AN EXTENSION THEORY FOR A CERTAIN CLASS OF LOOPS

R. H. BRUCK

Introduction. If $E$ is a group with a normal subgroup $K$ one may form the quotient group $E/K \cong M$. Conversely, for preassigned groups $K$, $M$, there is the extension problem: to determine (in some sense) all groups $E$ with $K$ as normal subgroup such that $E/K \cong M$. Much progress has been made on this problem, particularly through the work of Baer [1, 2, 3] and the cohomology theory of Eilenberg and MacLane [1, 2, 3]. The latter authors make it clear that insight is gained by relinquishing part of the associative law; specifically, by requiring that $E$ be merely a loop such that the associative law $(e_1 e_2)e_3 = e_1(e_2 e_3)$ holds if at least one of the $e_i$ belongs to a distinguished subgroup of $K$. We take this to be $K$ itself. It then becomes evident that the subclass of loops $E$ consisting of the groups is not the only one of interest; one may consider, for example, the Moufang loops, in which case it seems natural to allow $M$ also to be Moufang. Thus we approach the extension problem actually studied in the paper: $M$ is a given loop, $K$ is a group (not given, but with given centre $G$) and $E$ is to be any loop with $K$ as a normal subloop contained in the “associator” of $E$, such that $E/K \cong M$. This problem is more typical of group theory than of loop theory but is, nevertheless, a natural and significant special topic in the theory of loops.

For the sake of brevity no examples or applications are given and references to the bibliography are kept to a minimum. The Eilenberg-MacLane kernels, important for constructions, have been ignored. I may signal out as new: the inverse of a (noncentral) extension (§1), the specific results on central Moufang extensions (§6) and the all-pervading functions $F$ which generalize (even for $M$ a group) the Eilenberg-MacLane cocycles. As indicated by Theorem 8 (§4), additional information about the functions $F$ would probably increase our knowledge of cohomology groups.

1. Extensions. A loop $M$ is a system with a multiplication such
that: (a) in $xy=z$, any two of $x$, $y$, $z$ uniquely determine the third; (b) $M$ has a unit 1. The associator $A = A(M)$ is the subset of $M$ such that $(xy)z = x(yz)$ if at least one of $x$, $y$, $z$ is in $A$; the associator is an associative subloop (and therefore a group). A subloop $H$ of $M$ is normal in $M$ if and only if $H$ is the kernel of a homomorphism of $M$ into a loop; equivalently, $xH = Hx$, $(xy)H = x(yH)$, $(Hx)y = H(xy)$ for all $x$, $y$ in $M$. The mapping $x \mapsto xH$ of $M$ set up by a normal subloop $H$ is a homomorphism upon a quotient loop $M/H$. (See Bruck [1].)

If $M$ is given, we wish to study all loops $E$ such that (i) $E$ has a homomorphism $\theta$ upon $M$; (ii) the kernel $K$ of $\theta$ is a subgroup of $A(E)$. Let $G = Z(K)$ be the centre of $K$. For each $e$ in $E$ define the mapping $T(e)$ of $K$ by

$$kT(e) = e(kT(e)), \quad k \in K.$$

Applying $\theta$ to both sides of (1) we see that $kT(e)$ is in $K$. And to each $k'$ in $K$ corresponds a unique $k$ in $K$ such that $kT(e) = k'$. Furthermore, $e((k_1k_2)T(e)) = (k_1k_2)e = k_1(k_2e) = k_1(e \cdot k_2T(e)) = k_1e \cdot k_2T(e) = e(k_1T(e)) \cdot k_2T(e) = e(k_1T(e) \cdot k_2T(e))$. Thus $T(e)$ is an automorphism of $K$: $(k_1k_2)T(e) = k_1T(e) \cdot k_2T(e)$. In particular, $T(1)$ is the identity automorphism. Moreover, $(e_1e_2) \cdot kT(e_1e_2) = k(e_1e_2) = (k_1e_1)e_2 = (e_1 \cdot kT(e_1))e_2 = e_1(kT(e_1) \cdot e_2) = e_1(e_2 \cdot kT(e_1)T(e_2)) = e_1e_2 \cdot kT(e_1)T(e_2)$, or $kT(e_1e_2) = kT(e_1)T(e_2)$. In other words, the mapping $e \mapsto T(e)$ is a homomorphism of $E$ upon a group of automorphisms of $K$.

For our purposes a pair $(G, M)$ shall consist of an abelian group $G$, a loop $M$ and a single-valued product $gx$ from $GM$ to $G$ such that $g1 = g$, $(gg')x = (gx)(g'x)$ and $(gx)y = g(xy)$ for all $g$, $g'$ in $G$ and $x$, $y$ in $M$, where 1 is the unit of $M$. From (1), $T(e)$ is an inner automorphism if $e$ is in $K$. Thus, for arbitrary $g$ in $G = Z(K)$, $k$ in $K$, $e$ in $E$, we have $gT(ke) = gT(k)T(e) = gT(e)$. However, $eT = e\theta$ if and only if $e' = ke$ for $k$ in $K$; thus $gT(e)$ depends only on $g$ and $x = \theta e$. Hence if we set $gx = gT(e)$, $G$ and $M$ become a pair $(G, M)$. It is a mere matter of bookkeeping (which turns out to be useful) to pursue the study in terms of a fixed pair $(G, M)$. This leads to the basic definition:

DEFINITION 1. Let $(G, M)$ be a pair. A $(G, M)$ extension $(E, \theta)$ consists of a loop $E$ and a homomorphism $\theta$ of $E$ upon $M$ such that (i) $K = \theta^{-1}$ is in $A(E)$; (ii) $Z(K) = G$; (iii) $ge = e(gx)$ for $g$ in $G$, $e$ in $E$, $x = e\theta$.

It will be convenient to list here other fundamental definitions concerning extensions.

DEFINITION 2. $(E, \theta)$ is central if $1\theta^{-1} = G$.

DEFINITION 3. $(E_1, \theta_1)$ is equivalent to $(E_2, \theta_2)$ if there exists an iso-
morphism \( \pi \) of \( E_1 \) upon \( E_2 \) such that (i) \( \theta_1 = \pi \theta_2 \); (ii) \( g \pi = g \) for \( g \) in \( G \). (Notation: \( E_1 \sim E_2 \)).

Equivalence is reflexive, symmetric, transitive; it will serve as equality. Equivalence should be contrasted with inverse equivalence:

**Definition 4.** \((E_1, \theta_1)\) is inverse equivalent to \((E_2, \theta_2)\) if there exists an isomorphism \( \pi \) of \( E_1 \) upon \( E_2 \) such that (i) \( \theta_1 = \pi \theta_2 \); (ii) \( g \pi = g^{-1} \) for \( g \) in \( G \). (Notation: \( E_1 \sim^{-1} E_2 \)).

Inverse equivalence is symmetric, not always reflexive. Transitivity has three substitutes, one being:

\[ E \sim E_1 \sim E_2 \sim E \]

Therefore, since equivalence is to serve as equality, we may define the inverse \((E, \theta)^{-1}\) as any extension inverse equivalent to \((E, \theta)\). The inverse of \((E, \theta)\) may be constructed as follows. Let \( u(x) \) be any normalized system of representatives of \( M \) in \( E \); thus \( u(x) \theta = x \), \( u(1) = 1 \). If \( K = 1^0 \), every \( e \) in \( E \) has a unique representation \( e = u(x)k \) with \( x = e \theta, k \) in \( K \); define \( \pi \) by \( e \pi = u(x)k^{-1} \). Define a new operation \( (\theta) \) on the elements of \( E \) by \( e \theta' = (e \pi \cdot e \pi') \pi \); it is easy to see that this turns \( E \) into a loop \( E^{-1} \). I claim that \((E^{-1}, \theta)\) is the desired inverse. Indeed, \( \pi \) is an isomorphism of \( E \) upon \( E^{-1} \), and \( g \pi = g^{-1} \) for \( g \) in \( G \). Also \( \theta = \pi \theta \). Certainly \( \theta \) is a homomorphism of \( E^{-1} \) upon \( M \), the kernel being the group \( K \pi \) anti-isomorphic to \( K \), with centre \( G \pi = G \).

If at least one of \( e_1, e_2, e_3 \) is in \( K \pi \), \( (e_1 \circ e_2) \circ e_3 = (e_1 \pi \cdot e_2 \pi) \pi = (e_1 \pi \cdot (e_2 \pi \cdot e_3 \pi)) \pi = e_1 \pi (e_2 \circ e_3) \pi \); thus \( K \pi \) is in \( A \). For \( g \) in \( G \), \( e \) in \( E^{-1} \), \( x = e \theta \), we have \( g e (g^{-1}) = (g^{-1} \cdot e \pi) \pi = (e \pi \cdot (g^{-1} x)) \pi = e \pi (g x) \). This completes the proof.

**Definition 5.** The product \((E_1, \theta_1) \otimes (E_2, \theta_2) = (E, \theta)\) of two extensions \((E_j, \theta_j)\) is defined as follows: (i) The elements of \( E \) are the pairs \((e_j, e_2)\) with \( e_j \) in \( E_j \) and \( e_2 \theta_2 = e_2 \theta_2 \). (ii) \((e_1, e_2) = (e_1', e_2')\) if and only if \( e_1' = e_1 \theta, e_2' = e_2 \theta^{-1} \), for some \( g \) in \( G \). (iii) \((e_1, e_2) (e_1', e_2') = (e_1 \pi e_2, e \pi e \theta)\). (iv) \((e_1, e_2) \theta = e_1 \pi e_2 \theta_2 \). (v) \((g, 1) = g \) for \( g \) in \( G \). (Notation: \( E_1 \otimes E_2 = E \)).

For a more detailed discussion of the product see Eilenberg and MacLane [2, 3]. Straightforward but tedious calculation shows that \( E_1 \otimes E_2 \) is a \((G, M)\) extension such that

\[
\begin{align*}
(2) \quad & E_j \sim E'_j \quad (j = 1, 2), \quad E_1 \otimes E_2 \sim E'_1 \otimes E'_2, \\
(3) \quad & E_1 \otimes E_2 \sim E_2 \otimes E_1, \\
(4) \quad & (E_1 \otimes E_2) \otimes E_3 \sim E_1 \otimes (E_2 \otimes E_3).
\end{align*}
\]

Therefore the set \( S \) of all \((G, M)\) extensions, with equivalence as equality, and with multiplication as in Definition 5, is a commutative semigroup. It may also be shown that \( S \) has a unit \((E_0, \theta_0)\):

**Definition 6.** The unit extension \((E_0, \theta_0)\) is defined as follows: \( E_0 \) is the set of all pairs \((x, g)\), \( x \) in \( M \), \( g \) in \( G \), such that (i) \((x, g) \)

\[
\begin{align*}
&\text{\textit{AN EXTENSION THEORY FOR A CERTAIN CLASS OF LOOPS}} \quad 13
\end{align*}
\]
\[(y, g') \text{ if and only if } x = y, g = g'; \]
(ii) \((x, g)(y, g') = (xy, (gy)g')\);
(iii) \((1, g) = g. \text{ And } \theta_o \text{ is given by } (iv) (x, g)\theta_o = x.\)

It is essentially known (Baer [1], Eilenberg-MacLane [1]) that the subset \(S'\) of \(S,\) consisting of the central extensions, is an abelian group with unit \((E_0, \theta_o).\) For \((E, \theta)\) central, our inverse \((E, \theta)^{-1}\) is the inverse of \((E, \theta)\) in \(S'.\) Details are deferred until §6 (see Theorem 10) but the facts are assumed in §4.

2. The functions \(F.\) For any positive integer \(n\) let \(L_n\) be the free loop (Bates [1]) with (free) generators \(X_1, \ldots, X_n.\) Thus \(L_n\) is a loop containing the \(X_j,\) such that any mapping \(X_1 \rightarrow e_1, \ldots, X_n \rightarrow e_n\) into elements \(e_j\) of a loop \(E\) may be extended uniquely to a homomorphism \(\rho\) of \(L_n\) into \(E.\) By a (nonassociative) word \(W_n\) we mean any element of \(L_n.\) The image \(W_n\rho\) denoted by \(W_n(e_1, \ldots, e_n);\) this turns \(W_n\) into a function defined on every loop \(E\) (with values in \(E).\) The following fact is worth noting: if also \(\sigma\) is a homomorphism of \(E\) into a loop \(L,\) \(W_n(e_1, \ldots, e_n)\sigma = W_n(e_1\sigma, \ldots, e_n\sigma),\) since the homomorphism \(\rho \sigma\) of \(L_n\) maps \(X_j\) upon \(e_j\sigma.\)

**DEFINITION 7.** A word \(W_n\) is purely nonassociative (p.n.a.) if it “vanishes” on every group: If \(e_1, \ldots, e_n\) are group elements,
\[W_n(e_1, \ldots, e_n) = 1.\]

As an important example of a p.n.a. word, consider \(A_3,\) defined by \((X_1X_2)X_3 = (X_1(X_2X_3))A_3(X_1, X_2, X_3).\) If \(E\) is a loop, the set of all elements \(W_n(e_1, \ldots, e_n)\) \((n \text{ arbitrary, } W_n \text{ p.n.a., the } e_j \text{ in } E)\) generates a normal subloop \(E_{pna}\) which may be characterized as follows: a necessary and sufficient condition that \(E/F\) be associative (for a normal subloop \(F\) of \(E)\) is that \(F\) contain \(E_{pna}.\)

**THEOREM 1.** Let \((E, \theta)\) be a \((G, M)\) extension, \(W_n,\) a p.n.a. word, \(e_1, \ldots, e_n,\) elements of \(E.\) Write \(e^\theta = x_1, e_0 = W_n(e_1, \ldots, e_n).\) Then
(i) \(e_0k = ke_0\) for \(k\) in the kernel \(K;\) (ii) \(W_n(x_1, \ldots, x_n) = 1\) if and only if \(e_0\) is in \(G;\) (iii) \(e_0\) depends only on the \(x_j:\)
\[(5) \quad e_0 = W_n(e_1, \ldots, e_n) = F(W_n, E; x_1, \ldots, x_n).\]

**PROOF.** (i) If \(T\) is defined by \((1),\) the mapping \(e \rightarrow T(e)\) is a homomorphism of \(E\) upon a group of automorphisms of \(K.\) Thus \(T(e_0) = W_n(T(e_1), \ldots, T(e_n)) = 1,\) the identity automorphism.
(ii) \(e^\theta = W_n(x_1, \ldots, x_n),\) so (i) implies (ii).
(iii) For fixed \(n,\) and for every word \(A_n\) (not necessarily p.n.a.), define a function \(H(A_n; e, k) = H(A_n; e_1, \ldots, e_n; k_1, \ldots, k_n)\) by
\[(6) \quad A_n(e_1k_1, \ldots, e_nk_n) = A_n(e_1, \ldots, e_n)H(A_n; e, k).\]
Here the \( e_j \) are assigned fixed values in \( E \) and the \( k_j \) vary over \( K \). Applying \( \theta \) to (6) we find that \( H \) takes values in \( K \). Also from (6), direct computation, along with the fact that \( (A_n B_n)(e_1, \ldots, e_n) = A_n(e_1, \ldots, e_n) B_n(e_1, \ldots, e_n) \), gives

\[
H(A_n B_n; e, k) = H(A_n; e, k) T(B_n(e_1, \ldots, e_n)) H(B_n; e, k).
\]

Moreover, by specializing \( A_n \) in (6) to the "unit" word 1 and the words \( X_j \),

\[
H(1; e, k) = 1; \quad H(X_j; e, k) = k_{-1} (j = 1, 2, \ldots, n).
\]

In addition, if \( B_n C_n = A_n = D_n B_n \), we may derive from (7) formulas involving only \( A_n \) and \( C_n \) or \( A_n \) and \( D_n \). Hence, since \( L_n \) is free, the recurrence formula (7) and the initial conditions (8) define a unique function \( H \).

Next construct the holomorph \( \mathcal{H} \) of \( K \). This group is the set of all pairs \((g, k), k \in K, g \) an automorphism of \( K \), under the product \((g, k)(U, k') = (SU, kUk')\). The \( n \) elements \( f_j = (T(e_j), k_j) \) yield \( A_n(f_1, \ldots, f_n) = (T(A_n(e_1, \ldots, e_n)), H'(A_n; e, k)) \) where \( H' \) satisfies both (7) and (8). Therefore \( H = H' \). Since \( \mathcal{H} \) is a group, \( H'(W_n; e, k) = 1 \) for every p.n.a. word \( W_n \). Thus, by (6), \( W_n(e_1 k_1, \ldots, e_n k_n) = W_n(e_1, \ldots, e_n) = e_0 \), showing that \( e_0 \) depends only on the images \( x_j = e_j k_j \). This completes the proof of Theorem 1.

**Definition 8.** An ordered set \( x_1, \ldots, x_n \) of elements of \( M \) is called a spot for a p.n.a. word \( W_n \) if \( W_n(x_1, \ldots, x_n) = 1 \).

**Theorem 2.** At each spot for a p.n.a. word \( W_n \), the functions \( F \) (of Theorem 1) form a multiplicative abelian group:

1. \( E_1 \sim E_2 \) implies \( F(W_n, E_1) = F(W_n, E_2) \);
2. \( E_1 \sim^{-1} E_2 \) implies \( F(W_n, E_1) = F(W_n, E_2)^{-1} \);
3. \( F(W_n, E_1) F(W_n, E_2) = F(W_n, E_1 \otimes E_2) \).

**Proof.** Let \( x_1, \ldots, x_n \) be a spot for \( W_n \), and write \( F(W_n, E) = F(W_n, E; x_1, \ldots, x_n) \) for any extension \((E, \theta)\). By Theorem 1 (ii), \( F(W_n, E) \) is in \( G \). Let \( \pi \) be an isomorphism of \((E_1, \theta_1)\) upon \((E_2, \theta_2)\) satisfying (i) of Definitions 3, 4, and let \( e_j \) in \( E_1 \) satisfy \( e_j = x_j \); \( j = 1, 2, \ldots, n \). Then \( e_j \pi \) is in \( E_2 \), and \( e_j \pi \theta_2 = e_j \pi = x_j \). Hence \( F(W_n, E_1) \pi = W_n(e_1, \ldots, e_n) \pi = W_n(e_1 \pi, \ldots, e_n \pi) = F(W_n, E_2) \). According as \( \pi \) satisfies (ii) of Definition 3 or 4, we get (i) or (ii) of Theorem 2. To prove (iii), choose \( e_{1j} \) in \( E_1, e_{2j} \) in \( E_2 \) such that \( e_{1j} \theta_1 = e_{2j} \theta_2 = x_j \), and set \( e_j = (e_{1j}, e_{2j}) \); \( j = 1, 2, \ldots, n \). If \( g_1 = F(W_n, E_1) \), Definition 5 gives \( F(W_n, E_1 \otimes E_2) = W_n(e_1, \ldots, e_n) = (g_1, g_2) = (g_1 g_2, 1) = g_1 g_2 = F(W_n, E_1) F(W_n, E_2) \).

3. **Strongly grouplike and C extensions.** An extension \((E, \theta)\) is strongly grouplike (s.g.) if \( E \) inherits all relations between elements
implied by the associative law) which hold for the images in \( M \). This means: if \( W_n \) is p.n.a., and if \( W_n(e_1, \ldots, e_n) \theta = 1 \), then \( W_n(e_1, \ldots, e_n) = 1 \). In particular, if \( M \) is a group, the s.g. extensions are precisely the associative extensions. The following theorem is an immediate consequence of Theorem 2.

**Theorem 3.** (i) For any \((G, M)\) extension \( E \), \( E \otimes E^{-1} \) is s.g. (ii) If \( E \) is s.g., and if \( E_1 \sim E \) or \( E_1 \sim E^{-1} \), then \( E_1 \) is s.g. (iii) If \( E_1 \otimes E_2 = E_3 \), and if two of the \( E_j \) are s.g., so is the third.

Next let \( C \) be any set of p.n.a. words. Assume that if \( W_n \) is in \( C \) then \( W_n(x_1, \ldots, x_n) = 1 \) for all \( x_j \) in \( M \). Then a \((G, M)\) extension \((E, \theta)\) is "C" if \( W_n(e_1, \ldots, e_n) = 1 \) for each \( W_n \) in \( C \) and all \( e_j \) in \( E \). We get at once the following theorem.

**Theorem 4.** Every s.g. extension is C, and Theorem 3 remains true with "s.g." replaced by "C".

The following examples are of interest: (1) \( C \) consists of \( A_3 \), introduced after Definition 7. \( M \) is a group and the C-extensions are the associative ones. (2) \( C \) consists of \( B_3 \), defined by \( X_1X_2X_3 = (X_1X_2X_3X_1)B_3(X_1, X_2, X_3) \). \( M \) is a Moufang loop (Bruck [1]), characterized by the identity

\[ xy \cdot zx = x(yz \cdot x), \]

and the C-extensions are the Moufang ones.

**4. Groups of extensions.** First let \( S \) be any commutative semigroup. A subset \( N \) is a nucleus of \( S \) if there exists a homomorphism \( \rho \) of \( S \), with kernel \( N \), upon a group. Equivalently: (i) if \( a_1a_2 = a_3 \) for \( a_j \) in \( S \), and if two of the \( a_j \) are in \( N \), so is the third; (ii) to each \( a \) in \( S \) corresponds an \( a^{-1} \) in \( S \) such that \( aa^{-1} \in N \). The necessity of (i), (ii) is obvious. As for sufficiency, define \( a \equiv b \) mod \( N \) if \( an_1 = bn_2 \) for \( n_j \) in \( N \), and let \( \rho \) be the equivalence class of \( a \) mod \( N \); then \( \rho \) is a homomorphism, with kernel \( N \), of \( S \) upon the quotient group \( S/\rho = S/N \). If the nucleus \( N' \) contains the nucleus \( N \), one may establish the isomorphism \( S/N' \cong (S/N)/(N'/N) \). Furthermore, if \( S \) has a unit contained in a subgroup \( S' \) of \( S \), then \( NS' \) is a nucleus and one may establish the isomorphism \( (NS')/N \cong S'/\langle S \cap N \rangle \). These remarks lead to the following (restricted) definition.

**Definition 9.** A subset \( N \) of the semigroup \( S \) of \((G, M)\) extensions (or of the group \( S' \) of central extensions) is a nucleus of \( S \) (or \( S' \)) provided (i) if \( E_1 \otimes E_2 = E_3 \) for (central) extensions \( E_j \), and if two of the \( E_j \) are in \( N \), so is the third; (ii) for every (central) extension \( E \), \( E \otimes E^{-1} \) is in \( N \), where \( E^{-1} \) denotes the inverse extension.
The following are nuclei of $S$: (i) the set $N_{sg}$ of s.g. extensions (Theorem 3); (ii) the set $N_C$ of $C$-extensions (Theorem 4); (iii) $S' \otimes N_{sg}$; (iv) $S' \otimes N_C$. As nuclei of $S'$ we have the subgroups $N'_{sg} = S' \cap N_{sg}$, $N'_C = S' \cap N_C$. We define abelian groups $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{S}$ by

$$\mathfrak{A} = S/N_{sg}, \quad \mathfrak{B} = (S' \otimes N_{sg})/N_{sg} \cong S'/N'_{sg}, \quad \mathfrak{S} = \mathfrak{A}/\mathfrak{B}.$$  

Similar definitions hold for $\mathfrak{A}_C$, $\mathfrak{B}_C$, $\mathfrak{S}_C$. In view of Theorem 2, these groups are isomorphic to certain groups of functions $F$. A characterization of the latter would be highly enlightening. So far, however, not much is known. At the one end of the scale we have the following theorem.

**Theorem 5.** If the loop $M$ is free, $\mathfrak{A}$, $\mathfrak{B}$, and $\mathfrak{S}$ are groups of order 1.

**Proof.** Let $(E, \theta)$ be a $(G, M)$ extension. In particular, $\theta$ is a homomorphism of $E$ upon $M$. Since $M$ is free, there exists (Bates [1, Theorem 3.5]) an isomorphism $\rho$ of $M$ into $E$ such that $x\rho = x$ for each $x$ in $M$. Let $W_n$ be any p.n.a. word, $x_1, \ldots, x_n$ any spot for $W_n$. Then $F(W_n, E; x_1, \ldots, x_n) = W_n(x_1\rho, \ldots, x_n\rho) = W_n(x_1, \ldots, x_n)\rho = 1$. Therefore $S = N_{sg}$, which implies Theorem 5.

A similar result holds for $C$-extensions. Define a loop $L$ to be a $C$-loop if $W_n(y_1, \ldots, y_n) = 1$ for every $W_n$ in $C$ and all $y_1, \ldots, y_n$ in $L$. By previous agreement, $M$ is a $C$-loop, and $E$ is a $C$-loop for every $C$-extension $(E, \theta)$.

Restricting attention to $C$-extensions, the proof of Theorem 5 may be paralleled exactly to give the following theorem.

**Theorem 6.** If $M$ is a free $C$-loop, $N_C = N_{sg}$. In words: the $C$-extensions coincide with the strongly grouplike extensions.

At the other end of the scale, take $M$ to be a group. For $n \geq 0$, a (normalized) $n$-cochain $f_n$ is (Eilenberg and MacLane [1, 2, 3]) a single-valued function from $M$ to $G$, with values $f_n(x_1, \ldots, x_n)$, taking the value 1 if at least one of the $x_j$ is 1. These $n$-cochains form the $n$-cochain group $\mathfrak{C}_n$ under the product $(f_n h_n)(x_1, \ldots, x_n) = f_n(x_1, \ldots, x_n) h_n(x_1, \ldots, x_n)$. We define the $(n+1)$-coboundary $\delta f_n$ of $f_n$ as the normalized cochain

$$\delta f_n(x_1, \ldots, x_{n+1}) = (f_n(x_1, \ldots, x_n) x_{n+1}) \cdot f_n(x_2, \ldots, x_{n+1})^{c(0)}$$

$$\cdot \prod_{i=1}^{n} f_n(x_1, \ldots, x_{i-1}, x_i x_{i+1}, x_{i+2}, \ldots, x_{n+1})^{c(i)},$$

where $c(j) = (-1)^{n+1+j}$ for $j = 0, 1, \ldots, n$. For $n > 0$, $\mathfrak{B}_n$ is the group
of the \( n \)-coboundaries; \( B_n \) consists of the 0-cochain 1, = 1. An \( n \)-cocycle is an \( n \)-cochain \( f_n \) such that \( \delta f_n = 1_{n+1} \) (the identity of \( C_{n+1} \)) and \( B_n \) is the group of the \( n \)-cocycles. As a consequence of the associativity of \( M \), one may verify that \( \delta^2 = 0 \), in the sense that \( \delta(\delta f_n) = 1_{n+2} \); hence \( B_n \) is a subgroup of \( B_n \). The \( n \)th cohomology group \( H_n \) is defined by \( H_n = \ker \delta_n \). The next theorem is due to Eilenberg and MacLane [2, 3]:

**Theorem 7.** If \( M \) is a group, the homomorphism \( (E, \theta) \rightarrow F(A_3, E) \) induces the isomorphism \( H_n \cong \hat{H}_n \).

A partial sketch of the proof will be useful. For any \((G, M)\) extension \((E, \theta)\), define (see §3) \( f_a \) and \( f_m \) by

\[
\begin{align*}
  f_a(x, y, z) &= F(A_3, E; x, y, z); \\
  f_m(x, y, z) &= F(B_3, E; x, y, z).
\end{align*}
\]

Choose \( e_j \) in \( E \) such that \( e \theta = x_j \) for \( j = 1, 2, 3, 4 \). Then

\[
(12) \quad f_a(x, y, z) = F(A_3; E; x, y, z); \quad f_m(x, y, z) = F(B_3; E; x, y, z).
\]

Choose \( e_j \) in \( E \) such that \( e \theta = x_j \) for \( j = 1, 2, 3, 4 \). Then

\[
(13) \quad (e_1 e_2) e_3 = e_1 (e_2 e_3) f_a(x_1, x_2, x_3); \quad e_1 e_2 \cdot e_3 e_1 = e_1 (e_2 e_3) f_m(x_1, x_2, x_3)
\]

showing that \( f_a, f_m \) are normalized 3-cochains. If \((E, \theta)\) is central and if \( u(x) \) is a normalized system of representatives of \( M \) in \( E \), then \( u(x) u(y) = u(x y) h(x, y) \) for a normalized 2-cochain \( h \). Setting \( e_j = u(x_j) \) in (13) we find \( f_a = \delta h \). In any case, by (13), \( e_1 e_2 \cdot e_3 e_4 = (e_1 e_2 \cdot e_3) f_a(x_1, x_2, x_3) = (e_1 e_2 \cdot e_3) f_m(x_1, x_2, x_3, x_4) \) and also

\[
(14) \quad f_m(x, y, z) = f_a(x, y, z) f_a(y, z, x)^{-1}.
\]

The homomorphism \( \rho \) of \( B_3 \) into \( C_3 \), defined by \( (f_\rho)(x, y, z) = f_3(x, y, z) \), induces a homomorphism of \( C_3 \) upon a group \( \hat{B}_3 \). In view of (14) we may state the following theorem.

**Theorem 8.** If \( M \) is a group, let \( C \)-extensions be Moufang extensions. Then the homomorphism \((E, \theta) \rightarrow F(B_3, E) \) induces an isomorphism \( \hat{B}_3 \cong \hat{B}_3 \).

Theorems 5–8 have analogues for central extensions, for example (Baer [1], Eilenberg and MacLane [1]): if \( M \) is a group, the group of
central group extensions is isomorphic to the second cohomology group \$H_2\$.

5. Grouplike extensions. Conjugate extensions. A \((G, M)\) extension \((E, \theta)\) is grouplike if, for every subgroup (= associative subloop) \(H\) of \(M\), \(H\theta^{-1}\) is a subgroup of \(E\). Thus \((E, \theta)\) is grouplike if and only if \(F(A_3, E; x, y, z) = 1\) for all triples \(x, y, z\) which generate a subgroup of \(M\). Note that s.g. extensions are grouplike.

If \(E\) is any loop, define for each \(p\) in \(E\) permutations \(R_p, L_p\) by \(eR_p = ep, eL_p = pe,\) all \(e\) in \(E\). Choosing fixed \(f, g\) in \(E\), we may define a new operation \(\circ\) on \(E\) by

\[
e_1 \circ e_2 = (e_1 R_p^{-1})(e_2 L_p^{-1}).
\]

The elements of \(E\) form a loop \(E_0\) under \(\circ\); the unit is \(pq\). \(E_0\) is (Albert [1]) a (principal) isotope of \(E\). If, further, \((E, \theta)\) is a \((G, M)\) extension, write \(\theta = u, g\theta = v\). Then, if \(M_0\) is the principal isotope of \(M\) defined by

\[
xoy = (xR_u^{-1})(yL_u^{-1}),
\]

we find from (15), (16), with \(e\theta = x_i\), that \((e_1 \circ e_2)\theta = x_1 \circ x_2\).

For each \(a\) in the associator \(A(M)\), and for each \((G, M)\) extension \((E, \theta)\), define a loop \(E^a\) as follows: Choose \(p\) in \(E\) so that \(p\theta = a^{-1}\), and \(q\) in \(E\) so that \(pq = 1\). Then \(E^a\) is the loop \(E_0\) given by (15). We define \((E, \theta)^a = (E^a, \theta)\) to be a conjugate of \((E, \theta)\).

THEOREM 9. Let \((E, \theta)\) be a \((G, M)\) extension, and let \(a, b\) be in \(A(M)\). Then: (i) \(E^a\) is independent of the choice of \(p\) in its definition; (ii) \((E^a, \theta)\) is a \((G, M)\) extension; (iii) \(E_1 \sim E_2\) implies \(E_1^a \sim E_2^a\); (iv) \(E_1 \sim E_2^{-1}\) implies \(E_1^a \sim E_2^{-a}\); (v) \((E^a)^b \sim E^{ab}\); (vi) \((E_1 \otimes E_2)^a \sim E_1^a \otimes E_2^a\).

PROOF. (i) In (15), \(pq = 1\). Clearly we can construct a word \(W_s\), independent of the loop \(E\), so that (15) becomes \(e_1 \circ e_2 = e_1 e_2 W_s(e_1, e_2, p)\). If \(E\) is a group, (15) yields \(e_1 e_2 = (e_1 q^{-1})(p^{-1} e_2) = e_1 p^{-1} e_2 = e_1 e_2;\) thus \(W_s\) is p.n.a. Since, in (16), \(u = p\theta = a^{-1}, v = g\theta = a,\) with \(a\) in \(A(M)\), we have \(xoy = xa^{-1}.(a^{-1})^{-1}y = x(a^{-1}.ay) = xy\). Hence \(W_s(e_1, e_2, p)\theta = W_s(x_1, x_2, a^{-1}) = 1.\) By Theorem 1, \(W_s(e_1, e_2, p)\) lies in \(G\) and depends only on \(x_1, x_2, a\).

(ii) Since \(xoy = xy, \theta\) is a homomorphism of \(E^a\) upon \(M\). The kernel of \(\theta\) (in \(E^a\)) is the subloop \(K\) consisting of \(K\) under \(\circ\). Since \(pq = 1\) is the unit of \(E^a, W_s(1, e, p) = 1 = W_s(e, 1, p)\) for all \(e\) in \(E^a\). Hence, for \(k\) in \(K, eok = ekW_s(e, k, p) = ekW_s(e, 1, 1) = ek\) and \((e_1 e_2)ok = (e_1 e_2)k = e_1 e_2 W_s(e_1, e_2, p) = e_1 e_2 k = e_1 e_2 k W_s(e_1, e_2, p) = e_1 (e_2 k) = e_1 (e_2 k).\) Similarly \((e_1 e_2)ok = e_1 (koe_2), (koe_1)oe_2 = ko(e_1 e_2),\) so that \(K\) is in
A(\mathcal{E}_a). The element \( c \) of \( K_0 \) is in \( Z(K_0) \) if and only if \( cok = koc, ck = kc, \)
c is in \( G = Z(K) \). If \( g_1, g_2 \) are in \( G, g_1g_2 = g_2g_1 \); thus \( G = Z(K_0). \) Finally,
for \( g \) in \( G, e \) in \( E, x = e_0, goe = ge = e(gx) = e0(gx) \). This completes the
proof that \( (E^a, \theta) \) is a \((G, M)\) extension.

(v) Assume \( E^a = E_0 \) is defined by \((15), \) with \( \rho \theta = a^{-1}, \rho g = 1. \) Then
\( (E^a)^b = E_b^a \) must be defined, with operation \((\ast)\), by \( e_1 \ast e_2 = (e_1T) o (e_2S) = (e_1T R_{-1}^{-1}) (e_2S L_{-1}^{-1}), \) where \( e S^{-1} = soo = (sR_{-1}) (eL_{-1}^{-1}), e T^{-1} = e ot = (eR_{-1}) (tL_{-1}^{-1}) \) for \( s, t \) in \( E \) such that \( st = b^{-1}, 1 = sol = (sR_{-1}) (tL_{-1}^{-1}). \) The elements \( f = sR_{-1}, h = tL_{-1}^{-1} \) satisfy \( f \theta = b^{-1} a^{-1}, f h = 1. \) Moreover,
\( SL_{-1}^{-1} = L_{-1}^{-1} \) and \( TR_{-1}^{-1} = R_{-1}^{-1}. \) Therefore \( e_1 \ast e_2 = (e_1R_{-1}^{-1}) (e_2L_{-1}^{-1}) \), showing
that \( (E^a)^b = E_{ab}. \) The proofs of (iii), (iv), (vi) offer no difficulty, hence
are omitted.

6. Central and central Moufang extensions. For any pair \( (G, M) \)
we may define the groups \( \mathbb{C}_n, \mathbb{B}_n \) of (normalized) \( n \)-cochains and \( n \)-coboundaries. By \((11), \) the \( n \)-coboundaries for \( n = 2, 3 \) are given by

\[
(\delta f_1)(x, y) = (f_1(x) y) f_1(y) f_1(xy)^{-1},
\]

\[
(\delta f_2)(x, y, z) = (f_2(x, y) z) f_2(y, z)^{-1} f_2(xy, z) f_2(x, yz)^{-1}.
\]

If \( M \) is not associative we lose the important property \( \delta^2 = 0; \) in particular,

\[
(\delta^2 f_1)(x, y, z) = f_1(x \cdot yz) f_1(xy \cdot z)^{-1}.
\]

DEFINITION 10. Let \( f, h \) be normalized 2-cochains of \( (G, M) \). Then
\( f \) is equivalent to \( h \) if \( f = h \cdot 2c \) for some (normalized) 1-cochain \( c. \) (Notation: \( f \sim h. \) )

DEFINITION 11. If \( f \) is a normalized 2-cochain of \( (G, M), \) then
\( (G, M, f) \) is the central \((G, M)\) extension \((E, \theta)\) defined as follows:
(i) The elements of \( E \) are the pairs \( (x, g), x \) in \( M, g \) in \( G. \) (ii) \( (x, g) = (y, g') \) if and only if \( x = y, g = g'. \) (iii) \( (x, g)(y, g') = (xy, f(x, y) \cdot (gy)g'). \) (iv) \( (x, g) \theta = x. \) (v) \( (1, g) = g. \)

By Definition 6, the unit extension \((E_0, \theta_0)\) may be identified with
\((G, M, 1) \) where \( 1 \) is the identity \( 2 \)-cochain \( 1_2. \)

THEOREM 10. (i) Each central \((G, M)\) extension is equivalent to at
least one extension \((G, M, f)\) if and only if \( f \sim h. \) (ii) \( (G, M, f) \sim (G, M, h) \)
if and only if \( f \sim h. \) (iii) \( (G, M, f) \sim (G, M, h) \) if and only if \( f \sim h. \) (iv) \( (G, M, f) \)
\( \otimes (G, M, h) \sim (G, M, f \cdot h). \) (v) \( (G, M, f) \) is grouplike if and only if
\( (\delta f)(x, y, z) = 1 \) for all \( x, y, z \) which generate a subgroup of \( M. \) (vi) For
\( a \) in \( A(M), (G, M, f)^a \sim (G, M, f^a) \) where

\[
f^a(x, y) = f(x, y) \cdot (\delta f)(a^{-1}, a, y) \cdot ((\delta f)(xa^{-1}, a, y))^{-1}.
\]

COROLLARY. The set \( S' \) of central \((G, M)\) extensions is an abelian
group with unit \((E_0, \theta_0)\) and inverse \((E, \theta)^{-1}\).

**Proof.** (i) Let \((E, \theta)\) be a central extension, \(u(x)\) a normalized system of representatives of \(M\) in \(G\). Since \((u(x)u(y))\theta = xy = u(xy)\theta\), \(u(x)u(y) = u(xy)f(x, y)\) for \(f(x, y)\) in \(G\). Since \(u(1) = 1\), \(f\) is a normalized 2-cochain. Every \(e\) in \(E\) has a unique representation \(e = u(x)g\) with \(g\) in \(G\). Moreover \(u(x)g \cdot u(y)g' = u(x)u(y)(gy)g' = u(xy)f(x, y)\cdot (gy)g'\). Hence the mapping \(u(x)g \rightarrow (x, g)\) gives the equivalence of \((E, \theta)\) and \((G, M, f)\).

(ii), (iii), (iv). For \(j = 1, 2\), denote the elements of \((E_j, \theta_j) = (G, M, f_j)\) by \((x, g)_j\), where \((x, g)_j\). Set \(u_j(x) = (x, 1)_j\). If \(\pi\) is an isomorphism of \(E_1\) upon \(E_2\) such that \(\pi \theta_2 = \theta_1\), then necessarily \(u_1(x)\pi = u_2(x)c(x)\) = \((x, c(x))_2\) for a normalized 1-cochain \(c\); and \((x, g)_1\pi = (x, (g\pi)c(x))_2\). Also \(g \cdot x = g \cdot x\). Conversely, if \(\pi\) is any automorphism of \(G\) (such that \(g \cdot x = g \cdot x\)) and \(c\) any normalized 1-cochain, the definition \((x, g)_1\pi = (x, (g\pi)c(x))_2\) extends \(\pi\) to an isomorphism of \(E_1\) upon \(E_2\) such that \(\pi \theta_2 = \theta_1\). Direct calculation gives \(f_1(x, y)\pi = f_2(x, y)\cdot (\delta c)(x, y)\); (ii), (iii) come by assuming \(g \cdot x = x\). For \(E_1 \otimes E_2\) take the representatives \(u(x) = (u_1(x), u_2(x))\); Definition 5 gives \(u(x)u(y) = (u_1(xy)f_1(x, y), u_2(xy)f_2(x, y)) = u(xy)f_1(x, y)f_2(x, y)\), proving (iv). The corollary should be obvious.

Note that if \(c\) is a 1-cochain and if \(a\) is in \(A(M)\), (19) gives \((\delta c)(x, a, y) = (c(x, a)) = (x, (g\pi)c(x))_2 = (x, c(x))_2\) extends \(c\) to an isomorphism of \(E_1\) upon \(E_2\) such that \(\pi \theta_2 = \theta_1\). Thus it is evident from (20) that the cochain \(f^{a\cdot f^{-1}}\) is invariant under replacement of \(f\) by an equivalent cochain. We now turn to Moufang loops.

**Theorem 11.** Let \(M\) be a Moufang loop. Then: (i) \(xy \cdot zx = x(yz \cdot x)\) for all \(x, y, z\) in \(M\). (ii) \(x(yz) = (xy \cdot z)\) for all \(x, y, z\) in \(M\). (iii) Every loop \(M\) isotopic to \(M\) is Moufang. (iv) The subloop generated by any two elements \(x, y\) of \(M\) is a group. (v) If the three elements \(x, y, z\) satisfy
$xy \cdot z = x \cdot yz$, they generate an associative subloop. (vi) The central extension $(G, M, f)$ is Moufang if and only if $f$ satisfies one of the (equivalent) conditions for a Moufang cochain:

(21a) $f(xy, zx)(f(x, y)zx)f(z, x) = f(x, yz \cdot x)f(yz, x)(f(y, z)x)$;
(21b) $f(x, y \cdot zx) \cdot (\delta f)(x, y, zx) = f(x, yz \cdot x) \cdot (\delta f)(y, z, x)$.

(vii) The central Moufang $(G, M)$ extensions form a subgroup of the group of central extensions. (viii) If $f$ is a Moufang cochain, (20) simplifies to

(22) $f^a(x, y)f(x, y)^{-1} = (\delta f)(xa^{-1}, a, y)^{-1}$;

in particular, for each $a$ of $A(M)$, the 2-cochain defined by the right side of (22) is Moufang.

**Proof.** Items (i)–(v) are included for reference. For a proof that (i) and (ii) are equivalent, and for (iii), see Bruck [1, Chapter II]. Items (iv), (v) are due to Moufang [1]; see also Bruck [2]. As for (vi), the extension $E = (G, M, f)$ is Moufang if and only if the word $B_3$ of §3 vanishes on $E$. Assuming $u(x)u(y) = u(xy)f(x, y)$, the condition $B_3(u(x), u(y), u(z)) = 1$ gives precisely (21a), which, by (18), is equivalent to (21b). (vii) follows from (21) and Theorem 10. As for (viii), the elements $u(x), u(y)$ of the Moufang loop $E$ generate a group, by (iv). Since $u(x)^{-1} = u(x^{-1})g$ for some $g$ in $G$, the condition $u(x)^{-1}u(x) \cdot u(y) = u(x^{-1}u(x^{-1})u(y)$ reduces to $(\delta f)(x^{-1}, x, y) = 1$. In particular, (20) becomes (22). Since $E^a \otimes E^{-1} \sim (G, M, f^a f^{-1})$, (iii), (vii) imply the concluding statement of (viii).

**Theorem 12.** Let $M$ be a finite Moufang loop of order $m$. Let the least common multiple of the orders of the elements of $M$ be $n$. For any $a$ in $A(M)$, and for any central Moufang $(G, M)$ extension $(E, \theta)$:

(i) $E^a$ is Moufang. (ii) $E^{mn} \sim E_m$. (iii) $(E^a \otimes E^{-1})^{2m}$ is grouplike. (iv) If $M$ is commutative, $E^{2m}$ is grouplike. (v) If $n$ is odd, the exponent $2m$ in (iii), (iv) may be replaced by $m$. (vi) If $gx = g$ for all $g$ in $G, x$ in $M$, $E^m \sim E_0$.

**Proof.** (i) reflects Theorem 11 (iii) and was used for (viii). For the proof of (ii)–(vi), take $(E, \theta) = (G, M, f)$ where $f$ satisfies (21). Define the following (normalized) cochains:

(23) $c(x) = \prod_y f(x, y), \quad d(x) = \prod_y f(y, x),$

where the products are taken over the $m$ elements $y$ of $M$, and

(24) $h(x, y) = (c(x)y)c(x)^{-1}$. 


From (24),
\[(25) \quad h(x, yz) = (h(x, y)z)h(x, z).\]
This implies
\[(26) \quad h(w, xy z) = h(w, x yz),\]
since both sides reduce to \((h(w, x)y z)(h(w, y)z)h(w, z)\). If \(f_1(x, y) = h(y, xy)^{-1}\), we take products in (21a) over all \(y\), use (23), (24) and find \(f(x, x)^m = (h d)(x, x) \cdot f_1(x, x)\), or
\[(27) \quad f^m \sim f_1, \quad f_1(x, y) = h(y, xy)^{-1}.\]
If \(g x = g\) for all \(g, x, h = 1\) by (24) and \(f^m \sim 1\) by (27), proving Theorem 12 (vi).

Since 1 = \(f_1(1, y) = h(y, y)^{-1}\), or \(h(y, y) = 1\), (25) implies
\[(28) \quad h(x, x) = 1, \quad h(x, xy) = h(x, y), \quad h(x, yx) = h(x, y).\]
Since (21a) applies to \(f_1\), set \(z = 1\) and get \(f_1(xy, x)(f_1(x, y)x) = f_1(xy, x)\)
\(\cdot f_1(x, y)\). By (27), (28), and \(f_1(xy, x) = h(x, xy)^{-1} = h(x, y) = f_1(x, y)\), leaving \(f_1(x, y)x = f_1(xy, x) = h(y, yx)^{-1} = h(y, xyx)^{-1}\), or \(f_1(x, y) = h(yx, x)^{-1}\). Thus \(h(yx, x) = f_1(x, y) = h(y, xy)x\). Hence \(h(y, x)\),
\(h(yx, x) = h(y, x)\), or
\[(29) \quad h(xy, y) = h(x, y).\]

Returning to (21a), take products over all \(z\), getting
\[(30) \quad \Pi (f(x, y)z) = (c(y)x)c(x)c(xy)^{-1} = h(y, x)c(x)c(xy)^{-1} \cdot \Pi.\]
The left-hand element of (30) remains fixed when we operate with \(w\). Thus, by (24), \((h(y, x)w)h(y, x)^{-1}h(x, w)h(y, w)h(xy, w)^{-1} = 1\); whence, by (25),
\[(31) \quad h(y, xw)h(x, w) = h(y, x)h(xy, w).\]
Set \(w = y\) in (31) and use (29). Thus \(h(y, xy)h(x, y) = h(y, x)h(xy, y) = h(y, x)h(x, y), h(y, xy) = h(y, x)\), and
\[(32) \quad h(x, yx) = h(x, y).\]
In view of (28.3), (32), \(h(x, y)x = h(x, y)\). Hence, by (29), \(h(x, y)y = h(x, y)xy = h(xy, y)xy = h(xy, y) = h(x, y)\). Therefore
\[(33) \quad h(x, y)x = h(x, y) = h(x, y).\]
From (29) with \(y\) replaced by \(x^{-1}\), \(h(y, x^{-1}) = h(x, x^{-1})\). By (32) and (28.2), this implies \(h(y, x^{-1}) = h(x, y)\). Then, by (33), (25),
\[ h(x, y)h(y, x) = h(y, x^{-1})h(y, x) = (h(y, x^{-1})x)h(y, x) = h(y, x^{-1}x) = h(y, 1) = 1, \text{ or }\]
\[ h(y, x)^{-1} = h(x, y). \]

Hence (32), (34) give \( f_1(x, y) = h(y, xy)^{-1} = h(y, x)^{-1} = h(x, y), \) so
\[ f_1 = h. \]

Since \( h(x, y)y = h(x, y), \) a simple induction using (25) gives \( h(x, y^i) = h(x, y^i) \). Combining this with (34),
\[ \text{(36)} \quad h(x^i, y^j) = h(x, y)^{ij} \]
for all integers \( i, j. \) In particular, \( f_1(x, y)^n = h(x, y)^n = h(x, 1) = 1, \) and so \( f^m = f^n = 1. \) This proves Theorem 12 (ii).

If \( p = \delta f_1 = \delta h, \) (18) and (25) combine to give
\[ \text{(37)} \quad h(xy, z) = h(x, z)h(y, z)p(x, y, z), \quad p = \delta h. \]

Since \( h \) satisfies (21b), (26),
\[ \text{(38)} \quad p(x, y, zx) = p(y, z, x). \]

Operating on (37) by \( w, \) and using (25), we find
\[ \text{(39)} \quad p(x, y, zw) = (p(x, y, z)w)p(x, y, w). \]

Again, since \( h(x, z)s = h(x, z), \) (37) gives \( p(x, y, s) = p(x, y, z). \) Hence, by (38), \( p(x, y, zx)x = p(y, z, x) = p(x, y, z), \) or \( p(x, y, z)x = p(x, y, z). \)

Thus, finally, \( p(x, y, zx)y = p(y, z, x)y = p(y, z, x) = p(x, y, zx), \) and
\[ \text{(40)} \quad p(x, y, z)w = p(x, y, z), \quad w = x, y, z. \]

Since \( h(xy, x) = h(x, xy)^{-1} = h(x, y)^{-1} = h(y, x) \) and \( h(x, x) = 1, \) (37) with \( z = x \) gives \( p(x, y, x) = 1. \) Therefore, by (38), (39), (40), \( p(x, y, zx) = (p(x, y, z)x)p(x, y, x) = p(x, y, z), \) so that (38) becomes
\[ \text{(41)} \quad p(x, y, z) = p(y, z, x). \]

By (37), (24), and (25), \( p(x, y, z) = h(z, x)h(z, y)h(z, x, y)^{-1} = h(z, x) \cdot (h(z, x)y)^{-1}. \) Therefore, by (41), (34),
\[ \text{(42)} \quad p(x, y, z) = h(x, y)(h(x, y)z)^{-1} = p(y, x, z)^{-1}. \]

By this and (37),
\[ h(xy, z)h(yx, z)^{-1} = p(x, y, z)^2. \]

Hence, if \( M \) is commutative, (43) gives \( (\delta h)(x, y, z)^2 = 1 \) for all \( x, y, z. \)

In view of (19), the best we can say for \( k = f^m \) is that \( (\delta k)(x, y, z) = 1 \) for all \( x, y, z \) such that \( xy \cdot z = x \cdot yz. \) By Theorems 11(v), 10(v), this is
precisely the condition that $E^{2m}$ be grouplike. We have proved Theorem 12(iv).

Since $f^m \sim h$ and $p = \delta h$, we see from Theorem 11(viii) that $(E^a \otimes E^{-1})^{2m} \sim (G, M, q)$ where

$$q(x, y) = p(xa^{-1}, a, y)^{-2}.$$  

Define the (normalized) 4-cochain $r$ by

$$r(w, x, y, z) = (p(w, x, y)x)p(w, x, y)^{-1}.$$  

By (45), $r$ has the skew-symmetry (41), (42) of $p$ on its first three arguments. By (39),

$$p(w, x, yz) = p(w, x, y)p(w, x, z)r(w, x, y, z).$$  

By (47) and skew-symmetry, $r(w, x, y, z) = r(w, x, y, z) = r(w, x, z, y) = r(w, x, z, y)$ or

$$r(w, x, y, z)^2 = 1.$$  

From (44), (46), (48), $q(x, y)^{-1} = p(a, y, xa^{-1})^2 = p(a, y, x)^2p(a, y, a^{-1})^2$. Since $q(1, y) = 1$, the second factor is 1, and, by (42),

$$q(x, y)^{-1} = p(x, y, a)^2 = h(x, y)^2(h(x, y)a)^{-2}.$$  

Therefore, since $p = \delta h$, $(\delta q)(x, y, z)^{-1} = p(x, y, z)^2p(x, y, z)a^{-2}$. Hence, by (45), (48), $(\delta q)(x, y, z) = 1$ for all $x, y, z$. This proves Theorem 12 (iii).

As for (v), since $h^n = 1$, (37) gives $p^n = 1$ and then (45) gives $r^n = 1$. However, $r^2 = 1$, by (48). Hence, if $n$ is odd, $r = 1$ and (iii) holds with $2m$ replaced by $m$. A similar remark is true of (iv). This completes the proof of Theorem 12.

Theorem 12 should be compared with the simpler result for groups (Marshall Hall [1]): If $M$ is a group of order $m$ and if $(E, \theta)$ is a central associative $(G, M)$ extension, $E^m \sim E_o$.

**BIBLIOGRAPHY**

A. A. Albert

REINHOLD BAER

GRACE E. BATES

R. H. BRUCK

MAX DEURING

MARSHALL HALL

SAMUEL EILENBERG

SAMUEL EILENBERG AND SAUNDERS MACLANE

RUTH MOUFANG

HANS ZASSENHAUS

UNIVERSITY OF WISCONSIN