E_1) \, , \; V_2^1 = E_2 \cap \bar{p}(E_1) \, , \; V_3^1 = E_2 \cap \bar{p}(E_2) \, , \; V_4^1 = E_1 \cap \bar{p}(E_2) \, .$$

Again, we may conclude that the sets V_i^1 are of the same cardinality. Furthermore, we may assume that the following equations hold:

$$\begin{aligned}(22)\quad \operatorname{card}(V_1 \cap V_1^1) &= \operatorname{card}(V_1 \cap V_4^1) = \operatorname{card}(V_4 \cap V_1^1) = \operatorname{card}(V_4 \cap V_4^1)\\ &= \operatorname{card}(V_2 \cap V_2^1) = \operatorname{card}(V_2 \cap V_3^1) = \operatorname{card}(V_3 \cap V_2^1)\\ &= \operatorname{card}(V_3 \cap V_3^1) = \tfrac{1}{2}\operatorname{card}(V_1) = \tfrac{1}{4}\operatorname{card}(E_1)\\ &= \tfrac{1}{8}\operatorname{card}(N) = \tfrac{1}{8}\, n\,.\end{aligned}$$

For if the equations (22) do not hold we may argue as follows. Assume that, for instance,

$$(23)\qquad \operatorname{card}(V_1 \cap V_1^1) > \operatorname{card}(V_1 \cap V_4^1)\,.$$

Let $V_1 \cap V_1^1 = \{\bar{v}_1, \ldots, \bar{v}_\gamma\}$. We choose from $\mathfrak{G}$ permutations $\pi_i(x)$, $i = 1, \ldots, \gamma$, such that $\pi_i(v_1) = \bar{v}_i$, $\pi_i(v_2)$ equals some fixed element in $V_4 \cap V_1^1$ and $\pi_i(v_3)$ equals some fixed element in $V_4 \cap V_4^1$. If, for some i, $\pi_i(v_4) \notin V_1 \cap V_4^1$ we obtain a function of genus 2 and not of type (21). If, for all i, $\pi_i(v_4) \in V_1 \cap V_4^1$ we obtain, by (23), two permissible sets of representatives differing by one element only. Then we may argue as in the proof of lemma 5.

Equations (22) express the fact that N is divided into subsets as follows:

(24)

N							
E_1				E_2			
V_1		V_4		V_2		V_3	
V_1^1	V_4^1	V_1^1	V_4^1	V_2^1	V_3^1	V_2^1	V_3^1

We continue the process by forming a new partition of N into sets V_i^2, $i = 1, 2, 3, 4$. If we do not obtain a function of genus 2 and of some type other than (21) we obtain equations corresponding to (22). The common cardinality of the sets involved equals $\dfrac{1}{16}\, n$.

By repeating the argument for new partitions of N, we conclude that we either obtain a function of genus 2 and not of type (21) or $n = 2^r$. Thus, the part of our theorem concerning triply transitive groups follows.

Assume that $n \geqq 5$ and $\mathfrak{G}$ is a quadruply transitive group of degree n. Let $\mathfrak{F}$ be as above. The completeness of $\mathfrak{F}$ follows because we may choose from $\mathfrak{G}$ a permutation mapping the numbers v_i, $i = 1, 2, 3, 4$, into exactly three of the sets V_i. We, thus, obtain a permissible set of representatives whose elements are contained in exactly three sets V_i.

Therefore, we have established our theorem. We note, finally, that the main difficulties in the proof are due to the fact that no analogues of lemma 1.2 in [3] are available.

3. *Special cases.* We shall now show that the condition $n \neq 2^r$ in the statement of our theorem is essential. If $n = 2^r$ ($r \geqq 2$) there is a triply transitive group of degree n which is not a basic group for $\mathfrak{E}_n$. In what follows, we shall discuss the case $n = 8$ in detail.

Let $\mathfrak{G}_8$ be the holomorph of an Abelian group of order 8 and type (1, 1, 1), expressed in the usual way as a permutation group of degree 8. $\mathfrak{G}_8$ is generated by the two permutations (1376528) and (17)(46). It is of order 1344 and consists of 384 7-cycles, 224 permutations of cyclic structure 3×3, 224 permutations of cyclic structure 6×2, 252 permutations of cyclic structure 4×4, 49 permutations of cyclic structure $2\times2\times2\times2$, 42 permutations of cyclic structure 2×2, 168 permutations of cyclic structure 4×2 and the identity. The group $\mathfrak{G}_8$ can also be characterized by the following six defining relations:

$$X^7 = 1\,,\ Y^2 = 1\,,\ (YX^3)^4 = 1\,,\ (YX)^6 = 1\,,$$
$$(YX^3YX^2YX)^2 = 1\,,\ YX^3(YX)^2YX^4YX^5YX^6YX^5 = 1\,.$$

Obviously, the holomorph of an Abelian group of order 2^r and type $(1, 1, \ldots, 1)$ (i.e. the holomorph of a so-called *generalized Klein group*) is triply transitive. In particular, $\mathfrak{G}_8$ is triply transitive.

However, $\mathfrak{G}_8$ is not a basic group for $\mathfrak{E}_8$. Consider the following function $f(x, y)$ which satisfies Słupecki conditions:

$$f(2x - 1\,, y) = y\,, f(2x\,, y) = 9 - y\,.$$

Then the set $\mathfrak{F}$ consisting of $\mathfrak{G}_8$ and $f(x, y)$ is not complete.

To prove this, we quote some terminology and notations, from section 2. We let $E_1 = \{1, 2, 3, 4\}$, $E_2 = \{5, 6, 7, 8\}$, $V_1 = \{1, 2\}$, $V_4 = \{3, 4\}$, $V_2 = \{5, 6\}$ and $V_3 = \{7, 8\}$. The following (unordered) quadruples are called permissible sets of representatives:

1234, 1256, 1278, 1357, 1368, 1458, 1467,

2358, 2367, 2457, 2468, 3456, 3478, 5678.

The permutations in $\mathfrak{G}_8$ always map a permissible set of representatives into a permissible set. Furthermore, they preserve the subset structure (24) of N.

Let $\mathfrak{F}_8 \subset \mathfrak{E}_8$ be the set consisting of the following 1-place functions:

1) Permutations in $\mathfrak{G}_8$.

2) Constants.

3) Those functions of type [2, 2, 2, 2] whose values form a permissible set of representatives and which, furthermore, assume a constant value in the sets V_1^i, V_2^i, V_3^i and V_4^i, for some $i = 1, \ldots, 7$, where

$$\begin{aligned}
&V_1^1 = \{1\,,2\}\,, && V_2^1 = \{3\,,4\}\,, && V_3^1 = \{5\,,6\}\,, && V_4^1 = \{7\,,8\}\,;\\
&V_1^2 = \{1\,,3\}\,, && V_2^2 = \{2\,,4\}\,, && V_3^2 = \{5\,,7\}\,, && V_4^2 = \{6\,,8\}\,;\\
&V_1^3 = \{1\,,4\}\,, && V_2^3 = \{2\,,3\}\,, && V_3^3 = \{5\,,8\}\,, && V_4^3 = \{6\,,7\}\,;\\
&V_1^4 = \{1\,,5\}\,, && V_2^4 = \{2\,,6\}\,, && V_3^4 = \{3\,,7\}\,, && V_4^4 = \{4\,,8\}\,;\\
&V_1^5 = \{1\,,6\}\,, && V_2^5 = \{4\,,7\}\,, && V_3^5 = \{2\,,5\}\,, && V_4^5 = \{3\,,8\}\,;\\
&V_1^6 = \{1\,,7\}\,, && V_2^6 = \{3\,,5\}\,, && V_3^6 = \{2\,,8\}\,, && V_4^6 = \{4\,,6\}\,;\\
&V_1^7 = \{1\,,8\}\,, && V_2^7 = \{4\,,5\}\,, && V_3^7 = \{2\,,7\}\,, && V_4^7 = \{3\,,6\}\,.
\end{aligned}$$

4) Those functions of type [4, 4] which, for some i, assume a constant value in one of the sets $V_1^i \cup V_2^i$, $V_1^i \cup V_3^i$ or $V_1^i \cup V_4^i$.

The set $\mathfrak{F}_8$ is closed under composition. In classes 1)—4) there are, respectively, 1344, 8, 2352 and 392 functions. Thus, card $(\mathfrak{F}_8) = 4096$. This number can be computed more directly as follows. $\mathfrak{F}_8$ consists of all functions which map every permissible set of representatives into a permissible set, a quadruple of type [2, 2] or of type [4]. (In what follows, quadruples of these three forms are called *permissible images*.) Thus, we may choose arbitrarily the values $h(1), h(2), h(3)$ of a function $h(x) \in \mathfrak{F}_8$. They determine uniquely the value $h(4)$. Again, $h(5)$ may be chosen arbitrarily but then the values $h(6), h(7), h(8)$ are uniquely determined. Hence,

$$\text{card}\,(\mathfrak{F}_8) = 8^4 = 4096\,.$$

Our function $f(x, y)$ forms a closure in the set $\mathfrak{F}_8$, i.e. if $g_1(x), g_2(x) \in \mathfrak{F}_8$ then also $f(g_1(x), g_2(x)) \in \mathfrak{F}_8$. To prove this, it suffices to show that if (i_1, i_2, i_3, i_4) and (j_1, j_2, j_3, j_4) are two permissible images then also

$$(f(i_1\,, j_1)\,, f(i_2\,, j_2)\,, f(i_3\,, j_3)\,, f(i_4\,, j_4))$$

is a permissible image. This can be readily verified by considering the matrix of $f(x, y)$.

Thus, $\mathfrak{F}$ generates no 1-place functions other than the functions in $\mathfrak{F}_8$. This proves that $\mathfrak{F}$ is not complete. Clearly, instead of the function $f(x, y)$, we may choose any function which satisfies Słupecki conditions and forms a closure in the set $\mathfrak{F}_8$.

Consider the general case[1]) $n = 2^r, r \geqq 3$. Let $\mathfrak{G}_{2^r}$ be the holomorph of an Abelian group of order 2^r and type $(1, 1\,, \ldots, 1)$. The order of this triply transitive group $\mathfrak{G}_{2^r}$ equals

$$2^r(2^r - 1)(2^r - 2)(2^r - 2^2) \cdots (2^r - 2^{r-1})\,.$$

[1]) We have regarded the case $n = 8$ as the first exceptional case. In fact, also the case $n = 4$ may be considered as exceptional, the exceptional group being the holomorph of the four-group (which equals the symmetric group of degree 4). Our theorem is not valid for $n = 3$ because lemma 3 is not valid in this case.

Define a function $\varphi(x, y) \in \mathfrak{E}_{2^r}$ as follows:

$$\varphi(2x - 1, y) = y, \quad \varphi(2x, y) = 2^r + 1 - y.$$

The function $\varphi(x, y)$ forms a closure in a set $\mathfrak{F}_{2^r}$ consisting of $2^{r(r+1)}$ 1-place functions. This implies that the set $\mathfrak{F}$ consisting of $\mathfrak{G}_{2^r}$ and $\varphi(x, y)$ is not complete. Hence, the group $\mathfrak{G}_{2^r}$ is not a basic group for $\mathfrak{E}_{2^r}$.

References

[1] Яблонский, С. В.: Функциональные построения в k-значной логике. - Тр. Матем. инст. им. В. А. Стеклова, 51 (1958), 5—142.

[2] Salomaa, A.: A theorem concerning the composition of functions of several variables ranging over a finite set. - J. Symbolic Logic 25 (1960), 203—208.

[3] —»— Some completeness criteria for sets of functions over a finite domain. I. - Ann. Univ. Turkuensis, Ser. A I 53 (1962).

Printed November 1963.