IS A SEMIDIRECT PRODUCT OF GROUPS NECESSARILY A GROUP?

GARY F. BIRKENMEIER, C. BRAD DAVIS, KEVIN J. REEVES, AND SIHAI XIAO

(Communicated by Ronald M. Solomon)

ABSTRACT. The aim of this paper is to provide nonassociative commutative loops which are semidirect products of subgroups.

INTRODUCTION

It is well known that a direct product of groups is a group. Furthermore one may informally view a loop as a “nonassociative group”. Since semidirect products share many properties with direct products one can naturally ask, “if a loop is a semidirect product of *subgroups* must it necessarily be a group?” The answer to this question is provided by one of the main results of [5, Theorem 1] in which Chein provides a construction of a nonassociative Moufang loop which is a semidirect product of a nonabelian subgroup by a subgroup of order two. Thus the notion of semidirect product is not strong enough to force a loop to be a group even when the factors of the product are groups. However the fact that a *commutative* group which is a semidirect product of subgroups must be a direct product of these subgroups motivates a more intriguing question: if a *commutative* loop is a semidirect product of subgroups must it necessarily be a group?

In this paper we produce construction methods, different from Chein’s method, which yield nonassociative commutative loops which are semidirect products of subgroups and which have a unique factorization property. In fact, in our constructions if the loop is Moufang then it must be a group.

Definitions and notation. Recall that a *groupoid* is a nonempty set with a binary operation; a *quasigroup* is a groupoid, $(Q, \cdot)$, in which the equations $ax = b$ and $ya = b$ are uniquely solvable for all $a, b \in Q$; and a *loop* is a quasigroup with a unity element. Throughout this note $(L, \cdot)$ will denote a loop with unity 1. If $a \in L$, then a^{-1} denotes the unique element of L (if it exists) such that $aa^{-1} = 1 = a^{-1}a$, and $U(L)$ will be the set of invertible elements of $(L, \cdot)$. The *left*, *right*, and *middle* nuclei of L will be symbolized by $N_l(L)$, $N_r(L)$, and $N_m(L)$, respectively (Note: $N_l(L) = \{a \in L | a(xy) = (ax)y \text{ for}$

Received by the editors October 24, 1991.

1991 *Mathematics Subject Classification.* Primary 20N05; Secondary 20E22.

Key words and phrases. Loop, group, semidirect product, nucleus, field.

all $x, y \in L$ and similarly for $N_r(L)$ and $N_m(L)$ [4]. From [4, p. 57], $N_l(L)$, $N_r(L)$, and $N_m(L)$ are subgroups of $(L, \cdot)$. A subloop H of a loop $(L, \cdot)$ is a *normal* subloop of $(L, \cdot)$ if and only if H is the kernel of some homomorphism of $(L, \cdot)$ into a loop.

Definition. A loop $(L, \cdot)$ is a *semidirect product* of H by K if H and K are subloops of $(L, \cdot)$ such that: (i) H is a normal subloop of $(L, \cdot)$; (ii) $L = HK$; and (iii) $H \cap K = \{1\}$.

The set $E(G)$ in the following definition has several properties which are important in our constructions.

Definition. Let $(G, \cdot)$ be a groupoid and $c \in G$. We say c has the *left [right] inverse property* if there exists at least one $d \in G$ such that $d(cx) = x$ [$(xc)d = x$] for all $x \in G$. We say that c has the *inverse property* if it has both the left and right inverse properties. Define $E(G)$ to be the set of all elements of G which have the inverse property.

For a loop $(L, \cdot)$, $E(L)$ satisfies the following basic conditions:

- (i) $E(L) = \{a \in U(L) | ax = b \Rightarrow x = a^{-1}b \text{ and } ya = b \Rightarrow y = ba^{-1} \text{ for all } b \in L\}$;
- (ii) if $a \in E(L)$, then $a^{-1} \in E(L)$;
- (iii) if $(L, \cdot)$ and $(K, *)$ are loops and $h: L \rightarrow K$ is an epimorphism, then $h(E(L)) \subseteq E(K)$;
- (iv) if $E(L)$ is a subgroupoid of $(L, \cdot)$, then $E(L)$ is a subloop and $x, y \in E(L)$ implies $(xy)^{-1} = y^{-1}x^{-1}$.

In general $E(L)$ may not be a subloop of $(L, \cdot)$; however, there are a large number of loops for which $E(L) = L$ (e.g., Moufang loops [2, p. 293] and totally symmetric loops [3, p. 74]).

CONSTRUCTIONS

Henceforth, $(F, +, \cdot)$ denotes a field of characteristic not two, $F^\# = F - \{0\}$, and $W = \{(a, c, x) | a, c, x \in F\}$. Define a binary operation $*$ on W by

$$(a, c, x) * (b, d, y) = (ab, cd, 2^{-1}[(a+c)y + (b+d)x]).$$

In each of the following constructions, a routine calculation shows that $(L, *)$ is a loop.

Construction 1. Let $(F, +, \cdot)$ be a field such that $a^2 + 1 \neq 0$ for all $a \in F$. Take $L = \{(a, a^{-1}, x) | a \in F^\# \text{ and } x \in F\}$. Specific examples of such fields are:

- (i) any ordered field (i.e., any formally real field) [6, 7];
- (ii) any Galois field of order p (prime), where $(p-1)/2$ is odd [8, p. 64].

Furthermore it can be shown that if $(F, +, \cdot)$ is an arbitrary field (of characteristic not two), then $(\{(a, a^{-1}, x) | a \in F^\# \text{ and } x \in F\}, *)$ is a loop if and only if $a^2 + 1 \neq 0$ for all $a \in F$.

Construction 2. Let $(F, +, \cdot)$ be a field with $(H, \cdot)$ a subgroup of $(F^\#, \cdot)$ such that $-1 \notin H$. Take $L = \{(a, c, x) | a, c \in H \text{ and } x \in F\}$. Specific examples of such fields and the appropriate subgroups are:

- (i) any ordered field, where H is the set of “positive” elements;

- (ii) any Galois field of order p (prime), where $(p-1)/2$ is odd, and let $(H, \cdot)$ be the subgroup generated by an element of order $(p-1)/2$ in $(F^\#, \cdot)$;
- (iii) the field of complex numbers where $H = \{r(\cos(2\pi n/k) + i \sin(2\pi n/k)) \mid r \text{ is a positive real number, } n \text{ is an integer, and } k \text{ is a fixed odd integer}\}$.

Construction 3. Let $(F, +, \cdot)$ be any ordered field. Take $L = \{(a, c, x) \mid ac > 0 \text{ and } x \in F\}$.

The loop $(L, *)$ in all the above constructions has the following properties:

- (i) $*$ is a commutative binary operation. Hence $L = U(L)$ and $N_l(L) = N_r(L)$.
- (ii) $\{(1, 1, 0)\} \subset N_m(L) = E(L) = \{(a, c, x) \in L \mid a = c\}$, where $(1, 1, 0)$ is the unity of $(L, *)$.
- (iii) $(L, *)$ is a group if and only if $E(L) = L$ if and only if $N_l(L) = N_m(L)$. Hence $(L, *)$ is a Moufang loop if and only if it is a group.

(a) In Construction 1, $(L, *)$ is a group if and only if $(F, +, \cdot)$ is the Galois field of order three.

(b) In Construction 2, $(L, *)$ is a group if and only if $H = \{1\}$.

(c) In Construction 3, $(L, *)$ is never a group.

(iv) $L = E(L) * S = G * S$, where $S = \{(a, c, x) \in L \mid x = 0\}$ and $G = \{(a, c, x) \in L \mid a = 1 = c\}$. Observe that $(S, *)$, $(E(L), *)$, and $(G, *)$ are subgroups of $(L, *)$ with $(G, *)$ isomorphic to $(F, +)$. Also $S \cap G = \{(1, 1, 0)\}$, and the function $h: L \rightarrow S$ defined by $h((a, c, x)) = (a, c, 0)$ is a homomorphism from $(L, *)$ onto $(S, *)$ with $G = \ker h$. Hence G is a normal subgroup of $(L, *)$. Therefore $(L, *)$ is a semidirect product of $(G, *)$ by $(S, *)$.

(v) Each element of L may be uniquely expressed in the form $g * s$, where $g \in G$ and $s \in S$.

(vi) In Construction 1, $(L, *)$ completely assimilates the field operations in that $(S, *)$ and $(G, *)$ are isomorphic to $(F^\#, \cdot)$ and $(F, +)$, respectively.

For a more concrete realization of $(W, *)$ observe that $(W, *)$ is isomorphic to $(T, \odot)$, where T is the set of two-by-two upper triangular matrices over F and $\odot$ is the "Jordan Product" defined by

$$A \odot B = 2^{-1}[A \cdot B + B \cdot A],$$

with $+$ and $\cdot$ denoting the usual matrix operations [1].

REFERENCES

1. A. A. Albert, *On Jordan algebras of linear transformations*, Trans. Amer. Math. Soc. **59** (1946), 524–555.
2. R. H. Bruck, *Contributions of the theory of loops*, Trans. Amer. Math. Soc. **60** (1946), 245–354.
3. —, *What is a loop?* (A. A. Albert, ed.) MAA Stud. Math., vol. 2, Math. Assoc. Amer., Washington, DC, 1963.
4. —, *A survey of binary systems*, third printing, Springer-Verlag, New York, 1971.
5. O. Chein, *Moufang loops of small order. I*, Trans. Amer. Math. Soc. **188** (1974), 31–51.
6. N. Jacobson, *Basic algebra. I*, Freeman, San Francisco, CA, 1974.

7. ———, *Basic algebra*. II, Freeman, San Francisco, CA, 1980.
8. I. Niven and H. S. Zuckerman, *An introduction to the theory of numbers*, second printing, Wiley, New York, 1962.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHWESTERN LOUISIANA, LAFAYETTE,
LOUISIANA 70504