PSEUDO-AUTOMORPHISMS AND MOUFANG LOOPS

R. H. BRUCK

1. **Introduction.** A *loop* G is a system with a binary operation $(\cdot)$ such that: (i) in the equation $xy=z$, any two of x, y, z uniquely determine the third; (ii) G has a unit 1. The concept of subloop should be clear. A permutation U of G will be called a *pseudo-automorphism* of G provided there exists at least one element u of G such that

$$(xy)U\cdot u = xU\cdot(yU\cdot u) \tag{1.1}$$

for all x, y of G. The element u will be called a *companion* of U. It is readily verified that the *pseudo-automorphisms of a loop G form a group under composition.* Indeed, U^{-1} has p as a companion, where $pU\cdot u=1$. And, if V has companion v, then VU has companion $vU\cdot u$.

A *Moufang* loop is one which satisfies the identity

$$xy\cdot zx = x(yz\cdot x). \tag{1.2}$$

An extensive study of Moufang loops is given in [2].[1] One defect of that study is that it assumes Moufang's associativity theorem [6], the only published proof of which involves a complicated induction. Using pseudo-automorphisms along with recent methods of Kleinfeld and the author [5], we shall give simple noninductive proofs of three associativity theorems, one of which (Theorem 5.1) generalizes that of Moufang. As shown in [3], still simpler proofs of Moufang's theorem are possible in the commutative case. And, indeed, the following corollary of Theorem 5.3 can be obtained directly from Lemmas 2.1, 2.2: *Every associative subset of a commutative Moufang loop G is contained in an associative subloop of G.*

The present methods represent a considerable improvement over those of [2] (in particular, pseudo-automorphisms have displaced the cumbersome *autotopisms*) and the paper should serve as an introduction to the theory of Moufang loops. There is little overlapping, except possibly in §2, but we have added (Theorem 4.1) a more aesthetic proof of the fact that the *nucleus* (previously called the *associator*) of a Moufang loop is a normal subloop.

2. **Elementary properties.** Henceforth let G be a Moufang loop. From (1.2) with $z=1$,

Received by the editors July 18, 1950 and, in revised form, May 18, 1951.

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

$$(2.1) \qquad xy\cdot x = x\cdot yx.$$

Defining the inverse x^{-1} of x by $xx^{-1}=1$, we set $y=x^{-1}$ in (2.1) and find $x=x\cdot x^{-1}x$, $1=x^{-1}x$. Thus, also, $(x^{-1})^{-1}=x$. Setting $z=x^{-1}$ in (1.2), we have $xy=x(yx^{-1}\cdot x)$, $yx^{-1}\cdot x=y$. Again, from (1.2), (2.1), $zx=xx^{-1}\cdot zx=(x\cdot x^{-1}z)x$, $z=x\cdot x^{-1}z$. Therefore

$$(2.2) \qquad x^{-1}\cdot xy = y = yx\cdot x^{-1}.$$

If $z=xy$, then, by (2.2), $zy^{-1}=x$, $z^{-1}x=y^{-1}$, $y^{-1}x^{-1}=z^{-1}$; thus

$$(2.3) \qquad (xy)^{-1} = y^{-1}x^{-1}.$$

Setting $y=pz^{-1}$ in (1.2), and using (2.2), (2.1), we get $(x\cdot pz^{-1})(zx)=xp\cdot x$, whence, by (2.2), (2.3), $x\cdot pz^{-1}=(xp\cdot x)(x^{-1}z^{-1})$. From this, with $z^{-1}=xq$, $x(p\cdot xq)=(xp\cdot x)q$. Therefore, in view of (2.3), we have the Moufang identities,

$$(2.4) \qquad x(y\cdot xz) = (xy\cdot x)z, \qquad (zx\cdot y)x = z(x\cdot yx).$$

As Bol [1] was first to show, each of the identities (2.4) implies (1.2).

For each a of G, define permutations $L(a)$, $R(a)$ of G by $xL(a)=ax$, $xR(a)=xa$. In view of (2.2),

$$(2.5) \qquad L(x)^{-1} = L(x^{-1}), \qquad R(x)^{-1} = R(x^{-1}).$$

In this notation, (1.2) becomes

$$(2.6) \qquad yL(x)\cdot zR(x) = (yz)R(x)L(x).$$

Again, setting $x=p^{-1}$, $y=q^{-1}$, $z=qr$ in (1.2), we have $(p^{-1}q^{-1})(qr\cdot p^{-1})=p^{-1}\cdot rp^{-1}$ and hence $(qp)(p^{-1}\cdot rp^{-1})=qr\cdot p^{-1}$. Equivalently,

$$(2.7) \qquad yR(x)\cdot zR(x^{-1})L(x^{-1}) = (yz)R(x^{-1}).$$

Let $\mathfrak{G}$ be the permutation group generated by all the $L(x)$, $R(x)$, and let $\mathfrak{I}$ be the subgroup consisting of those U of $\mathfrak{G}$ such that $1U=1$. An element of $\mathfrak{I}$ is known as an *inner mapping* of the loop G. We are ready to prove a basic lemma.

LEMMA 2.1. *Every inner mapping of a Moufang loop G is a pseudo-automorphism of G.*

PROOF. In view of (2.5), every element U of $\mathfrak{G}$ has the form $U=U_1U_2\cdots U_n$ where $U_i=L(a_i)$ or $R(a_i)$ for an element a_i of G. We see from (2.6), (2.7) that for each i there exist elements V_i, W_i of $\mathfrak{G}$ such that $xU_i\cdot yV_i=(xy)W_i$ for all x, y of G. Thus, if $V=V_1V_2\cdots V_n$, $W=W_1W_2\cdots W_n$,

$$(2.8) \qquad xU\cdot yV = (xy)W$$

for all x, y of G. If U is in $\mathfrak{J}$, $1U=1$, so that (2.8) with $x=1$ gives $V=W$. Now set $u=1V$. Then (2.8) with $y=1$ gives $xU\cdot u=xW$, so that (2.8) becomes (1.1). We shall use this proof as a method of computing a companion of an inner mapping.

A better result holds for commutative Moufang loops:

LEMMA 2.2. *Every pseudo-automorphism of a commutative Moufang loop G is an automorphism of G.*

PROOF. If G is commutative, interchange of x and y in (1.1) gives $xU\cdot(yU\cdot u)=yU\cdot(xU\cdot u)$. Setting $xU=p$, $yU=qu^{-1}$ in this, we get $pq=(qu^{-1})(pu)=pu\cdot qu^{-1}$, whence, by (2.4), $pq\cdot u=(pu\cdot qu^{-1})u=p\cdot uq=p\cdot qu$ for all p, q, of G. Therefore (1.1) yields $(xy)U\cdot u=(xU\cdot yU)u$, $(xy)U=xU\cdot yU$.

If $h(x_1, \cdots, x_n)$ is a single-valued function from G to G, and if A_i $(i=1, \cdots, n)$ are subsets of G, $h(A_1, \cdots, A_n)$ denotes the set of all elements $h(a_1, \cdots, a_n)$ with a_i in A_i. Subsets consisting of one element will usually be denoted by that element. Note the meanings of A^{-1}, A^2, AA.

3. **Invariant elements of pseudo-automorphisms.** In (1.1) set $x=y=1$ and get $1U\cdot u=1U\cdot(1U\cdot u)$, $1=1U$. Then set $y=x^{-1}$ and get $u=xU\cdot(x^{-1}U\cdot u)$,

$$1U = 1, \qquad x^{-1}U = (xU)^{-1}. \tag{3.1}$$

Next replace y in (1.1) by yx and use (2.1), (1.1), (2.4) to get $(xyx)U\cdot u=xU\cdot((yx)U\cdot u)=xU\cdot(yU\cdot(xU\cdot u))=(xU\cdot yU\cdot xU)u$,

$$(xyx)U = xU\cdot yU\cdot xU. \tag{3.2}$$

The identity (3.2) states that *every pseudo-automorphism of a Moufang loop G is a semi-automorphism of G.* And it is easily seen that (3.2) implies (3.1). In the following theorem, we could use semi-automorphisms, but pseudo-automorphisms seem more natural.

THEOREM 3.1. *Let $\mathfrak{S}$ be any set of pseudo-automorphisms of a Moufang loop G. Let $F=F(\mathfrak{S})$ be the set of all x of G left fixed by $\mathfrak{S}$, and let $M=M(\mathfrak{S})$ be the set of all m of G such that $mF\subset F$. Then*: (i) 1 *is in F*; (ii) $F^{-1}=F$ *and* $xFx=F$ *for x in F*; (iii) M *is a subset of F and a subloop of G*; (iv) $mF=F=Fm$ *for every m of M.*

COROLLARY. *If G is also commutative, $M=F$.*

PROOF. (i), (ii) reflect (3.1), (3.2). By (i), F contains $M\cdot 1=M$. If m is in M, x in F, $x^{-1}m^{-1}=(mx)^{-1}$ is in $F^{-1}=F$, and thus $m^{-1}x=x(x^{-1}m^{-1})x$ is in $xFx=F$. Hence $M^{-1}=M$. Moreover, $F=m\cdot m^{-1}F$

$\subset mF \subset F$, so that $mF = F$, and, similarly, $Fm = F$. If also m' is in M, $mm' \cdot x = (mm')(xm^{-1} \cdot m) = m(m' \cdot xm^{-1})m$ is in $mFm = F$. Hence $MM \subset M$. This is enough to show that M is a subloop of G. If G is commutative, Lemma 2.2 shows that $FF \subset F$, $M = F$, proving the corollary.

4. **Some basic lemmas.** The *commutator* (x, y) and *associator* (x, y, z) of a loop G are defined by

$$xy = (yx)(x, y), \qquad xy \cdot z = (x \cdot yz)(x, y, z). \tag{4.1}$$

LEMMA 4.1. *In a Moufang loop G, the equation $(a, b, c) = 1$ implies all of the equations obtained by permuting the elements a, b, c and replacing any of these elements by their inverses.*

PROOF (cf. [6]). We give a proof which illustrates the use of Theorem 3.1. Assume that

$$(a, b, c) = 1, \qquad ab \cdot c = a \cdot bc. \tag{4.2}$$

Clearly (4.2) can be written in the form $aU = a$ where $U = R(b)R(c)R(bc)^{-1}$, $1U = 1$. By Lemma 2.1, U is a pseudo-automorphism. Thus, by Theorem 3.1 (ii), (4.2) implies $(a^{-1}, b, c) = 1$. Similarly, (4.2) implies $(a, b^{-1}, c) = (a, b, c^{-1}) = 1$. Also (4.2) implies $c^{-1} \cdot b^{-1}a^{-1} = c^{-1}b^{-1} \cdot a^{-1}$ and hence $(c^{-1}, b^{-1}, a^{-1}) = 1 = (c, b, a)$. Next, from $(a^{-1}, b, c) = 1$, we get $a^{-1}b \cdot c = a^{-1} \cdot bc$, $bc \cdot a = a(a^{-1} \cdot bc)a = a(a^{-1}b \cdot c)a = b \cdot ca$, $(b, c, a) = 1$. This completes the proof.

LEMMA 4.2. *Let a, b, c, d be elements of a Moufang loop G, each three of which associate (satisfy $(x, y, z) = 1$). Then the following equations are equivalent*: (i) $(a, b, cd) = 1$; (ii) $(c, d, (a, b)) = 1$; (iii) $(c, d, (ab)^2) = 1$; (iv) $(c, d, ab) = 1$; (v) $(d, a, bc) = 1$. *Hence* (i) *is equivalent to each of the equations obtained by permuting the elements a, b, c, d and replacing any of these elements by their inverses.*

PROOF (cf. [5, Lemma 2.1]). By Lemma 4.1, the equation $(a, b, x) = 1$ is equivalent to $(b^{-1}, a^{-1}, x) = 1$. The latter may be written as $xU = x$ where $U = L(a^{-1})L(b^{-1})L(ab)$. Using the proof of Lemma 2.1, we see that U has companion $u = 1R(a^{-1})R(b^{-1})R(ab) = (a, b)$. Then $ab = ba \cdot u$, $aba = (ba \cdot u)a = b(aua)$. Therefore $b(aua)b = aba \cdot b = (ab \cdot a)(a^{-1} \cdot ab) = (ab)(aa^{-1})(ab)$,

$$b(aua)b = (ab)^2. \tag{4.3}$$

Now (i) is equivalent to $cd \cdot u = (cd)U \cdot u = cU \cdot (dU \cdot u) = c \cdot du$, $(c, d, u) = 1$, or (ii). Since $(c, d, x) = 1$ is equivalent to $xV = x$ for an inner mapping V, (4.3) and Theorem 3.1 (ii) show that (ii) is equivalent to

(iii). Hence (i) is equivalent to (iii). Similarly (iv) is equivalent to $(a, b, (cd)^2) = 1$. However, since $x \cdot 1 \cdot x = x^2$, (i) implies $(a, b, (cd)^2) = 1$ and (iv). Conversely (iv) implies (i); together they imply $(a \cdot bc)d = (ab \cdot c)d = ab \cdot cd = a(b \cdot cd) = a(bc \cdot d)$, $(a, bc, d) = 1$, or, (v). And if (i) implies (v), then, equally, (v) implies (i). This, together with Lemma 4.1, suffices for the proof of Lemma 4.2.

If A is any subset of a Moufang loop G, we define the *adjoint* A' *of* A *in* G as the set of all c in G such that $(A, c, G) = 1$. We define the *closure* A^* *of* A *in* G by $A^* = (A')'$. In view of Lemma 4.1, the closure has the usual properties: (i) $A \subset A^*$; (ii) $A^{**} = A^*$; (iii) if $A \subset B$, $A^* \subset B^*$.

LEMMA 4.3. *The adjoint* A' *and closure* A^* *of a subset* A *of a Moufang loop* G *are subloops of* G, *and* $A \subset A^*$. *Moreover,* $(A, A, G) = 1$ *implies* $(A^*, A^*, G) = 1$.

PROOF (cf. [8]). Let $B = A'$. By Theorem 3.1, $B^{-1} \subset B$. For a in A, b, b' in B, x in G, we have, by three uses of the definition and two uses of (2.4), $((a \cdot b'b)x)b = ((ab' \cdot b)x)b = (ab')(bxb) = a(b' \cdot bxb) = a((b'b \cdot x)b) = (a(b'b \cdot x))b$. Therefore $(a \cdot b'b)x = a(b'b \cdot x)$, $(A, BB, G) = 1$, $BB \subset B$. Hence B is a subloop. Since $A^* = B'$, A^* is also a subloop. If $(A, A, G) = 1$, then $A \subset A'$. Hence $(A, A^*, G) = 1$, $A^* \subset A'$. Thus, finally, $(A^*, A^*, G) = 1$.

The *nucleus* N of a Moufang loop G is the set of all n of G such that $(n, G, G) = 1$. (In [2, 4] and elsewhere, N is called the *associator*.)

THEOREM 4.1. *If* G *is a Moufang loop with nucleus* N, *every pseudo-automorphism of* G *induces an automorphism of* N. *In particular,* N *is a characteristic normal subloop of* G.

PROOF (cf. [2]). Since $N = G'$, N is a subloop. If n is in N, and U is any pseudo-automorphism, let $a = nU$, $V = U^{-1}$. Then $(ax)V \cdot v = n \cdot (xV \cdot v) = (n \cdot xV)v$ or $(ax)V = n \cdot xV$ for every x of G. Hence $(ax \cdot y)V \cdot v = (ax)V \cdot (yV \cdot v) = (n \cdot xV)(yV \cdot v) = n(xV \cdot (yV \cdot v)) = n \cdot ((xy)V \cdot v) = (n \cdot (xy)V)v = (a \cdot xy)V \cdot v$, $ax \cdot y = a \cdot xy$, $a \in N$, $NU \subset N$. Then $N = (NV)U \subset NU \subset N$, $NU = N$. And, for n, n' in N, $(nU \cdot n'U)V = n \cdot n'UV = nn'$, or $nU \cdot n'U = (nn')U$. This proves the first sentence. Since $N\mathfrak{I} = N$, N is normal. (See Lemma 2.1 and the theory of normality in [2].) And since automorphisms are pseudo-automorphisms, N is characteristic.

5. **Associativity theorems.** In view of (2.1) and Lemma 4.1, we have $(x, x, G) = 1$ for every element x of the Moufang loop G.

THEOREM 5.1. *Let* A, B, C *be subsets of a Moufang loop* G *such that*

$(A, A, G)=(B, B, G)=(C, C, G)=(A, B, C)=1$. *Then the subset* $D=A\cup B\cup C$ *is contained in an associative subloop* H *of* G.

COROLLARY. *Any two elements* a, b *of a Moufang loop* G *(or any three elements* a, b, c *such that* $ab\cdot c=a\cdot bc$*) are contained in an associative subloop of* G.

PROOF (cf. [3, 5, 6, 7, 8]). Let F be the set of all elements x in G such that $(D, D, x)=(AB, C, x)=1$, and let M be the set of all m in G such that $mF\subset F$. By Theorem 3.1, M is a subloop of G such that $(D, D, M)=1$. In view of Lemmas 4.1, 4.2, A, B, and C play symmetrical rôles in the definition of F. We now use Lemma 4.2 four times along with Lemma 4.1. Since $(A, A, D)=(A, A, F)=(A, A, DF)=1$, then also $(AA, D, F)=(AD, A, F)=(DA, A, F)=1$. From this, and by symmetry, $(DD, D, F)=1$, and hence $(DD, A, F)=1$. Since $(D, D, D)=(D, D, F)=(DD, D, F)=1$, then $(D, D, DF)=1$. In particular, $(D, D, AF)=(D, A, AF)=1$. Since $(A, A, DD)=(A, A, F)=(DD, A, F)=(A, A, DD, F)=1$, also $(DD, A, AF)=1$. And, since $(D, D, A)=(D, D, AF)=(D, A, AF)=(DD, A, AF)=1$, then $(AD, D, AF)=1$. In particular, $(AB, C, AF)=1$. Thus $(D, D, AF)=(AB, C, AF)=1$, $A\subset M$. By symmetry, $D\subset M$, and we may take H to be the closure of D in M. For the corollary, set $A=a$, $B=C=b$ or $A=a$, $B=b$, $C=c$ according to the case.

A subset A of the Moufang loop G is called *associative* if $(A, A, A)=1$. An associative subset (subloop) A is called a *maximal* associative subset (subloop) provided A is contained in no associative subset (subloop) of G distinct from A. On the basis of Zorn's Lemma, it is clear that every associative subset (subloop) is contained in at least one maximal associative subset (subloop).

THEOREM 5.2. *Let* A *be an associative subloop of a Moufang loop* G*, and let* B *be a subset of* G *such that* $(A, A, B)=(B, B, G)=1$. *Then the subset* $D=A\cup B$ *is contained in an associative subloop* H *of* G.

COROLLARY. *Every maximal associative subloop of a Moufang loop* G *is a maximal associative subset of* G.

PROOF (cf. [5]). Let F be the set of all x in G such that $(D, D, x)=1$, and let M be the set of all m in G such that $mF\subset F$. By Theorem 3.1, M is a subloop of G such that $(D, D, M)=1$. Since $AA=A$, $(A, A, D)=(A, A, F)=(A, D, F)=(AA, D, F)=1$, and hence $(A, D, AF)=(A, A, DF)=1$. Since $(B, B, AF)=1$, we have $(D, D, AF)=1$, $A\subset M$. Since $(B, B, D)=(B, B, F)=(B, D, F)=(B, B, DF)=1$, then $(B, D, BF)=1$. Since $(A, A, DF)=1$, then $(A, A, BF)=1$. Therefore

$(D, D, BF) = 1$, $B \subset M$. Hence $D \subset M$, and we may take H to be the closure of D in M. If A is a maximal associative subloop, the relations $A \subset D \subset H$ imply $D = A$, $B \subset A$; the case $B = b$ shows that A is a maximal associative subset.

THEOREM 5.3. *Let G be a Moufang loop such that $(G, G, (G, G)) = 1$. Then every maximal associative subset A of G is a maximal associative subloop of G.*

REMARK. If G has nucleus N, the condition $(G, G, (G, G)) = 1$ means that $(G, G) \subset N$, or that the quotient loop G/N is commutative. As M. F. Smiley has pointed out (private communication), there exist Moufang loops G for which the conclusion of Theorem 5.3 is false.

PROOF (cf. [3, 5]). By Lemma 4.2, for a, b, c, d in A, the valid equation $(c, d, (a, b)) = 1$ implies $(a, b, cd) = 1$. Hence $(A, A, AA) = 1$. Thus, for x in AA, $A \cup x$ is an associative subset, $x \in A$, $AA \subset A$. Similarly, by Theorem 4.1, $A^{-1} = A$. This completes the proof.

BIBLIOGRAPHY

1. G. Bol, *Geweben und Gruppen*, Math. Ann. vol. 114 (1937) pp. 414–431.

2. R. H. Bruck, *Contributions to the theory of loops*, Trans. Amer. Math. Soc. vol. 60 (1946) pp. 245–354.

3. ———, *On a theorem of R. Moufang*, Proceedings of the American Mathematical Society vol. 2 (1951) pp. 144–145.

4. ———, *An extension theory for a certain class of loops*, Bull. Amer. Math. Soc. vol. 57 (1951) pp. 11–26.

5. R. H. Bruck and Erwin Kleinfeld, *The structure of alternative division rings*, Proceedings of the American Mathematical Society vol. 2 (1951) pp. 878–890.

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

7. M. F. Smiley, *The radical of an alternative ring*, Ann. of Math. vol. 49 (1948) pp. 702–709.

8. Max Zorn, *Theorie der alternativen Ringe*, Abh. Math. Sem. Hamburgischen Univ. vol. 8 (1931) pp. 123–147.

UNIVERSITY OF WISCONSIN