COMMUNICATIONS IN ALGEBRA, 23(11), 4245–4255 (1995)

SPLIT EXTENSIONS AND REPRESENTATIONS OF MOUFANG LOOPS

A. DHARWADKER
DEPARTMENT OF MATHEMATICS, STATISTICS AND
COMPUTER SCIENCE, MARQUETTE UNIVERSITY
MILWAUKEE, WISCONSIN 53233, U.S.A.

AND

J.D.H. SMITH
DEPARTMENT OF MATHEMATICS
IOWA STATE UNIVERSITY
AMES, IOWA 50011, U.S.A.

I. Introduction.

In a recent paper [Lo], Loginov introduced a concept of linear representation for Moufang loops, based on an idea of Eilenberg [Ei] generalizing the concept of the split extension of a group module by the group. Earlier [S1] [S2], a concept of representation in a variety of quasigroups had been introduced, both abstractly as a module object in a comma category and concretely as a module for a certain ring associated with a quasigroup in the given variety. The current paper is concerned with investigating the relationship between these two approaches to a representation theory for Moufang loops. In the process, the general theory of representations in a variety of quasigroups is specialized explicitly to the case of Moufang loops for the first time. Elementary definitions are given in the second section. The third and fourth sections present a quick summary of representation theory in varieties of quasigroups (referring to [S1] for fuller details). However, the fourth section is of interest for exhibiting the linearization process of [S1] as a form of differentiation (cf. [Fo]) explicitly introducing notation from the differential calculus. The fifth section applies the general theory to the variety of Moufang loops. In the sixth section, it is shown that modules in the Eilenberg-Loginov sense fall within the framework of the representation theory in varieties. On the other hand, the seventh section gives an important example of a representation in the variety of Moufang loops, namely the Zassenhaus-Bruck construction of a free commutative Moufang loop on three generators, that cannot be described as an Eilenberg-Loginov module. One may summarize by saying that, while Eilenberg-Loginov split extensions and representations are equivalent for groups, they are no longer equivalent for Moufang loops.

2. Elementary definitions.

A *quasigroup* $(Q, \cdot)$ is a set Q together with a binary operation of *multiplication* on Q, denoted by $\cdot$ or juxtaposition (with the latter binding more strongly than infix operators like $\cdot$), such that in the equation $x \cdot y = z$, knowledge of any two of x, y, z specifies the third uniquely. Thus for an element y of Q, the *right multiplication*

$$R(y) : Q \to Q; x \mapsto xy \tag{2.1}$$

and *left multiplication*

$$L(y) : Q \to Q; x \mapsto yx \tag{2.2}$$

are bijections of Q. The subgroup of the permutation group $Q!$ generated by $\{R(y),\ L(y) | y \in Q\}$ is called the (*combinatorial*) *multiplication group* $MltQ$ of Q. For universal algebraic purposes, it is better to define a quasigroup in terms of identities. Introducing *right division*

$$/ : Q \times Q \to Q : (x, y) \mapsto xR(y)^{-1} \tag{2.3}$$

and *left division*

$$\backslash : Q \times Q \to Q : (x, y) \mapsto yL(x)^{-1}, \tag{2.4}$$

the identities

$$\begin{cases} (ER) & (x/y) \cdot y = x; \\ (UR) & (x \cdot y)/y = x; \\ (EL) & y \cdot (y \backslash x) = x; \\ (UL) & y \backslash (y \cdot x) = x \end{cases} \tag{2.5}$$

are satisfied by a quasigroup $(Q, \cdot, /, \backslash)$. Conversely [S1, 117], an algebra $(Q, \cdot, /, \backslash)$ with three binary operations satisfying (2.5) is a quasigroup $(Q, \cdot)$. A *loop* is a quasigroup Q satisfying the identity

$$x/x = y \backslash y. \tag{2.6}$$

If a loop Q is non-empty, then its *identity element* $e = x/x = y \backslash y$ for any x, y in Q satisfies

$ex = x = xe$. A loop Q is a *Moufang loop* if it satisfies the *Moufang identity*

$$x_1 x_2 \cdot x_3 x_1 = x_1(x_2 x_3 \cdot x_1). \tag{2.7}$$

Groups are Moufang loops. Examples of non-associative Moufang loops are furnished by the loops of invertible elements of the Cayley numbers over various fields, and by free commutative Moufang loops on three or more generators (cf. Section 7 below). Recall Moufang's Theorem [B2, VII. 4] that Moufang loops are *diassociative* – the subloop of a Moufang loop generated by any pair of elements is associative.

If Q is a group, then a *Q-module* M is an abelian group $(M, +)$ equipped with a group homomorphism

$$T : Q \to AutM; q \mapsto (m \mapsto mT(q)). \tag{2.8}$$

Setting $\tau(q) = T(q^{-1})$ for q in Q, the set $M \times Q$ equipped with the multiplication

$$(m_1, q_1)(m_2, q_2) = (m_1 + m_2\tau(q_1), q_1 q_2) \tag{2.9}$$

becomes a group $M \sqsupset Q$ known as the *split extension* of M by Q. Indeed, there is an exact sequence of groups

$$1 \to M \xrightarrow{i} M \sqsupset Q \xrightarrow{\pi} Q \to 1 \tag{2.10}$$

with $i : M \to M \sqsupset Q; m \mapsto (m, e)$ and

$$\pi : M \sqsupset Q \to Q; (m, q) \mapsto q \tag{2.11}$$

split by

$$0 : Q \to M \sqsupset Q; q \mapsto (0, q). \tag{2.12}$$

The group action (2.8) is recovered from the split extension by

$$mT(q)i = miR((0, q))L((0, q))^{-1} \tag{2.13}$$

for m in M and q in Q.

Now let Q be a Moufang loop with identity element e. Let (σ, τ) be a pair of maps from Q to the automorphism group of an abelian group M. Then M is said to be an *Eilenberg-Loginov module* for Q if the set $M \times Q$ equipped with the multiplication

$$(m_1, q_1)(m_2, q_2) = (m_1\sigma(q_2) + m_2\tau(q_1), q_1 q_2) \tag{2.14}$$

is a Moufang loop $M \sqsupset Q$ with identity $(0, e)$ (cf. [Lo,§2]). The maps i, π and 0 as above yield a split extension (2.10) of Moufang loops.

3. Representations in varieties of quasigroups.

A *variety* $\mathcal{V}$ of quasigroups is a class of quasigroups defined as universal algebras $(Q, \cdot, /, \backslash)$ with three binary operations satisfying (2.5) and some additional set of identities known as the *relative equational basis* of $\mathcal{V}$ in the variety $\mathcal{Q}$ of all quasigroups. For example, the variety $\mathcal{L}$ of loops has the relative equational basis (2.6), while the variety $\mathcal{M}$ of Moufang loops has basis (2.6), (2.7). A variety becomes a category on taking homomorphisms as morphisms. Such categories are bicomplete [HS, §32]. For a fixed member Q of $\mathcal{V}$, the *comma category* $\mathcal{V}/Q$ has $\mathcal{V}$-morphisms $\pi : E \to Q$ as objects. The morphisms of $\mathcal{V}/Q$ are $\mathcal{V}$-morphisms $\theta : E \to F$ such that the diagram

(3.1)
$$\begin{array}{ccc} E & \xrightarrow{\theta} & F \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ Q & = & Q \end{array}$$

commutes in $\mathcal{V}$. The comma category $\mathcal{V}/Q$ has finite products. The empty product is the identity $1 : Q \to Q$. The product of $\pi : E \to Q$ and $\varphi : F \to Q$ is $\pi \times_Q \varphi : E \times_Q F \to Q; (e, f) \mapsto e\pi$, where $E \times_Q F = \{(e, f) \in E \times F | e\pi = f\varphi\}$. Then a *representation of* Q *in* $\mathcal{V}$ is an abelian group in the comma category $\mathcal{V}/Q$, an object $E \to Q$ of $\mathcal{V}/Q$ equipped with $(\mathcal{V}/Q)$-morphisms *zero* $O : Q \to E$, *negation* $: E \to E$ and *addition* $+ : E \times_Q E \to E$, such that the abelian group identities, written as commuting diagrams in $\mathcal{V}/Q$, are satisfied. For example, the abelian group identity $x + (-x) = 0$ becomes the commuting of

(3.2)
$$\begin{array}{ccc} E & \xrightarrow{1\times -} & E \times_Q E \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle +} \\ Q & \xrightarrow[O]{} & E \end{array}$$

in $\mathcal{V}/Q$. If $\mathcal{G}$ is the variety of groups and Q is a group with identity element e, then a Q-module M as in (2.8) gives a representation (2.11) of Q in $\mathcal{G}$. The zero is the splitting (2.12), negation is $(m, q) \mapsto (-m, q)$, and addition is $((m_1 q), (m_2, q)) \mapsto (m_1 + m_2, q)$. Conversely, a representation $\pi : E \to Q$ of Q in $\mathcal{G}$ yields a Q-module $M = \pi^{-1}\{e\}$ with action (2.8) given by the inner automorphisms as in (2.13).

The definition of a representation of Q in $\mathcal{V}$ as an abelian group in the comma category $\mathcal{V}/Q$ is somewhat abstract. Quasigroup theory provides a more concrete approach in terms of representations of groups and rings. If Q is a subquasigroup of P, then the *relative multiplication group* $Mlt_P Q$ *of* Q *in* P is the subgroup of the combinatorial multiplication group $Mlt\ P$ of P generated by the subset $\{R(y),\ L(y) | y \in Q\}$ of right and left multiplications by elements of Q. (For example, if P is a group, then the orbits of the action of $Mlt_P Q$ on P are the double cosets of the subgroup Q.) The relative multiplication group $Mlt_P Q$

acts on Q. If e is an element of Q, then its stabilizer $(Mlt_P Q)_e$ in $Mlt_P Q$ is generated by the elements

$$\begin{cases} T_e(q) &= R(e \setminus q)L(q/e)^{-1}; \\ R_e(q,r) &= R(e \setminus q)R(r)R(e \setminus qr)^{-1}; \\ L_e(q,r) &= L(q/e)L(r)L(rq/e)^{-1} \end{cases} \tag{3.3}$$

for q, r in Q [S1,2.4]. If Q is a loop with identity element e, then the suffices e are dropped from T, L, R (and the right hand sides of (3.3) simplify). Now let $Q[X]$ denote the coproduct in the variety $\mathcal{V}$ of the quasigroup Q with the free $\mathcal{V}$-quasigroup on one generator ("*indeterminate*") X. The relative multiplication group of Q in $Q[X]$ is called the *universal multiplication group* $U(Q;\mathcal{V})$ *of* Q *in* $\mathcal{V}$. If Q is a group, then $U(Q;\mathcal{G})$ is the square $Q \times Q$ [S1, 235]. For any quasigroup Q, the group $U(Q;\mathfrak{Q})$ is free on the set $2Q$ (the disjoint union of two copies of the set Q) [S1, 238] [FS]. For a quasigroup Q with element e, representations of Q in $\mathfrak{Q}$ are equivalent to modules for the stabilizer $U(Q;\mathfrak{Q})_e$ of e in $U(Q;\mathfrak{Q})$ [S1,336] [S2, 3.2] [FS]. The equivalence works as follows. Given a representation $\pi : E \to Q$ of Q in $\mathfrak{Q}$, the zero embeds Q as a subquasigroup of E. The universal multiplication group $U(Q;\mathfrak{Q})$ acts on E via the projection $U(Q;\mathfrak{Q}) \to Mlt_E Q$ given by $R(y) \mapsto R(y)$ and $L(y) \mapsto L(y)$ for y in Q [S1, 334]. The abelian group $M = \pi^{-1}\{e\}$ is invariant under $U(Q;\mathfrak{Q})_e$, which acts as a group of automorphisms, making M a $U(Q;\mathfrak{Q})_e$-module. Conversely, given a $U(Q;\mathfrak{Q})_e$-module M, a representation $\pi : E \to Q$ is built via the induced $U(Q;\mathfrak{Q})$-module $M^{U(Q;\mathfrak{Q})} = M \otimes_{\mathbb{Z}U(Q;\mathfrak{Q})_e} \mathbb{Z}U(Q;\mathfrak{Q})$ by $E = \dot{\bigcup}_{q\in Q} M \otimes \rho(e,q)$ with $\pi : M \otimes \rho(e,q) \to \{q\}$, where $\rho(e,q)$ denotes a typical element $R(e\backslash e)^{-1}R(e\backslash q)$ making up a transversal $\{\rho(e,q) | q \in Q\}$ to $U(Q;\mathfrak{Q})_e$ in $U(Q;\mathfrak{Q})$. The quasigroup operations are given on E by the formulas

$$\begin{cases} a \cdot b &= aR(b\pi) + bL(a\pi); \\ a/b &= (a - bL(a\pi/b\pi))R(b\pi)^{-1}; \\ a \setminus b &= (b - aR(a\pi \setminus b\pi))L(a\pi)^{-1} \end{cases} \tag{3.4}$$

[S1,332].

4. Differentiation of the relative basis.

The equivalence between representations of a quasigroup Q with element e in the variety $\mathfrak{Q}$ of all quasigroups and modules over the universal stabilizer $U(Q;\mathfrak{Q})_e$ may be specialized to representations of Q in a variety $\mathcal{V}$ containing it. This specialization requires an analysis of the relative equational basis of $\mathcal{V}$ in $\mathfrak{Q}$, based on a *linearization* [S1, p.57] or *differentiation* (cf. [Fo]) process for quasigroup words. The integral group algebra $\mathbb{Z}U(Q;\mathfrak{Q})_e$ of the universal stabilizer is a $U(Q;\mathfrak{Q})_e$-module, and thus furnishes a representation $\pi : E \to Q$ of Q in $\mathfrak{Q}$. To facilitate useful intuitions from calculus, it is convenient to write elements of $\mathbb{Z}U(Q;\mathcal{Q})_e$ as infinitesimals. A typical element $dx \otimes \rho(e,x)$ of E will then be written as $x + dx$. Now consider a word $f(x_1,\ldots,x_n)$ in the quasigroup operations $\cdot, /$ and $\backslash$. Without loss of generality, one may assume that this word has been reduced using the quasigroup identities (2.5). Then by repeated use of (3.4) [S1, 338], there are maps

$$\frac{\partial f}{\partial x_i} : Q^n \to \mathbb{Z}U(Q;\mathcal{Q})_e \tag{4.1}$$

for $i = 1,\ldots,n$ such that

$$f(x_1 + dx_1,\ldots,x_n + dx_n) = f(x_1,\ldots,x_n) + \sum_{i=1}^{n} dx_i \frac{\partial f}{\partial x_i}(x_1,\ldots,x_n) \tag{4.2}$$

holds in E. As in calculus, the arguments $x_1,\ldots,x_n$ of the "partial derivative" $\frac{\partial f}{\partial x_i}$ will not necessarily be written out explicitly. The partial derivatives $\frac{\partial f}{\partial x_1},\ldots,\frac{\partial f}{\partial x_n}$ are described respectively as the 1st, $\ldots$, n-th components of the *gradient* ∇f. Other notational conventions from calculus may be used. Thus

$$\frac{\partial}{\partial x_1}(x_1x_2) = R(e\backslash e)^{-1}R_e(x_1,x_2)R(e\backslash e) \tag{4.3}$$

and

$$\frac{\partial}{\partial x_2}(x_1x_2) = R(e\backslash e)^{-1}T_e(x_2)L_e(x_2,x_1)T_e(x_1x_2)^{-1}R(e\backslash e) \tag{4.4}$$

(cf. [S1, 339(a)]).

There is an epimorphism $U(Q;\mathcal{Q}) \to U(Q;\mathcal{V}); R(x) \mapsto R(x), L(x) \mapsto L(x)$, restricting to an epimorphism $U(Q;\mathcal{Q})_e \to U(Q;\mathcal{V})_e$ of universal stabilizers. This epimorphism in turn yields a ring homomorphism $\mathbb{Z}U(Q;\mathcal{Q})_e \to \mathbb{Z}U(Q;\mathcal{V})_e$. Derivatives (4.1) of quasigroup words may thus be interpreted in $\mathbb{Z}U(Q;\mathcal{V})_e$. Let B denote the set of pairs (f,g) of quasigroup words constituting identities $f(x_1,\ldots,x_n) = g(x_1,\ldots,x_n)$ of the relative equational basis of $\mathcal{V}$ in $\mathcal{Q}$. Let $\mathbb{Z}\mathcal{V}Q$ denote the quotient of the integral group ring $\mathbb{Z}U(Q;\mathcal{V})_e$ by the ideal $J\mathbb{Z}U(Q;\mathcal{V})_e$ generated by the set

$$\{\frac{\partial f}{\partial x_i}(q_1,\ldots,q_n) - \frac{\partial g}{\partial x_i}(q_1,\ldots,q_n) | (f,g) \in B,\ q_j \in Q\} \tag{4.5}$$

of differences of corresponding gradient components of words in identities in the relative basis. Representations of Q in $\mathcal{V}$ are then described concretely as follows.

FUNDAMENTAL THEOREM OF REPRESENTATIONS IN VARIETIES 4.1 [S1, 343] [S2,4.6]. *Let Q be a $\mathcal{V}$-quasigroup with element e. Then the category of representations of Q in $\mathcal{V}$ is equivalent to the category of $\mathbb{Z}\mathcal{V}Q$-modules.* □

Remark 4.2: [cf. S1, 424].

Let $\pi : E \to Q$ be a representation of a loop Q with identity element e in the variety $\mathcal{Q}$ of quasigroups. Since $q/q = q \setminus q$ for all q in Q, one has $R(q \setminus q) = L(q/q) = 1$. The second and third formulas (3.4) then show that $a/a = b \setminus b = 0 \otimes \rho(e, e)$ in E, so E is a loop. Hence $\pi : E \to Q$ is a representation of Q in $\mathcal{Q}$ if and only if it is a representation of Q in the variety $\mathcal{L}$ of loops. In particular, it follows from (4.1) that the loop identity (2.6) makes no contribution to (4.5).

5. Moufang Loops.

Let Q be a Moufang loop with identity element e. Then Q is an ***inverse property loop***: each element x of Q has an inverse x^{-1} with $R(x^{-1}) = R(x)^{-1}$ and $L(x^{-1}) = L(x)^{-1}$ [B2, Lemma VII. 3.1]. Furthermore [B1, Lemma II. 4.D] [B2, VII. (5.3)] [Do], the following relations are satisfied in the relative multiplication groups of Q in Moufang loops (using Doro's notation $P(x) = L(x)^{-1}R(x)^{-1}$, not to be confused with [B2, VII. (5.4)]):

$$P(e) = R(e) = L(e) = P(x)R(x)L(x) = 1; \tag{5.1}$$

$$P(xyx) = P(x)P(y)P(x),\ R(xyx) = R(x)R(y)R(x),\ L(xyx) = L(x)L(y)L(x); \tag{5.2}$$

$$\begin{cases} P(x)^{R(y)} = P(xy)P(y^{-1}), & P(x)^{L(y)} = P(yx)P(y^{-1}), \\ R(x)^{L(y)} = R(xy)R(y^{-1}), & R(x)^{P(y)} = R(yx)R(y^{-1}), \\ L(x)^{P(y)} = L(xy)L(y^{-1}), & L(x)^{R(y)} = L(yx)L(y^{-1}). \end{cases} \tag{5.3}$$

The free group on $\{P(x),\ R(x),\ L(x) | x \in Q\} = 3Q$ subject to the relations (5.1)-(5.3) is called the ***universal group $D(Q)$ with triality on the Moufang loop Q*** (the group $G(Q)$ of [Do, (19)]). Since the universal multiplication group $U(Q; \mathcal{M})$ satisfies (5.1)-(5.3), it is a quotient of the universal group with triality on Q. On the other hand, the universal group with triality is a quotient of the universal multiplication group $U(Q; \mathcal{L})$ of Q in the variety of loops (since by [S1, 422], $U(Q; \mathcal{L})$ is free on the disjoint union of two copies of $Q - \{e\}$).

PROBLEM 5.1 Is the universal multiplication group $U(Q, \mathcal{M})$ of a Moufang loop Q in the variety $\mathcal{M}$ of Moufang loops a proper quotient of the universal group with triality on Q?

Addressing a different problem in the representation theory of quasigroups, recall that a variety $\mathcal{V}$ of quasigroups is *universally finite* if the universal multiplication group $U(F; \mathcal{V})$ of a finite member F of $\mathcal{V}$ is finite. A variety is *locally finite* if all its finitely generated members are finite. The general problem [S1, 356] is to determine large universally finite varieties that are not locally finite, since such varieties are likely to have interesting structure. Of course, any subvariety of a universally finite variety is universally finite.

Proposition 5.2. *The variety $\mathcal{M}$ of Moufang loops is universally finite, but not locally finite.*

Proof. Let F be a finite Moufang loop. The universal group $G(F)$ with triality on F is finite [Do, Corollary 3]. Then $U(F;\mathcal{M})$, as a quotient of $G(F)$, is finite. □

Using the notation of (3.3) - which simplifies to Bruck's notation [B2, IV. (1.5)] for loops –one may now specialize Theorem 4.1.

Theorem 5.3. *Let Q be a Moufang loop with identity element e. Then representations of Q in the variety $\mathcal{M}$ of Moufang loops are equivalent to modules over the quotient of the integral group algebra $\mathbb{Z}U(Q;\mathcal{M})_e$ by the ideal generated by all*

(5.4) $R(a,b)R(ab,ca)+T(a)L(a,c)L(ca,ab)T(ab\cdot ca)^{-1}-R(a,bc\cdot a)-T(a)T(ab\cdot ca)^{-1}$

for elements a,b,c of Q.

Proof. The relative equational basis of $\mathcal{M}$ in $\mathcal{Q}$ consists of the loop identity (2.6) and the Moufang identity (2.7). By (*) the identity (2.6) makes no contribution to (4.5). Let w_l and w_r respecitvely denote the words on the left and right of (2.7). Since x_2 and x_3 appear uniquely above the line [S1, p.63] on each side of 2.7, one has $\frac{\partial w_l}{\partial x_2}=\frac{\partial w_r}{\partial x_2}$ and $\frac{\partial w_l}{\partial x_3}=\frac{\partial w_r}{\partial x_3}$ [S1, 353].

Applying (4.3) and (4.4), one obtains

$$(5.5)\qquad \frac{\partial w_l}{\partial x_1}=R(x_1,\ x_2)R(x_1x_2,\ x_3x_1) + T(x_1)L(x_1,x_3)L(x_3x_1,\ x_1x_2)T(x_1x_2\cdot x_3x_1)^{-1}$$

and

$$(5.6)\qquad \frac{\partial w_r}{\partial x_1}=R(x_1,\ x_2x_3\cdot x_1) + T(x_1)L(x_1,\ x_2x_3)L(x_2x_3\cdot x_1,\ x_1)T(x_1x_2\cdot x_3x_1)^{-1}.$$

The latter summand of (5.6) may be simplified working with elements (3.3) of $U(Q;\mathcal{M})$ and using the third relation in (5.2):

$$\begin{aligned}
&T(a)L(a,bc)L(bc\cdot a,a)T(ab\cdot ca)^{-1}\\
=&T(a)L(a)L(bc)L(bc\cdot a)^{-1}L(bc\cdot a)L(a)L(ab\cdot ca)^{-1}L(ab\cdot ca)R(ab\cdot ca)^{-1}\\
=&T(a)L(a)L(bc)L(a)R(ab\cdot ca)^{-1}\\
=&T(a)L(ab\cdot ca)R(ab\cdot ca)^{-1}\\
=&T(a)T(ab\cdot ca)^{-1}.
\end{aligned}$$

The form of (5.4) follows. □

6. Eilenberg-Loginov modules.

Consider an Eilenberg-Loginov module M for a Moufang loop Q with identity element e. The module yields a split extension (2.10) with Moufang loop multiplication defined by (2.14).

Proposition 6.1. *The Moufang loop homomorphism* $\pi : M \sqsupset Q \to Q$ *is an abelian group in the comma category* $\mathcal{M}/Q$ *of Moufang loops over* Q *with zero (2.12), negation* $(m,q) \mapsto (-m,q)$ *and addition* $((m_1,q),(m_2,q)) \mapsto (m_1+m_2,q)$.

Proof. The verifications are routine, given the assumptions that $M \sqsupset Q$ is a Moufang loop and that σ and τ map to the automorphism group of the abelian group M. □

Proposition 6.1 shows that the Eilenberg-Loginov Module M for Q affords a representation of Q in $\mathcal{M}$. By Theorem 5.3, M affords a corresponding representation of $U(Q;\mathcal{M})_e$ and $\mathbb{Z}\mathcal{M}Q$. Indeed, this representation lifts to a restriction of a representation of the universal group with triality on Q.

Proposition 6.2. *By means of*

$$R(x) \mapsto \sigma(x),\ L(x) \mapsto \tau(x), \tag{6.1}$$

the Eilenberg-Loginov module M *for* Q *affords a representation of the universal group with triality over the Moufang loop* Q.

Proof. First note $\sigma(e) = \tau(e) = 1$, since $M \sqsupset Q$ has identity element $(0,e)$ (cf. [Lo, (3)]). Because $U(Q;\mathcal{L})$ is free on $2(Q-\{e\})$, the specification (6.1) makes M a $U(Q;\mathcal{L})$-module. This module is a lift of a module for the universal group with triality, since opposite sides of the relations (5.1)-(5.3) have the same action on M. For example, to verify that $L(y)^{-1}R(x)L(y)$ and $R(xy)R(y^{-1})$ have the same action, i.e. to verify the relation

$$\tau(y^{-1})\sigma(x)\tau(y) = \sigma(xy)\sigma(y^{-1}), \tag{6.2}$$

note that $L((0,y)^{-1})R((0,x))L((0,y)) = R((0,x)(0,y))R((0,y)^{-1})$ holds in the relative multiplication group of Q (i.e. of the image of the zero map (2.12)) in $M \sqsupset Q$ by [B1, II. (4.7)]. The respective images of an element (m,e) of Mi under these equal group elements are $(m\tau(y^{-1})\sigma(x))\tau(y), y^{-1}xy)$ and $(m\sigma(xy)\sigma(y^{-1}),\ y^{-1}xy)$. The relation (6.2) is then obtained by equating the first components of these image elements. □

Remark 6.3. The proof of Proposition 6.2 offers an alternative derivation of those relations (7)-(9) of [Lo] which involve at most two elements of Q (i.e. all but those involving addition of module elements). For example, the last relations of (8), (9) follow from (5.2).

Corollary 6.4. *The representations of* $U(Q;\mathcal{M})_e$ *and* $\mathbb{Z}\mathcal{M}Q$ *corresponding to the Eilenberg-Loginov module* M *are given by*

$$\begin{cases} T(q) &= \sigma(q)\tau(q^{-1}) \\ R(q,r) &= \sigma(q)\sigma(r)\sigma(qr)^{-1} \\ L(q,r) &= \tau(q)\tau(r)\tau(rq)^{-1} \end{cases} \tag{6.3}$$

(using the notation of (3.3)). □

Remark 6.5. For the case where Q is associative and $\sigma(Q) = \{1\} \leq Aut(M, +)$, Corollary 6.4 recovers the relationship between (2.8) and (2.9) for group modules and extensions (cf. [S1, 4.1]).

Starting with the $\mathbb{Z}\mathcal{M}Q$-, $U(Q;\mathcal{M})_e$- or $U(Q;\mathcal{Q})_e$-module given by (6.3), one may build the abelian group object $\pi : E \to Q$ on $E = \dot{\bigcup}_{q\in Q} M \otimes \rho(e,q)$ with operations (3.4) as summarized at the end of the third section. The final result of the current section relates the two objects $E \to Q$ and $M \sqsupset Q \to Q$.

Proposition 6.6. *The abelian group objects $\pi : E \to Q$ and $\pi : M \sqsupset Q \to Q$ of the comma category $\mathcal{M}/Q$ are isomorphic via*

$$\theta : E \to M \sqsupset Q; m \otimes \rho(e,q) \mapsto (m\sigma(q), q). \tag{6.4}$$

Proof. The morphism θ respects the abelian group operations since $\sigma(q)$ is an automorphism of $(M, +)$. To verify that θ is a loop homomorphism, one may use (4.4), (4.5) and (6.3) as follows:

$$\begin{aligned}
&[(m \otimes R(q))(n \otimes R(r))]\theta \\
=&[(mR(q,r) + nT(r)L(r,q)T(qr)^{-1}) \otimes R(qr)]\theta \\
=&[(m\sigma(q)\sigma(r)\sigma(qr)^{-1} + n\sigma(r)\tau(q)\sigma(qr)^{-1}) \otimes R(qr)]\theta \\
=&(m\sigma(q)\sigma(r) + n\sigma(r)\tau(q),\ qr) \\
=&(m\sigma(q),\ q)(n\sigma(r),\ r) \\
=&[m \otimes R(q)]\theta \cdot [n \otimes R(r)]\theta
\end{aligned}$$

working with elements of $U(Q;\mathcal{M})$ rather than $U(Q;\mathcal{Q})$ for brevity. □

7. The Zassenhaus-Bruck Construction.

Let Q be the abelian group $\mathbb{Z} \oplus \mathbb{Z}$. Let M be the abelian group $\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Let E be $M \times Q$. Define the product of two elements $((m_i, m_i' + 3\mathbb{Z}),\ (q_i, q_i'))$ (with $i = 1,2$) of E to be

$$((m_1 + m_2, m_1' + m_2' + (m_1 - m_2)(q_1q_2' - q_1'q_2) + 3\mathbb{Z}), (q_1 + q_2, q_1' + q_2')). \tag{7.1}$$

Then E with this product is the free commutative Moufang loop on its three-element subset

$$\{((1,0),(0,0)),\ ((0,0),(1,0)),\ ((0,0),(0,1))\} \tag{7.2}$$

[B1, Theorem II. 9A], [S2, §6]. In particular E, being nilpotent of class 2, is not associative. Furthermore, (7.3) $$\pi : E \to Q; ((m, m' + 3\mathbb{Z}),\ (q, q')) \mapsto (q, q')$$

is a representation of Q in the variety $\mathcal{M}$ – and indeed in the variety of commutative Moufang loops [S2, Theorem 6.3]. However, E cannot be recovered as a split extension $M \sqsupset Q$ from an Eilenberg-Loginov module structure for Q on M.

Proposition 7.1. *There are no maps $\sigma, \tau : Q \to AutM$ such that E with the product (7.1) can be written as a split extension $M \sqsupset Q$ with product (2.14).*

Proof. Assume the existence of suitable maps σ, τ, so that

(7.4) $$\begin{cases} & (m_1 + m_2, m_1' + m_2' + (m_1 - m_2)(q_1 q_2' - q_1' q_2) + 3\mathbb{Z}) \\ = & (m_1, m_1' + 3\mathbb{Z})\sigma(q_2, q_2') + (m_2, m_2' + 3\mathbb{Z})\tau(q_1, q_1'). \end{cases}$$

Set $q_1 = q_1' = m_2 = 1,\ m_1 = m_1' = m_2' = 0$. Then for all q, q' in $\mathbb{Z}$, one obtains

(7.5) $$(1, q - q' + 3\mathbb{Z}) = (1, 3\mathbb{Z})\tau(1, 1).$$

Thus $\tau(1, 1)$ cannot be well-defined. □

References.

[B1] R.H. BRUCK, *Contributions to the theory of loops*, Trans. Amer. Math. Soc. **60** (1946), 245–354.

[B2] R.H. BRUCK, *A Survey of Binary Systems*, Springer, Berlin, 1958.

[Do] S. DORO, *Simple Moufang Loops*, Math. Proc. Camb. Phil. Soc. **83** (1978), 377-392.

[Ei] S. EILENBERG, *Extensions of general algebras*, Ann. Soc. Polon. Math. **21** (1948), 125–134.

[Fo] R.H. FOX, *Free differential calculus*, Ann. of Math. **57** (1953), 547–560.

[FS] T.S.R. FUAD and J.D.H. SMITH, *Quasigroups, right quasigroups and category coverings*, Alg. Univ., to appear.

[HS] H. HERRLICH and G.E. STRECKER, *Category Theory*, Allyn and Bacon, Boston, 1973.

[Lo] E.K. LOGINOV, *On linear representations of Moufang Loops*, Comm. in Alg. **21** (1993), 2527–2536.

[S1] J.D.H. SMITH, *Representation Theory of Infinite Groups and Finite Quasigroups*, Les Presses de L'Université de Montréal, Montréal, 1986.

[S2] J.D.H. SMITH, *Quasigroup representation theory*, in "Universal Algebra and Quasigroup Theory" (A. ROMANOWSKA and J.D.H. SMITH, eds.), Heldermann, Berlin 1992, pp. 195–207.

Received: October 1994