EXTENSIONS OF GROUPS

A Thesis Presented for the
Degree of Master of Arts

by

Gerhard Albert Baum, B.A.

The Ohio State University
1947

Approved by: H.B. Mann
Introduction.

In 1926, O. Schreier proposed the problem of the extension of groups, a problem which can be described as follows: Given two groups $A$ and $H$, find all groups $G$ which contain $A$ as a normal subgroup and whose factor group $G/A$ is isomorphic to the given group $H$. $G$ is called an extension of $A$ by $H$.

Schreier has shown that the extension $G$ of $A$ depends on two sets of quantities:

1. the automorphisms of $A$,
2. a set of elements of $A$, the so-called factor set, which is a function of the representatives of the cosets of $A$ in $G$.

He developed a necessary and sufficient condition for quantities 1. and 2. such that they define an extension of $A$ by $H$, a condition which merely constitutes an "existence theorem" and is not designed to construct extensions of $A$ by $H$, leave alone all such extensions. However this condition can be refined in case the structure of $H$ is known, in particular if $H$ is abelian.

In 1933, R. Baer devoted a paper to the theory of group extension, treating in particular the automorphisms of the normal subgroup $A$. He showed that the group of automorphisms of $A$ determines uniquely the factor group $G/C$, where $C$ is the centre of $A$. If the centre of $A$ is the identity, its automorphisms determine $G$. 
Of the subsequent publications on the theory of extension, the most important one is by M. Hall who investigated central extensions, i.e. extensions of $A$ which have their factor sets in the centre of $A$. Making use of the theory of free groups, developed by O. Schreier and K. Reidemeister (1927), M. Hall reduces the problem of finding the central extensions of $A$ to the simpler one of solving 'linear' equations in a group ring. Using this method, all central extensions can be constructed.

A process for extending a non-abelian group $A$ with a factor set not wholly contained in its centre has not been developed so far.

The purpose of this thesis is an exposition of the theory of extension, a description of its development, giving proofs of the most important theorems. In an appendix applications of the theory to the extension of particular groups are given. A complete bibliography is attached which enables the reader to orient himself in the literature on the subject.
Extensions of Groups

1. Fundamental theorem on extensions .... 1
2. Extensions by a finite abelian group.. 5
3. The automorphisms of A ...............12
4. Normal product ..........................14
5. Central extensions ......................19
6. Appendix .................................30
7. Bibliography ............................36
1. Fundamental Theorem on Extensions.

A group $G$ is said to be an extension of a group $A$ by a group $H$, if $A$ is normal in $G$ and if the factor group $G/A$ is isomorphic to $H$.

Assume $G$ is such an extension. Then we may write

$$G = \overline{u} A + \overline{\mu} A + \overline{v} A + \cdots + \overline{w} A$$

where $\overline{u}$ is the representative of the coset associated with $u$ of $H$ by the isomorphism. We observe that each element of $G$ can be represented in the normal form $\overline{\alpha} \overline{\mu}$, where $\alpha$ is some element belonging to $A$. The group $G$ will be known, as soon as we discover the rules for multiplication, i.e. as soon as we determine the normal forms of $\alpha \overline{u}$ and $\overline{uv}$. To this purpose we define:

$$\alpha \overline{\mu} = \overline{\mu} \alpha \mu$$

where $\alpha = \overline{\mu}^{-1} \alpha \overline{\mu}$

$$\overline{\alpha \overline{u}} = \overline{\alpha u} \ (u, \overline{u})$$

where $(\mu, u) \in A$.

Since $A$ is normal in $G$, we have for all elements $\alpha$ of $A$:

$$\overline{\mu} \alpha \overline{\mu} = \alpha \mu \in A$$

(1,1)

$$(\alpha, \alpha_1) = \alpha \mu \alpha_1$$

(1,2)

$$(\alpha_1, \alpha_2) = \alpha_1 \mu \alpha_2$$

(1,3)

$$\overline{(\alpha \mu)^{u}} = \overline{(\alpha \mu)^{u}} = \overline{(\alpha \mu)^{u}} = \overline{(u, \overline{u}) \overline{(\alpha \mu)^{u}}}$$

(1,4)

$$\overline{1 \cdot \overline{1}} = \overline{1} (1,1) \ i.e. \overline{1} = (1,1)$$

(1,5)

$$\overline{\alpha \mu \alpha_1} = \overline{\mu \alpha_1 \overline{\mu}} \alpha_1 \alpha_2 = \overline{\mu \alpha_1 (u, \overline{u}) \alpha_1 \alpha_2}$$
Since the associative law holds in $G$, we have
\[ \mu(\bar{u} \bar{v}) = \mu \bar{v} \bar{w} (v, w) = \mu \bar{u} \bar{v} (u, v, w) \]
and
\[ (\mu \bar{v}) \bar{w} = \mu \bar{u} (u, \bar{v}, \bar{w}) = \mu \bar{u} \bar{v} (u, v, w)(\mu, w) \]
from which follows
\[ (\mu v_1, \mu w) (u, v) = (\mu, w)(v, w). \]

Conversely, if with every $u$ of $H$ there is associated a
mapping of $A$ unto itself, symbolically $A^u$, and with every $u$ and $v$ of $H$ an element $(u, v)$ of $A$, satisfying the following conditions:

1. (\mu) \mu = \mu \mu = 1
2. (\mu') \mu = (\mu, v)^{-1} \mu (u, v), \quad \alpha' = \alpha = \lambda
3. \mu (u, v) \mu (u, v) = (\mu, u \mu, v \mu)(u, v)

we shall construct a group $G$ which has a normal subgroup $A$ isomorphic to $A$ and a factor group $G/A$ isomorphic to $H$.

Let $G$ be the set of all elements $\mu d_1$ where multiplication is defined by:
\[ \mu_1 d_1 \cdot \mu_2 d_2 = \mu_1 \mu_2 (u, v) \mu_1 d_1 \mu_2 d_2, \]
and equality by: $\mu d_1 = \mu d_2$ if and only if $\mu = \mu$ and $d_1 = d_2$.

Consider the product
\[ \mu d_1 (\mu d_2, \mu d_3) = \mu d_1 \mu (v, w) d_2 \omega d_3 \]
\[ = \mu \mu (v, w) d_1 \omega d_2 \omega d_3 \]
\[ = \mu (u, v, w)(u, v) d_1 \omega d_2 \omega d_3 \quad \text{by II} \]
\[ = \mu (u, v, w)(u, v) d_1 \omega d_2 \omega d_3 \quad \text{by III} \]
which proves the associativity.

Putting \( v = w = 1 \) in III,

\[
(u,1)(u,1)' = (u,1)(1,1)
\]

(1,7) \( (u,1) = (1,1) \)

and putting \( u = v = 1 \) in III,

\[
(1,w)(1,1)^w = (1,w)(1,w)
\]

(1,8) \( (1,w) = (1,1)^w \)

Therefore \( i = 1 (1,1)^{-1} \) is the right identity:

\[
\overline{\mu} d \cdot i = \overline{\mu} d \cdot (1,1)^{-1} = \overline{\mu} (u,1) d' (1,1)^{-1}
\]

\[
= \overline{\mu} d' (1,1) (1,1)^{-1}
\]

\[
= \overline{\mu} d'.
\]

It remains to be shown that there exists a right inverse, i.e. that

\[
\overline{\mu} d' \cdot \overline{\mu} a^y = T (u,1)^{-1}
\]

has a solution.

Multiplying out, we have

\[
\overline{\mu} a^y (u,1) d' a^y = T (1,1)
\]

from which

\[
\overline{\mu} a^y = \overline{\mu}^{-1} \quad \text{and} \quad d' a^y = d^{-1} (u,1) (1,1)^{-1}.
\]

Therefore \( G \) is a group. The set \( \{ \bar{i}d \} \) forms a subgroup \( \bar{A} \) of \( G \):

\[
T (1,1)^{-1} d_1 \cdot T (1,1)^{-1} d_2 = T (1,1)^{-1} (1,1)^{-1} d_1 d_2
\]

(1,9)

and for \( d = 1 \), we have \( 1 \in \bar{A} \).
From (1.9) we also observe that \( \tilde{A} \) is isomorphic to \( A \) under the correspondence \( i_A \rightarrow A \).

Putting \( \tilde{\nu} = \lambda_\cdot \) we shall show that the element \( \tilde{\nu} \) form a system of representatives of \( \tilde{A} \) in \( G \):

\[
\tilde{\nu} \cdot i_A = \tilde{\mu} \cdot (1,1)^{-1} \cdot i_A = \tilde{\mu} (u,1) (1,1)^{-1} \cdot i_A
\]

(1.10) \( \tilde{\nu} \cdot i_A = \tilde{\mu} \cdot i_A \) from (1.7)

\[
\tilde{\nu} \cdot \omega = \tilde{\mu} \cdot (u,1) (1,1)^{-1} \cdot \omega = \tilde{\mu} \cdot (u,1) (1,1)^{-1} \cdot \omega
\]

(1.10) \( \tilde{\nu} \cdot \omega = \tilde{\mu} \cdot (u,1) (1,1)^{-1} \cdot \omega \)

(1.8) \( \tilde{\nu} \cdot \omega = \tilde{\mu} \cdot (u,1) (1,1)^{-1} \cdot \omega \)

(1.8) \( \tilde{\nu} \cdot \omega = \tilde{\mu} \cdot i_A \)

:: \( (i_A)^{\omega} = \tilde{\nu} \cdot i_A \)

We conclude: \( \tilde{A} \) is a normal subgroup of \( G \) with a system of representatives \( \tilde{\nu} \) corresponding to \( u \) of \( H \) under the mapping \( u \rightarrow \tilde{u} \rightarrow \tilde{u} \cdot L \) and inducing automorphisms \( \tilde{A}^u \), and a factor set \( i(u,v) \). \( \tilde{A} \) is isomorphic to \( A \) under the mapping \( i_A \rightarrow A \). This establishes

**Theorem 1.1**: Equations I, I, II, III are the necessary and sufficient conditions that an extensions of \( A \) by \( H \) is defined by the mapping \( \tilde{\nu} \cdot \tilde{A} = \tilde{A}^u \cdot i_A \), \( \cdot \in \tilde{A} \), and the factor set \( (u, v) = \frac{\tilde{\mu} \cdot \omega}{\tilde{\mu} \cdot \omega} \).
2. Extension by a Finite Abelian Group.

In case H is abelian, the necessary and sufficient conditions for the extension of A by H can be simplified considerably.

First we shall consider the extension of A by a cyclic group \( H = \{ \mu \} \) of order \( n \). As before we shall find the necessary conditions and then show that these are sufficient.

Let \( \bar{u} \) be the representative of the coset of A in G assigned to u of H. Then \( 1, \mu, \mu^2, \ldots, \mu^{n-1} \) may be taken as a system of representatives of A in G. Since A is normal in G, \( \bar{u} \) transforms A into itself, so that \( \bar{u} \) may be said to induce an isomorphism of A unto itself, symbolically \( A^u \).

The element \( \mu^n \) will again belong to A, say \( \mu^n = \alpha \) so that
\[
\alpha^u = (\mu^n)^u = \mu^u \mu^n \mu = \mu^n
\]
and
\[
\alpha^{u^n} = \bar{\mu}^{-n} \alpha \bar{\mu}^n = \bar{\alpha}^n \alpha = \alpha^n.
\]

Then
\[
\mu^j \mu^k = \mu^{j+k} (\mu, \mu^k) = \begin{cases} 1, & j + k < n \\ \alpha, & j + k \geq n \end{cases}
\]
where
\[
(\mu^j, \mu^k) = \begin{cases} 1, & j + k < n \\ \alpha, & j + k \geq n \end{cases}
\]

Conversely, we have

**Theorem 2.1**: If to each u of H corresponds a mapping \( A^u \) of A unto itself, and if the following conditions are given
\[
(\alpha_1, \alpha_2) = \alpha_1 \alpha_2^u, \quad \alpha_1, \alpha_2 \in A
\]
2,II  
\[ \alpha^n = \alpha^a \quad , \quad \alpha \in A \]

2,III  
\[ \alpha^u = \alpha \quad , \quad \alpha \in A \]

then there exists one and only one extension G of A such that \( G/A = \{aA\} \cong H \) where \( \mu^{-1} \mu = \alpha \) and \( \mu^n = \alpha \).

Proof: Let us construct G.

Define
\[
\begin{cases}
(u^j, u^k) = 1 & j+k < n \\
(u^j, u^k) = \alpha & j+k \geq n
\end{cases}
\]

Then 1, I is satisfied by virtue of 2, I. Condition 1, II is fulfilled since
\[
(d_\alpha^j u^k) = (u^j, u^k)^{-1} u^i u^k (u^j, u^k)
\]
holds for \( j+k < n \) and \( j+k \geq n \). There remains the verification of 1, III which becomes
\[
(u^{i+j}, u^k)(u^i, u^j) = (u^i, u^{j+k})(u^j, u^k)
\]
for all \( i,j,k \), since \( (u^i, u^j) = (u^i, u^j) \). We observe that this relation is merely an identity in \( l \) and \( a \), depending on \( i,j,k \) alone, independent of the structure of A. Indeed it could be verified by considering all possible combinations of inequalities between the \( i,j,k \), and \( n \).

There is however a better way to verify 1, III. The infinite cyclic group \( \{\mu\} \) is an extension of the infinite cyclic group \( \{\mu^n\} \) by our given group H, so that 1, III must be satisfied for this case. Since the validity of
1,III is independent of the structure of $A$ and since in this case the element $a = \overline{u}^n$ is bound by no relations, 1,III will be valid for all $A$. This proves the theorem.

Since the extension $G$ is uniquely determined by $A$, $\overline{u}$, and $a$, we may refer to it by the symbol $G(A, \overline{u}, a)$.

What is the condition that $G(A, \overline{u}, a)$ and $G(A, \overline{u}, a^*)$ define the same abstract group? Assuming that they define the same group, $\overline{u}^n = \overline{x}^\rho$ for $\alpha \in A$, and $(n,p) = 1$.

We may write

$$\overline{u}^n = a^* = (\overline{x}^\rho \alpha)^n = \overline{x}^{np} \cdot \alpha \cdot 1 + \alpha \cdot \ldots \cdot \alpha \cdot \alpha$$

or

$$a^* = \alpha \cdot \ldots \cdot \alpha$$

(2,1)

Conversely if $\overline{A}^\mu = \overline{A}^\mu \alpha$, $(n,p) = 1$ and condition (2,1) is satisfied, then the extensions $(A, \overline{u}, a)$ and $(A, \overline{u}, a^*)$ define the same abstract group.

Now we consider the extension $G$ of $A$ by an abelian group $H$, which is given as the direct product of cyclic groups of prime power order.

$$H = \{u_i\} \times \{u_1\} \times \ldots \times \{u_l\}$$

where $n_i$ is the order of $\{u_i\}$. Again we shall find the necessary conditions, assuming that the extension $G$ is known, and then show that these conditions are actually sufficient to construct $G$ from $A$ by $H$.

Let $\overline{u}_i A$ be the coset assigned to $u_i$ of $H$. Then the following relations are valid in $G$:

$$\overline{\mu}_i^{-1} \alpha \overline{\mu}_i = \alpha \overline{u}_i \in A$$

since $A$ is normal.
\[ \overline{\mu_i}^{n_i} = a_i \in A \quad \text{since} \{\mu_i\} \text{ is cyclic.} \]
\[ \overline{\mu_i} \overline{\mu_k} \overline{\mu_i} \overline{\mu_k} = [\overline{i}, \overline{k}] \in A \quad \text{since} \overline{u_i} \overline{u_k} \text{ and } \overline{u_k} \overline{u_i} \text{ belong to the same coset.} \]

For the automorphisms \( A^u \) of \( A \) the following rules hold:
\[
\begin{align*}
(a_1, a_2) &= (a_1, a_2) \overline{u_i} \\
\overline{u_i} &= a_i^{-1} \\
\overline{u_i}^{n_i} &= a_i^{-n_i} \\
\overline{u_i}^u &= a_i^{-u} \\
\overline{u_i} u_k &= u_k \overline{u_i} [\overline{i}, \overline{k}] \\
\overline{u_i} \overline{u_k} &= a_k^{-1} u_i [\overline{i}, \overline{k}] \
\end{align*}
\]

Since \( \{\mu_i\} \) is cyclic.

For the commutator element \([\overline{i}, \overline{k}]\) the following relations must hold:
\[
\begin{align*}
[\overline{i}, \overline{k}][\overline{h}, \overline{i}] &= \overline{\mu_i}^{-1} \overline{\mu_h}^{-1} \overline{\mu_i} \overline{\mu_h} - \overline{\mu_i}^{-1} \overline{\mu_h}^{-1} \overline{\mu_i} \overline{\mu_h} \\
&= 1 \\
\overline{u_i}^{-1} &= \overline{a_k}^{-1} \overline{u_i}^{-1} \\
\overline{a_k}^{-1} &= \overline{\mu_i}^{-1} \overline{\mu_h}^{-1} \overline{\mu_i} \overline{\mu_h} \\
&= \overline{\mu_i}^{-1} \overline{\mu_k} \overline{\mu_i} \overline{\mu_k} \overline{\mu_i} \overline{\mu_k} \cdots n_k \text{ times} \\
&= (\overline{\mu_i} \overline{\mu_h} \overline{\mu_i})^{n_k} = (\overline{\mu_h} [\overline{i}, \overline{k}])^{n_k} \\
&= \overline{\mu_i}^{n_k} \overline{\mu_h}^{-1/2} \overline{[\overline{i}, \overline{k}]} \overline{\mu_h}^{-1/2} \overline{[\overline{k}, \overline{i}]} \overline{\mu_h}^{n_k-2} \\
&= \cdots \overline{\mu_h}^{n_k-1} \overline{[\overline{k}, \overline{i}]} \overline{\mu_h}^{-1} \overline{[\overline{i}, \overline{k}]} \\
&= a_k [\overline{k}, \overline{i}] \overline{\mu_k}^{n_k-1} [\overline{k}, \overline{i}]^{n_k} + \cdots [\overline{k}, \overline{i}]^{u_k [\overline{k}, \overline{i}]} \\
&= (2, 2) \\
\end{align*}
\]
and finally
\[
[\overline{k}, \overline{i}]^{\overline{\mu_k}} = (\overline{\mu_h}^{\overline{i}} \overline{\mu_e}^{\overline{i}} \overline{\mu_h} \overline{\mu_e})^{\overline{\mu_k}} = (\overline{\mu_i}^{\overline{i}} \overline{\mu_h} \overline{\mu_i})^{\overline{\mu_k}} (\overline{\mu_i}^{\overline{i}} \overline{\mu_h} \overline{\mu_i}) / (\overline{\mu_i}^{\overline{i}} \overline{\mu_h} \overline{\mu_i})
\]
\[
\begin{align*}
&= (\mu_k [b, i])^{-1} (\mu_e [p, c])^{-1} \mu_k [b, i] \mu_e [p, c] \\
&= (\mu_e [p, c] \mu_k [b, i])^{-1} \mu_k [b, i] \mu_e [p, c] \\
&= (\mu_k \mu_e [l, i] \mu_k [b, i])^{-1} \mu_k [b, i] \mu_e [p, c] \\
&= [k, i]^{-1} [p, c]^{- \mu_k} \mu_k^{-1} \mu_e^{-1} \mu_k [b, i] \mu_e [p, c] \\
&= [k, i]^{-1} [p, c]^{- \mu_k} [l, i] [h, c] \mu_e [p, c] \\
(2,3) &= [k, i]^{-1} [p, c]^{- \mu_k} [l, i] [h, c] \mu_e [p, c]
\end{align*}
\]

or, making use of \([c, h] [b, i] = 1\)

\[(c, h) \mu_e [b, i]^{-1} [p, c]^{- \mu_k} [l, i] [c, h]^{-1} = 1\]

Conversely, assuming a group \(A\) is given with elements \(a_i, [1, k] (1, k = 1, \ldots, r)\) belonging to it and a set of mappings \(A^{u_i}\) corresponding to elements \(u_i\) of \(H\), obeying the rules

\[
\begin{align*}
1. & \quad (d_1 d_2)^{u_i} = d_1^{u_i} d_2^{u_i} \\
2. & \quad d^{u_i} = d^{a_i}, \quad a_i^{u_i} = a_i \\
3. & \quad u_i u_k = u_k^{[c, h]} [k, i][c, h] = 1 \\
4. & \quad a_k = q_k [k, i] \\
5. & \quad [c, h]^{u_i} [b, i]^{-1} [p, c]^{- \mu_k} [l, i] [c, h]^{-1} = 1
\end{align*}
\]

then we shall prove

**Theorem 2.2**: The group \(G\) with generators \(\overline{u}_i\) and \(d \in A\), multiplication defined by relations (2,4) and the following laws

\[
\begin{align*}
\text{a)} \quad & \quad \overline{u}_i^{-1} d \overline{u}_i = a^{u_i}
\end{align*}
\]
\[ \overline{\mu}_r^{n_r} = \alpha_r \]

possesses \( A \) as a normal subgroup, and its factor group \( G/A \)
is the direct product of cyclic groups \( \{ \overline{\mu}_z A \} \) of order \( n_z \).

Proof: For \( r = 1 \), the theorem is equivalent to theorem 2.1 and therefore holds, while 3, 4, 5, and c have no significance. For \( r > 1 \), we shall assume that the theorem is valid if in addition to \( \alpha \in A \) only \( \overline{\mu}_1, \ldots, \overline{\mu}_{r-1} \) occur as generators, and complete the proof by induction.

Let \( G, \alpha \) be the group generated by the \( \alpha \in A \) and \( \overline{\mu}_1, \ldots, \overline{\mu}_{r-1} \)
subject to the relations 1. to 5. and the rules a, b, c, with indices varying from 1 to \( r-1 \).

Consider the cyclic group \( \{ \mu_r \} \) of order \( n_r \), and let \( A^u_r \)
be an automorphism of \( A \). We define the element \( \overline{\mu}_r \) such that
\[ (2,5) \quad \overline{\mu}_r^{n_r} = \alpha_r \]
and with rules of multiplication defined by
\[ (2,6) \quad \overline{\mu}_r^{-1} \cdot \overline{\mu}_r = \alpha^{\mu_r} \quad \text{and} \]
\[ (2,7) \quad \overline{\mu}_r^{-1} \cdot \overline{\mu}_k \cdot \overline{\mu}_r = \overline{\mu}_k [k, r] \quad k = 1, \ldots, r-1. \]

Since (2,4) 1. to 5. hold, we can show that \( \overline{\mu}_r \) induces an
automorphism on \( G, : \)
\[ \overline{\alpha}_r \quad \overline{\alpha}_{r-1} \]
from 1.
\[ (\overline{\mu}_k \cdot \overline{\alpha}_r \cdot \overline{\alpha}_r) = \overline{\mu}_r \cdot \overline{\mu}_k \cdot \overline{\alpha}_r \cdot \overline{\alpha}_r = \overline{\mu}_r \cdot \overline{\mu}_k \cdot \overline{\mu}_r \cdot \overline{\mu}_r \cdot \overline{\mu}_r \cdot \overline{\mu}_r \cdot \overline{\mu}_r \cdot \overline{\mu}_r \cdot \overline{\alpha}_r \]
\[ = \overline{\mu}_k \cdot \overline{\alpha}_r \cdot \overline{\alpha}_r \cdot \overline{\alpha}_r \]

On account of 3, 4, and 5, for \( r = 1 \), this mapping has
a unique effect on \( \alpha^{u_k}, \alpha_k \), and \( [k, \ell] \) respectively, for
all \( k, \ell < r \). From this follows that the mapping of \( G, \) induced by \( \overline{\alpha}_r \) satisfies condition 2,1 of theorem 2.1.
From (2,4) 2. \[ a_r^{u_r n_r} = \alpha_r \]
and
\[ \bar{\alpha}_r^{u_r n_r} \bar{\mu}_r^{n_r - u_r n_r} = \bar{\alpha}_r \left[ u_r \right] \mu_r \ldots \mu_r^{u_r n_r + u_r n_r} \]
so that 2,II is satisfied. Also from 2. and (2,5) it follows that 2,III is fulfilled. Therefore we may apply theorem 2.1 to the cyclic extension of \( G_1 \) by \( \{ u_r \} \) of order \( n_r \), and conclude that there exists a unique extension \( G \) such that \( G/G_1 = \{ \bar{\alpha}_r \} \). Since \( A \) is normal in \( G_1 \) and on account of (2,6), \( A \) is also normal in \( G \). From (2,7) it follows that \( G/A \) is abelian; in fact \( G/A \) is the direct product \( G/G \times G/A \). Applying the induction assumption to \( G_1/A \), we see that \( G/A \) is generated by the elements \((\bar{u}_1 A), (\bar{u}_2 A), \ldots, (\bar{u}_r A)\).

It remains to be shown that the invariants of \( G/A \) are indeed \((n_1, n_2, \ldots, n_r)\). Let \[ \prod_{i=1}^{r} \left( \bar{\alpha}_i A \right)^{v_i} = 1 \]
or simply \[ \prod_{i=1}^{r} \bar{\alpha}_i^{v_i} = 1 \pmod{\alpha A} \]
Since \( u_1, \ldots, u_{r-1} \) form a basis of \( G_1 \pmod{A} \Rightarrow G_1/A \)
\[ \bar{\alpha}_r^{v_r} \equiv 1 \pmod{A} \]
i.e. \( v_r \equiv 0 \pmod{n_r} \)
Therefore \( G/A \) is the direct product of cyclic groups \( \left\{ \bar{\alpha}_i A \right\} \)
i = 1, \ldots, r , having orders \( n_i \). In other words the invariants of \( G/A \) are \((n_1, n_2, \ldots, n_r)\).
3. The Automorphisms of A.

G is an extension of A by H; we may write

\[ G = \overline{u}A + \overline{\mu}A + \overline{\nu}A + \cdots + \overline{\omega}A \]

where \( \overline{u}A \overline{u} = A^u \) and \( \overline{u} \overline{v} = \overline{uv} \) \((u,v), (u,v) \leq A\). We shall investigate the requirements which condition 1,II

\[ (\lambda^\mu)^\nu = (u,v)^{-1} \lambda^\mu (u,v) \]

puts on the automorphisms of A.

Let \( \mathfrak{A} \) be the group of all automorphisms of A, and \( \mathfrak{I} \) the group of inner automorphisms, then 1,II implies

\[ (\lambda^\mu)^\nu = \lambda^{\mu \nu} (\text{mod } I) \]

so that

\[ (1) \quad H \xrightarrow{\text{in}_I} \mathfrak{A}/\mathfrak{I} \]

is a homomorphism. However, as we shall see, the mapping must fulfill a stronger condition. Every element u of H corresponds to an element \( K(u) \) under the mapping (1)

\[ \mu \longrightarrow K(u), \]

where \( K(u) \) is a class of automorphisms, every two of which differ only by an inner automorphism.

Let C be the centre of A. Elements belonging to the same coset of C in G induce the same automorphisms on A. In addition, if \( g_1C \) and \( g_2C \) are two such cosets then \( g_1g_2 \) belongs to the coset \( g_1g_2C \) though, of course, \( g_1g_2 \) need not be chosen as its representative. Hence the mapping

\[ (2) \quad G/C \xrightarrow{\text{in}_I} \mathfrak{A} \]

is a homomorphism.

It is clear that the elements in \( \overline{u}A \) should induce auto-
morphisms by the mapping (2) which are all contained in the class of automorphisms $K(u)$ induced by the mapping (1). We require therefore that the homomorphism

$$\begin{align*}
(1) \quad H \twoheadrightarrow G/A \xrightarrow{\text{in}_I} \mathcal{O}/J
\end{align*}$$

is actually contained in the mapping (2).

Since elements belonging to the same coset of $C$ in $A$ produce the same inner automorphism,

$$A/C \twoheadrightarrow J.$$

$A/C$ is normal in $G/C$ and $J$ is normal in $\mathcal{O}$, so that (1) is contained in (2) as the mapping of the factor groups due to isomorphic normal subgroups:

$$G/C \twoheadrightarrow A/C = G/A \xrightarrow{\text{in}_I} \mathcal{O}/J.$$

We therefore say that every mapping (1) $u \rightarrow K(u)$ determines the larger homomorphism (2) $G/C \rightarrow \mathcal{O}$ of which it is a part. From this R. Baer derived the following theorem the proof of which is too complicated to be given here.*

Theorem 3.1: Given two groups $A$ and $H$, the correspondence $u \rightarrow K(u)$ determines uniquely the extension $G$ (mod $C$).

Corollary: If $C = 1$, the mapping $u \rightarrow K(u)$ determines the extension $G$ uniquely.

* R. Baer "Erweiterung von Gruppen und ihren Isomorphismen" (see bibliography) p. 378.
4. The Normal Product.

Let us investigate conditions when two extensions $G$ and $G'$ define the same abstract group. Again we let

$$G = \overline{A} A + \overline{A} A + \overline{A} A + \ldots + \overline{A} A$$

and let us choose new representatives $\overline{u} = u \varphi(u)$ where $\varphi(u) \in A$. Then

$$\overline{u} \varphi = \overline{u} \varphi \varphi(\varphi) = \overline{u} \varphi (u, \varphi) \varphi \varphi(\varphi) = \overline{u} \varphi (u, \varphi) \varphi \varphi(\varphi)$$

which we write

$$= \overline{u} \varphi (u, \varphi)'$$

where

$$\varphi(\varphi) = (u, \varphi)' \varphi(\varphi) \varphi \varphi(\varphi) \varphi \varphi(\varphi)$$

The automorphisms may be written

$$\overline{u} \varphi = \overline{u} \varphi \varphi(\varphi) \varphi \varphi(\varphi) \varphi \varphi(\varphi)$$

or

$$\overline{\varphi} \varphi = \overline{\varphi} \varphi \varphi(\varphi) \varphi \varphi(\varphi) \varphi \varphi(\varphi)$$

so that the mappings induced by $\overline{u}$ and $\overline{u}$ differ only by an inner automorphism. Two extensions of $A$ given by the automorphisms $\overline{u}$ and $\overline{u}$, and the factor sets $(u, \varphi)$ and $(u, \varphi)'$ always define the same abstract group if there are elements $\varphi(\varphi)$ in $A$ for each $u$ of $H$, such that (4,1) and (4,2) are satisfied. Factor sets satisfying (4,1) are called equivalent, in symbols

$$(u, \varphi) \sim (u, \varphi)'$$

It can easily be verified that this equivalence is symmetric, reflexive, and transitive. Groups which define the same abstract group are sometimes called equivalent.

A factor set $(u, \varphi)$ is equivalent to the factor set con-
sisting of the identity alone, if elements \( \alpha(\mu) \) exist in A for all \( \mu \) of H, such that
\[
(4,3) \quad 1 = \alpha(\mu_2)^{-1} (\mu_1, \mu_2) \alpha(\mu_1) \alpha(\mu_2).
\]
This means that there is a complete system of representatives which forms a group, since \( \overline{\mu} \overline{\nu} = \overline{\mu \nu} \). A factor set equivalent to the identity is called normal, and the extension due to it, is called a normal product of A by H.

We notice that a normal product reduces to the direct product \( G = A \times H \) in case the automorphisms of A are all the identical mapping of A unto itself.

Factor sets belonging to the centre of A are called abelian factor sets and the extensions defined by them are termed central extensions of A.

Let the factor set \((\mu, \nu)\) belong to the centre of A for all \(\mu\) and \(\nu\) of H. Keeping \(\nu\) fixed, let us multiply \((\mu, \nu)\) over all \(\mu\) of H, obtaining an element \( y' \) in C which is a function of \(\nu\) alone. We put
\[
y'(\nu) = \prod_{\mu} (\mu, \nu), \quad y'(\nu) \in C.
\]
Multiplying condition 1,III over all \(\mu\), we have
\[
y'(\omega) y'(\nu) = y'(\omega \nu) (\nu, \omega)^n
\]
where \(n\) is the order of H,

or
\[
(\nu, \omega)^n = y'(\omega)^{-1} y'(\nu) y'(\omega).
\]

Comparing this with the condition of normality of factor sets \((4,3)\), we observe that
(4,4) \quad (v,w)^n \sim 1.

Hence we have

**Theorem 4.1**: If \( n \) is the order of \( H \), then the \( n \)th power of any abelian factor set is an normal factor set.

Making use of this result, we come to the main theorem of this section.

**Theorem 4.2**: If the order of \( H \) is prime to the order of \( A \) then the extension of \( A \) by \( H \) is a normal product.

**Proof:** Let \( n \) be the order of \( H \), and \( m \) the order of \( A \).

We must show that any extension \( G \) of \( A \) by \( H \) contains a subgroup of order \( n \). For \( m = 1 \), the theorem is true. For \( m > 1 \), we shall assume the theorem true whenever the order of the normal subgroup is less than \( m \), and complete the proof by induction. (We shall also assume the Sylow-Theorems, in particular that the number of \( p \)-Sylow groups \( S_p \) is the index of \( N_p \), the normaliser of \( S_p \), in \( G \); See A. Speiser "Die Theorie der Gruppen von endlicher Ordnung", p. 67.)

Let \( p \) be a prime factor of \( m \). Then \( p \) is prime to \( n \), and each \( p \)-Sylow group \( S_p \) of \( G \) lies in \( A \), so that there are as many \( S_p \) in \( G \) as there are in \( A \). Hence, if we let the symbol \( (X/Y) \) stand for the index of \( Y \) in \( X \), we have

\[
(G/N_p) = (A/A \cap N_p) \quad \text{or} \quad (N_p/A \cap N_p) = (G/A) = \kappa.
\]

*H. Zassenhaus gives this proof (see bibliography), referring it to Schur without indicating where it was published. I could not find this proof in the literature.*
Since $A \cap N_p$ is normal in $N_p$, the factor group $A_nN_p/S_p$ is normal in the factor group $N_p/S_p$ and from the preceding sentence of index $(N_p/A_nN_p) = n$. The order of $N_p/S_p$ therefore is $n$ times a divisor of $m$.

The induction assumption may be applied, and we have a group $K/S_p \subset N_p/S_p$, where $K/S_p$ is of order $n$. Again $S_p$ is normal in $K$, and hence $S_p/C_p$ normal in $K/C_p$ where $C_p$ is the centre of $S_p$, and from the preceding sentence of index $(K/S_p) = n$. The order of $K/C_p$ is $n \cdot (a$ divisor of $m)$, so that the induction assumption may be applied again. We have a subgroup $L/C_p \subset K/C_p$, where $L/C_p$ is of order $n$.

Let $(u,v)$ be a factor set of $L$ over its normal subgroup $C_p$. The order $c$ of $C_p$ is prime to $n$, so that the congruence $hn' \equiv 1 \pmod{c}$ can be solved for $n'$. Therefore we may interpret the factor set $(u,v)$ as the $n'$th power of the factor set $(u,v)^n$, which according to theorem 4.1 is normal:

$$(u,v)^n \sim 1$$

$$[u,v]^n = (u,v)(u,v)^{\alpha} = (u,v) \sim 1$$

We conclude that $L$ is the normal product of $C_p$ by a group $H$ of order $n$. But $\overline{H} \subset K \subset G$. Q.E.D.

It might be mentioned that there is a very useful classical theorem which actually deals with the problem of extension: A normal subgroup which is a complete group is a direct factor. (For the proof we refer the reader to A. Speiser, op. cit., p. 125, Satz 110.)
Now consider a fixed mapping of \( H \) into the group of automorphisms of \( A \), such that to each \( u \) there corresponds an automorphism \( A^u \) independent of the representative of the coset of \( A \) in \( G \) which is associated with \( u \). Then from (4,2), we have
\[
\overline{\mu}^{-1} \overline{A} \overline{\mu} = \alpha(u)^{-1} \left( \overline{\mu}^{-1} \overline{A} \overline{\mu} \right) \alpha(u) = \overline{\mu}^{-1} \overline{A} \overline{\mu}
\]
so that \( \alpha(u) \) belongs to \( C \) for all \( u \) of \( H \).

Let \( (u,v)_1 \) and \( (u,v)_2 \) be two abelian factor sets satisfying condition 1,III and let \( (u,v)_3 = (u,v)_1 \cdot (u,v)_2 \), then condition 1,III is satisfied by \( (u,v)_3 \), since
\[
(u,v)_1 (u,v)_2 \left[ \left( (u,v)_1 \right) (u,v)_2 \right] \omega = (u,v)_1 (u,v)_2 \left[ \left( (u,v)_1 \right) (u,v)_2 \right] \omega
\]
implies
\[
(u,v)_3 (u,v)_3 \omega = (u,v)_3 (u,v)_3 .
\]
Hence \( (u,v)_3 \) is a factor set. Moreover there is an identity factor set consisting of the identity alone, and an inverse set to \( (u,v) \) obtained by replacing \( (u,v) \) by \( (u,v)^{-1} \) throughout. We conclude therefore that the totality of abelian factor sets form a group.

We denote by \( \overline{\alpha} \) equivalence of two extensions with the same automorphisms \( A^u \). If \( (u,v)_1 \overline{\sim} (u,v)_1 \) and \( (u,v)_2 \overline{\sim} (u,v)_2 \) then
\[
(u,v)_1 (u,v)_1 \overline{\sim} (u,v)_1 (u,v)_2
\]
since
\[
(u,v)_1 (u,v)_2 = \alpha(u)^{-1} (u,v)_1 \alpha(u) \cdot \alpha(u)^{-1} (u,v)_2 \alpha(u) . \alpha(u)^{-1} (u,v)_1 \alpha(u) \alpha(u)^{-1} (u,v)_2 \alpha(u)
\]
\[
= \alpha_{12}(u)^{-1} \left[ \alpha(u)^{-1} \alpha_{12}(u) \right] \overline{\alpha} \alpha(u)^{-1} \alpha_{12}(u) \cdot \alpha(u)^{-1} \alpha_{12}(u) \overline{\alpha} \alpha(u)^{-1} \alpha_{12}(u)
\]
\[
= \alpha_{12}(u)^{-1} \alpha_{12}(u) \overline{\alpha} \alpha_{12}(u) \cdot \alpha(u)^{-1} \alpha_{12}(u) \overline{\alpha} \alpha(u)^{-1} \alpha_{12}(u)
\]
satisfies (4,3). We notice that the fact that \((u,v)\) and 
\(\varphi(\lambda)\) belong to the centre of \(A\) is essential.

Hence the totality of abelian factor sets form a group, 
even after equivalent sets with the same automorphisms 
\(A^u\) have been identified. Distinct elements of this group 
define distinct extensions; it is therefore called the 
\textit{group of extensions}.

5. Central Extensions.

Let us first consider several introductory definitions. 
Let \(\lambda\) be an element of \(C\), the centre of \(A\), and 
\(\lambda \rightarrow \lambda^\mu\) 
be an automorphism of \(A\) induced by \(u\) of \(H\), where we again 
assume that the set of automorphisms \(A^u\) is fixed, inde­
pendent of the choice of representatives.
Define \((a^n)^h = (a^u)^h\) or simply \(a^n^h\), where \(n\) is an integer. Then

\[
d^u \cdot d^s \cdot \cdots \cdot d^t^w = d^{u+s+w+\cdots + t^w}
\]

and if \(h\) belongs to the group ring \(H^* = \sum \eta^u\), \(n\) an integer and \(u \in H\), the element \(a^n^h\) is uniquely defined. The following rules will hold:

\[
(d^h)^{\beta} = d^{h \beta}, \quad d^{h+k} = d^h \cdot d^k
\]

(5,1)

\[
(d^{h/k}) = d^{h/k}
\]

Now consider the free abelian group on a set of generators

(5,2) \(a^i, a^u, a^v, \ldots, l, u, v, \ldots\) from \(H\).

Its elements are of the form \(a^n^h\) with \(h\) from \(H^*\) and obey the rules (5,1). Among its automorphisms are the permutations of its generators

(5,3) \(\omega = \begin{pmatrix} a^u \\ a^v \end{pmatrix}\)

which form a group isomorphic to \(H\). Since the group is not restricted by any relations,

(5,4) \(a^n^h = 1\) implies \(h = 0\).

Such a group will be called operator free.

In the following paragraphs an elementary knowledge of free groups is assumed. For an introduction the reader is referred to Reidemeister, "Einführung in die kombinatorische Topologie," chpt. 1 to 3.

We shall consider a central extension \(G\) of \(A\) by \(H\), and assume that \(H\) is given by its generators and defining relations.
Let \( x, y, z, \ldots \) be a set of generators of \( H \) and let each element in \( H \) be represented by a definite word in \( x, y, z, \ldots \). We shall choose as the representatives of the cosets of \( A \) the corresponding words in \( \bar{x}, \bar{y}, \bar{z}, \ldots \), which will generate a subgroup \( \bar{G} \) of \( G \).

The free group on elements \( x, y, z, \ldots \) is mapped homomorphically onto \( \bar{G} \) by the correspondence \( x \rightarrow \bar{x}, y \rightarrow \bar{y}, \ldots \), and \( \bar{G} \) in turn is mapped homomorphically onto \( H \) by the correspondence \( \bar{x} \rightarrow x, \bar{y} \rightarrow y, \ldots \). Thus we have a double mapping \( x \rightarrow \bar{x} \rightarrow x \) which takes \( F \rightarrow \bar{G} \rightarrow H \).

Let the defining relations of \( H \) be

\[
(5,5) \quad \phi_i(x,y,z,\ldots) = 1 \quad i = 1, \ldots, r.
\]

The words mapped on the identity of \( H \) form the least normal subgroup \( R \) of \( F \) containing the elements \( \phi_i(x,y,z,\ldots) \).

But the relations \( x\bar{y} \bar{x} \bar{y} \) in the factor set \( (x,y) = \bar{x}\bar{y} \bar{x}\bar{y} \) are mapped on the identity of \( H \), so that the corresponding words lie in \( R \). These words in fact generate \( R \).*

Since for central extensions the factor sets lie in \( C \), we have by the above double mapping

\[
R \rightarrow \bar{C} \rightarrow 1
\]

where \( \bar{C} \) is a subgroup of \( C \).

---

* If \( F = R + \tilde{x} R + \tilde{y} R + \ldots \), where the representatives of the cosets are the words corresponding to the elements of \( H \), then \( R \) is generated by all those elements of \( F \) which correspond to \( \bar{x}\bar{y}^{-1} \bar{x} \bar{y} \), which are precisely \( (x,y) \). See Reidemeister, op. cit., p. 67. \( \)
Hence

\[(5,6) \quad \Phi_i(x, y, z, \ldots) = \alpha_i \in \mathcal{C}, \quad i = 1, \ldots, r.\]

Since \(\Phi_i(x, y, z, \ldots)\) generate \(\mathcal{R}\), i.e., since all words of \(\mathcal{R}\) corresponding to factor sets, can be expressed as products or transforms of \(\Phi_i(x, y, z, \ldots)\), we observe that equations \((5,6)\) determine for each element of \(\mathcal{R}\) its image in \(\mathcal{C}\). In particular \((5,6)\) determines all factor sets as products and transforms of the \(\alpha_i\).

Since \(\mathcal{C}\) is abelian, the commutator group \(\mathcal{K}\) of \(\mathcal{R}\) is mapped on the identity of \(\overline{G}\):

\[\mathcal{K} \rightarrow 1 \rightarrow 1\]

Hence elements of \(F\) congruent mod \(\mathcal{K}\) are mapped on the same element of \(\overline{G}\). We shall use this result to establish the Theorem 5.1: A necessary and sufficient condition that

\(\Phi_i(x, y, z, \ldots) = \alpha_i, \quad i = 1, \ldots, r,\) define a central extension of \(A\) by \(H\) is that whenever

\[\prod \Phi_i^h \equiv 1 \quad \text{in} \quad F \mod \mathcal{K}\]

we have

\[\prod \alpha_i^h \equiv 1.\]

Proof: Elements \(\prod \Phi_i^h\) in \(F\) mod \(\mathcal{K}\) are mapped on \(\prod \Phi_i^h\) in \(\overline{G}\), or simply on \(\prod \alpha_i^h\), so that the necessity is obvious. Conversely, the factor set and therefore the \(\alpha_i\) must satisfy condition 1,III if we are to have an extension of \(A\) by \(H\).

1,III is nothing but an elementary deformation of identities in \(F\) and all the more therefore in \(F\) mod \(\mathcal{K}\):
\[(\overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}})(\overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}}) = (\overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}})(\overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}})\]
\[
\overline{\mu \omega^{-1}}(\overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}}) = \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}} = \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}} \overline{\mu \omega^{-1}}
\]

and since to all identities in \(F \mod k\) correspond identities in the \(\alpha_i\), the elements \(\alpha_i\) satisfy condition I, III.

Let us now change the representatives of the cosets by putting \(x = \xi x, \ y = \eta y, \ldots\), where \(\xi, \eta, \ldots\) are arbitrary elements of \(\mathbb{C}\). Then

\[(5,7) \quad \phi_c(\overline{x, y, \ldots}) = \phi_c(\overline{x, y, \ldots}) \xi \eta \ldots\]

if we move \(\xi, \eta, \ldots\) to the end of the words according to the rule

\[\xi h_{\omega^{-1}} = \overline{\mu} \xi h_{\omega^{-1}}\]

The elements \(x_i, y_i, \ldots\) from \(H^*\), defined by the equations (5,7) are of great significance for the following theorems, which together with theorem 5.1 determine all central extensions of \(A\) by \(H\).

**Theorem 5.2**: \(\prod \phi_{\xi}^{h_i} = 1\) if and only if \(\sum x_i h_i = 0, \sum y_i h_i = 0\), etc.

**Theorem 5.3**: The group of central extensions of \(A\) by \(H\) is the group of

\[\left[\alpha_1, \alpha_2, \ldots, \alpha_r\right] \mod (\beta_1, \beta_2, \ldots, \beta_r)\]

with \(\prod \alpha_i^{h_i} = 1\) for all relations of theorem 5.1 and

\[\beta_i = \xi x_i \eta y_i \ldots\]

determined by equations (5,7).

The meaning of these theorems is clear: Being given the relations \(\phi_c\) of \(H\), we can find \(x_i, y_i, \ldots\) by equations (5,7), and \(x_i, y_i, \ldots\) are in fact independent of \(\xi, \eta, \ldots\), i.e. independent of the normal subgroup \(A\).
which in turn determine the \( h_i \) by the equations of the theorem 5.2. Then all possible sets of \( [d_1, d_2, \ldots, d_r] \) can be found which satisfy the conditions of theorem 5.1, and reducing these sets \( \text{mod}(\beta_1, \beta_2, \ldots, \beta_r) \), we obtain the sets \( [d_i] \) which will define all extensions of \( \mathcal{A} \). In particular, equations (5,6) will enable us to express the factor sets of these extensions in terms of products and transforms of the \( d_i \).

The proof of theorem 5.2 is long and we shall precede it by several lemmas, while theorem 5.3 is actually quite brief. Proof of theorem 5.3:

\[ [d_1, d_2, \ldots, d_r] \] defines an extension of \( \mathcal{A} \) by \( \mathcal{H} \) if and only if all the relations \( \prod d_i = 1 \) of theorem 5.1 are satisfied. Since the factor sets generate \( \mathcal{G} \), every \( d_i \) can be expressed as a product \( d_i = (u,v) \ldots (w,z) \) and from \( (u,v)^t (u,v)^n = (u,v)^n \) follows \( d_i^t d_i = d_i^n \). Hence the sets of \( d_i \) form a group.

Moreover we know that in this group, factor sets equivalent

---

* W. Magnus (see bibliography) proves theorem 5.2 in a somewhat briefer manner by showing that \( \mathcal{G} \) can be represented faithfully by the correspondence \( x \rightarrow (t_x, i) \) where \( t_x \) is an independent parameter function of \( x \). In this way he avoids the study of the equations of theorem 5.2 whose properties will actually be of importance in application. For this reason, and on account of Magnus' greater dependence on the theory of free groups, we prefer M. Hall's proof at this point.
to the identity are those which can be obtained from the identity by a change of the representatives of the co­
sets. But these are precisely $\beta_1, \beta_2, \ldots, \beta_r$ with $\xi$, $\gamma, \ldots$ arbitrary from $C$.

$[d_1, d_2, \ldots, d_r] \mod (\beta_1, \beta_2, \ldots, \beta_r)$ is then the group of factor sets with equivalent sets identified, i.e the group of extensions.

The following theorems and lemmas lead up to and finally establish the result of theorem 5.2.

We may regard an identity $\phi_1^{h_1} \phi_2^{h_2} \cdots \phi_r^{h_r} \equiv 1 \mod (K)$ from theorem 5.1 as belonging to a vector $[h_1, h_2, \ldots, h_r]$ with elements in $H^*$.

**Theorem 5.4:** The set of vectors $[h_1, h_2, \ldots, h_r]$ for which $\prod \phi_i^{h_i} \equiv 1 \mod (K)$ forms a right vector-ideal $M$ (modulus) over $H^*$.

**Proof:** Since $R \mod K$ is abelian, $\prod \phi_i^{h_i} \equiv 1$, $\prod \phi_i^{h_i} \equiv 1$ imply $\prod \phi_i^{h_i} \equiv 1 \mod K$ or

$[h_1, h_2, \ldots, h_r], [k_1, k_2, \ldots, k_r] \in M \rightarrow [h_1+k_1, h_2+k_2, \ldots, h_r+k_r] \in M$

Also if $\lambda \in H^*$, $\prod \phi_i^{h_i} \equiv 1 \mod (K)$ which means

$[h_1, h_2, \ldots, h_r] \in M, \lambda \in H^* \rightarrow [h_1 \lambda, h_2 \lambda, \ldots, h_r \lambda] \in M$.

We notice that the operators of the ring $H^*$ are from the domain of all integers, hence $H^*$ may be embedded in an algebra $\mathcal{O}_L$ over the group $H$ with operators from the field of rationals.
Clearly, there is a least modulus \( M \) in \( \mathcal{O} \) which contains \( M \). If every vector of \( \mathcal{M} \) with components in \( H^* \) belongs to \( M \), we say that modulus \( M \) is closed.

**Theorem 5.5**: The right modulus of theorem 5.4 is closed.

A vector \( v \) of \( \mathcal{M} \) is of the form \( v = \lambda_1 + \lambda_2 + \cdots + \lambda_s \) with \( \lambda_1, \lambda_2, \cdots, \lambda_s \) belonging to \( \mathcal{O} \) and \( \lambda_i, \lambda_2, \cdots, \lambda_s \) belonging to \( \mathcal{O} \). Let \( m \) be a multiple of all denominators of the \( \lambda_i \), then \( \lambda_i m, \lambda_2 m, \cdots, \lambda_s m \) are elements of \( \mathcal{H}^* \), so that the vector \( \mathcal{V}m \) belongs to \( \mathcal{M} \). To prove that \( M \) is closed, it is sufficient to show that \( V = [h_1, h_2, \cdots, h_s] \) with \( h_i \in H^* \) belongs to \( M \) if \( \mathcal{V}m \) belongs to \( \mathcal{M} \).

\( \mathcal{R} \) is a subgroup of the free group \( \mathcal{F} \), hence again a free group. \( \prod_i \phi_i^{h_i} \) is then an element of the free abelian group \( \mathcal{R} \) mod \( \mathcal{K} \), so that

\[
\prod_i \phi_i^{h_i} \equiv 1
\]

Hence we have \( \mathcal{V}m \in \mathcal{M} \) or \( \prod_i \phi_i^{h_i} \equiv 1 \) implying

\[
\prod_i \phi_i^{h_i} \equiv 1 \quad \text{or} \quad \prod_i \phi_i^{h_i} \equiv 1 \quad \text{or} \quad \mathcal{V} \in \mathcal{M}
\]

since an abelian free group contains no elements of finite order.

Let \( \mathcal{V}_r \) be the set of all vectors \([k_1, \cdots, k_r]\) with elements from \( H^* \), and \( T \), a subset of \( \mathcal{V}_r \), be the set of vectors \([t_1, t_2, \cdots, t_r]\) each of which annihilates \([x_1, x_2, \cdots, x_r]\), etc. on the right. This is
equivalent to saying that each vector of $T$ satisfies
\begin{align*}
\chi_1 t_1 + \chi_2 t_2 + \cdots + \chi_r t_r &= 0 \\
y_1 t_1 + y_2 t_2 + \cdots + y_r t_r &= 0
\end{align*}

$T$ is a right modulus over $H^*$. To prove theorem 5.2 we must show that $T = M$.

Let $A$ be an operator free abelian group (see p. 190) with elements $a^h$, $h \in H^*$, and let $A^\mu$ be the automorphisms defined by (5.3), then
\begin{equation}
\phi_i (x, y, \ldots) = a^\mu_i \quad i = 1, 2, \ldots, r
\end{equation}
defines an extension of $A$ if and only if (theorem 5.1)
\begin{equation}
\prod (a^\mu_i)^{h_i} = 1
\end{equation}
for every $[h_1, \ldots, h_r]$ of $M$. Since $A$ is operator free, (5.9) and (5.4) imply
\begin{equation*}
\sum \mu_i h_i = \mu_1 h_1 + \mu_2 h_2 + \cdots + \mu_r h_r = 0
\end{equation*}
Therefore the vectors $U = [\mu_1, \mu_2, \ldots, \mu_r]$ associated with each extension of type (5.8), are annihilators of $M$ on the left.

The proof of the following theorem will be given later to prevent an interruption of the line of development at this point.

**Theorem 5.6**: The only extensions of an operator free group $A = \{a^h\}$ by $H$ are the normal products of $A$ by $H$.

By this theorem, for any $[\mu_1, \mu_2, \ldots, \mu_r]$ of $U$
In the terminology of theorem 5.3, \([\beta_1, \ldots, \beta_r] \sim [1, \ldots, 1]\)
if and only if
\[ \beta_i = \sum \xi \eta \gamma, \quad i = 1, 2, \ldots, r, \]
which applied to (5,10) becomes
\[ a_i = (a^h)^{x_i} (a^h)^{y_i} \ldots = h x_i + k y_i + \ldots \]
or
\[ a_i = h x_i + k y_i + \ldots, \quad i = 1, 2, \ldots, r. \]

\(U\) therefore is a left vector modulus over \(\mathbb{H}\) with
basis \([x_1, x_2, \ldots, x_r]\), \([y_1, y_2, \ldots, y_r]\), etc. By definition \(T\) consists of all those vectors which annihilate on
the right the basis of \(U\), and hence all of \(U\).

So far we have shown that \(U\) is the set of left annihilators of \(M\) and \(T\) is the set of right annihilators of \(U\),
from which follows
\[ M \subseteq T. \]

However to prove the sufficiency of theorem 5.2, in which
after all lies its usefulness, we must show that \(M = T\).

We shall consider certain general properties of rings.
Definition: In a ring \(\mathbb{R}\), the right (left) annihilators
of the left (right) annihilators of a set of vectors \(S\)
is called the right (left) closure \(S_r\) (\(S_L\)) of \(S\).

If every right (left) vector modulus of \(\mathbb{R}\) is
its own right (left) closure, we say that \(\mathbb{R}\) is closed.

The following two properties of rings shall be taken for
granted without proof:

* H. Hall, Group rings and extensions, (see bibliography) pp. 231.
1. An algebra $\mathcal{O}$ over a group $\mathcal{H}$ is semi-simple, and
2. a semi-simple algebra is a closed ring.

It follows therefore that $\mathcal{M}$, the least right modulus of $\mathcal{O}$ containing $\mathcal{M}$, is its own closure. This implies: if we let $\mathcal{U}$ be the left modulus annihilating all vectors of $\mathcal{M}$ on the left, and $\mathcal{M}'$ be the right modulus of right annihilators of $\mathcal{U}$, then $\mathcal{M} = \mathcal{M}'$.

Any element of $\mathcal{M}$ is equal to an element of $\mathcal{M}$ divided by an integer, so that any left annihilator of $\mathcal{M}$ is also an annihilator of $\mathcal{M}'$. Consequently $\mathcal{U}$ is the intersection of $\mathcal{U}$ and $\mathcal{V}_r$. Hence $\mathcal{T}$ is the intersection of $\mathcal{M}'$ and $\mathcal{V}_r$, i.e. $\mathcal{T} = \mathcal{M}' \cap \mathcal{V}_r$.

There remains the auxiliary theorem 5.6 which requires proof:

Theorem 5.6: The only extensions of an operator free group $\mathcal{A} = \{\alpha^h\}$ by $\mathcal{H}$ are the normal products of $\mathcal{A}$ by $\mathcal{H}$.

Every element $b \in \mathcal{A}$ can be expressed in the form

$$b = \prod_{\tau} a_b^a \tau,$$

$\tau \in \mathcal{H}$, $b_\tau$ an integer. Since $(u,v) \in \mathcal{A}$

(5.11) $$\mu, v) = \prod_{\alpha} (u, \omega+\tau,$$

and it must satisfy 1,III. Due to the independence of the elements $\alpha^u, \alpha^v, \ldots$, condition 1,III becomes


** M.Hall "Group Rings and Extensions I" (see bibliography) p. 231.
\[(u,v,w)^{\tau} (\mu,\nu,\xi)^{\tau} (u,v,\xi)^{\tau} (u,\nu,\xi)^{\tau} \alpha^\tau = \alpha \int_{\alpha} (\mu,\nu)^{\tau} (-\tau) \int_{\alpha}
\]

for all \(u,v,\xi, \ldots\). Now we shall define \(\overline{\mu} = \overline{\mu} \int_{\alpha} (\mu,\nu)^{\tau} (-\tau)\) and prove \(\overline{\mu} \overline{\nu} = \overline{\mu \nu}\).

\[
\overline{\mu} \overline{\nu} = \overline{\mu} \int_{\alpha} (\mu,\nu)^{\tau} (-\tau) \int_{\alpha} (\nu,\xi)^{\tau} (-\tau) \\
= \overline{\mu \nu} \int_{\alpha} (\mu,\nu)^{\tau} (-\tau) \int_{\alpha} (\nu,\xi)^{\tau} (-\tau) \\
= \overline{\mu \nu} \int_{\alpha} (\mu,\nu)^{\tau} (-\tau) \int_{\alpha} (\nu,\xi)^{\tau} (-\tau) \\
= \overline{\mu \nu} \overline{\nu} \\
= \overline{\mu \nu} \overline{\nu}
\]

From (5.12)
\[
\overline{\mu} \overline{\nu} = \overline{\mu \nu}
\]
so that
\[
\overline{\mu} = \overline{\mu} \overline{\nu} \overline{(\nu,\xi)^{\tau}} (-\tau) \overline{\nu} (-\tau)
\]

Since \(\sum_{\tau} (t - \tau \nu) = 0\) and \(\sum_{\tau} (t - \tau) = 0\), \(\overline{\nu} = 1\) and
\[
\overline{\mu} \overline{\nu} = \overline{\mu \nu}.
\]
6. Appendix.

The following examples are given to illustrate the meaning and the use of the theory of extension, and at each step of the calculation reference is made to the particular theorem used.

Example 1.

Given \( A : a^6 = b^2 = 1, \ ab = b a^{-1} \); \( H : \mu = 1 \)

Inner automorphisms of \( A : \ a' A a = a \) \( (a \to a, \ b \to a^2 b) \)
\( b' A b = b \) \( (a \to a^{-1}, \ b \to b) \)

outer automorphisms of \( A : \nu (a \to a, \ b \to a b) \)

therefore the group of automorphisms \( \mathcal{A} = \mathcal{J} + \nu \mathcal{J} \)

where \( \mathcal{J} : \nu_1 = b^2 = 1, \ \mu b = b \nu_1 \) and \( \mathcal{J}^2 = \nu \mu, \ \nu b = b \mathcal{J}^2 \).

From theorem 3.1, \( H \to \mathcal{A} / \mathcal{J} \), which gives us two choices

I. \( \nu (\nu) = \mathcal{J}, \ \nu (\mu) = \nu \mathcal{J} \) and

II. \( \nu (\nu) = \nu (\mu) = \mathcal{J} \)

Let us consider I.

Write \( \mathcal{A}^\nu = \mathcal{J} \) then \( \mu_1 = \gamma, \ \gamma \in \mathcal{A} \). By theorem 2.1, \( \times = \gamma \) and \( \mathcal{J} = \gamma \mu = \gamma \mathcal{J}^2 = \gamma \nu, \ \nu \in \mathcal{A} \) so that \( \gamma = \alpha \leftrightarrow \alpha \gamma \).

According to (2.1) p. \( \mathcal{F} \), the two extensions are equivalent if and only if \( \alpha = \alpha d^{1+\mu} \) has a solution for \( \nu \in \mathcal{A} \), which is not the case here. Hence we have two extensions

\( G_1 : \ a^6 = b^2 = 1, \ \mu_1 = \alpha \gamma; \ ab = b \ a^{-1}, \ b \mu = \mu \ a b \)
\( G_2 : \ a^6 = b^2 = 1, \ \bar{\mu} = \alpha; \ \bar{a} b = b \ a^{-1}, \ b \bar{\mu} = \bar{\mu} \ a b \).
We observe that while apparently the normal product is not possible, we may choose another automorphism which will make the existence of the normal product evident.

Let $A^\mu = A^3$ then $\mu^2 = \gamma$, $\gamma \in A$ and (theorem 2.1) $\gamma^2 = \mu^2 = 1$, $\alpha \in A$. Therefore $\gamma = 1$ or $\alpha^i$ for all $i$. Reducing this set by all those powers of $\alpha$ for which $1 = \alpha^i \mu^{a+1}$ can be solved for $\alpha$, we obtain $\gamma = 1, \alpha$.

The two extensions are

$$G'_1 : \quad \alpha^6 = b^2 = \mu^2 = 1, \quad \alpha b = b \alpha^{-1}, \quad b \mu = \mu \alpha^3 b$$

$$G'_2 : \quad \alpha^6 = b^2 = 1, \quad \mu^2 = \alpha, \quad \alpha b = b \alpha^{-1}, \quad b \mu = \mu \alpha^3 b$$

We observe that $G'_1 \cong G'_2$, since $G_1$ is also a normal product: it contains a subgroup of order 2 which may be used as a system of representatives, $1, \mu \alpha, (\mu \alpha)^2 = 1$. Therefore $G'_1 \cong G'_2$ and $G'_2 \cong G'_2$.

Since $\alpha^6 \equiv \alpha \equiv \alpha \pmod{C}$ we notice that $G'_1$ and $G'_2$ are equivalent mod $C$. The same must be true for $G'_1$ and $G'_2$. Indeed in $G'_2$, $(\mu \alpha)^2 \equiv 1 \pmod{C}$, so that both $G'_1$ and $G'_2$ mod $C$ are normal products.

Next let us consider II.

$A^\mu = 1$ then $\gamma = 1, \alpha^3$ and we have two different extensions since $1 = \alpha^3 \mu^2$ has no solution for $\alpha \in A$.

$$G'_2 : \quad \alpha^6 = b^2 = 1, \quad \mu^2 = \alpha^3, \quad \alpha b = b \alpha^{-1}, \quad b \mu = \mu b.$$
Example 2.

Let us investigate an extension for which the normal product is not possible.

\[ A : \ a^5 = b^2 = 1, \ ab = ba^{-1} ; \ H : \ u^2 = 1 \]

\[ \alpha' A a = u (a \rightarrow a, b \rightarrow b a^2), \ \omega^5 = 1, \ u v = b \ \omega^4 \]

\[ a \rightarrow a^y, \ b \rightarrow b \]

\[ \alpha \rightarrow \alpha^y, \ \beta \rightarrow \beta \]

Choose \( A^u = \tau \) then \( G \) must be uniquely determined:

(Corollary, p.13) \( \mu = \chi \), where \( \chi = \chi \) and for every \( \alpha \in A \), \( \alpha^x = \alpha^u = \tau = b \). The only solution is \( \chi = b \).

\[ G : \ a^5 = b^2 = 1, \ \mu^2 = b \ ; \ ab = ba^{-1}, \ a \mu = \mu \ a^2 \]

Now consider the same group \( A \) and let \( H \) be the elementary abelian group defined by \( \mu^2 = \nu^2 = \omega^2 = 1 \).

Let \( A^\mu = \chi, \ A^\nu = \nu, \ A^\omega = \omega \). Again \( G \) should be uniquely determined. The following characteristic elements are determined by theorem 2.2:

\[ \mu^2 = \chi, \ \chi^\mu = \chi, \ \alpha^x = \alpha^u = \lambda = b \]

\[ \nu^2 = \chi, \ \nu^\nu = \chi, \ \lambda = \lambda^2 = \nu^2 \]

\[ \omega^2 = \chi, \ \omega = \chi, \ \lambda = \lambda^2 = \omega^2 = 1 \]

and

\[ \mu^u = \nu, \ \nu^2 = \nu \lambda^2 = \nu \mu^2, \ \mu = \lambda^u \alpha^2 \]

\[ [\nu, \omega] = \chi \]

\[ \nu^\omega = \nu \lambda = \nu \mu^2 = \nu \omega, \ \omega^2 = \omega^u \alpha^3 \]

\[ [\nu, \omega] = \omega^3 \]

\[ \lambda = \nu \mu = \nu \lambda^2 = \omega^u \]

\[ [\nu, \omega] = 1 \]
It can easily be seen that these elements satisfy conditions (2,11), 1 to 5.

\[ G: \quad a^5 = b^2 = \bar{a}^{-2} = 1, \quad \bar{a}^2 = b, \quad \bar{a}^2 = a; \quad a b = b a^{-1} \]
\[ \bar{a} \bar{a} = \bar{a} a, \quad \bar{a} \bar{a} = \bar{a} a \alpha^3, \quad \bar{a} \bar{a} = \bar{a} \bar{a} \]
\[ a \bar{a} = \bar{a} a^2, \quad a \bar{a} = a \bar{a}, \quad a \bar{a} = \bar{a} a^4 \]
\[ b \bar{a} = a b, \quad b \bar{a} = a b a^2, \quad b \bar{a} = a b \]

Example 3.

Central extensions worked by the method of § 5.

Let \( \mathcal{H} \) be the \textit{dihedral group (M.Hall)}

\[ \chi^n = 1, \quad \gamma^2 = 1, \quad \gamma \chi = \chi' \gamma \]

The equations (5,7) are

\[ \bar{x}^n = (\xi \bar{x})^n = \bar{x}^{1+x+\cdots+x^n-1} \]
\[ \bar{y}^2 = (\eta \bar{y})^2 = \bar{y}^{1+\gamma} \]
\[ \xi \bar{x} \bar{y} = \eta \bar{y} \bar{x} \eta \xi \bar{y} = \xi \bar{x} \bar{y} \bar{x} = \xi \bar{x} \bar{y} \bar{x} = \xi \bar{x} \gamma \bar{x} \]

so that

\[ \chi_1 = 1 + x + \cdots + x^{n-1}, \quad \gamma_1 = 0 \]
\[ \chi_2 = 0 \quad \gamma_2 = \gamma + 1 \]
\[ \chi_3 = x + y, \quad \gamma_3 = 1 - x \]

Central extensions of a group \( \mathcal{A} \) by \( \mathcal{H} \) will be defined by

\[ \bar{x}^n = \alpha, \quad \bar{y}^2 = \beta, \quad \gamma \bar{x} \bar{y} \bar{x} = \gamma \] if \( \alpha, \beta, \gamma \) in \( C \) satisfy

\[ \alpha \beta \gamma h = 1 \quad (\text{th. 5.1}) \]

The elements \( h_i \) are given by theorem 5.2 as the solutions of the equations

\[ (1 + x + \cdots + x^{n-1}) h_1 + (\gamma + x) h_3 = 0 \]
\[ (1 + \gamma) h_2 + (1 - x) h_3 = 0 \]

Since the solutions form a right vector ideal, they
can be found by first guessing the obvious solutions $s$, and then finding the remaining solutions among the set of vectors reduced mod $s$. In our case the solutions are

$$ \begin{bmatrix} x^{-1}, 0, 0 \end{bmatrix}, \begin{bmatrix} 0, y^{-1}, 0 \end{bmatrix} $$

$$ \begin{bmatrix} y+1, 0, -1+\ldots+x^{n-1} \end{bmatrix} $$

$$ \begin{bmatrix} 0, x^{-1}, 1-x^{-1}y \end{bmatrix} . $$

Hence the conditions which $d, \beta, y$ must satisfy are:

$$ d \cdot x^{-1} = 1 $$

$$ y \cdot y^{-1} = 1 $$

$$ d \cdot (1+\ldots+x^{n-1}) = 1 $$

$$ \beta \cdot (1-x^{-1}y) = 1 $$

Now let $n = 3$, so that we are dealing with the dihedral group of order 6. Without knowing $A$ we can express the factor set in terms of $d, \beta, y$:

$$ (x,x) = 1 \quad (x^2,x) = \lambda \quad (y,x) = \lambda \cdot y \cdot \beta \cdot y^{-1} \cdot y \quad (y,x,y) = \lambda \cdot y \cdot \beta \cdot y $$

$$ (x,x^2) = \lambda \quad (x^2,x^2) = \lambda \cdot y \quad (y,x^2) = \lambda \cdot y \cdot \beta \cdot y \quad (y,x^2,y) = \lambda \cdot y \cdot \beta \cdot y $$

and finally

$$ (x^2y,x) = \lambda \cdot y \cdot \beta \cdot y \cdot x^{-1}y \quad (x^2y,x^2) = \lambda \cdot y \cdot \beta \cdot y \cdot x^{-1}y \quad (x^2y,x^2y) = \lambda \cdot y \cdot \beta \cdot y \cdot x^{-1}y \quad (x^2y,x^2y) = \lambda \cdot y \cdot \beta \cdot y \cdot x^{-1}y $$

The conditions which $d, \beta, y$ must satisfy become

$$ d \cdot x = \lambda $$

$$ \beta \cdot y = \beta $$

$$ \lambda \cdot y \cdot y = \beta \cdot y \cdot \beta \cdot y $$

$$ \beta \cdot y \cdot y = \beta \cdot y \cdot \beta \cdot y $$
Finally we must reduce the set $[d, \beta, \gamma] \mod (\xi, \eta)$ where $\xi, \eta$ are arbitrary from $C$.

Let $A$ be the cyclic group of order 3: $\alpha^3 = 1$

Then $\sigma : \psi (\alpha \rightarrow \alpha^2) , \mu \alpha^2 = 1$ and $H \rightarrow \sigma \mathcal{L}$.

1. Put $K(x) = K(\omega) = K(x) = 1$ and $k(\gamma) = k(x\gamma) = k(x\gamma) = 1$

then the conditions on the $d, \beta, \gamma$ become

$$d = d, \quad \beta = \beta^\gamma, \quad \gamma^d = \gamma^3 = 1$$

so that $\gamma = 1, \beta = 1, d = 1, \alpha, \alpha^2$

$$[1, 1, 1], [\alpha, 1, 1], [\alpha^2, 1, 1] \quad \text{reduced mod (1,1,1)}$$

give three distinct extensions of $A$ by $H$. The factor sets are in order

$$\begin{array}{ccccccccc}
1 & a & a & a & 1 & a^2 & a^2 & a^2 & 1 \\
a & a & a & a & a & a & a & a & 1 \\
a^2 & a^2 & a^2 & 1 & a & a & a & a & 1 \\
\end{array}$$

2. Put $K(\omega) = 1$ for all $u$ of $H$.

Then $d = 1, \beta = 1, \alpha, \alpha^2, \gamma = 1, \alpha, \alpha^2$ and $[d, \beta, \gamma]$ must be reduced mod $(1, \eta^2, \xi^2), \eta, \xi = 1, \alpha, \alpha^2$. Hence

$$[d, \beta, \gamma] \rightarrow [1, 1, 1] \quad \text{for all choices of } d, \beta \text{ and } \gamma.$$  

The only extension is the normal — in fact the direct product.
Bibliography.


Bergström: Ueber Erweiterungen Abelscher Gruppen.*

Bergström: Struktur der Erweiterungen Abelscher Gruppen.

Marshall Hall: Group Rings and Extensions I.

W. Magnus: On a Theorem by Marshall Hall.
Ann. of Mathematics, no. 40, 1939.

O. Schreier: Ueber die Erweiterung von Gruppen I.
Monatsheft für Math. und Phys., no. 34, 1926.

O. Schreier: Ueber die Erweiterung von Gruppen II.
Hamburger Abhandlungen, vol. 4, 1926.

Shoda: Ueber die Schreiersche Erweiterungstheorie.

A. Turing: The extensions of a group.
Compositio Math., no. 5, 1938.

Teubner Verlag, Leipzig 1937.
Chap.III,6,7,8; IV,7.

* The theorems of this paper are not valid, since they are based on a faulty proof. For counter example see F. Tuan's review of the article, Math. Review, no.7, (1946) p. 6.