ON A THEOREM OF R. MOUFANG

R. H. BRUCK

A loop is a system with a binary operation, possessing a unit 1, and such that any two of the elements in the equation \(xy = z\) uniquely determine the third. A Moufang loop \([1, \text{chap. 2}]\) may be characterized by the identity \(xy \cdot zx = (x \cdot yz)x\). The following theorem is due to R. Moufang \([2]\).

**Theorem.** If \(ab \cdot c = a \cdot bc\) for three elements \(a, b, c\) of a Moufang loop, the subloop generated by them is associative.

We give a particularly simple proof for the commutative case. (This proof, although complete in itself, stems from the theory of autotopisms introduced in \([1]\), which will be applied elsewhere to the noncommutative case.) Henceforth let \(G\) be a commutative Moufang loop. For each \(x\) in \(G\) define the permutation \(R(x)\) by \(yR(x) = yx\). The defining relation can be written in the two forms

\[(1)\quad yx \cdot zx = (yz \cdot x)x, \quad yR(x) \cdot zR(x) = (yz)R(x)^2.\]

If we take \(z = x\) in (1), \(yx \cdot xx = (yx \cdot x)x\). If we replace \(yx\) by \(y\),

\[(2)\quad y \cdot xx = yx \cdot x.\]

If \(x^{-1}\) is defined by \(xx^{-1} = 1\) (so that \((x^{-1})^{-1} = x\), (1) with \(z = x^{-1}\) gives \(yx = (yx^{-1} \cdot x)x\), \(y = yx^{-1} \cdot x\) and

\[(3)\quad yx \cdot x^{-1} = y, \quad R(x)^{-1} = R(x^{-1}).\]

Let \(\mathcal{G}\) be the group generated by the \(R(x)\), and consider its elements \(S = R(a_1)R(a_2) \cdots R(a_n), \quad T = R(a_1)^2R(a_2)^2 \cdots R(a_n)^2\). By (3), every element of \(\mathcal{G}\) can be put in the form \(S\). By repeated application of (1), \(yS \cdot zS = (yz)T\). If the \(a_i\) are chosen so that \(1S = 1\), let \(y = 1\) and have \(S = T\). Thus the subgroup \(\mathcal{S}\) of \(\mathcal{G}\), consisting of the \(S\) with \(1S = 1\), is a group of automorphisms of \(G\). We use this "remark" several times; its value lies in the readily verified fact that the elements left invariant by a set of automorphisms of a loop form a subloop.

Let \(H\) be the subloop of the theorem and \(H_1\) the subset consisting of the \(z\) in \(H\) such that \(ab \cdot z = a \cdot bz\). Equivalently, \(zS = z\) where \(S = R(ab)R(a^{-1})R(b^{-1})\). By the remark, \(S\) induces an automorphism of \(H\), so \(H_1\) is a subloop of \(H\). Moreover \(H_1\) contains \(c\), by hypothesis,
and $a$, $b$, by (2). Hence $H_1 = H$.

In particular, therefore, $ab \cdot c^{-1} = a \cdot bc^{-1}$. If we apply (3) and (1) in turn, $ab = (a \cdot bc^{-1})c$, $ab \cdot c = ac \cdot b$. It is now easy to see that the relation $ab \cdot c = a \cdot bc$ remains true under all permutations of $a$, $b$, $c$. We deduce among other things that $ac \cdot z = a \cdot cz$ for all $z$ in $H$.

Let $H_2$ be the subset consisting of the $y$ in $H$ such that $ay \cdot z = a \cdot yz$ for all $z$ in $H$. By the remark, $H_2$ is a subloop of $H$, containing $a$, by (2), and $b$, $c$, by the above proofs. Hence $H_2 = H$.

A similar argument now gives $xy \cdot z = x \cdot yz$ for all $x$, $y$, $z$ in $H$.

REFERENCES


UNIVERSITY OF WISCONSIN