2) This integral exists in virtue of (1).
3) Which is bounded above.

Department of Mathematics, St. Paul's University.

ON FINITE GROUPS, WHOSE SYLOW-GROUPS ARE ALL CYCLIC

By Kin-ya HONDA

This is a complete exposition of the author's study, formerly reported as abstract with the same title in the Proceedings of the Japan Academy, Vol.25 (1949), No.5.

I. Structure Theory.

1) Hypercyclic Groups.

We shall call those finite groups, whose Sylow-groups are all cyclic, hypercyclic. The group of order 1 will also be called hypercyclic. The following properties are obtained easily from the definition.

1) Any subgroup of a hypercyclic group is hypercyclic.
2) Any group, homomorphic to a hypercyclic one, is hypercyclic.
3) Any abelian, hypercyclic group is cyclic.
4) Let \( p \) be a prime, and assume that \( p^k \) divides the order of a hypercyclic group \( G \), then any two subgroups of order \( p^k \) are conjugate.

In this paper we shall denote the l.c.m. of two integers \( a \), \( b \) as \( a \vee b \), and their g.c.f. as \( a \wedge b \). The order of a group \( G \) will be denoted as \([G]\).

Theorem 1. Let \( K \) be a normal subgroup of a hypercyclic group \( G \), and let \( H \) be any subgroup of \( G \). Then

\[
[H \cup K] = [H] \vee [K],
\]

\[
[H \cap K] = [H] \wedge [K].
\]

Proof. Let \( p \) be any prime dividing \([G]\), and let \( p^k \) and \( p^l \) be the highest powers of \( p \) dividing \([H]\) and \([K]\) respectively. Assume now that \( p^r \) is a subgroup of order \( p^{r+k+l} \), contained in \( G \). Then, by 4), \( p^r \leq H \wedge K \). Hence \( p^r \leq [H] \wedge [K] \). It follows that \( p^{r+k} \mid [H \cup K] \). Therefore \([H] \wedge [K] \mid [H \cap K]\). On the other hand, it is evident that \([H \cap K] \mid [H] \wedge [K]\). Hence we obtain (2). Now that
It follows that

\[ \frac{\langle x \rangle \cup \langle y \rangle}{\langle x \rangle \cap \langle y \rangle} = \frac{\langle x \rangle}{\langle x \rangle \cap \langle y \rangle} \uplus \frac{\langle y \rangle}{\langle x \rangle \cap \langle y \rangle}, \]

Thus we obtain the formula (1).

By this theorem we can prove easily the following properties.

5) If \( \mathcal{K} \) is a normal subgroup of a hypercyclic group \( \mathcal{G} \) and if \( \mathcal{H} \) is any subgroup of \( \mathcal{G} \), then \( \mathcal{H} \subseteq \mathcal{K} \) when \( [\mathcal{K}] \subseteq [\mathcal{H}] \), and \( \mathcal{H} \subseteq \mathcal{K} \) when \( [\mathcal{K}] [\mathcal{H}] = [\mathcal{H}] \).

6) If there exists a normal subgroup \( \mathcal{K} \) of order \( n \) in a hypercyclic group \( \mathcal{G} \), then there is no other subgroup of the same order \( n \).

7) Any normal subgroup of a hypercyclic group is a characteristic subgroup.

8) Let \( \mathcal{K} \) be a normal subgroup of a hypercyclic group \( \mathcal{G} \), and let \( \mathcal{K}' \) be a normal subgroup of \( \mathcal{K} \). Then \( \mathcal{K}' \) is a normal subgroup of \( \mathcal{G} \). For any characteristic subgroup of a characteristic subgroup is also characteristic, and therefore, normal.

9) If \( \mathcal{K} \) is a normal subgroup of a hypercyclic group \( \mathcal{G} \) and if \( \mathcal{H} \) and \( \mathcal{K} \) are two subgroups of \( \mathcal{G} \) such that \( \mathcal{H}, \mathcal{K} \) is a subgroup of \( \mathcal{G} \) and that \( [\mathcal{H}, \mathcal{K}] = 1 \), then

\[ \mathcal{K} \cap \mathcal{H} \cap \mathcal{K} = (\mathcal{K} \cap \mathcal{H}) \cap (\mathcal{K} \cap \mathcal{K}). \]

Proof. Of course we have

\[ \mathcal{K} \cap \mathcal{H} \cap \mathcal{K} \leq (\mathcal{K} \cap \mathcal{H}) \cap (\mathcal{K} \cap \mathcal{K}). \]

By assumption \( \mathcal{K} \cap \mathcal{H} \cap \mathcal{K} = \mathcal{E} \) (the unit subgroup of \( \mathcal{G} \)) and therefore

\[ (\mathcal{K} \cap \mathcal{H}) \cap (\mathcal{K} \cap \mathcal{K}) = \mathcal{E}. \]

Hence the number of elements of the right-hand of (3) is \( (\mathcal{K} \cap \mathcal{H}) \times (\mathcal{K} \cap \mathcal{K}) = (\mathcal{K} \cap \mathcal{H}) \times (\mathcal{K} \cap \mathcal{K}) = [\mathcal{K} \cap \mathcal{H}] = [\mathcal{K} \cap \mathcal{K}] = [\mathcal{K} \cap \mathcal{K}]. \)

Therefore in (3) the very equality holds.

2. First Splitting Theorem.

Let \( \mathcal{G} \) be a (not necessarily hypercyclic) group, which has a subgroup \( \mathcal{U} \) and a normal subgroup \( \mathcal{L} \), such that

\[ \mathcal{U} \cap \mathcal{L} = \mathcal{E}, \]

where \( \mathcal{E} \) denotes the unit subgroup of \( \mathcal{G} \). Then we say that \( \mathcal{G} \) has a splitting to \( \mathcal{U} \) and \( \mathcal{L} \). Every element \( a \) of \( \mathcal{U} \) gives rise to an automorphism

\[ \tau_a : x \mapsto a^{-1} x a \quad (x \in \mathcal{L}), \]

of the group \( \mathcal{L} \). If \( \tau_a \) correspond to \( a \), then we have a homomorphic mapping \( \sigma \) of \( \mathcal{U} \) into the group of automorphisms of \( \mathcal{L} \). Hence we denote the above splitting as

\[ \mathcal{G} = (\mathcal{U}, \mathcal{L}; \sigma). \]

Evidently the group \( \mathcal{G} \) is determined by these three factors \( \mathcal{U}, \mathcal{L} \) and \( \sigma \). Let \( \mathcal{F} \) be the kernel of this homomorphic mapping \( \sigma \). Then it is a normal subgroup of \( \mathcal{G} \) and we call it the foundation group of the splitting (1). In finite groups, the index \( \frac{[\mathcal{U} : \mathcal{F}]}{\mathcal{L}} \) will be called the \( \mathcal{S} \)-index of the splitting (1).

When there exist two systems of subgroups of a group \( \mathcal{G} \)

\[ \{a_1, a_2, \ldots, a_{r-1}, a_r\}, \quad \{b_1, b_2, \ldots, b_{r-1}, b_r\}, \quad \{c_1, c_2, \ldots, c_{r-1}, c_r\}, \]

and

\[ \{d_1, d_2, \ldots, d_{r-1}, d_r\}, \quad \{e_1, e_2, \ldots, e_{r-1}, e_r\}, \quad \{f_1, f_2, \ldots, f_{r-1}, f_r\}, \quad \{g_1, g_2, \ldots, g_{r-1}, g_r\}, \]

then we say that \( \mathcal{G} \) has a successive splitting to \( \mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_r \), and denote it as

\[ (1) \quad \mathcal{G} = (\mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_r; \sigma_1, \sigma_2, \ldots, \sigma_r). \]

Let \( f_i \) be the \( S \)-index of the splitting \( \mathcal{F}_{i+1} = (\mathcal{F}_i, \mathcal{U}_i; \sigma_i) \) \((i = 1, 2, \ldots, r-1)\), then we shall call the ordered system of integers \( f_1, f_2, \ldots, f_r \), the system of \( S \)-indices of the splitting (2).

First Splitting Theorem. Let the factorization into prime-powers of the order \( n \) of a hypercyclic group \( \mathcal{G} \) be

\[ n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}, \]

where \( p_1, p_2, \ldots, p_k \) are distinct primes. Then there exists a successive splitting

\[ (3) \quad \mathcal{G} = (\mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_r; \sigma_1, \sigma_2, \ldots, \sigma_r), \]

where every \( \mathcal{U}_i \) is a \( p_i \)-Sylow-group of \( \mathcal{G} \).

If \( \mathcal{U}_1 < \mathcal{U}_2 < \ldots < \mathcal{U}_r \), it holds evidently \( p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \) in this particular case the splitting (3) will be called the fundamental...
splitting of \( G \).

Proof. Let \( H \) be a \( \phi \)-Sylow-group of \( G \) and let \( \mathcal{H}_n \) be the group of automorphisms of \( H \). The order of \( \mathcal{H}_n \) is \( p^m = p^{n_1} \cdot p^{n_2} \), and is not divisible by \( p \), \( n > 1 \). Hence \( H \) is included in the centre of its normalizer. By the well-known theorem of Burnside there exists a normal subgroup \( \mathcal{A}_n \) of order \( \frac{p^m}{p^2} \) in \( G \). Similarly, there is a normal subgroup \( \mathcal{A}_2 \) of order \( \frac{p^m}{p^2} \) in \( H \). \( H \) is a normal subgroup of \( G \). Pushing this step forward, we have finally a normal subgroup \( \mathcal{G}_n \) of order \( \frac{p^m}{p^2} \) in \( G \). By the theorem of Schur (Zassenhaus 57, p.125) there exists a subgroup \( \mathcal{G}_{n-1} \) of order \( \frac{p^m}{p^2} \), and we have a splitting

\[ G = ( \mathcal{G}_{n-1}, \mathcal{G}_n \cup \sigma_n ). \]

Similarly we can split \( \mathcal{G}_{n-1} \) such as

\[ \mathcal{G}_{n-1} = ( \mathcal{G}_{n-2}, \mathcal{G}_{n-3} \cup \sigma_{n-3} ). \]

and so on. Finally we can reach the desired successive splitting.

\section{3. Simple Splitting.}

Let \( G \) be a hypercyclic group with a splitting

\[ G = ( G_0, G_1, \ldots ) \]

where \( G_0 \) is a Sylow-group of \( G \). Then we shall call it a simple splitting of \( G \). If we denote the foundation group of this splitting as \( F \), then \( F/\phi \) is isomorphic to a certain subgroup of the group \( \mathcal{H}_n \) of all automorphisms of \( G \). Since \( \mathcal{H}_n \) is abelian, it follows from 1), 2), and 3) of \( \S \) 1:

1) \( F/\phi \) is cyclic.

Now we shall denote as \( [G] = n \), \( [\mathcal{G}_n] = n_2 \).

\[ n = n_2 \cdot p^2 \]

where \( p \) is a prime. If there exists another subgroup \( \mathcal{G}' \), of order \( p^m \), \( \mathcal{G}' \) has a splitting

\[ G = ( \mathcal{G}', \mathcal{G}_n \cup \sigma' ). \]

Let \( \mathcal{G}' \) be the foundation group. Since

\[ G \cap \mathcal{P} = \mathcal{G}_n \cap \mathcal{P} = \epsilon, \]

every coset mod \( \mathcal{P} \) includes one and only one element of \( \mathcal{G}_n \), and also one and only one element of \( \mathcal{G}_n' \). Hence \( \mathcal{G}_n/\mathcal{P} \leq \mathcal{G}_n'/\mathcal{P}' \). It follows that \( F \) and \( F' \) have the same order, as they are normal subgroups of the same order, we get by 6) of \( \S \) 1:

2) \( F = F' \).

Now we can take \( \varepsilon \in G \) such that

\[ G = \mathcal{G}_n \cup \{ \varepsilon \}, \]

where \( \{ \varepsilon \} \) means the cyclic group generated by \( \varepsilon \). Then \( G \) is determined by \( F \) and \( \varepsilon \). As the number of elements of the coset including \( \varepsilon \) is \( \phi \), it follows that

3) In the group \( G \) there are at most \( \phi \) subgroups of order \( p^m \).

\section{4. The Group of Automorphisms of a Cyclic \( \phi \)-Group.}

Let \( \mathcal{P} \) be a cyclic group of order \( \phi \), where \( \phi \) is a prime, and let

\begin{align*}
\mathcal{P} = \mathcal{P}_n \circ \mathcal{P}_{n-1} \circ \cdots \mathcal{P}_0 = \epsilon
\end{align*}

be a descending series of subgroups of \( \mathcal{P} \), each of order \( \phi \), \( \phi^{-1}, \cdots, \phi^{-n} \).

Now we denote the group of automorphisms of \( \mathcal{P} \) as \( \mathcal{U} \). Those elements of \( \mathcal{U} \) against which all elements of \( \mathcal{P} \) are invariant, form a subgroup \( \mathcal{C}_n \) of \( \mathcal{U} \), and we have

\[ \mathcal{E} = \mathcal{C}_n \leq \mathcal{C}_{n-1} \leq \cdots \leq \mathcal{C}_1 \leq \mathcal{C}_0 = \mathcal{U}, \]

where \( \mathcal{E} \) denotes the unit subgroup of \( \mathcal{U} \). We shall call \( \mathcal{C}_n \) the invariant group on \( \mathcal{P} \). Now we calculate the orders of \( \mathcal{C}_n \).

\begin{align*}
\mathcal{P} = \{ \varepsilon \}, & \quad \text{then } \mathcal{P} = \{ \varepsilon \mathcal{C}_n \}.
\end{align*}

An automorphism

\[ \varepsilon \longrightarrow \varepsilon \mathcal{C}_n \]

is contained in \( \mathcal{C}_n \), if and only if \( \varepsilon \mathcal{C}_n \mathcal{C}_n^{-1} = \varepsilon \mathcal{C}_n^{-1} \), namely

\[ \varepsilon \mathcal{C}_n^{-1} = \varepsilon \mathcal{C}_n^{-1} \mathcal{C}_n^{-1} \]

i.e.
(2) Assume that $i \equiv 1 \pmod{\lambda}$. There are just $\lambda$ integers mod $\lambda^{*}$, which satisfy (2). Namely, they are $\lambda, \lambda^2, \lambda^3, \ldots, \lambda^{*}$, which are congruent mod $\lambda^{*}$ to an integer of (3). Hence there are $\lambda$ integers mod $\lambda^{*}$, which satisfy (2). Pushing this consideration forward, we shall finally find that there are (mod $\lambda^{*}$) $\lambda^{*}$ integers, which satisfy (2). As $i \equiv 1$, they are not divisible by $\lambda$. Hence we have:

1) The order $[C_i]$ of the invariant group $C_i$ on $\mathcal{P}$ is equal to $\lambda^{i-1}$ for $i \geq 1$.

We shall now denote the subgroup of $\mathcal{U}$, which is formed by all the elements of $\mathcal{U}$, that do not remove every coset of $\mathcal{P}$ mod $\mathcal{P}_i$, as $\mathcal{U}_i$. We shall call it the cosets-invariant group of $\mathcal{P}_i$. Then we have $\mathcal{U} = \mathcal{U}_0 \supset \mathcal{U}_1 \supset \cdots \supset \mathcal{U}_i \supset \mathcal{U}_n = \mathcal{P}$.

The automorphism $\alpha \rightarrow \alpha^* (\lambda \cdot \alpha)$ is an element of $\mathcal{U}$, if and only if $\alpha^{-1} \in \mathcal{U}_i = \{ \alpha \alpha^{-1} \}$, namely $\lambda \cdot \alpha = \lambda^{-1} \cdot \alpha (\lambda^*)$ for an integer $\lambda$, i.e., $\lambda^{i-1} \cdot \alpha = \lambda^{i-1} \cdot \alpha$, therefore $\alpha = \lambda^{i-1}$.

Assume that $i \equiv 1 \pmod{\lambda}$. Then there are $\lambda$ integers mod $\lambda^{*}$, which satisfy (4). They are not divisible by $\lambda$. Thus we get:

2) The order $[\mathcal{U}_i]$ of the cosets-invariant group on $\mathcal{P}$ is equal to $\lambda^*$ for $i \equiv 1 \pmod{\lambda}$.

5. Conjugate Theorem.

The main purpose of this paragraph is to prove the following

Conjugate Theorem. Let $\mathcal{S}_1$, $\mathcal{S}_2$ be two subgroups of a hyper-

cyclic group $\mathcal{S}$. If $[\mathcal{S}_1]$ is divisible by $[\mathcal{S}_2]$, a certain conjugate $\mathcal{S}_2 \cdot x$ of $\mathcal{S}_2$ includes $\mathcal{S}_2$. Hence, two subgroups of the same order are always conjugate.

Lemma 1. Let $\mathcal{G} = (\mathcal{G}_0, \mathcal{G}_1, \ldots, \mathcal{G}_n)$ be a simple splitting of $\mathcal{G}$ and let $[\mathcal{G}_i] = \mathcal{N}_i$. Then any subgroup of order $\mathcal{N}_i$ is a conjugate of $\mathcal{G}_i$.

We shall prove it for hypercyclic groups. For general groups (with a certain condition) confer Zassenhaus [p. 126].

Let $[\mathcal{G}] = \mathcal{N}$, $\mathcal{N} = \mathcal{N}_i \mathcal{N}_j$, $\mathcal{N}_i \mathcal{N}_j$ be the normaliser of $\mathcal{G}_i$ and $[\mathcal{G}_j] = \mathcal{N}_j$. Then

$[\mathcal{G}_j] = [\mathcal{G}_i \cdot \mathcal{N}_j] = [\mathcal{G}_i \mathcal{N}_j]$, where $\mathcal{G}_i$ is a subgroup of order $\mathcal{N}_i$, included in $\mathcal{G}_j$. Hence $\mathcal{N}_j \subseteq \mathcal{G}_j$, where $\mathcal{G}_j$ is the invariant group on $\mathcal{P}_i$. If $i \equiv 1 \pmod{\lambda}$, then $[\mathcal{G}_i] = \mathcal{N}_i^{*}$ by (1) of 1. On the other hand, we have $[\mathcal{G}_j] \cap [\mathcal{G}_i] = [\mathcal{P}] = 1$. Hence $\mathcal{G}_j = \mathcal{P}$ (the foundation group). Thus $\mathcal{G}_j$ is a normal subgroup of $\mathcal{G}$ and in this case our lemma follows from 6) of 1.

In case of $i = 0$, $\mathcal{N}_j = \mathcal{P}$. Hence there are $\mathcal{N}_j$ conjugates of $\mathcal{G}_j$. But there are at most $\mathcal{N}_j$ subgroups of order $\mathcal{N}_j$ (1), (2)). Therefore, every subgroup of order $\mathcal{N}_j$ is a conjugate of $\mathcal{G}_j$, q.e.d.

Lemma 2. For any subgroup $\mathcal{S}_i$, whose order is a divisor of $\mathcal{N}_j$, there exists an element $\alpha$ in $\mathcal{S}_i$, such that $\mathcal{S}_i \cdot \alpha = \mathcal{S}_i$.

Since $\mathcal{S}_i \cap \mathcal{P} = \mathcal{P}$, any coset mod $\mathcal{P}$ includes at most one element of $\mathcal{S}_i$. Thus, as in 1, we have an isomorphism between $\mathcal{S}_i$ and a certain subgroup $\mathcal{S}_i$ of $\mathcal{S}_j$, using the cosets mod $\mathcal{P}$ and moreover $\mathcal{S}_i \cap \mathcal{P} = \mathcal{S}_i \cdot \mathcal{P}$.

Applying lemma 1 to this hypercyclic group $\mathcal{S}_i \mathcal{P} = \mathcal{S}_i \mathcal{P}$, it holds for a certain element $\alpha \in \mathcal{S}_i$ $\mathcal{S}_i \cdot \alpha = \mathcal{S}_i \cdot \alpha \subseteq \mathcal{S}_i \cdot \mathcal{P}$.

If we write $\mathcal{S}_i = \alpha \cdot \mathcal{P}$ ( $\alpha \in \mathcal{S}_i$, $\alpha \in \mathcal{P}$), $\mathcal{S}_i \cdot \alpha = \mathcal{S}_i \cdot \alpha \subseteq \mathcal{S}_i \cdot \mathcal{P}$.
Lemma 3. Let \( S \) be any subgroup of \( G \). Then there exists \( x \in P \) such that
\[
x'' S x = S, P' \quad (S \leq G, P' \leq P).
\]
Let \( \{ S \} = \{ S' \} \quad (S \leq G, P' \leq P) \), then
\[
x'' S x = S, P' \quad ([S] = S, P' \leq P).
\]
Applying lemma 2 to \( S \), there exists \( x \in P \) such that
\[
x'' S x = S, P' \quad (S \leq G, P' \leq P).
\]
Then
\[
x'' x \times x = x'' x \times P' x = x'' x, P' \quad \forall x'.
\]

Proof of the theorem. The theorem is true for cyclic \( \alpha \)-groups.
Hence we take a simple splitting of \( G \)
\[
G = (S, P; \sigma)
\]
and assume that the theorem is true for \( G \). By lemma 3
\[
x'' S x = S, P' \quad (S \leq G, P' \leq P)
\]
for some \( x, x' \). Then \( P' \unlhd P'' \) and \([S] \) is divisible by \([S']\). By assumption
\[
\sigma S, \sigma S, \sigma S \in G.
\]
for some element \( \sigma \in G \). As \( P'' = P'' P \times \sigma \),
\[
(x, x') S, (x, x') = x'' (S, P'') x'' = x'' S, x'' P'' x'' \in S, (x, x') \in S.
\]
Hence
\[
(x, x') S, (x, x') \in S, \quad \forall x, x'.
\]
q.e.d.

Theorem 2. Let \( G = (S, P; \sigma) \) be a simple splitting of a hypercyclic group \( G \), and let \( F \) be the foundation group. If \( S' \) and \( P' \) are subgroups of \( S \) and \( P \) respectively, and if \( P' \) is not the unit group \( G \), then the foundation group \( F' \) of
\[
G' = (S', P'; \sigma)
\]
is \( G \cap F' \). Of course \( F' = G' \), when \( P' = G \).

Proof. Every element of \( F' \) is commutative with any element of \( P' \).
Hence \( P' \) is included in the invariant group on \( P' \). When \( P' = G \),
the invariant group is of order \( \alpha \). Hence \([P']^{\sigma} = 1 \) and it follows \( F' \leq F \). Therefore
\[
F' \leq G \cap F.
\]
On the other hand, every element of \( G \cap F \) is commutative with any element of \( P' \).
Hence
\[
G \cap F' \leq F'.
\]
Therefore we have the equality \( F' = G \cap F \). q.e.d.

Theorem 3. Let \( F \) be the foundation group of a simple splitting
\[
G = (S, P; \sigma)
\]
of a hypercyclic group \( G \) and let \( P = \{ a, [P] = \alpha \} \). If \( i \neq 0 \) \((\alpha)\), then
\[
G \cap \alpha' P = F.
\]

Proof. Since \( G / P \) is cyclic, we take \( c \) such that
\[
G = F \cdot \{ c \}.
\]
Then \( a' G a' = F \cdot \{ c' a' \} \). Let any element of \( G \cap a' P \) be
\[
\beta = f, c' = f, a' a' c' = (f, f, e) \quad \forall \beta \in F
\]
and let \( c' a' c' = a' \). Then \( c' a' c' = a' \). Hence \( c' a' c' = a' \).
\[
\sigma c' \quad \sigma \sigma c = c' \quad \text{and we get}
\]
\[
f, c' = f, c' \sigma a' \sigma a' c' = f, c' \sigma a' \sigma a' c'.
\]
As \( f, c' \) and \( f, c' \sigma a' \sigma a' c' \) are contained in \( G \), and as \( G \cap P = \{ c \} \) we have
\[
\sigma c' \sigma a' \sigma a' c' = c'.
\]
Hence \( \sigma c' \sigma a' \sigma a' = c' \), and by the assumption of the theorem
\[
\beta = (\sigma c') \sigma a' \sigma a' c' = (\sigma c') \sigma a' \sigma a' c'.
\]
Now that \( c' a' c' = a' \), this congruence implies that \( \sigma c') \sigma a' \sigma a' c' \)
is contained in the invariant group on the group \( \alpha' \), which is of order \( \alpha \). Thus, alike before, the order of \( c') \sigma a' \sigma a' c' \) is 1, and therefore
\[
\sigma c' \sigma a' \sigma a' c' = c' \in F.
\]
Hence \( \sigma c' \sigma a' \sigma a' c' = c' \), and it follows
\[
G \cap a' P = F.
\]
The converse relation \( 2 \) follows from \( 2 \) of \( \beta \). Hence we reach the equality. q.e.d.
§ 6. Reduction Theorems.

Let

\[ \varphi = (\mathcal{F}, \mathcal{P}; \sigma) \]

be a simple splitting of a hypercyclic group \( \mathcal{F} \), and let \( \mathcal{K} \) be an arbitrary normal subgroup of \( \mathcal{F} \). Then by \( 8 \) of \( \S 1 \)

\[ \mathcal{K} = \mathcal{K} \cdot \mathcal{P}', \]

where \( \mathcal{K} = \mathcal{K} \cap \mathcal{F} \) and \( \mathcal{P}' = \mathcal{K} \cap \mathcal{P} \), and \( \mathcal{K} \) is a normal subgroup of \( \mathcal{F} \). But, for an arbitrary normal subgroup \( \mathcal{K}_0 \) of \( \mathcal{F} \), \( \mathcal{K} \cdot \mathcal{P}' \) is not necessarily a normal subgroup of \( \mathcal{F} \). Now we shall prove the following

**Reduction Theorem on Normal Subgroups.** Let

\[ \varphi = (\mathcal{F}, \mathcal{P}; \sigma) \]

be a simple splitting of a hypercyclic group \( \mathcal{F} \) and let \( \mathcal{F} \) be its foundation group. If \( \mathcal{K}_0 \) and \( \mathcal{P}' \) are normal subgroups of \( \mathcal{F}_0 \) and \( \mathcal{P}' \) respectively,

1. \( \mathcal{K} \cdot \mathcal{P}' \) is always a normal subgroup of \( \mathcal{F} \),
2. \( \mathcal{K} \cdot \mathcal{P}' \cdot (\mathcal{P}' \cdot \mathcal{P}) \) is a normal subgroup of \( \mathcal{F} \), if and only if \( \mathcal{K}_0 \subseteq \mathcal{F} \).

**Proof.** We shall prove first that \( \mathcal{K} \cdot \mathcal{P}' \) is a normal subgroup of \( \mathcal{F} \), if and only if \( \mathcal{K}_0 \) is included in the cosets-invariant group on \( \mathcal{P}' \).

Let \( \xi, \xi' \in (\mathcal{K} \cdot \mathcal{P}') \) be arbitrary elements of \( \mathcal{K} \cdot \mathcal{P}' \) and let \( \xi \) be an arbitrary element of \( \mathcal{P}' \). Since \( \mathcal{K}_0 \) is normal in \( \mathcal{F}_0 \) and \( \varphi = \mathcal{F}, \mathcal{P}, \mathcal{K} \cdot \mathcal{P}' \) is normal in \( \mathcal{F} \), if and only if

\[ \xi' \xi \xi' = \xi \cdot \mathcal{K} \cdot \mathcal{P}' \]

namely

\[ \xi' \xi \xi' = \xi \cdot \mathcal{K} \cdot \mathcal{P}' \quad (\xi, \xi' \in \mathcal{K} \cdot \mathcal{P}') \]

As \( \mathcal{K} \cdot \mathcal{P}' = \mathcal{K} \cdot \mathcal{P} \), put

\[ \xi' \xi = \xi \cdot \mathcal{K} \cdot \mathcal{P}' \]

From (1) it follows

\[ \xi' \xi \xi' = \xi \cdot \mathcal{K} \cdot \mathcal{P}' \]

i.e.

\[ \xi' \xi = \xi \cdot \mathcal{K} \cdot \mathcal{P}' \]

\[ \xi' \xi = \xi' \xi \]

\[ \xi' \xi = \xi' \xi \]

Since \( \mathcal{P} \) is abelian, (4) can be written as

\[ \xi' \xi = \xi' \xi \]

hence

\[ \xi' \xi = \xi' \xi \]

But from (2) it follows

\[ \xi' \xi = \xi' \xi \]

and therefore (6) shows that every coset of \( \mathcal{P} \) mod \( \mathcal{P}' \) is invariant by any element of \( \mathcal{K}_0 \). Conversely, if (6) holds, then we put \( \xi' \xi = \xi' \xi \)

and we get

\[ \xi' \xi = \xi' \xi \]

Thus

\[ \xi' \xi = \xi' \xi \]

and we have (1), i.e. \( \mathcal{K} \cdot \mathcal{P}' \) is normal in \( \mathcal{F} \).

\( \mathcal{K} \cdot \mathcal{P} \) is normal for the cosets-invariant group on \( \mathcal{P} \) is the entire group of all the automorphisms of \( \mathcal{P} \).

If \( \mathcal{P}' \neq \mathcal{P} \), then by \( 2 \) of \( \S 4 \), \( \mathcal{K} \cdot \mathcal{P}' \) is normal if and only if the order of \( \mathcal{K}_0 \) is equal to 1, i.e.

\( \mathcal{K}_0 \subseteq \mathcal{F} \).

q.e.d.

The commutator group \( \mathcal{E} \) of a hypercyclic group \( \mathcal{F} \) is characterized by the following properties:

1. \( \mathcal{E} \) is normal in \( \mathcal{F} \) and \( \mathcal{F} / \mathcal{E} \) is cyclic.
2. If \( \mathcal{K} \) is normal in \( \mathcal{F} \) and \( \mathcal{F} / \mathcal{K} \) is cyclic, then \( \mathcal{K} \) includes \( \mathcal{E} \).

**Reduction Theorem on Commutator Groups.** Let

\[ \varphi = (\mathcal{F}, \mathcal{P}; \sigma) \]

be a simple splitting of a hypercyclic group \( \mathcal{F} \), and let \( \mathcal{K}, \mathcal{K}_0 \) be the commutator groups of \( \mathcal{F}, \mathcal{F}_0 \) respectively. Then, in case of \( \varphi = \mathcal{F}, \mathcal{P} \),

\[ \mathcal{E} = \mathcal{K}_0 \cdot \mathcal{P} \]

and in another case

\[ \mathcal{E} = \mathcal{K}_0 \cdot \mathcal{P} \]

**Proof.** As \( \mathcal{K}_0 \) is normal in \( \mathcal{F} \) and \( \mathcal{F} \cap \mathcal{P} = \mathcal{E} \),
\[ \frac{\gamma \cdot \mathfrak{p}}{\mathfrak{p} \cdot \mathfrak{p}} \simeq \frac{\gamma}{\mathfrak{p}}. \]

The right-hand of this isomorphism is cyclic, and \( \gamma = \gamma \cdot \mathfrak{p} \). Hence
\[ \mathfrak{p} \cdot \mathfrak{p} \geq \mathfrak{p}. \]

Since \( \mathfrak{p} \) is normal in \( \gamma \), by 9) of \( \gamma \)
\[ \mathfrak{p} = (\gamma \cap \mathfrak{p})(\gamma \cap \mathfrak{p}). \]

It follows that
\[ \frac{\gamma}{\gamma \cap \mathfrak{p}} \simeq \frac{\gamma}{\mathfrak{p}}. \]

The left-hand is cyclic. Hence
\[ \mathfrak{p} \cap \gamma \simeq \mathfrak{p}. \]

But \( [\mathfrak{p} \cap \gamma] \) divides \( [\gamma] \) by (7) and (8). Therefore
\[ \mathfrak{p} \cap \gamma \simeq \mathfrak{p}. \]

It follows
\[ \mathfrak{p} = \frac{\mathfrak{p}}{\mathfrak{p} \cap \gamma}. \]

Let \( \mathfrak{f} \) be the foundation group of \( (\gamma, \mathfrak{p}, \mathfrak{f}) \). As \( \gamma / \mathfrak{f} \) is cyclic, \( \mathfrak{f} \simeq \gamma \). Hence (10) implies
\[ \mathfrak{p} = \mathfrak{p} \cdot \mathfrak{f} \cdot \gamma. \]

If \( \mathfrak{p} = \mathfrak{f} \cdot \gamma \), then evidently
\[ \mathfrak{p} = \mathfrak{f} \cap \gamma \]

for \( \mathfrak{f} \) is the commutator group of \( \gamma \).

If \( \mathfrak{f} \neq \mathfrak{f} \), then \( \mathfrak{f} \cap \gamma \neq \mathfrak{f} \); for otherwise the subgroup \( \gamma \cdot (\mathfrak{f} \cap \gamma) \) is not normal in \( \gamma \) by Reduction Theorem on Normal \( \gamma \) Subgroups, and, on the other hand,
\[ \frac{\gamma}{\gamma \cdot (\mathfrak{f} \cap \gamma)} \simeq \frac{\mathfrak{f} \cap \gamma}{\mathfrak{f} \cap \gamma} = \mathfrak{f}, \]

and \( \frac{\gamma}{\mathfrak{f} \cap \gamma} \) is cyclic, hence \( \frac{\gamma}{\gamma \cdot (\mathfrak{f} \cap \gamma)} \) is normal in \( \gamma \). That (1) is a contradiction. Hence \( \gamma \cap \mathfrak{p} = \mathfrak{p} \), and we get from (10)
\[ \mathfrak{p} = \mathfrak{f} \cap \gamma. \]

q.e.d.

The following theorem is evident by the above one.

Theorem 4. The commutator group of a hypercyclic group is a direct product of several Sylow-groups, and therefore cyclic.

Now, by Schur's theorem (Zassenhaus') p.155), we obtain.

Second Splitting Theorem. Any hypercyclic group \( \gamma \) has a splitting \( \gamma = (\gamma, \mathfrak{p}, \mathfrak{f}) \), where \( \gamma \) and \( \mathfrak{f} \) are cyclic and \( [\gamma] \cdot [\mathfrak{f}] = 1 \), and conversely. We can take the commutator group of \( \gamma \) for \( \mathfrak{f} \), (cf. Zassenhaus') p.139)

The following theorem is a generalization of a theorem of O. Hölder concerning groups of order \( \mathfrak{p} \mathfrak{q} \cdots \mathfrak{r} \), where \( \mathfrak{p} \) denote different primes. (cf. Burnside') p.358)

Theorem 5. Let
\[ \mathfrak{p}, \mathfrak{p}, \ldots, \mathfrak{p}, \mathfrak{q} \]

be all the normal Sylow-groups of a hypercyclic group \( \gamma \) and let \( \mathfrak{f} \) be their product \( \mathfrak{p}, \mathfrak{p}, \ldots, \mathfrak{p}, \mathfrak{q} \). Then \( \gamma / \mathfrak{p} \) and \( \mathfrak{f} \) are cyclic.

Proof. Since \( \mathfrak{p} = \mathfrak{p}, \mathfrak{p}, \ldots, \mathfrak{p}, \mathfrak{q} \), \( \mathfrak{f} \) is cyclic. Let \( \mathfrak{p} \) be the commutator group of \( \gamma \). By Theorem 4, any Sylow-group of \( \mathfrak{p} \) is a normal Sylow-group of \( \gamma \). Hence \( \mathfrak{p} \leq \mathfrak{f} \), and \( \gamma / \mathfrak{p} \) is cyclic, q.e.d.

Now we shall call the centraliser \( \mathcal{U} \) of the commutator group \( \mathfrak{p} \) of a hypercyclic group \( \gamma \) the ramification kernel of \( \gamma \), and shall call
\[ [\gamma : \mathcal{U}] \]

the ramification constant of \( \gamma \). Since \( \mathfrak{p} \leq \mathfrak{f} \), \( \gamma / \mathcal{U} \) is cyclic.

Reduction Theorem on Ramification Kernels. Let
\[ \gamma = (\gamma, \mathfrak{p}, \mathcal{U}) \]

be a simple splitting of a hypercyclic group \( \gamma \) and let \( \mathfrak{p} \) be the foundation group. Denoting the ramification kernels of \( \gamma, \mathfrak{f} \) as \( \mathcal{U}, \mathcal{U} \), respectively, we have
\[ \mathcal{U} = (\mathcal{U} \cap \mathfrak{p}) \times \mathfrak{p}. \]

Proof. In case of \( \gamma = \gamma, \mathfrak{p}, \mathfrak{f} = \mathcal{U} \mathfrak{p} \), and we can see easily
\[ \gamma = (\mathfrak{p} \cap \gamma) \times \mathfrak{p}. \]

Now we assume that \( \mathfrak{f} \neq \mathfrak{f} \). Then \( \mathfrak{p} = \mathfrak{f} \mathfrak{p} \). As \( \mathfrak{p} \leq \mathfrak{f} \), we get
\[ \mathcal{U} = \mathfrak{f} \mathfrak{p} (\mathfrak{p} = \mathcal{U} \cap \gamma). \]

Since \( \mathcal{U} \leq \mathcal{U} \) and \( \mathfrak{p} \leq \mathfrak{f} \), every element of \( \mathcal{U} \) is commutative with any element of \( \mathfrak{p} \). Hence
\[ \mathcal{U} = \mathfrak{f} \mathfrak{p} \mathcal{U} \leq \mathfrak{f} \mathfrak{p}. \]

As \( \mathfrak{p} = (\mathfrak{f} \cap \gamma) \mathfrak{p} \), Hence

-17-
Conversely, every element of \( V\cap F \) is commutative with any element of \( V \) and also with any element of \( K \). Hence \( V\cap F = V' \). Since 
\[ V \cap F = V', \]
we get
\[ V = ( V \cap F ) \times P. \]

By (11), (12), (13) it holds
\[ V = ( V \cap F ) \times P. \]

Now we calculate the ramification constant.

**Theorem 6.** Let 
\[ f, f_2, \ldots, f_{r-1} \]
be the system of \( S \)-indices of a successive splitting of a hypercyclic group \( G \) to its Sylow-groups. Then the ramification constant \( v \) of \( G \) is equal to 
\[ v = f, v = f_2, \ldots, v = f_{r-1}. \]

**Proof.** Assume that the above successive splitting is obtained from the simple splitting 
\[ G = ( G_\infty, P \; ; \; v ) \]
by pursuing further splittings. Denoting the ramification kernels of \( G, \; G_\infty \) as \( K, \; K_\infty \) respectively and the foundation group as \( F \), we have
\[ V = ( V_\infty \cap F ) \times P. \]

Hence it follows
\[
\begin{align*}
[ G : V ] &= \left[ G_\infty, P \; ; \; ( V_\infty \cap F ) \times P \right] \\
&= \left[ G_\infty, V_\infty \cap F \right] \\
&= \left[ G_\infty, \frac{V_\infty \cap F}{[ V_\infty \cap F ]} \right] \\
&= \left[ V_\infty, \frac{V_\infty \cap F}{[ V_\infty \cap F ]} \right] \\
&= \left[ V_\infty, \frac{V_\infty \cap F}{[ V_\infty \cap F ]} \right] \\
&= \left[ G_\infty, V_\infty \cap F \right].
\end{align*}
\]

Since the ramification constant of a cyclic \( K \)-group is equal to 1, we have by induction 
\[ v = f, v = f_2, \ldots, v = f_{r-1}. \]

Finally we shall return to general subgroups and shall prove the last reduction theorem:

**Reduction Theorem on Subgroups.** Let 
\[ G = ( G_\infty, P \; ; \; v ) \]
be a simple splitting of a hypercyclic group \( G \) and let \( P = \{ a \} \),
then \( G_\infty, G_\infty' \) are subgroups of \( G_\infty \) and \( P_1, P_2 \) are subgroups of \( P \), it holds
\[ a^{-i}, a^{-i}, P_1, a^{-i}, P_2, a^{-i}. \]
If and only if,
\[ f_0 \geq f_2, \quad P_1 \leq P_2. \]
and in case of \( f_0 \geq f_2 \), with additional condition
\[ a^{-i} \in P. \]

We remark that any subgroup of \( G \) can be written in the form
\[ a^{-i} G_\infty, P_1 \]
(§6, Lemma 3)

**Proof.** We get from (14)
\[ f_0, f_2 \geq a^{-i}, f_2, a^{-i}, P_2. \]

Hence we have
\[ [ a^{-i}, G_\infty, a^{-i}, P_1 ] \]
\[ [ P_1 ] \]
(14)
Then (16) is readily obtained from (10). By (10) and Lemma 2 in §5, it holds for \( a \in P \),
\[ f_0 \geq f_2, \quad a \in P_1, \quad a \in P_2, \quad a \in P_2. \]

Hence
\[ f_0 \geq f_2, \quad a \in P_1, \quad a \in P_2, \quad a \in P_2. \]

If \( f_0 \geq f_2 \), every element of \( f_2 \) is commutative with \( a \).

Hence we obtain (15) from (21).

In case of \( f_0 \geq f_2 \), by Theorem 3 in §5 and (22) we can conclude,
\[ a^{-i} \in \{ a \}, \]
(1.e.
\[ a^{-i} \in P, \]
namely the condition (17), and (21) turns out to be (15).

Conversely, if \( f_0 \geq f_2 \) and (16) as well as (15) holds, then we have (16) and therefore (14). If \( f_0 \geq f_2 \) and (15), (16), (17) hold,
then

\[ \mathcal{S}_1, \mathcal{P}_2 \geq a, b, c, d \geq \mathcal{S}_2, \mathcal{S}_3, a, b, c \]

Hence we obtain (16) and therefore (14). q.e.d.

II. Classification Theory.

3.1. \( L \)-Similar Classes.

The lattice, made by all subgroups of a group \( \mathcal{G} \), will be denoted as \( L(\mathcal{G}) \). Two finite groups \( \mathcal{G} \) and \( \mathcal{F} \) will be called \( L \)-similar, and will be denoted as \( \mathcal{G} \cong \mathcal{F} \), when there exists a lattice-isomorphic correspondence \( \mathcal{P} \) of \( L(\mathcal{G}) \) and \( L(\mathcal{F}) \) with the following properties:

1) Any two corresponding subgroups are of the same order.

2) Let \( \mathcal{S}_1, \mathcal{S}_2 \) be subgroups of \( \mathcal{G} \), which is a subgroup of \( \mathcal{G} \), and let \( \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3 \) be the corresponding subgroups of \( \mathcal{F} \) respectively. If \( \mathcal{S}_1 \) and \( \mathcal{S}_2 \) are conjugate in \( \mathcal{G} \), then \( \mathcal{S}_1 \) and \( \mathcal{S}_2 \) are also conjugate in \( \mathcal{F} \), and conversely.

This is entirely the same notion as A. Rottlaender's "Situations-trenheit". But in this paper we adopt the word of \( L \)-similarity. In the author's paper, which we mentioned at the beginning, this word has been used in a bit weaker sense, nevertheless the two definitions coincide to each other in case of hypercyclic groups. For a slight generalization of this notion confer Baer 11.

We remark first that \( L \)-similar groups are of the same order.

Some of the following properties have been mentioned in the paper of Rottlaender.

1) If (by an \( L \)-similar correspondence) \( \mathcal{F} \) corresponds to \( \mathcal{G} \), then \( \mathcal{F} \) and \( \mathcal{G} \) are \( L \)-similar.

2) If \( \mathcal{F} \) corresponds to \( \mathcal{G} \), then the normaliser of \( \mathcal{F} \) corresponds to that of \( \mathcal{G} \).

3) To a normal subgroup always corresponds a normal subgroup.

4) A decomposition into direct product always leads to such a decomposition in the corresponding group:

\[ \mathcal{G} = \mathcal{A} \times \mathcal{B} \leftrightarrow \mathcal{F} = \mathcal{C} \times \mathcal{D} \]

5) To a cyclic \( \mathcal{A} \)-group always corresponds an isomorphic cyclic \( \mathcal{A} \)-group. For the subgroup lattice of a cyclic \( \mathcal{A} \)-group is a chain and conversely.

6) Let \( \mathcal{A} \) and \( \mathcal{B} \) be corresponding normal subgroups of \( \mathcal{G} \) and \( \mathcal{F} \) respectively. If \( \mathcal{A}/\mathcal{B} \) is abelian, then \( \mathcal{A}/\mathcal{B} \) is also abelian, and \( \mathcal{A}/\mathcal{B} \cong \mathcal{F}/\mathcal{B} \).

Proof. Let \( \mathcal{A}, \mathcal{A}_1, \ldots, \mathcal{A}_m \) be normal subgroups of \( \mathcal{G} \) such that \( \mathcal{A}/\mathcal{B} = \mathcal{A}_1/\mathcal{B} \times \mathcal{A}_2/\mathcal{B} \times \cdots \times \mathcal{A}_m/\mathcal{B} \) and that \( \mathcal{A}_i/\mathcal{B} \) is cyclic \( \mathcal{A} \)-group \((i = 1, 2, \ldots, m)\). Then, by \( L \)-similar correspondence,

\[ \mathcal{A}/\mathcal{B} = \mathcal{A}_1/\mathcal{B} \times \mathcal{A}_2/\mathcal{B} \times \cdots \times \mathcal{A}_m/\mathcal{B} \]

where \( \mathcal{A}_i/\mathcal{B} \) corresponds to \( \mathcal{A}_i \). Since the subgroups between \( \mathcal{A}_i \) and \( \mathcal{B} \) form a chain, \( \mathcal{A}_i/\mathcal{B} \) is a cyclic \( \mathcal{A} \)-group isomorphic to \( \mathcal{A}_i/\mathcal{B} \).

q.e.d.

7) To an abelian group corresponds an isomorphic abelian group, and to a cyclic, an isomorphic cyclic one. For the proof we have only to take the unit subgroup \( \mathcal{E} \) for \( \mathcal{A} \) in 6).

8) To the commutator group of \( \mathcal{G} \) corresponds that of \( \mathcal{F} \).

9) To the centraliser of a subgroup \( \mathcal{S} \) corresponds that of \( \mathcal{S} \).

Proof. The centraliser of \( \mathcal{F} \) is characterised as the join of all such cyclic groups \( \mathcal{A} \) that \( \mathcal{A} \cup \mathcal{A} \) is abelian, where \( \mathcal{A} \) is an arbitrary cyclic subgroup of \( \mathcal{F} \).

q.e.d.

10) To the ramification kernel of a (hypercyclic) group \( \mathcal{G} \) corresponds that of \( \mathcal{F} \).

11) To a hypercyclic group always corresponds a hypercyclic one.

12) In case of hypercyclic groups the condition 2) in the definition of \( L \)-similarity is superfluous. This is obvious by Conjugateness Theorem.

Now two \( L \)-similar groups are not necessarily isomorphic. Rottlaender has already given an example. In this paper we shall state a systematic study on \( L \)-similarity and isomorphism of hypercyclic groups. Namely,
we shall study the following two problems:

**First Problem.** Find out all \( L \)-similar classes of hypercyclic groups with a given order.

**Second Problem.** Find out all hypercyclic groups, which are not isomorphic, one another, in a given \( L \)-similar class.

The former will be solved in §2, and the latter in §3.

§2. \( L \)-Similar Classes of Hypercyclic Groups.

We shall prove first the following main result:

**L-Similarity Theorem.** Let

\[
G = (\varphi, \varphi_1, \ldots, \varphi_v; \tau, \tau_1, \ldots, \tau_v)
\]

be a successive splitting of Sylow-groups of a hypercyclic group \( G \), with the system of \( S \)-indices

\[
f, f_1, \ldots, f_{v-1},
\]

and let \( \overline{G} \) be a hypercyclic group of the same order. Then we have

\[
G \simeq \overline{G},
\]

if and only if

\[
\overline{G} = (\overline{\varphi}, \overline{\varphi}_1, \ldots, \overline{\varphi}_v; \overline{\tau}, \overline{\tau}_1, \ldots, \overline{\tau}_v)
\]

\[
\varphi_i \simeq \overline{\varphi}_i \quad (i = 1, 2, \ldots, v)
\]

and the system of \( S \)-indices of this latter splitting coincides with (1).

**Proof.** Denote the subgroup \( \varphi, \varphi_1, \ldots, \varphi_v \), as \( \varphi_v \). Then we have a simple splitting

\[
G = (\varphi_v; \tau)
\]

\[
(\varphi_v = \varphi_v, \tau = \tau_v).
\]

Let \( \overline{G} \) be the foundation group. Hence \([\varphi_v; \overline{G}] = f_{v-1}\).

Now we assume that

\[
G \simeq \overline{G},
\]

and let \( \varphi_v, \overline{\varphi}_v, \overline{\varphi} \) be the corresponding subgroups of \( \varphi_v, \overline{\varphi}_v \), \( \overline{\varphi} \) respectively. \( \overline{\varphi} \) is the largest normal subgroup of \( \varphi_v \), included in \( \varphi_v \), and so is \( \overline{\varphi} \) concerning \( \overline{\varphi}_v \) and \( \overline{\varphi}_v \). Hence \( \overline{\varphi} \) is the foundation group of the splitting \( \overline{G} = (\overline{\varphi}, \overline{\varphi}_v; \overline{\tau}) \), and we have

\[
[\overline{\varphi}_v; \overline{\tau}] = [\varphi_v; \overline{G}] = f_{v-1}.
\]

Thus, by induction, we obtain the necessary condition for \( G \simeq \overline{G} \), mentioned in the theorem.

Conversely, we take two hypercyclic groups with following simple splittings:

\[
G = (\varphi_v; \tau), \quad \overline{G} = (\overline{\varphi}_v; \overline{\tau}),
\]

and let \( \overline{\varphi} \) and \( \overline{\varphi}_v \) be the foundation groups of \( G \) and \( \overline{G} \) respectively. Now we assume that

\[
\varphi_v \simeq \overline{\varphi}_v, \quad \tau \simeq \overline{\tau},
\]

and

\[
[\varphi_v; \overline{G}] = [\overline{\varphi}_v; \overline{G}].
\]

Then \( \overline{\varphi} \) corresponds to \( \overline{\varphi}_v \) by the \( L \)-similar correspondence \( \varphi_v \) between \( \varphi_v \) and \( \overline{\varphi}_v \). (Cf. §1.9.1, 6.)

In the following we shall extend \( \varphi_v \) to an \( L \)-similar correspondence between \( \varphi_v \) and \( \overline{\varphi}_v \).

Let \( a, a \) be generating elements of \( \varphi_v, \overline{\varphi}_v \) respectively, and we establish the following correspondence \( \rho \)

\[
a_i^j \varphi_v \{a_i^j a\} \longleftrightarrow \overline{a}_i^j \overline{\varphi}_v \{a_i^j \overline{a}\}
\]

where \( i, j \) are arbitrary integers, and \( \varphi_v, \overline{\varphi}_v \), are (by \( \varphi_v \) ) corresponding (arbitrary) subgroups of \( \varphi_v, \overline{\varphi}_v \) respectively. A subgroup \( \varphi \) can be written in the form \( a_i^j \varphi_v \{a_i^j a\} \) in various ways, but the corresponding group \( \overline{\varphi} = \overline{a}_i^j \overline{\varphi}_v \{a_i^j \overline{a}\} \) is uniquely determined by \( \varphi \). We certify it in a generalized way as follows.

Let

\[
a_i^j \varphi_v \{a_i^j a\} \longleftrightarrow \overline{a}_i^j \overline{\varphi}_v \{a_i^j \overline{a}\},
\]

\[
a_i^j \varphi_v \{a_i^j a\} \longleftrightarrow \overline{a}_i^j \overline{\varphi}_v \{a_i^j \overline{a}\},
\]

be two corresponding pairs of subgroups by \( \rho \). Now we assert that from

\[
(a)
\]

it follows

\[
(b)
\]

and conversely.

By Reduction Theorem on Subgroups ( §1.6) (2) implies that

\[
\varphi_v \{a_i^j a\} \leftrightarrow \varphi_v \{a_i^j a\},
\]

and in case of \( \varphi_v \varphi_v \), \( \{a_i^j a\} \leftrightarrow \{a_i^j a\} \).

\[
a_i^j \overline{a}_i^j \in \{a_i^j a\}.
\]
Then we have
\[ \overline{z}_n \cdot \overline{z}_n = \overline{z}_n, \{ \overline{z}_i \} \cdot \{ \overline{z}_i \}, \]
and in case of
\[ \overline{z}_n \cdot \overline{z}_n = \overline{z}_n, \{ \overline{z}_i \} \in \{ \overline{z}_i \}. \]

Hence we obtain (3). The proof of the converse is just the same. As a special case we observe that
\[ a_i \cdot \overline{z}_n = \overline{z}_n, \{ a_i \} \in \{ a_i \}, \]
implies
\[ \overline{z}_n \cdot \overline{z}_n = \overline{z}_n, \{ \overline{z}_i \} \in \{ \overline{z}_i \}, \]
and conversely. Thus the correspondence \( \rho \) gives a one-to-one correspondence between \( L(\mathcal{G}) \) and \( L(\overline{\mathcal{G}}) \), and it is a lattice-isomorphism. The coincidence of orders of corresponding subgroups is quite obvious. Therefore the theorem has been completely proved.

Now a hypercyclic group \( \mathcal{G} \) has, in general, several successive splittings to Sylow-groups, and therefore the system of \( S \)-indices is not uniquely determined by the group. But the system of \( S \)-indices of a fundamental splitting \( (I, 3) \) is uniquely determined by \( \mathcal{G} \). We shall call it the \( L \)-invariants of \( \mathcal{G} \). Then, by \( L \)-Similarity Theorem, we have the following:

**Theorem 1.** Two hypercyclic groups of the same order are \( L \)-similar, if and only if they have the same \( L \)-invariants.

Thus our first problem in the preceding paragraph turns out to be the following one:

Find out all systems of integers, which are the \( L \)-invariants of hypercyclic groups of a given order.

Let \( \alpha \) be a given integer \( \geq 1 \), and let \( \mathcal{G} \) be a hypercyclic group of order \( \alpha \). We factorize \( \alpha \) as follows:
\[ \alpha = \alpha_1 \alpha_2 \cdots \alpha_r, \]
where \( \alpha_i \) are such primes that
\[ \alpha_1 < \alpha_2 < \cdots < \alpha_r. \]

Then, by First Splitting Theorem, \( \mathcal{G} \) has a successive splitting
\[ \mathcal{G} = (\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_r, \tau_1, \ldots, \tau_r), \]
where \( \mathcal{P}_i \) is a \( \alpha_i \)-Sylow-group of \( \mathcal{G} \). Let
\[ f_i = a_{i1} a_{i2} \cdots a_{ir} \tau_1, \ldots, \tau_r, \quad (i = 1, 2, \ldots, r), \]
be the \( L \)-invariants of \( \mathcal{G} \). We construct a matrix
\[ F(\mathcal{G}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rr} \end{pmatrix} = (a_{ij}), \]
and call it the \( L \)-matrix of \( \mathcal{G} \).

Next we consider the following integers
\[ \alpha_i \cdot \alpha_j \cdot (\alpha_{ij} - 1) = \alpha_i \alpha_j \alpha_{ij} \cdots \alpha_{ij-r}, \]
\[ \alpha_i \alpha_j \cdot (\alpha_{i} - 1) = \alpha_i \alpha_j \alpha_i \alpha_{i+1} \cdots \alpha_{i-r}, \]
\[ \alpha_i \cdot \alpha_j \cdot (\alpha_{i} - 1) = \alpha_i \alpha_j \alpha_{i+1} \cdot \alpha_{i+1} \cdots \alpha_{i-r}, \]
and construct a matrix
\[ K(\alpha) = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1r} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{r1} & \alpha_{r2} & \cdots & \alpha_{rr} \end{pmatrix} = (a_{ij}). \]
We call it the \( K \)-matrix of \( \alpha \). Now we prove the following:

**Theorem 2.** Let \( K(\alpha) = (a_{ij}) \) be the \( K \)-matrix of an integer \( \alpha \). A matrix \( (a_{ij}) \) where \( a_{ij} \) are non-negative integers, denotes the \( L \)-matrix of a hypercyclic group \( \mathcal{G} \) of order \( \alpha \), if and only if the following two conditions are satisfied:
1) \( a_{ij} \leq a_{ij} \) \( (i, j = 1, 2, \ldots, r - 1) \).
2) If \( a_{ij} = 0 \), then for every \( i \), \( d_{i, i+1} = 0 \).

Proof. Assume that \( (a_{ij}) \) is the \( L \)-matrix of a hypercyclic group \( \mathcal{G} \) of order \( \alpha \). \( \mathcal{G} \) has a fundamental splitting
\[ \mathcal{G} = (\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_r, \tau_1, \ldots, \tau_r), \]
Let \( \mathcal{G}_i = \mathcal{P}_{i1} \mathcal{P}_{i2} \ldots \mathcal{P}_{ir}, (i = 1, 2, \ldots, r), \) and let \( f_i \) be the foundation group of \( \mathcal{G}_{i+1} = (\mathcal{P}_{i1}, \mathcal{P}_{i2}, \ldots, \mathcal{P}_{ir}, \tau_{i+1}) \). Then \( f_i = a_{i1} a_{i2} \cdots a_{ir} \tau_{i+1} = \frac{\mathcal{G}_{i+1}}{\mathcal{G}_i} \)
\([\mathcal{G}_i : f_i]\). Hence

\[
f_i \mid [\mathcal{G}_i] = \mathcal{A}_i^* \cdot \mathcal{A}_i^{*1} \cdots \mathcal{A}_i^{*r}
\]

On the other hand,

\[
\mathcal{A}_i \cong \mathcal{A}_{i+1},
\]

where \(\mathcal{A}_{i+1}\) is a subgroup of the automorphism group \(\mathcal{A}_{i+1}\) of \(\mathcal{P}_{i+1}\). Since \([\mathcal{A}_{i+1}] = \mathcal{A}_i^{*1} / (f_i^{*1} - 1)\), it holds that

\[
f_i \mid \mathcal{A}_i^{*1} - 1.
\]

Hence we have

\[
d_i \leq f_i.
\]

In the next place, we assume that \(d_i \cdot f_i \neq 0\). Then \(f_i \neq 1\).

If we denote the commutator group of \(\mathcal{G}_i\) as \(\mathcal{K}_i\), it follows from Reduction Theorem on Commutator Groups

\[
\mathcal{K}_i = \mathcal{K}_i / \mathcal{P}_i^{*1},
\]

and therefore

\[
\mathcal{K}_i \cong \mathcal{P}_i^{*1},
\]

Then \(f_i \geq \mathcal{P}_i^{*1}\), we have

\[
\mathcal{A}_i^{*1} \cdot \mathcal{P}_i^{*1} = \mathcal{K}_i^{*1}.
\]

As it is evident that \(\mathcal{A}_i^{*1} \cdot \mathcal{P}_i^{*1} = \mathcal{K}_i^{*1}\), it holds for every \(i\)

\[
d_i \cdot f_i = 0.
\]

We shall now prove by induction.

When \(r = 2\), then

\[
f_i = \mathcal{A}_i^{*2} / (\mathcal{A}_i^{*2} - 1).
\]

Let \(\mathcal{P}_1\), \(\mathcal{P}_2\) be cyclic groups of order \(\mathcal{A}_i^{*2}\), \(\mathcal{A}_i^{*2}\) respectively, \(\mathcal{P}_1\) has a subgroup \(f_i\), whose order is \(\mathcal{A}_i^{*2} - 1\). As \(\mathcal{A}_i^{*2} - 1\), \(\mathcal{A}_i^{*2}\) is an odd prime and the automorphism group of \(\mathcal{P}_1\) has a cyclic subgroup of order \(\mathcal{A}_i^{*2}\). Hence we can construct a group

\[
\mathcal{G}_i = (\mathcal{P}_1, \mathcal{P}_2; \sigma)
\]

where the \(S\)-index is \(\mathcal{A}_i^{*2} = f_i\).

Assume now that \(r \geq 3\) and a matrix \((\mathcal{A}_i^{*2})\) satisfies the two conditions of the theorem and that for the system of integers

\[
f_i, f_2, \ldots, f_{r-1},
\]

where \(f_i = \prod \mathcal{A}_i^{*2}\), there exists a hypercyclic group \(\mathcal{G}_i\) of order \(\mathcal{A}_i^{*2} \cdots \mathcal{A}_i^{*r-1}\), the \(L\)-invariants of which are \(f_i, f_2, \ldots, f_{r-1}\). Let \(\mathcal{K}_i\) be the commutator group of \(\mathcal{G}_i\), and \(\mathcal{P}\) be the cyclic group of order \(\mathcal{A}_i^{*r}\). If \(\mathcal{K}_i\) divides \([\mathcal{K}_i]\), then, by Reduction Theorem on Commutator Groups, \(f_i\) is not equal to 1, and therefore \(d_i \cdot f_i \neq 0\) for some \(i\). Hence, by the condition 2) of the theorem, we get \(d_i \cdot f_i = 0\), i.e., \(\mathcal{A}_i^{*r-1} \cdot f_i = 1\). Thus \(f_i\) divides \([\mathcal{K}_i : \mathcal{K}_i]\) and since \(\mathcal{K}_i = \mathcal{P}_i / \mathcal{K}_i\), there is a normal subgroup \(\mathcal{P}\) of \(\mathcal{K}_i\) such that \(\mathcal{P} \cong \mathcal{K}_i\) and \([\mathcal{G}_i : \mathcal{P}] = f_i\).

As \(\mathcal{A}_i^{*2}\) is an odd prime, the commutator \(\mathcal{G}_i\) of \(\mathcal{P}\) is cyclic, and has a cyclic subgroup \(\mathcal{K}_i\) of order \(\mathcal{A}_i^{*2}\), \(f_i = \mathcal{A}_i^{*2} / (\mathcal{A}_i^{*2} - 1)\), for \(f_i\) divides \(\mathcal{A}_i^{*2} - 1\) by the condition 1) of the theorem.

Hence we can construct a hypercyclic group

\[
\mathcal{G}_i = (\mathcal{G}_i, \mathcal{P}; \sigma)
\]

whose foundation group is \(\mathcal{P}\), and \([\mathcal{G}_i : \mathcal{P}] = f_{i-1}\). This group \(\mathcal{G}_i\) has \(f_i, f_2, \ldots, f_{r-1}\) as its \(L\)-invariants, and \((\mathcal{A}_i^{*2})\) as its \(L\)-matrix. q.e.d.

Hence our first problem in §1 has been completely solved. We shall now consider the second problem.

§3. Ramification Theory.

Let

\[
\mathcal{G}_i = (\mathcal{G}_i, \mathcal{P}; \sigma)
\]

be a simple splitting of a hypercyclic group \(\mathcal{G}_i\). \(\mathcal{G}_i\) is (up to isomorphism) uniquely determined by \(\mathcal{G}_i, \mathcal{P}\) and \(\sigma\). Let \(\mathcal{K}\) be the foundation group. Then, by \(L\)-Similarity Theorem, the \(L\)-similar class, to which \(\mathcal{G}_i\) belongs, is uniquely determined by \(\mathcal{G}_i, \mathcal{P}\) and \(\mathcal{K}\).

Now we consider another group

\[
\mathcal{G}_i' = (\mathcal{G}_i, \mathcal{P}; \sigma'),
\]

whose foundation group is also \(\mathcal{K}\). Then \(\mathcal{G}_i' \cong \mathcal{G}_i\) but not necessarily \(\mathcal{G}_i' \cong \mathcal{G}_i\). If there exists a group \(\mathcal{G}_i'\) such that \(\mathcal{G}_i'\) is not isomorphic to \(\mathcal{G}_i\), then we say that the extension

\[
\mathcal{G}_i \rightarrow (\mathcal{G}_i, \mathcal{P}; \sigma)
\]

is a non-trivial extension.
ramifies. We shall investigate it as follows:

Let \( [\mathcal{G}] = \mathfrak{p}^{\mathfrak{a}} \), where \( \mathfrak{p} \) is a prime. If \( \mathfrak{p} = 2 \), then the \( 2 \)-index \( f = [\mathcal{G}, \mathcal{F}] \) divides \( 2 - 1 = 1 \), and therefore \( m = 1 \).

Thus, in this case, there is only one group, namely

\[ \mathcal{G} = \mathcal{G}_0, \mathcal{F} = \mathfrak{p}^{\mathfrak{a}}. \]

Therefore we shall assume henceforth that \( \mathfrak{p} \) is an odd prime. Let \( \mathfrak{d} \) be a fixed primitive root mod \( \mathfrak{p}^2 \). Then we obtain the homomorphic mapping \( \mathcal{F} \) by corresponding \( \mathcal{F}^\mathfrak{a} \) to an element \( \mathfrak{d} \in \mathcal{G}_0 \), for which \( \mathfrak{d}^f \) is a generating element of \( \mathcal{G}_0 / \mathcal{F} \). Thus we can write

\[ \mathcal{G} = (\mathcal{G}_0, \mathcal{F}, \mathfrak{d}) \]

in place of \( \mathcal{G} = (\mathcal{G}_0, \mathcal{F}, \sigma) \). Therefore, we shall fix the groups \( \mathcal{G}_0, \mathcal{F}, \mathfrak{d} \) and the primitive root \( \mathfrak{d} \), and only the element \( \mathfrak{d} \) can vary. Now we have the fundamental

**Ramification Theorem.** We have an isomorphism

\[ (\mathcal{G}_0, \mathcal{F}; \mathfrak{d}) \cong (\mathcal{G}_0, \mathcal{F}; \mathfrak{d}'), \]

if and only if

\[ \mathfrak{d}, \mathfrak{d}' \in \mathcal{U}_0, \]

where \( \mathcal{U}_0 \) is the ramification kernel of \( \mathcal{G}_0 \).

The proof of this theorem is rather long. We shall consider first a certain automorphism of a hypercyclic group.

Let

\[ \mathcal{G} = (\mathcal{G}_0, \mathcal{F}; \sigma) \]

be a simple splitting of a hypercyclic group \( \mathcal{G} \) and let \( \mathcal{F} \) be the foundation group. We can split \( \mathcal{G}_0 \) such as

\[ \mathcal{G}_0 = (\mathcal{C}_0, \mathcal{K}_0; \mathcal{L}_0), \]

where \( \mathcal{K}_0 \) is the commutator group of \( \mathcal{G}_0 \). Let

\[ \mathcal{C}_0 = \{c\}, \mathcal{K}_0 = \{k\}, \mathcal{L}_0 = \{l\}, \]

and let

\[ [\mathcal{C}_0] = \mathcal{C}_0, [\mathcal{K}_0] = \mathcal{K}_0, [\mathcal{L}_0] = \mathcal{L}_0, [\mathcal{G}_0, \mathcal{F}] = f, \]

where \( \mathfrak{p} \) denotes a prime.

Henceforth we shall write

\[ \langle u \mod \mathfrak{p} \rangle = \mathcal{F}, \]

where \( u = (\mathcal{G}_0, \mathcal{F}; \mathfrak{d}) \) and \( u^* = (\mathcal{G}_0, \mathcal{F}; \mathfrak{d}^*) \) for \( 0 < \mathfrak{d} < \mathfrak{p} \).

Now that \( \mathcal{F} \geq \mathcal{G}_0, \mathcal{F} \) is defined by the following relations:

\[ \begin{align*}
\text{i)} & \quad \mathcal{L}^\mathfrak{a} \mathfrak{d} = \mathfrak{d} \\
\text{ii)} & \quad \mathcal{C}^\mathfrak{a} \mathfrak{d} = \mathfrak{d}^\mathfrak{a} \\
\end{align*} \]

where \( \langle u \mod \mathfrak{p} \rangle = f \).

\[ \begin{align*}
\text{iii)} & \quad \mathcal{L}^\mathfrak{a} \mathfrak{d} = \mathfrak{d}^\mathfrak{a} \\
\end{align*} \]

where \( \langle u \mod \mathfrak{p} \rangle = \mathcal{F} \),

when we denote the ramification kernel of \( \mathcal{G}_0 \) as \( \mathcal{U}_0 \), and let

\[ [\mathcal{G}_0, \mathcal{U}_0] = \mathcal{U}_0 \]

Now we shall consider such an automorphism \( \tau \) of \( \mathcal{G}_0 \) as

\[ \mathcal{G}_0 = \mathcal{G}_0. \]

Then

\[ \mathcal{K}_0^\tau = \mathcal{K}_0, \mathcal{P}_0^\tau = \mathcal{P}_0, \]

since every normal subgroup of a hypercyclic group is characteristic.

Let

\[ \begin{align*}
\text{(1)} & \quad \mathcal{L}^\mathfrak{a} = \mathcal{L}^\mathfrak{a} \\
\text{(2)} & \quad \mathcal{C}^\mathfrak{a} = \mathcal{C}^\mathfrak{a} \\
\end{align*} \]

where \( \mathfrak{a}, \mathfrak{b} \) are integers, and

\[ \begin{align*}
\text{(3)} & \quad \beta \wedge \mathfrak{b} = 1, \\
\text{(4)} & \quad \mathfrak{a} \wedge \mathfrak{b} = 1, \\
\end{align*} \]

By Conjugateness Theorem, \( \mathcal{C}_0 \) and \( \mathcal{C}_0^\tau \) are conjugate. Hence there exist integers \( \mathfrak{s}, \tau \) such that

\[ \begin{align*}
\text{(5)} & \quad \mathcal{C}_0^\tau = \mathcal{L}^{-\mathfrak{a}} \mathcal{C}^\mathfrak{a} \mathcal{L}^\mathfrak{s}, \\
\text{(6)} & \quad \mathfrak{a} \wedge \mathfrak{m}_\mathfrak{s} = 1. \\
\end{align*} \]

Conversely \( \tau \) is determined by (1), (2), (5). For the purpose of \( \tau \) being an automorphism, it is necessary and sufficient that

\[ \begin{align*}
\text{i')} & \quad \mathcal{L}^\mathfrak{a} \mathcal{L}^\mathfrak{a} = \mathcal{L}^\mathfrak{a} \\
\text{ii')} & \quad (\mathcal{L}^\mathfrak{a} \mathcal{C}^\mathfrak{a} \mathcal{L}^\mathfrak{s})^\mathfrak{a} (\mathcal{L}^{-\mathfrak{a}} \mathcal{C}^\mathfrak{a} \mathcal{L}^\mathfrak{s}) = \mathcal{L}^\mathfrak{a} \\
\text{iii')} & \quad (\mathcal{L}^\mathfrak{a} \mathcal{C}^\mathfrak{a} \mathcal{L}^\mathfrak{s})^\mathfrak{a} (\mathcal{L}^{-\mathfrak{a}} \mathcal{C}^\mathfrak{a} \mathcal{L}^\mathfrak{s}) = \mathcal{L}^\mathfrak{a}, \\
\end{align*} \]
Now we shall consider the sufficient condition for \( i \), \( i' \), \( ii' \), \( iii' \) to be obtained from \( i \), \( i \), \( ii \), \( iii \).

First \( ii' \) is instantly gained from \( ii \).

If \( i \)

\[ t = 1 \quad (f) \]

then

\[ u_i = 1 \quad (a) \]

It follows that

\[ a u_i = 1 \quad (a') \]

By (a) we can calculate the left-hand of \( ii' \) as

\[ (c^t c^{-1}) a^t (c^t c^{-1}) = a^{c^t} c^{a^{c^t}} \]

Hence we get \( ii' \)

Now we assume that

\[ t = 1 \quad (u_i) \]

Then

\[ u_{ii'} = 1 \quad (u_i) \]

Hence

\[ a u_{ii'} = a u_i \quad (a') \]

Thus the left-hand of \( ii' \) is

\[ (c^t c^{-1}) a^t (c^t c^{-1}) = a^{c^t} c^{a^{c^t}} \]

Hence we get \( ii' \). Therefore we have the following:

**Lemma 1.** Under the above notations, for any \( a, \alpha \), which satisfy

\[ a \wedge c = 1, \quad \alpha \wedge a = 1, \]

and for any conjugate \( c \), \( c^t \) of \( c \), in \( G \), there exists an automorphism \( \tau \) of \( G \) such that

\[ a^t = a^\beta, \quad c^t = c^\alpha, \quad c_{ii'} = c_{ii'}^t, \quad c_{ii'} = c_{ii'} \]

For \( t = 1 \) evidently satisfies (6), (7), (8).

**Lemma 2.** Let \( G \) be a finite cyclic group and let \( \alpha \) be a homomorphic mapping from \( G \) on a cyclic group \( \overline{G} \). Then, to any generating element of \( \overline{G} \) corresponds by \( \alpha \) at least one generating element of \( G \).

**Proof.** Let

\[ \overline{G} = G_1 \times G_2 \times \cdots \times G_n \]

be the direct decomposition of \( G \) into its Sylow-groups, and let

\[ G_i = G_1 \times G_2 \times \cdots \times G_i \]

then

\[ \overline{G_i} = \overline{G_1} \times \overline{G_2} \times \cdots \times \overline{G_i} \]

If it is proved that the lemma is true for these pairs of \( G \)-groups \( G_i \) and \( \overline{G_i} \), then it is also true for \( G \) and \( \overline{G} \). Thus we assume now that \( [\overline{G}] = \overline{G} \), where \( \alpha \) is a prime, and \( [\overline{G}] \) = \( \overline{G} \). As the lemma is trivial for \( d = 1 \), we assume further that \( d = 1 \).

The number of generating elements of \( \overline{G} \) is

\[ \gamma(a^d) = a^{d-1}(\alpha - 1) \]

and that of \( G \) is

\[ \gamma(a) = a^{d-1}(\alpha - 1) \]

Now that to any generating element of \( G \) corresponds necessarily a generating element of \( \overline{G} \), all generating elements of \( G \) are included in \( \mathcal{K} \), where \( \mathcal{K} \) denotes the set of all elements of \( G \), which correspond to the generating elements of \( G \). On the other hand, just \( \alpha^d \)-elements of \( G \) correspond to one element of \( \overline{G} \). Hence the number of elements of \( \mathcal{K} \) is by (10)

\[ \alpha^d \cdot \alpha^{d-1}(\alpha - 1) = \alpha^{d-1}(\alpha - 1) \]

and is equal to (11). Hence every element of \( \mathcal{K} \) is a generating element of \( G \), q.e.d.

We shall now return to the proof of Ramification Theorem.

In the symbol \( (\overline{G}, \overline{G}; d) \) we can choose \( d \) arbitrarily from the coset \( \overline{G} \) mod \( G \) since the constructed groups are all isomorphic to each other. Thus we choose the following special elements.

Since \( \overline{G} \supset \mathcal{K} \), and since every coset of \( \overline{G} \) mod \( \mathcal{K} \) includes just one element of \( \mathcal{K} \), \( \overline{G}/\mathcal{K} \) is homomorphic to \( \mathcal{K} \). Therefore, by Lemma 2, a coset (mod \( \mathcal{K} \)), which generates \( \overline{G}/\mathcal{K} \), includes at least one generating element of \( \mathcal{K} \). Hence we can assume that \( d \), \( d \), in Ramification Theorem are generating elements of \( \mathcal{K} \) and that \( d = 1 \). Then Ramification Theorem is transformed into the following form:
Let $\mathfrak{I}$ be an integer such that

$$\mathfrak{I}_1 \geq \mathfrak{I}_2.$$

The analogue of $\mathfrak{I}_2$, which corresponds to $\mathfrak{I}_2$, by the isomorphism between $\mathfrak{I}_1$ and $\mathfrak{I}_2$, is the conjugate to $\mathfrak{I}_2$, and corresponds to $\mathfrak{I}_2$. Therefore, we have an isomorphism between $\mathfrak{I}_1$ and $\mathfrak{I}_2$ such that

$$\mathfrak{I}_1 \leftrightarrow \mathfrak{I}_2.$$

By Lemma 1, the product of this isomorphism and an inner automorphism of $\mathfrak{I}_2$, we obtain an isomorphism of $\mathfrak{I}_2$ which makes $\mathfrak{I}_1$ correspond to $\mathfrak{I}_2$. Furthermore, by

$$\mathfrak{I}_1 \leftrightarrow \mathfrak{I}_2,$$

and the following defining relations

$$\mathfrak{I}_1 \leftrightarrow \mathfrak{I}_2$$

where $\mathfrak{I}_1$ is transformed by $a = a_1$, $b = b_1$, $c = c_1$, and $d = d_1$. Thus, by (ii) and (iv),

$$\mathfrak{I}_1 = \mathfrak{I}_2.$$
(17) \( u^c = u \) \((\text{mod } \alpha)\).

Conversely, by (16) and (17), (16) gives surely an isomorphism.
Hence the proposition 2) is transformed into:

3) The necessary and sufficient condition for the existence of \( t \) satisfying (16), (17) is that
\[
j \equiv 1 \pmod{\nu}.
\]

We shall further transform (16), (17).
As \( u \equiv u \pmod{\alpha} \), (17) implies
\[
t \equiv (\nu)\equiv 1 \pmod{\nu}.
\]
Now that \( j \equiv 1 \pmod{\nu} \), such \( j^c \) is uniquely (mod \( \nu \) ) determined as
\[
j = j^c \equiv 1 \pmod{\nu}.
\]
Since \( f \) divides \( \nu \),
\[
j \equiv 1 \pmod{f}\),
\[
\text{As } u^j \equiv u \pmod{\alpha} \text{ and } u^j \equiv 1 \pmod{\alpha}, \text{ we have}
\[
u^j \equiv u^j \pmod{\alpha}.
\]
Hence by (16)
\[
u^j \equiv u \pmod{\alpha},
\]
\text{namely}
\[
j \equiv 1 \pmod{f}.
\]
Conversely (16) follows from (20). Hence 3) is transformed into the following form:

4) Let \( j \equiv 1 \pmod{\nu} \), and let \( j^c \) be determined by (19). The necessary and sufficient condition for the existence of \( t \) satisfying (18), (20) and \( t \equiv 1 \pmod{\nu} \), is that
\[
j \equiv 1 \pmod{\nu}.
\]

We can easily prove the necessity.
We have
\[
j^c (j - t) = 0 \pmod{f}
\]
from \( j^c = 1 \pmod{f} \) and (20). As \( j \equiv 1 \pmod{f} \),
\[
j \equiv t \pmod{f}.
\]
Hence by (18)
\[j = 1 \pmod{\nu} \times f\).

Conversely, if (21) holds, (20) follows for \( j^c \) determined by (19). Thus we have only to prove

5) Let \( S \) be a finite cyclic group, and let \( S_1, S_2 \) be its subgroups.
If
\[
a, a^{-1} \in S_1, S_2, \]
where \( a, a \) are both generating elements of \( S \), then there exists a generating element \( \alpha \) of \( S \) such that
\[
\alpha a^{-1} \in S_1, \quad \alpha a^{-1} \in S_2.
\]
For, if (5) is true, and let
\[
[S] = \alpha, \quad [S : S_1] = \nu,
\]
then it follows that, since \( j \) and \( t \) correspond to \( a, \alpha \) in (5) respectively, and 1 in \( \alpha \), (i.e. \( a = a^f, \alpha = a^f \))
Now we shall reduce the proof of (5) into an easier case.
We decompose \( S \) into a direct product of Sylow subgroups:
\[
S = P_1 \times P_2 \times \cdots \times P_r.
\]
Also we have
\[
S_1 = P_1 \times P_2 \times \cdots \times P_r \quad (P_i \subseteq P_i),
\]
\[
S_2 = P_1 \times P_2 \times \cdots \times P_r \quad (P_i \subseteq P_i),
\]
\[
a_1 = a_1 a_2 \cdots a_r \quad (a_i \in P_i),
\]
\[
a_2 = a_1 a_2 \cdots a_r \quad (a_i \in P_i).
\]
Then \( a_1, a_2 \) are generating elements of \( P_i \) for every \( i \), and
\[
a_1 a_2^{-1} \in P_1 P_2.
\]
Hence, if (5) is true for \( P \), there is \( \alpha \), which generates
\[
P_i, \quad \text{for every } i \text{ such that}
\]
\[
\alpha a_1^{-1} \in P_i, \quad \alpha a_2^{-1} \in P_i.
\]
Then \( \alpha = \alpha, \cdots \alpha \) generates \( S \) and
\[
\alpha a_2^{-1} \in S_1, \quad \alpha a_2^{-1} \in S_2.
\]
Therefore, we have only to prove (5) in the case of \( P \).
When \( \mathcal{G} \) is a cyclic \( \mathcal{C} \)-group, then it holds that either \( \mathcal{G}_2 \supseteq \mathcal{G}_1 \), or \( \mathcal{G}_2 \supseteq \mathcal{G}_1 \). In the former case, put \( \mathcal{C} = \mathcal{G}_1 \), and in the latter, \( \mathcal{C} = \mathcal{G}_2 \).

The proof of the Ramiification Theorem has thus been completed.

By Ramiification Theorem we can solve the second problem in \( T_1 \) — i.e. finding out all hypercyclic groups in a given \( \mathcal{C} \)-similar class — as follows:

Let \( \mathcal{G}_2 \) be a hypercyclic group with the ramiification kernel \( \mathcal{V}_2 \), and let \( \mathcal{G} \) be a cyclic \( \mathcal{C} \)-group such that \( [\mathcal{V}_2] \wedge [\mathcal{G}] = 1 \). Then we can construct a hypercyclic group

\[ \mathcal{G} = (\mathcal{G}_2, \mathcal{G}; \zeta) \]

If we fix the foundation group \( \mathcal{F} \), then the number of all such groups \( \mathcal{G} \), which are not isomorph to each other, is equal to

\[ \gamma([\mathcal{G}_2; \mathcal{G}; \zeta]) \]

Proof. Since \( \mathcal{G} \) generates \( \mathcal{G}_2/\mathcal{F} \), \( \mathcal{G}_2/\mathcal{F} \) generates \( \mathcal{G}_2/\mathcal{G}_2 \mathcal{F} \), conversely, a coset module \( \mathcal{V}_2/\mathcal{F} \), which generates \( \mathcal{G}_2/\mathcal{G}_2 \mathcal{F} \), by Lemma 2 of Ramiification Theorem, contains a coset module \( \mathcal{F} \), which generates \( \mathcal{G}_2/\mathcal{F} \). Hence, by Ramiification Theorem, we obtain the above proposition. Q.E.D.

We remark that if \( \mathcal{G}_2 \) is cyclic, then \( \mathcal{G}_1 = \mathcal{V}_2 \), and therefore \( \gamma([\mathcal{G}_2; \mathcal{G}; \zeta]) = 1 \), whatever \( \mathcal{F} \) may be. In this case the extension does not ramify.

Now we take a hypercyclic group \( \mathcal{G} \) such that

\[ \mathcal{G} = (\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_n; \zeta, \zeta_1, \ldots, \zeta_n) \]

where \( \mathcal{G}_i \) are Sylow-groups of \( \mathcal{G} \). Let

\( f, f_1, \ldots, f_{n-1} \)

be the \( \mathcal{L} \)-invariants of \( \mathcal{G} \). Then we shall find out all hypercyclic groups, which are \( \mathcal{L} \)-similar to \( \mathcal{G} \).

In our first step of extension

\[ \mathcal{G}_1 \longrightarrow (\mathcal{G}_1; \mathcal{G}_2; \zeta_j) \]

as \( \mathcal{G}_1 \) is cyclic, the ramiification does not arise. We denote this uniquely determined group \( (\mathcal{G}_1, \mathcal{G}_2; \zeta_j) \) as \( \mathcal{G}_1^{(1)} \), and write \( \mathcal{G}_1 = \mathcal{G}_1^{(0)} \).

In the next step

\[ \mathcal{G}_1^{(0)} \longrightarrow (\mathcal{G}_1^{(1)}, \mathcal{G}_2; \zeta_j) \]

there arises, in general, some ramification. Namely we assume that there are \( \mathcal{V}_2 \) (not isomorphic to each other) groups:

\[ \mathcal{G}_1^{(1)}, \mathcal{G}_1^{(2)}, \ldots, \mathcal{G}_1^{(t)} \]

We construct further for every \( i \)

\[ \mathcal{G}_1^{(i)} = (\mathcal{G}_1^{(i)}, \mathcal{G}_2; \zeta_j) \]

The number of all such groups, gained from the same \( \mathcal{G}_1^{(0)} \), is all the same for any \( i \). Let it be denoted as \( \mathcal{V}_i \). We construct then

\[ \gamma^{(i)} = (\mathcal{G}_1^{(i)}, \mathcal{G}_2; \zeta_j) \]

and so on. We can find thus all hypercyclic groups with the given \( \mathcal{L} \)-invariants \( f, f_1, \ldots, f_{n-1} \). Now we calculate the number \( \gamma \) of these groups.

Let \( \gamma_i \) be the number of groups, obtained from the same group of the form

\[ \mathcal{G}_1^{(i)} = (\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_n; \zeta, \zeta_1, \ldots, \zeta_n) \]

Let \( \gamma_i \) be the ramification constant of \( \mathcal{G}_1^{(i)} \), then by the preceding proposition

\[ \gamma_i = \gamma ([\mathcal{G}_1^{(i)}]) \]

By Theorem 6 of \( T_6 \)

\[ \gamma_i = f, f_1, f_2, \ldots, f_{n-1} \]

Since the above number \( \gamma \) is equal to \( \prod \gamma_i \), we obtain the last theorem:

**Enumeration Theorem.** The number of all hypercyclic groups of a given order and with the same \( \mathcal{L} \)-invariants

\[ f, f_1, \ldots, f_{n-1} \]

is equal to

\[ \prod \gamma_i \gamma ([f, f_1, f_2, \ldots, f_{n-1}] \wedge f_{n-1}) \]

for \( \gamma \equiv 1 \), and is equal to 1 for \( \gamma \equiv 2 \).

Finally we shall find out all hypercyclic groups of order \( \equiv 100 \), including that of order 1.
In the positive integers not exceeding 100, there are 36 primes or prime-powers (including 1), for every one of which there exists just one cyclic group.

Next we consider the integers of the form \( \mathcal{A} \mathcal{B}^2 \), where \( \mathcal{A}, \mathcal{B} \) are primes and \( \mathcal{A} < \mathcal{B} \). Let \( \mathcal{A}' = \mathcal{A} \mathcal{A} (\mathcal{B} - 1) \), then all the possible \( \mathcal{L} \)-invariants are

\[
1; \mathcal{A}; \ldots; \mathcal{A}',
\]

and the number of \( \mathcal{L} \)-similar classes is \( \mathcal{A}' + 1 \). There is no ramification in these groups. The number of them amounts to 104.

The rest integers are

\[
\begin{align*}
(\text{I}) & \\
30 & = 2 \cdot 3 \cdot 5, \\
66 & = 2 \cdot 3 \cdot 11, \\
70 & = 2 \cdot 5 \cdot 7, \\
78 & = 2 \cdot 3 \cdot 13, \\
84 & = 2 \cdot 3 \cdot 7, \\
(\text{II}) & \\
30 & = 2 \cdot 3 \cdot 5, \\
66 & = 2 \cdot 3 \cdot 11, \\
70 & = 2 \cdot 5 \cdot 7, \\
78 & = 2 \cdot 3 \cdot 13, \\
84 & = 2 \cdot 3 \cdot 7,
\end{align*}
\]

and

\[
60 = 2^3 \cdot 3 \cdot 5.
\]

Every integer of \( \text{(I)} \) has the \( \mathcal{K} \)-matrix

\[
\begin{pmatrix}
2 & 1 \\
1 & 1
\end{pmatrix}
\]

Hence the possible \( \mathcal{L} \)-matrices are

\[
F_1 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},\quad F_3 = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix},\quad F_4 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.
\]

In every \( \mathcal{L} \)-similar class, there is only one group.

Every integer of \( \text{(II)} \) has the \( \mathcal{K} \)-matrix

\[
\begin{pmatrix}
3 & 1 \\
2 & 3
\end{pmatrix}
\]

The possible \( \mathcal{L} \)-matrices are

\[
F_1, F_2, F_3, F_4, F_5 = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}, F_6 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.
\]

Every class contains only one group.

The integer \( 2^3 \cdot 3 \cdot 5 \) has for its \( \mathcal{K} \)-matrix

\[
\begin{pmatrix}
3 & 1 \\
2 & 3
\end{pmatrix}
\]

All possible \( \mathcal{L} \)-matrices are

\[
F_1, F_2, F_3, F_4, F_5' = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}, F_6' = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}.
\]

Every class consists of one group.

Thus the number of all hypercyclic groups of order \( \leq 100 \) is

\[
36 + 10 \cdot 4 + 2 \cdot 4 + 3 \cdot 6 + 6 = 180.
\]

We have a proper ramification, i.e. an \( \mathcal{L} \)-similar class with plural hypercyclic groups, at the integer

\[
180 = 2^3 \cdot 3 \cdot 5.
\]

for the first time.

( ) Received September 23, 1932.


Department of Mathematics, Nikkio University.