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

BY

ARTO SALOMAA

HELSEINKI 1963
SUOMALAINEN TIEDEAKATEMIA

https://doi.org/10.5186/aasfm.1964.338
Communicated 13 September 1963 by P. J. Myrberg and K. Inkeri
On basic groups for the set of functions over a finite domain

1. Results. Let \( \mathcal{C}_n \) be the set of functions whose variables, finite in number, range over a fixed finite set
\[
N = \{1, 2, \ldots, n\}, \quad n \geq 2
\]
and whose values are elements of \( N \). If \( \mathcal{F} \subset \mathcal{C}_n \) we denote by \( \overline{\mathcal{F}} \) the closure of \( \mathcal{F} \) under composition. \( \mathcal{F} \) is said to be complete if \( \overline{\mathcal{F}} = \mathcal{C}_n \).\(^1\)

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 \( \mathcal{F} \) of \( \mathcal{C}_n \) is a basic set for \( \mathcal{C}_n \) if \( \mathcal{F} \) is not complete but the addition to \( \mathcal{F} \) 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 \( \mathcal{C}_n \).

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

On the other hand, it is shown in [2] that the symmetric group of degree \( n \) is a basic group for \( \mathcal{C}_n \).\(^2\) Furthermore, according to [3], the alternating group of degree \( n \) is a basic group for \( \mathcal{C}_n \). (Obviously, the latter result implies the former.) These results are valid for all values of \( n \geq 5 \). Counterexamples 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 \( n \geq 5 \). In proofs of completeness criteria for subsets of \( \mathcal{C}_n \), 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 $\mathfrak{S}_n$. Counter-examples are found, for instance, by considering prime values of $n$ and linear groups. A triply transitive group is basic for $\mathfrak{S}_n$ if $n$ is not a power of 2. A quadruply transitive group is always basic for $\mathfrak{S}_n$ (provided the condition $n \geq 5$ 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 $\mathfrak{S}_n$, provided $n \geq 5$. If, in addition, $n = 2^r$ then every triply transitive group of degree $n$ is a basic group for $\mathfrak{S}_n$.

It is a consequence of this theorem that if a quadruply transitive group of degree $n$ is contained in the closure of a function $f \in \mathfrak{S}_n$ (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 $n = 2^r$, $r \geq 3$. It is very likely that the statement holds true for arbitrary triply transitive groups, perhaps even for arbitrary doubly transitive groups if $n \geq 3$.

In section 3, we consider the exceptional cases in our theorem: $n = 2^r$, $r \geq 3$. We construct a triply transitive group of degree $2^r$ which is not a basic group for $\mathfrak{S}_{2^r}$. 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 $\mathfrak{S}_n$) as defined in [3]. Assume that $G_i$, $i = 1, \ldots, k$, are non-empty subsets of $N$. Then, for any function $f(x_1, \ldots, x_k) \in \mathfrak{S}_n$, 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 $n \geq 3$ and $f(x_1, \ldots, x_k)$ satisfies Slupecki conditions. Then for any $j$, $3 \leq j \leq n$, 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 $n \geq 4$ and $\mathfrak{G} \subset \mathfrak{S}_n$ contains a triply transitive group $\mathfrak{G}$ (of degree $n$) and a function $f(x_1, \ldots, x_k)$ satisfying Slupecki conditions. Then $\mathfrak{G}$ 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 \( \mathcal{F} \) generates a function \( g(x) \) whose genus \( \gamma \) satisfies \( 1 < \gamma < n \).

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

\[
(1) \quad f(G_1, \ldots, G_k) = N
\]

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

\[
(2) \quad f(a'_1, \ldots, a'_k) = f(a_1, \ldots, a_k)
\]

and \( a'_i = a_i \), for \( i = 1, \ldots, k \). We choose from \( \emptyset \) \( k \) 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 \( \emptyset \) is doubly transitive. Then the function

\[
(2) \quad f(p_1(x), \ldots, p_k(x))
\]

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, \( \mathcal{F} \) 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

\[
(3) \quad f(b_1, b_2, \ldots, b_k) = b ,
\]

\[
(4) \quad f(b'_1, b_2, \ldots, b_k) = b'
\]

and

\[
(5) \quad f(b'_1, b'_2, \ldots, b'_k) = b'' .
\]

Consider the 1-place function

\[
g_1(x) = f(x, b_2, \ldots, b_k)
\]

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

\[
(6) \quad g_1(c_1) = b'' .
\]

Then necessarily \( c_1 \neq b_1, b'_1 \). Choose numbers \( c_2 \) and \( c_{3,i}, i = 2, \ldots, k \), such that \( c_2 = b_1, b'_1, c_1 \) and \( c_{3,i} = b_i, b'_i \) if \( b_i = b'_i \) but \( c_{3,i} = b_i \) if \( b_i = b'_i \). The choice is possible because \( n \geq 4 \).

Assume that

\[
(7) \quad f(c_2, c_{3,2}, \ldots, c_{3,k}) = b'' .
\]
Let \( q_i(x), \ i = 1, \ldots, k \), be constants in \( \mathcal{F} \) or permutations in \( \mathfrak{S} \), defined as follows. The function \( q_i(x) \) is a permutation such that \( q_1(1) = c_2, q_1(2) = b_1 \) and \( q_1(3) = b_1' \). Let \( 2 \leq i \leq k \) and \( b_i \neq b_i' \). Then \( q_i(x) \) is a permutation such that \( q_i(1) = c_i, q_i(2) = b_i \) and \( q_i(3) = b_i' \). Let \( 2 \leq i \leq k \) 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

\[
f(c_2, c_3, \ldots, c_k) = b''.
\]

Let \( q_1(x) \) be a permutation in \( \mathfrak{S} \) 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, \( \mathcal{F} \) generates a function \( g(x) \) whose genus \( \gamma \) satisfies \( 1 < \gamma < n \).

II. Assume that \( \gamma > 2 \). We shall now prove that \( \mathcal{F} \) generates a function \( h(x) \) whose genus \( \gamma_1 \) satisfies \( 2 \leq \gamma_1 < \gamma \). By repeating the argument, we may conclude that \( \mathcal{F} \) 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 \( \mathfrak{S} \) a permutation \( p(x) \) such that \( p(u) = u_1, p(v) = u_2 \) and \( p(v) = v_1 \). Then the function

\[
h(x) = gpg(x)
\]

is of genus \( \gamma_1 \) where \( 2 \leq \gamma_1 < \gamma \).

We have, thus, shown that \( \mathcal{F} \) 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 \( \mathfrak{S} \) a permutation \( q(x) \) such that \( q(d) = d_1 \) and \( q(d') = d_2 \). Then \( h_1 q h_1(x) = d \). Thus, \( \mathcal{F} \) generates the constant \( d \). Because \( \mathcal{F} \) contains a transitive group, we may conclude that \( \mathcal{F} \) generates all constants. Hence, lemma 3 follows.

**Lemma 4.** Assume that \( n \geq 3 \) and \( \mathcal{F} \subset \mathcal{G}_n \) contains a triply transitive group \( \mathfrak{S} \) (of degree \( n \)), a function \( f(x_1, \ldots, x_k) \) satisfying Slupecki conditions and a function \( g(x) \) of type \([n - 1, 1]\). Then \( \mathcal{F} \) 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 \( \mathcal{G}_n, n \geq 3 \).
Proof. Obviously, any function of type \([n - 1, 1]\) may be expressed in the form \(p_2p_1(x)\) where \(p_1(x)\) and \(p_2(x)\) are permutations belonging to \(\mathfrak{S}\). In fact, \(p_2\) may be chosen from any transitive subgroup of \(\mathfrak{S}\) and \(p_1\) may be chosen from any doubly transitive subgroup of \(\mathfrak{S}\). 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

\[
[n - i, 1, \ldots, 1]
\]

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

\[
[n - (i + 1), 1, \ldots, 1].
\]

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 \(h(x) \in \mathfrak{F}\).

The function \(h(x)\) assumes \(i + 2\) distinct values. Let \(\alpha_1\) 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 \(\text{card}(U)\)) is at least 2. Finally, let the other values assumed by \(h(x)\) be \(\alpha_2, \ldots, \alpha_{i+2}\) and let \(u_v\) be numbers such that \(h(u_v) = \alpha_v\), for \(v = 2, \ldots, i + 2\).

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

\[
f_1(x_1, \ldots, x_k) = p(f(x_1, \ldots, x_k)).
\]

Clearly, \(f_1(x_1, \ldots, x_k)\) satisfies Slupecki conditions. Therefore, it is possible to choose numbers \(\alpha^\mu_v, \mu = 1, \ldots, i - 1, v = 1, \ldots, k\), such that \(f_1\) applied to the \(\mu\)th row vector of the matrix

\[
\begin{vmatrix}
\alpha_1^1 & \cdots & \alpha_k^1 \\
\vdots & \ddots & \vdots \\
\alpha_1^{i-1} & \cdots & \alpha_k^{i-1}
\end{vmatrix}
\]

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:
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 \( \overline{\mathfrak{Y}} \). Because the functions \( h_i(x) \) satisfy this condition, we may conclude that \( h_i(x) \in \overline{\mathfrak{Y}} \), 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 \( \overline{\mathfrak{Y}} \).

We conclude, by induction, that all functions of type

\[
(12) \quad [2, 1, \ldots, 1] \quad \text{\( n-2 \) terms}
\]

are generated by \( \overline{\mathfrak{Y}} \). 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 \( \overline{\mathfrak{Y}} \) is complete.

**Lemma 5.** Assume that \( n \geq 3 \) and \( \overline{\mathfrak{Y}} \subset \mathfrak{E}_n \) 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 \( a = \frac{n}{2} \). Then \( \overline{\mathfrak{Y}} \) is complete.

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

By the hypothesis, \( n - a \not= a \). 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 \( a \geq 2 \). We shall show that \( \overline{\mathfrak{Y}} \) generates a function \( g_1(x) \) of type \([n - a_1, a_1] \) where \( 1 \leq a_1 < a \). By repeating the argument, we conclude that \( \overline{\mathfrak{Y}} \) generates a function of type \([n - 1, 1]\).
Let $E_1$ and $E_2$ be disjoint subsets of $N$ such that $\text{card}(E_1) = n - a$, $\text{card}(E_2) = a \geq 2$ and $g(x)$ assumes a constant value both in $E_1$ and in $E_2$. Because $\mathfrak{A}$ 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

$$
V_1 = E_1 \cap p(E_1), \quad V_2 = E_2 \cap p(E_1),
$$

$$
V_3 = E_2 \cap p(E_2), \quad V_4 = E_1 \cap p(E_2).
$$

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

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

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

$$
\text{card}(V_1) = \frac{1}{3} \text{card}(E_1) > \frac{1}{3} \text{card}(E_2) = \text{card}(V_3).
$$

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 $\mathfrak{G}$:

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

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

$$
\tilde{g}(x) = p'(f(h_i(x), h_2 p^{-1}(x), \ldots, h_k p^{-1}(x)))
$$

It follows from the definitions of the functions involved that

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

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

Suppose $v' \not\in V_4$. Then $\tilde{g}^2(x)$ is a function of genus 3 and type $[t_1, t_2, t_3]$ where at least one of the numbers $t_i$ is assumed at least twice and $u_3$ exactly $t_4$ times. Choose numbers $u_1, u_2$ and $u_3$ such that $\tilde{g}^2(u_1) = \tilde{g}^2(u_2) = u_1$ and $\tilde{g}^2(u_3) = u_3$. Furthermore, choose a permutation $p_1(x) \in \mathfrak{G}$ mapping the ordered triple $(u_1, u_2, u_3)$ into the ordered triple $(u_1', u_2', u_3')$.

Then we may choose

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

Clearly $g_1(x)$ is of type $[n - t_3, t_3]$ where $1 \leq t_3 < a$. 
Thus, we may assume that \( v' = v_4 \in V_4 \). The equations (15) may be written in the form
\[
\tilde{g}(x) = v_i, \quad \text{for} \quad x \in V_i, \quad i = 1, 2, 3, 4.
\]
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 \( \emptyset \) mapping \( v_i \) into \( \zeta_i \), \( i = 1, 2, 3, 4 \). 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 \( \tilde{g} \circ p_{\zeta}(x) \) is of type \([t_1, t_2, t_3]\) where \( 1 \leq t_3 < a \). 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
\[
\text{card} (V_{\alpha(1)}) \geq \text{card} (V_{\alpha(2)}) \geq \text{card} (V_{\alpha(3)}) \geq \text{card} (V_{\alpha(4)})
\]
then necessarily
\[
\text{card} (V_{\alpha(1)}) > \text{card} (V_{\alpha(4)}).
\]
Furthermore, by (14),
\[
1 \leq \text{card} (V_{\alpha(4)}) < \text{card} (E_2) = a, \quad \text{for} \quad i = 2, 3, 4.
\]
Let \( V_{\alpha(1)} = \{ v^{(1)}_{\alpha(1)}, \ldots, v^{(\beta)}_{\alpha(1)} \} \). Consider the numbers \( v_i \) in the equations (16). Choose from \( \emptyset \) \( \beta \) permutations \( q_i(x) \), \( i = 1, \ldots, \beta \), such that
\[
q_i(v_{\alpha(1)}) = v_{\alpha(2)}', \quad q_i(v_{\alpha(2)}) = v_{\alpha(1)}', \quad q_i(v_{\alpha(3)}) = v_{\alpha(3)}'.
\]
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 \( \mu \) and \( v, \mu = v \),
\[
q_\mu(v_{\alpha(4)}) = q_\mu(v_{\alpha(4)}) = v^*_{\alpha(4)} \in V_{\alpha(4)}.
\]
We have, thus, constructed the following two permissible sets of representatives which differ by one element only
\[
(v_{\alpha(2)}, v^*_{\alpha(1)}, v_{\alpha(3)}, v^*_{\alpha(4)}); \quad (v_{\alpha(3)}, v^*_{\alpha(4)}, v_{\alpha(3)}, v^*_{\alpha(4)}).
\]
We now choose from \( \emptyset \) a permutation \( q'(x) \) such that
\[
q'(v^*_{\alpha(1)}) = v_{\alpha(2)}, \quad q'(v^*_{\alpha(4)}) = v_{\alpha(3)}, \quad q'(v_{\alpha(3)}) = v_{\alpha(1)}.
\]
Consider the values
\[
q'(v_{\alpha(2)}) \text{ and } q'(v_{\alpha(3)}).
\]
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

\[ g_1(x) = \tilde{g}q'\tilde{g}(x) . \]

The function \( g_1(x) \) assumes the value \( v_{\alpha(2)} \) for \( x \in V_{\alpha(2)} \) and the value \( v_{\alpha(0)} \), otherwise. By (18), it is of type \([n - a_1, a_1]\) where \( 1 \leq a_1 < a \).

This completes the proof of lemma 5.

**Proof of the theorem.** We assume first that \( n \geq 5, n = 2^r \) and \( \emptyset \) 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 \( \emptyset \) is basic for \( \mathbb{C}_n \), we prove that the set \( \tilde{V} \) consisting of \( \emptyset \) and \( f \) is complete.

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

\[ (21) \quad \left[ \frac{1}{2}n, \frac{1}{2}n \right] . \]

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 \( \tilde{g}(x) \) 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 \( \emptyset \) a permutation \( \tilde{p}(x) \) which maps some element of \( V_1 \) into itself and some other element of \( V_1 \) into \( V_3 \) and denoting

\[ V_1^1 = E_1 \cap \tilde{p}(E_1), \quad V_2^1 = E_2 \cap \tilde{p}(E_1), \quad V_3^1 = E_2 \cap \tilde{p}(E_2), \quad V_4^1 = E_1 \cap \tilde{p}(E_2) . \]

Again, we may conclude that the sets \( V_i^1 \) are of the same cardinality. Furthermore, we may assume that the following equations hold:
For if the equations (22) do not hold we may argue as follows. Assume that, for instance,

\[ \text{card}(V_1 \cap V_1) \geq \text{card}(V_1 \cap V_1) \).

Let \( V_1 \cap V_1 = \{ \bar{v}_1, \ldots, \bar{v}_\gamma \} \). We choose from \( \mathcal{G} \) 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 \( V_4 \cap V_1 \) and \( \pi_i(v_3) \) equals some fixed element in \( V_4 \cap V_1 \). If, for some \( i \), \( \pi_i(v_4) \in V_1 \cap V_1 \) we obtain a function of genus 2 and not of type (21). If, for all \( i \), \( \pi_i(v_4) \in V_1 \cap V_1 \) 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:

<table>
<thead>
<tr>
<th></th>
<th>( E_1 )</th>
<th>( E_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( V_1 \cap V_1 )</td>
<td>( V_4 )</td>
<td>( V_1 \cap V_1 )</td>
</tr>
<tr>
<td>( V_1 \cap V_1 )</td>
<td>( V_1 \cap V_1 )</td>
<td>( V_1 \cap V_1 )</td>
</tr>
<tr>
<td>( V_1 \cap V_1 )</td>
<td>( V_1 \cap V_1 )</td>
<td>( V_1 \cap V_1 )</td>
</tr>
</tbody>
</table>

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 \( \frac{1}{16} n \).

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 \( n \geq 5 \) and \( \mathcal{G} \) is a quadruply transitive group of degree \( n \). Let \( \mathcal{G} \) be as above. The completeness of \( \mathcal{G} \) follows because we may choose from \( \mathcal{G} \) 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 \( n = 2^r \) in the statement of our theorem is essential. If \( n = 2^r \) \((r \geq 2)\) there is a triply transitive group of degree \( n \) which is not a basic group for \( G_n \). In what follows, we shall discuss the case \( n = 8 \) in detail.

Let \( G_8 \) be the holomorph of an Abelian group of order \( 8 \) and type \((1,1,1,1)\), expressed in the usual way as a permutation group of degree \( 8 \). \( G_8 \) is generated by the two permutations \((1376528)\) and \((17)(a6)\). It is of order \( 1344 \) and consists of 384 7-cycles, 224 permutations of cyclic structure \( 3 \times 3 \), 224 permutations of cyclic structure \( 6 \times 2 \), 252 permutations of cyclic structure \( 4 \times 4 \), 49 permutations of cyclic structure \( 2 \times 2 \times 2 \times 2 \), 42 permutations of cyclic structure \( 2 \times 2 \), and the identity. The group \( G_8 \) can also be characterized by the following six defining relations:

\[
\begin{align*}
X^7 &= 1, \\
Y^2 &= 1, \\
(YX^3)^4 &= 1, \\
(YX)^6 &= 1, \\
(YX^3YX^2YX)^2 &= 1, \\
YX^3(YX)^2YY^4YY^5YY^6YY^7 &= 1.
\end{align*}
\]

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, \( G_8 \) is triply transitive.

However, \( G_8 \) is not a basic group for \( G_n \). Consider the following function \( f(x,y) \) which satisfies Slupecki conditions:

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

Then the set \( \tilde{N} \) consisting of \( G_8 \) 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:

\[
\begin{align*}
1234, & \quad 1256, \quad 1278, \quad 1357, \quad 1368, \quad 1458, \quad 1467, \\
2358, & \quad 2367, \quad 2457, \quad 2468, \quad 3456, \quad 3478, \quad 5678.
\end{align*}
\]

The permutations in \( G_8 \) always map a permissible set of representatives into a permissible set. Furthermore, they preserve the subset structure \( (24) \) of \( N \).

Let \( \tilde{N}_8 \subseteq G_8 \) be the set consisting of the following 1-place functions:

1) Permutations in \( G_8 \).

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 \( V_1^i, V_2^j, V_3^k \) and \( V_4^l \), for some \( i = 1, \ldots, 7 \), where
\[ V_1^1 = \{1, 2\}, \ V_2^1 = \{3, 4\}, \ V_3^1 = \{5, 6\}, \ V_4^1 = \{7, 8\}; \]
\[ V_1^2 = \{1, 3\}, \ V_2^2 = \{2, 4\}, \ V_3^2 = \{5, 7\}, \ V_4^2 = \{6, 8\}; \]
\[ V_1^3 = \{1, 4\}, \ V_2^3 = \{2, 3\}, \ V_3^3 = \{5, 8\}, \ V_4^3 = \{6, 7\}; \]
\[ V_1^4 = \{1, 5\}, \ V_2^4 = \{2, 6\}, \ V_3^4 = \{3, 7\}, \ V_4^4 = \{4, 8\}; \]
\[ V_1^5 = \{1, 6\}, \ V_2^5 = \{4, 7\}, \ V_3^5 = \{2, 5\}, \ V_4^5 = \{3, 8\}; \]
\[ V_1^6 = \{1, 7\}, \ V_2^6 = \{3, 5\}, \ V_3^6 = \{2, 8\}, \ V_4^6 = \{4, 6\}; \]
\[ V_1^7 = \{1, 8\}, \ V_2^7 = \{4, 5\}, \ V_3^7 = \{2, 7\}, \ V_4^7 = \{3, 6\}. \]

4) Those functions of type \([4, 4]\) which, for some \(i\), assume a constant value in one of the sets \(V_i^1 \cup V_i^2, V_i^1 \cup V_i^3, \) or \(V_i^1 \cup V_i^4\).

The set \(\mathcal{G}_8\) is closed under composition. In classes 1)–4) there are, respectively, 1344, 8, 2352 and 392 functions. Thus, card \((\mathcal{G}_8) = 4096.

This number can be computed more directly as follows. \(\mathcal{G}_8\) consists of all functions which map every permissible set of representatives into a permissible set, a quadruple of type \([2, 2]\) or of type \([4, 4]\). (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 \(h \in \mathcal{G}_8\). 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,

\[ \text{card } (\mathcal{G}_8) = 8^4 = 4096. \]

Our function \(f(x, y)\) forms a closure in the set \(\mathcal{G}_8\), i.e. if \(g_1(x), g_2(x) \in \mathcal{G}_8\) then also \(f(g_1(x), g_2(x)) \in \mathcal{G}_8\). 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, \(\mathcal{G}\) generates no 1-place functions other than the functions in \(\mathcal{G}_8\). This proves that \(\mathcal{G}\) is not complete. Clearly, instead of the function \(f(x, y)\), we may choose any function which satisfies Slupecki conditions and forms a closure in the set \(\mathcal{G}_8\).

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

\[ 2^r(2^r - 1)(2^r - 2)(2^r - 2^3) \cdots (2^r - 2^{r-1}). \]

\(^1\) 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 \( \varphi(x, y) \in G_x \) as follows:

\[
\varphi(2x - 1, y) = y, \quad \varphi(2x, y) = 2^x + 1 - y.
\]

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

References