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**][1] 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 $(e_1e_2)e_3 = e_1(e_2e_3)$ 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)[2] 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

An address delivered before the Chicago Meeting of the Society on November 25, 1949, by invitation of the Committee to Select Hour Speakers for Midwestern Sectional Meetings; received by the editors February 28, 1950.

[1] Numbers in brackets refer to the bibliography at the end of the paper.

[2] Slightly weaker results on central Moufang extensions were obtained in 1946–1947 with the support of a Guggenheim Fellowship supplemented by a grant from the Wisconsin Alumni Research Foundation. (See Bull. Amer. Math. Soc. Abstract 53-1-11.)

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, $xH=Hx$, $(xy)H=x(yH)$, $(xH)y=x(Hy)$, $(Hx)y=H(xy)$ for all x, y in M. The mapping $x\to xH$ 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 θ upon M; (ii) the kernel K of θ 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

$$ke = e(kT(e)), \qquad k \in K. \tag{1}$$

Applying θ 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, $e((k_1k_2)T(e)) = (k_1k_2)e = k_1(k_2e) = k_1(e\cdot k_2T(e)) = k_1e\cdot k_2T(e) = (e\cdot k_1T(e))\cdot k_2T(e) = e(k_1T(e)\cdot k_2T(e))$. 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, $(e_1e_2)\cdot kT(e_1e_2)=k(e_1e_2)=(ke_1)e_2 =(e_1\cdot kT(e_1))e_2=e_1(kT(e_1)\cdot e_2)=e_1(e_2\cdot kT(e_1)T(e_2))=(e_1e_2)\cdot kT(e_1)T(e_2)$, or $kT(e_1e_2)=kT(e_1)T(e_2)$. In other words, *the mapping $e\to T(e)$ 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, $e'\theta=e\theta$ if and only if $e'=ke$ for k in K; thus $gT(e)$ *depends only on g and $x=e\theta$.* 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, θ) consists of a loop E and a homomorphism θ of E upon M such that (i) $K=1\theta^{-1}$ 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, θ) is *central* if $1\theta^{-1}=G$.

DEFINITION 3. (E_1, θ_1) is *equivalent* to (E_2, θ_2) if there exists an isomorphism π 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, θ_1) is *inverse equivalent* to (E_2, θ_2) if there exists an isomorphism π 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: $E\sim^{-1}E_1$, $E_1\sim E_2$ imply $E\sim^{-1}E_2$. Therefore, since equivalence is to serve as equality, we may define *the* inverse $(E, \theta)^{-1}$ as any extension inverse equivalent to (E, θ). The inverse of (E, θ) 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 $K=1\theta^{-1}$, every e in E has a unique representation $e=u(x)k$ with $x=e\theta$, k in K; define π by $e\pi=u(x)k^{-1}$. Define a new operation (o) on the elements of E by $eoe'=(e\pi\cdot e'\pi)\pi$; it is easy to see that this turns E into a loop E^{-1}. I claim that (E^{-1}, θ) is the desired inverse. Indeed, π is an isomorphism of E upon E^{-1}, and $g\pi=g^{-1}$ for g in G. Also $\theta=\pi\theta$. Certainly θ 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 $K\pi$, $(e_1oe_2)oe_3=((e_1\pi\cdot e_2\pi)\cdot e_3\pi)\pi=(e_1\pi\cdot(e_2\pi\cdot e_3\pi))\pi=e_1o(e_2oe_3)$; thus $K\pi$ is in $A(E^{-1})$. For g in G, e in E^{-1}, $x=e\theta$, we have $goe=(g^{-1}\cdot e\pi)\pi=(e\pi\cdot(g^{-1}x))\pi=eo(gx)$. This completes the proof.

DEFINITION 5. The *product* $(E_1, \theta_1)\otimes(E_2, \theta_2)=(E, \theta)$ of two extensions (E_j, θ_j) is defined as follows: (i) The elements of E are the pairs (e_1, e_2) with e_j in E_j and $e_1\theta_1=e_2\theta_2$. (ii) $(e_1, e_2)=(e_1', e_2')$ if and only if $e_1'=e_1g$, $e_2'=e_2g^{-1}$ for some g in G. (iii) $(e_1, e_2)(e_1', e_2')=(e_1e_1', e_2e_2')$. (iv) $(e_1, e_2)\theta=e_1\theta_1=e_2\theta_2$. (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

$$\text{If } E_j\sim E_j' \ (j=1, 2),\quad E_1\otimes E_2\sim E_1'\otimes E_2', \tag{2}$$

$$E_1\otimes E_2\sim E_2\otimes E_1, \tag{3}$$

$$(E_1\otimes E_2)\otimes E_3\sim E_1\otimes(E_2\otimes E_3). \tag{4}$$

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_o, θ_o):

DEFINITION 6. The *unit* extension (E_o, θ_o) is defined as follows: E_o is the set of all pairs (x, g), x in M, g in G, such that (i) (x, g)

$=(y, g')$ if and only if $x=y$, $g=g'$; (ii) $(x, g)(y, g')=(xy, (gy)g')$; (iii) $(1, g)=g$. And θ_o 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_o, θ_o)*. For (E, θ) central, our inverse $(E, \theta)^{-1}$ is the inverse of (E, θ) 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 $X_1, \cdots, X_n$. Thus L_n is a loop containing the X_j, such that any mapping $X_1 \rightarrow e_1, \cdots, X_n \rightarrow e_n$ into elements e_j of a loop E may be extended uniquely to a homomorphism ρ of L_n into E. By a (nonassociative) *word* W_n we mean any element of L_n. The image $W_n\rho$ is denoted by $W_n(e_1, \cdots, e_n)$; this turns W_n into a function defined on *every* loop E (with values in E). The following fact is worth noting: if also σ is a homomorphism of E into a loop L, $W_n(e_1, \cdots, e_n)\sigma = W_n(e_1\sigma, \cdots, e_n\sigma)$, 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 $e_1, \cdots, e_n$ are group elements,

$$W_n(e_1, \cdots, e_n) = 1.$$

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 $W_n(e_1, \cdots, e_n)$ (n arbitrary, W_n p.n.a., the e_j 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, θ) be a (G, M) extension, W_n, a p.n.a. word, $e_1, \cdots, e_n$, elements of E. Write $e_j\theta=x_j$, $e_o=W_n(e_1, \cdots, e_n)$. Then* (i) *$e_ok=ke_o$ for k in the kernel K*; (ii) *$W_n(x_1, \cdots, x_n)=1$ if and only if e_o is in G*; (iii) *e_o depends only on the x_j*:

$$e_o = W_n(e_1, \cdots, e_n) = F(W_n, E; x_1, \cdots, x_n). \tag{5}$$

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 $T(e_o) = W_n(T(e_1), \cdots, T(e_n))=1$, the identity automorphism.

(ii) $e_o\theta = W_n(x_1, \cdots, x_n)$, so (i) implies (ii).

(iii) For fixed n, and for every word A_n (not necessarily p.n.a.), define a function $H(A_n; e, k)=H(A_n; e_1, \cdots, e_n; k_1, \cdots, k_n)$ by

$$A_n(e_1k_1, \cdots, e_nk_n) = A_n(e_1, \cdots, e_n)H(A_n; e, k). \tag{6}$$

Here the e_j are assigned fixed values in E and the k_j vary over K. Applying θ to (6) we find that H takes values in K. Also from (6), direct computation, along with the fact that $(A_nB_n)(e_1, \cdots, e_n) = A_n(e_1, \cdots, e_n)B_n(e_1, \cdots, e_n)$, gives

$$(7) \quad H(A_nB_n; e, k) = H(A_n; e, k)T(B_n(e_1, \cdots, e_n) \cdot H(B_n; e, k).$$

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

$$(8) \qquad H(1; e, k) = 1; \qquad H(X_j; e, k) = k_j \qquad (j = 1, 2, \cdots, n).$$

In addition, if $B_nC_n = A_n = D_nB_n$, 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 $\mathfrak{K}$ of K. This group is the set of all pairs (S, k), k in K, S an automorphism of K, under the product $(S, k)(U, k') = (SU, kU \cdot k')$. The n elements $f_j = (T(e_j), k_j)$ yield $A_n(f_1, \cdots, f_n) = (T(A_n(e_1, \cdots, e_n)), H'(A_n; e, k))$ where H' satisfies both (7) and (8). Therefore $H = H'$. Since $\mathfrak{K}$ is a group, $H'(W_n; e, k) = 1$ for every p.n.a. word W_n. Thus, by (6), $W_n(e_1k_1, \cdots, e_nk_n) = W_n(e_1, \cdots, e_n) = e_o$, showing that e_o depends only on the images $x_j = e_j\theta = (e_jk_j)\theta$. This completes the proof of Theorem 1.

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

Theorem 2. *At each spot for a* p.n.a. *word* W_n, *the functions* F (*of Theorem* 1) *form a multiplicative abelian group*: (i) $E_1 \sim E_2$ *implies* $F(W_n, E_1) = F(W_n, E_2)$; (ii) $E_1 \sim^{-1} E_2$ *implies* $F(W_n, E_1) = F(W_n, E_2)^{-1}$; (iii) $F(W_n, E_1)F(W_n, E_2) = F(W_n, E_1 \otimes E_2)$.

Proof. Let $x_1, \cdots, x_n$ be a spot for W_n, and write $F(W_n, E) = F(W_n, E; x_1, \cdots, x_n)$ for any extension (E, θ). By Theorem 1 (ii), $F(W_n, E)$ is in G. Let π be an isomorphism of (E_1, θ_1) upon (E_2, θ_2) satisfying (i) of Definitions 3, 4, and let e_j in E_1 satisfy $e_j\theta_1 = x_j$ $(j = 1, 2, \cdots, n)$. Then $e_j\pi$ is in E_2, and $e_j\pi\theta_2 = e_j\theta_1 = x_j$. Hence $F(W_n, E_1)\pi = W_n(e_1, \cdots, e_n)\pi = W_n(e_1\pi, \cdots, e_n\pi) = F(W_n, E_2)$. According as π 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 $e_j = (e_{1j}, e_{2j})$, $(j = 1, 2, \cdots, n)$. If $g_i = F(W_n, E_i)$, Definition 5 gives $F(W_n, E_1 \otimes E_2) = W_n(e_1, \cdots, e_n) = (g_1, g_2) = (g_1g_2, 1) = g_1g_2 = F(W_n, E_1)F(W_n, E_2)$.

3. **Strongly grouplike and C extensions.** An extension (E, θ) 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 $W_n(e_1, \cdots, e_n)\theta = 1$, then $W_n(e_1, \cdots, e_n) = 1$. 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* $E_1 \sim^{-1} E$, *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 $W_n(x_1, \cdots, x_n) = 1$ for all x_j in M. Then a (G, M) extension (E, θ) is "C" if $W_n(e_1, \cdots, e_n) = 1$ 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 $X_1X_2 \cdot X_3X_1 = (X_1(X_2X_3 \cdot X_1))B_3(X_1, X_2, X_3)$. M is a Moufang loop (Bruck [1]), characterized by the identity

$$xy \cdot zx = x(yz \cdot x), \tag{9}$$

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 ρ 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 $a\rho$ be the equivalence class of a mod N; then ρ 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 $(NS')/N \cong S'/(S \cap N)$. 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 $\mathfrak{Z}$, $\mathfrak{B}$, $\mathfrak{H}$ by

$$(10)\qquad \mathfrak{Z} = S/N_{sg}, \qquad \mathfrak{B} = (S'\otimes N_{sg})/N_{sg} \cong S'/N'_{sg}, \qquad \mathfrak{H} = \mathfrak{Z}/\mathfrak{B}.$$

Similar definitions hold for $\mathfrak{Z}_C$, $\mathfrak{B}_C$, $\mathfrak{H}_C$. 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, $\mathfrak{Z}$, $\mathfrak{B}$, and $\mathfrak{H}$ are groups of order* 1.

PROOF. Let (E, θ) be a (G, M) extension. In particular, θ is a homomorphism of E upon M. Since M is free, there exists (Bates [1, Theorem 3.5]) an isomorphism ρ of M into E such that $x\rho\theta = x$ for each x in M. Let W_n be any p.n.a. word, $x_1, \cdots, x_n$ any spot for W_n. Then $F(W_n, E; x_1, \cdots, x_n) = W_n(x_1\rho, \cdots, x_n\rho) = W_n(x_1, \cdots, x_n)\rho = 1\rho = 1$. 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 $W_n(y_1, \cdots, y_n) = 1$ for every W_n in C and all $y_1, \cdots, y_n$ in L. By previous agreement, M is a C-loop, and E is a C-loop for every C-extension (E, θ). The notion of a free C-loop may be defined as in Bates [1, Appendix]. 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 $n \geqq 0$, a (*normalized*) *n-cochain* f_n is (Eilenberg and MacLane [1, 2, 3]) a single-valued function from M to G, with values $f_n(x_1, \cdots, x_n)$, 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 $(f_nh_n)(x_1, \cdots, x_n) = f_n(x_1, \cdots, x_n)h_n(x_1, \cdots, x_n)$. We define the $(n+1)$-*coboundary* δf_n of f_n as the normalized cochain

$$(11)\qquad \begin{aligned}(\delta f_n)(x_1, \cdots, x_{n+1}) = {} & (f_n(x_1, \cdots, x_n)x_{n+1})\cdot f_n(x_2, \cdots, x_{n+1})^{c(0)} \\ & \cdot \prod_{i=1}^{n} f_n(x_1, \cdots, x_{i-1}, x_ix_{i+1}, x_{i+2}, \cdots, x_{n+1})^{c(i)},\end{aligned}$$

where $c(j) = (-1)^{n+1+j}$ for $j = 0, 1, \cdots, n$. For $n > 0$, $\mathfrak{B}_n$ is the group of the n-coboundaries; $\mathfrak{B}_0$ consists of the 0-cochain $1_0 = 1$. An *n-cocycle* is an n-cochain f_n such that $\delta f_n = 1_{n+1}$ (the identity of $\mathfrak{C}_{n+1}$) and $\mathfrak{Z}_n$ 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 $\mathfrak{B}_n$ is a subgroup of $\mathfrak{Z}_n$. The nth cohomology group $\mathfrak{H}_n$ is defined by $\mathfrak{H}_n = \mathfrak{Z}_n/\mathfrak{B}_n$. The next theorem is due to Eilenberg and MacLane [2, 3]:

THEOREM 7. *If M is a group, the homomorphism $(E, \theta) \to F(A_3, E)$ induces the isomorphism $\mathfrak{H} \cong \mathfrak{H}_3$.*

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

$$(12) \qquad f_a(x, y, z) = F(A_3, E; x, y, z); \; f_m(x, y, z) = F(B_3, E; x, y, z).$$

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

$$(13) \quad (e_1e_2)e_3 = e_1(e_2e_3)f_a(x_1, x_2, x_3); \; e_1e_2 \cdot e_3e_1 = e_1(e_2e_3 \cdot e_1)f_m(x_1, x_2, x_3),$$

showing that f_a, f_m are normalized 3-cochains. If (E, θ) is central and if $u(x)$ is a normalized system of representatives of M in E, then $u(x)u(y) = u(xy)h(x, y)$ 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), $(e_1e_2 \cdot e_3)e_4 = (e_1e_2 \cdot e_3e_4) \cdot f_a(x_1x_2, x_3, x_4) = (e_1(e_2 \cdot e_3e_4))f_a(x_1, x_2, x_3x_4)f_a(x_1x_2, x_3, x_4)$ and also

$$\begin{aligned}(e_1e_2 \cdot e_3)e_4 &= ((e_1 \cdot e_2e_3)f_a(x_1, x_2, x_3))e_4 = (e_1 \cdot e_2e_3)e_4(f_a(x_1, x_2, x_3)x_4) \\ &= e_1(e_2e_3 \cdot e_4)f_a(x_1, x_2x_3, x_4)(f_a(x_1, x_2, x_3)x_4) \\ &= (e_1(e_2 \cdot e_3e_4))f_a(x_2, x_3, x_4)f_a(x_1, x_2x_3, x_4)(f_a(x_1, x_2, x_3)x_4),\end{aligned}$$

whence comparison gives $\delta f_a = 1_4$. Thus f_a is a 3-cocycle. It can be shown conversely that every 3-cocycle (3-coboundary) is an $F(A_3, E)$ (an $F(A_3, E)$ for E central).

Again, $e_1e_2 \cdot e_3e_1 = e_1(e_2 \cdot e_3e_1)f_a(x_1, x_2, x_3x_1)$ and $e_1(e_2e_3 \cdot e_1) = e_1(e_2 \cdot e_3e_1) f_a(x_1, x_2, x_3)$, whence, by (13),

$$(14) \qquad f_m(x, y, z) = f_a(x, y, zx)f_a(y, z, x)^{-1}.$$

The homomorphism ρ of $\mathfrak{Z}_3$ into $\mathfrak{C}_3$, defined by $(f_3\rho)(x, y, z) = f_3(x, y, zx) \cdot f_3(y, z, x)^{-1}$, induces a homomorphism of $\mathfrak{H}_3$ upon a group $\mathfrak{H}_3\rho = \mathfrak{Z}_3\rho/\mathfrak{B}_3\rho$. 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 $(E, \theta) \to F(B_3, E)$ induces an isomorphism $\mathfrak{H}_C \cong \mathfrak{H}_3\rho$.*

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* $\mathfrak{H}_2$.

5. **Grouplike extensions. Conjugate extensions.** A (G, M) extension (E, θ) is *grouplike* if, for every subgroup (=associative subloop) H of M, $H\theta^{-1}$ is a subgroup of E. Thus (E, θ) 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 p, q in E, we may define a new operation (o) on E by

$$e_1oe_2 = (e_1R_q^{-1})(e_2L_p^{-1}). \tag{15}$$

The elements of E form a loop E_o under (o); the unit is pq. E_o is (Albert [1]) a *(principal) isotope* of E. If, further, (E, θ) is a (G, M) extension, write $p\theta=u$, $q\theta=v$. Then, if M_o is the principal isotope of M defined by

$$xoy = (xR_v^{-1})(yL_u^{-1}), \tag{16}$$

we find from (15), (16), with $e_j\theta=x_j$, that $(e_1oe_2)\theta=x_1ox_2$.

For each a in the associator $A(M)$, and for each (G, M) extension (E, θ), 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_o given by (15). We define $(E, \theta)^a=(E^a, \theta)$ to be a *conjugate* of (E, θ).

THEOREM 9. *Let (E, θ) 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, θ) is a (G, M) extension*; (iii) *$E_1 \sim E_2$ implies $E_1^a \sim E_2^a$*; (iv) *$E_1 \sim^{-1} E_2$ implies $E_1^a \sim^{-1} E_2^a$*; (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_3, independent of the loop E, so that (15) becomes $e_1oe_2=e_1e_2\cdot W_3(e_1, e_2, p)$. If E is a group, (15) yields $e_1oe_2=(e_1q^{-1})(p^{-1}e_2)=e_1pp^{-1}e_2=e_1e_2$; thus W_3 is p.n.a. Since, in (16), $u=p\theta=a^{-1}$, $v=q\theta=a$, with a in $A(M)$, we have $xoy=xa^{-1}\cdot(a^{-1})^{-1}y=x(a^{-1}\cdot ay)=xy$. Hence $W_3(e_1, e_2, p)\theta =W_3(x_1, x_2, a^{-1})=1$. By Theorem 1, $W_3(e_1, e_2, p)$ lies in G and depends only on x_1, x_2, a.

(ii) Since $xoy=xy$, θ is a homomorphism of E^a upon M. The kernel of θ (in E^a) is the subloop K_o consisting of K under (o). Since $pq=1$ is the unit of E^a, $W_3(1, e, p)=1=W_3(e, 1, p)$ for all e in E^a. Hence, for k in K, $eok=ekW_3(e, k, p)=ekW_3(e, 1, p)=ek$ and $(e_1oe_2)ok =(e_1oe_2)k=e_1e_2W_3(e_1, e_2, p)k=e_1e_2kW_3(e_1, e_2, p)=e_1o(e_2k)=e_1o(e_2ok)$. Similarly $(e_1ok)oe_2=e_1(koe_2)$, $(koe_1)oe_2=ko(e_1oe_2)$, so that K_o is in

$A(E^a)$. The element c of K_o is in $Z(K_o)$ if and only if $cok=koc$, $ck=kc$, c is in $G=Z(K)$. If g_1, g_2 are in G, $g_1og_2=g_1g_2$; thus $G=Z(K_o)$. Finally, for g in G, e in E, $x=e\theta$, $goe=ge=e(gx)=eo(gx)$. This completes the proof that (E^a, θ) is a (G, M) extension.

(v) Assume $E^a=E_o$ is defined by (15), with $p\theta=a^{-1}$, $pq=1$. Then $(E^a)^b=E_o^b$ must be defined, with operation $(*)$, by $e_1*e_2=(e_1T)o(e_2S)=(e_1TR_q^{-1})(e_2SL_p^{-1})$, where $eS^{-1}=soe=(sR_q^{-1})(eL_p^{-1})$, $eT^{-1}=eot=(eR_q^{-1})(tL_p^{-1})$ for s, t in E such that $s\theta=b^{-1}$, $1=sot=(sR_q^{-1})(tL_p^{-1})$. The elements $f=sR_q^{-1}$, $h=tL_p^{-1}$ satisfy $f\theta=b^{-1}a^{-1}$, $fh=1$. Moreover, $SL_p^{-1}=L_f^{-1}$ and $TR_q^{-1}=R_h^{-1}$. Therefore $e_1*e_2=(e_1R_h^{-1})(e_2L_f^{-1})$, 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 $\mathfrak{C}_n$, $\mathfrak{B}_n$ of (normalized) n-cochains and n-coboundaries. By (11), the n-coboundaries for $n=2, 3$ are given by

$$(\delta f_1)(x, y) = (f_1(x)y)f_1(y)f_1(xy)^{-1}, \tag{17}$$

$$(\delta f_2)(x, y, z) = (f_2(x, y)z)f_2(y, z)^{-1}f_2(xy, z)f_2(x, yz)^{-1}. \tag{18}$$

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

$$(\delta^2 f_1)(x, y, z) = f_1(x\cdot yz)f_1(xy\cdot z)^{-1}. \tag{19}$$

DEFINITION 10. Let f, h be normalized 2-cochains of (G, M). Then f is equivalent to h if $f=h\cdot\delta c$ 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, θ) 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_o, θ_o) 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).* (ii) *$(G, M, f)\sim(G, M, h)$ if and only if $f\sim h$.* (iii) *$(G, M, f)\sim^{-1}(G, M, h)$ if and only if $f\sim h^{-1}$.* (iv) *$(G, M, f)\otimes(G, M, h)\sim(G, M, fh)$.* (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*

$$f^a(x, y) = f(x, y)\cdot(\delta f)(a^{-1}, a, y)\cdot((\delta f)(xa^{-1}, a, y))^{-1}. \tag{20}$$

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

PROOF. (i) Let (E, θ) 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, $x = e\theta$. 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, θ) and (G, M, f).

(v) In the notation of (i), consider the equality $u(x)u(y) \cdot u(z) = u(x) \cdot u(y)u(z)$.

(vi) In view of Theorem 9, E^a may be defined by $e_1 o e_2 = (e_1 R_q^{-1}) \cdot (e_2 L_p^{-1})$ where $p = u(a^{-1})$ and $q = u(a)f(a^{-1}, a)^{-1}$. Write $u(x)ou(y) = u(xy)h(x, y)$, so that $h = f^a$. Let $P = (u(xa^{-1})q)o(pu(ay))$. On the one hand, $P = (u(xa^{-1})R_q R_q^{-1})(u(ay)L_p L_p^{-1}) = u(xa^{-1})u(ay) = u(xa^{-1} \cdot ay)f(xa^{-1}, ay) = u(xy)f(xa^{-1}, ay)$. On the other hand, since $u(xa^{-1})q = u(xa^{-1}) \cdot u(a)f(a^{-1}, a)^{-1} = u(x)f(xa^{-1}, a)f(a^{-1}, a)^{-1}$, $pu(ay) = u(a^{-1}) \cdot u(ay) = u(y)f(a^{-1}, ay)$ and $(u(x)g)o(u(y)g') = u(xy)h(x, y)(gy)g'$, $P = u(xy)h(x, y)(f(xa^{-1}, a)y)(f(a^{-1}, a)y)^{-1}f(a^{-1}, ay)$. Comparison of the two expressions for P gives $h(x, y) = f(xa^{-1}, ay)(f(a^{-1}, a)y) \cdot (f(xa^{-1}, a)y)^{-1}f(a^{-1}, ay)^{-1}$. However, substitution from (18) in the right-hand side of (20) yields precisely this expression for $h = f^a$.

(ii), (iii), (iv). For $j = 1, 2$, denote the elements of $(E_j, \theta_j) = (G, M, f_j)$ by $(x, g)_j$, where $(x, g)_j\theta_j = x$. Set $u_j(x) = (x, 1)_j$. If π 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 $g\pi x = gx\pi$. Conversely, if π is any automorphism of G (such that $g\pi x = gx\pi$) and c any normalized 1-cochain, the definition $(x, g)_1\pi = (x, (g\pi)c(x))_2$ extends π 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 $g\pi = g$, $g\pi = g^{-1}$ respectively. 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 $(\delta^2 c)(xa^{-1}, a, y) = c(xa^{-1} \cdot ay)c(xy)^{-1} = 1$. Thus it is evident from (20) that *the cochain* $f^a f^{-1}$ *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) $x(y \cdot xz) = (xy \cdot x)z$ *for all* x, y, z *in* M. (iii) *Every loop* M_o *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:*

$$f(xy, zx)(f(x, y)zx)f(z, x) = f(x, yz\cdot x)f(yz, x)(f(y, z)x); \tag{21a}$$

$$f(x, y\cdot zx)\cdot(\delta f)(x, y, zx) = f(x, yz\cdot x)\cdot(\delta f)(y, z, x). \tag{21b}$$

(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*

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

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 $u(x)^{-1}u(x)\cdot u(y)=u(x)^{-1}\cdot u(x)u(y)$ reduces to $(\delta f)(x^{-1}, x, y)=1$. In particular, (20) becomes (22). Since $E^a\otimes E^{-1}\sim(G, M, f^af^{-1})$, (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, θ):* (i) *E^a is Moufang.* (ii) *$E^{mn}\sim E_0$.* (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:

$$c(x) = \prod_y f(x, y), \qquad d(x) = \prod_y f(y, x), \tag{23}$$

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

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

From (24),

$$h(x, yz) = (h(x, y)z)h(x, z). \tag{25}$$

This implies

$$h(w, xy\cdot z) = h(w, x\cdot yz), \tag{26}$$

since both sides reduce to $(h(w, x)yz)(h(w, y)z)h(w, z)$. If $f_1(x, y) = h(y, xy)^{-1}$, we take products in (21a) over all y, use (23), (24) and find $f(z, x)^m = (\delta d)(z, x)\cdot f_1(z, x)$, or

$$f^m \sim f_1, \qquad f_1(x, y) = h(y, xy)^{-1}. \tag{27}$$

If $gx = g$ 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

$$h(x, x) = 1, \qquad h(x, xy) = h(x, y), \qquad h(x, yx) = h(x, y)x. \tag{28}$$

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

$$h(xy, y) = h(x, y). \tag{29}$$

Returning to (21a), take products over all z, getting

$$\prod_z (f(x, y)z) = (c(y)x)c(x)c(xy)^{-1} = h(y, x)c(x)c(y)c(xy)^{-1}. \tag{30}$$

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),

$$h(y, xw)h(x, w) = h(y, x)h(xy, w). \tag{31}$$

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

$$h(x, yx) = h(x, y). \tag{32}$$

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

$$h(x, y)x = h(x, y)y = h(x, y). \tag{33}$$

From (29) with y replaced by $x^{-1}y$, $h(y, x^{-1}y) = h(x, x^{-1}y)$. By (32) and (28.2), this implies $h(y, x^{-1}) = h(x, y)$. Then, by (33), (25),

$h(x, y)h(y, x) = h(y, x^{-1})h(y, x) = (h(y, x^{-1})x)h(y, x) = h(y, x^{-1}x) = h(y, 1) = 1$, or

$$h(y, x)^{-1} = h(x, y). \tag{34}$$

Hence (32), (34) give $f_1(x, y) = h(y, xy)^{-1} = h(y, x)^{-1} = h(x, y)$, so

$$f_1 = h. \tag{35}$$

Since $h(x, y)y = h(x, y)$, a simple induction using (25) gives $h(x, y^j) = h(x, y)^j$. Combining this with (34),

$$h(x^i, y^j) = h(x, y)^{ij} \tag{36}$$

for all integers i, j. In particular, $f_1(x, y)^n = h(x, y)^n = h(x, y^n) = h(x, 1) = 1$, and so $f^{mn} \sim f_1^n = 1$. This proves Theorem 12 (ii).

If $p = \delta f_1 = \delta h$, (18) and (25) combine to give

$$h(xy, z) = h(x, z)h(y, z)p(x, y, z), \qquad p = \delta h. \tag{37}$$

Since h satisfies (21b), (26),

$$p(x, y, zx) = p(y, z, x). \tag{38}$$

Operating on (37) by w, and using (25), we find

$$p(x, y, zw) = (p(x, y, z)w)p(x, y, w). \tag{39}$$

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

$$p(x, y, z)w = p(x, y, z), \qquad w = x, y, z. \tag{40}$$

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

$$p(x, y, z) = p(y, z, x). \tag{41}$$

By (37), (24), and (25), $p(x, y, z) = h(z, x)h(z, y)h(z, xy)^{-1} = h(z, x) \cdot (h(z, x)y)^{-1}$. Therefore, by (41), (34),

$$p(x, y, z) = h(x, y)(h(x, y)z)^{-1} = p(y, x, z)^{-1}. \tag{42}$$

By this and (37),

$$h(xy, z)h(yx, z)^{-1} = p(x, y, z)^2. \tag{43}$$

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 $k = f^{2m}$ 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

$$q(x, y) = p(xa^{-1}, a, y)^{-2}. \tag{44}$$

Define the (normalized) 4-cochain r by

$$r(w, x, y, z) = (p(w, x, y)z)p(w, x, y)^{-1}. \tag{45}$$

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

$$p(w, x, yz) = p(w, x, y)p(w, x, z)r(w, x, y, z). \tag{46}$$

By (34), (26), $h(wx \cdot y, z) = h(w \cdot xy, z)$. Expand each side of this last equation by (38), in the form $h(w, z)h(x, z)h(y, z)$. Equate, and use (46) to get $r(y, z, w, x) = r(z, w, x, y)$, whence $r(z, w, y, x) = r(z, w, x, y)$ or

$$r(w, x, y, z) = r(w, x, z, y). \tag{47}$$

By (47) and skew-symmetry, $r(w, x, y, z) = r(w, x, z, y) = r(x, z, w, y) = r(x, z, y, w) = r(y, x, z, w) = r(y, x, w, z) = r(w, x, y, z)^{-1}$, or

$$r(w, x, y, z)^2 = 1. \tag{48}$$

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

$$q(x, y)^{-1} = p(x, y, a)^2 = h(x, y)^2(h(x, y)a)^{-2}. \tag{49}$$

Therefore, since $p = \delta h$, $(\delta q)(x, y, z)^{-1} = p(x, y, z)^2(p(x, y, z)a)^{-2}$. 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, θ) is a central associative (G, M) extension, $E^m \sim E_o$.*

Bibliography

A. A. Albert

1. *Quasigroups*. I, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 507–519.
2. *Quasigroups*. II, Trans. Amer. Math. Soc. vol. 55 (1944) pp. 401–419.

REINHOLD BAER

1. *Erweiterungen von Gruppen und ihren Isomorphismen*, Math. Zeit. vol. 38 (1934) pp. 375–416.
2. *Automorphismen von Erweiterungsgruppen*, Actualités Scientifiques et Industrielles, no. 205, Paris, 1935.
3. *Representations of groups as quotient groups*. II. *Minimal chains of a group*, Trans. Amer. Math. Soc. vol. 53 (1943) pp. 348–389.

GRACE E. BATES

1. *Free loops and nets and their generalizations*, Amer. J. Math. vol. 69 (1947) pp. 499–550.

R. H. BRUCK

1. *Contributions to the theory of loops*, Trans. Amer. Math. Soc. vol. 60 (1946) pp. 245–354.
2. *On a theorem of R. Moufang*. To appear in the Proceedings of the American Mathematical Society.

MAX DEURING

1. *Algebren*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 4, Chelsea, New York, 1948.

MARSHALL HALL

1. *Group rings and extensions*, I, Ann. of Math. vol. 39 (1938) pp. 220–234.

SAMUEL EILENBERG

1. *Topological methods in abstract algebra. Cohomology theory of groups*, Bull. Amer. Math. Soc. vol. 55 (1949) pp. 3–37.

SAMUEL EILENBERG AND SAUNDERS MACLANE

1. *Cohomology theory in abstract groups*, I, Ann. of Math. vol. 48 (1947) pp. 51–78.
2. *Cohomology theory in abstract groups*, II. *Group extensions with a non-abelian kernel*, Ann. of Math. vol. 48 (1947) pp. 326–341.
3. *Algebraic cohomology groups and loops*, Duke Math. J. vol. 14 (1947) pp. 435–463.

RUTH MOUFANG

1. *Zur Struktur von Alternativkörpern*, Math. Ann. vol. 110 (1935) pp. 416–430.

HANS ZASSENHAUS

1. *The theory of groups* (trans. by Saul Kravetz), New York, 1949.

UNIVERSITY OF WISCONSIN