Canad. J. Math. Vol. **59** (2), 2007 pp. 296–310

Bol Loops of Nilpotence Class Two

Orin Chein and Edgar G. Goodaire

Abstract. Call a non-Moufang Bol loop *minimally non-Moufang* if every proper subloop is Moufang and *minimally nonassociative* if every proper subloop is associative. We prove that these concepts are the same for Bol loops which are nilpotent of class two and in which certain associators square to 1. In the process, we derive many commutator and associator identities which hold in such loops.

1 Introduction

Over 100 years ago, G. A. Miller and and H. C. Moreno characterized nonabelian groups with the property that all subgroups are Abelian [MM]. (See also [S, §6.5].) Motivated by this paper, the authors have, in recent years, begun a study of *minimal nonassociativity* in loops [CG3, CG5, CG4]. We call a loop *minimally nonassociative* (MNA) if it is not associative, but every proper subloop is associative.

A loop is *Moufang* if it satisfies the identity $(xy \cdot z)y = x(y \cdot zy)$ and (right) *Bol* if $(xy \cdot z)y = x(yz \cdot y)$ is an identity.[1]

Bol loops take their name from Gerrit Bol [B] who showed that the Bol identity corresponds to a certain configuration in 3-webs [Pf, §II.3]. Michael Kallaher and Ted Ostrom have studied quasifields whose multiplicative loop satisfies the right Bol identity [KO]. In the last ten years, Bol loops have been used to construct right alternative loops that are not left alternative [GR1, GR2] (such rings are scarce [Ku]) and, in turn, they have been shown to arise as loops of units in right alternative loop rings [G].

The (seemingly small) difference in the order of multiplication on the right side of the Moufang and Bol identities makes a world of difference to the loops. For example, Moufang loops are *diassociative*, meaning that the subloop generated by any pair of elements is a group. In particular, $y \cdot zy = yz \cdot y$ for any y, z in a Moufang loop, so a Moufang loop is right Bol.

Bol loops satisfy some weak associativity conditions, but not others. For example, any (right) Bol loop satisfies the *right alternative identity*, $(xy)y = xy^2$ (set $z = 1$ in the right Bol identity) and this, together with a straightforward induction argument can be used to show that Bol loops are *power associative*, meaning that powers of a single element are well defined. In fact, Bol loops satisfy the *right power alternative identity*, $(xy^n)y^m = xy^{n+m}$ for any integers n and m.

Received by the editors August 25, 2004; revised October 19, 2004.

The second author is grateful for the hospitality provided by the Department of Mathematics of Temple University where he was a visitor while this work was completed. His research was supported by the Natural Sciences and Engineering Research Council of Canada, Grant No. OGP0009087.

AMS subject classification: 20N05.

Keywords: Bol loop, Moufang loop, nilpotent, commutator, associator, minimally nonassociative.

[1] A loop is left Bol if it satisfies the reflection of the right Bol identity, namely, $y(z \cdot yx) = (y \cdot zy)x$. Throughout this paper, whether or not we say so explicitly, we assume that Bol loops are *right* Bol.

On the other hand, a Bol loop which is not Moufang cannot even satisfy the *left alternative identity*, $x(xy) = x^2y$. We refer the reader to the text by Pflugfelder [Pf] where she will find more than enough background on Bol and Moufang loops for this paper.

We will often focus on some particular subloops of a loop L.

The left, middle, and right *nuclei* of a loop L are defined, respectively, by

$$N_\lambda(L) = \{a \in L \mid (a, x, y) = 1 \text{ for all } x, y \in L\},$$
$$N_\mu(L) = \{a \in L \mid (x, a, y) = 1 \text{ for all } x, y \in L\},$$
$$N_\rho(L) = \{a \in L \mid (x, y, a) = 1 \text{ for all } x, y \in L\}.$$

The *nucleus* of L is $N(L) = N_\lambda(L) \cap N_\mu(L) \cap N_\rho(L)$. The *centrum* of L is

$$\mathcal{C}(L) = \{a \in L \mid (a, x) = 1 \text{ for all } x \in L\}$$

and the *centre* of L is $\mathcal{Z}(L) = N(L) \cap \mathcal{C}(L)$.

In general, the three nuclei of a loop may be different, but in a Bol loop, the right and middle nuclei coincide, and in a Moufang loop, all three nuclei are equal.

By analogy with the concept of minimal nonassociativity, it is natural to think about Bol loops which are not Moufang, but in which every proper subloop is Moufang. We call such a subloop *minimally non-Moufang* (MNM). It is not hard to see that an MNM Bol loop B must be generated by two elements. For this, note first that because B is not Moufang, there exist $x, y \in B$ with $x(xy) \neq x^2y$. Since the subloop $\langle x, y\rangle$ generated by x and y is not Moufang, it cannot be proper.

In their study of MNA Moufang loops, the authors first characterized commutative MNA Moufang loops and then considered a class of loops which are very nearly commutative, namely, those with a unique nonidentity commutator, which is also a unique nonidentity associator. Since a commutative Bol loop is Moufang, it seems reasonable that our first foray into a study of MNM Bol loops would concern those with a unique nonidentity commutator/associator. A number of interesting identities hold in such loops. As we discovered when we began to study this class of loops, however, we do not need the full hypothesis to establish many of these identities. For example, some can be proved if we simply assume B is nilpotent of class two, that is, all commutators and associators in B are central. Thus much of the focus of this paper is concerned with such loops.

If x, y, and z are elements of a loop B, we use the notation (x, y) and (x, y, z) for the commutator of x and y and the associator of x, y, and z, respectively. Thus, by definition, $xy = yx(x, y)$ and $(xy)z = [x(yz)](x, y, z)$. The subloop of a loop L generated by the commutators and associators is called the commutator/associator subloop of L and is denoted by L'.

With this notation, the right power alternative identity may be expressed in the form

$$(x, y^n, y^m) = 1. \tag{1.1}$$

https://doi.org/10.4153/CJM-2007-012-7 Published online by Cambridge University Press

If we assume that a Bol loop B has a unique nonidentity commutator s which is also a unique nonidentity associator, then s must be central and of order two. (This was first proved for Moufang loops by the authors [CG2], and for Bol loops by the second author with D. A. Robinson [GR1, Lemma 3.2].)

In Section 2, we exhibit a number of identities satisfied by any Bol loop which is nilpotent of class two. In Section 3, we first add the additional constraint that associators square to 1, and then we add the further assumption that commutators also square to 1, so that the commutator/associator subloop B' is a central elementary Abelian 2-group. In Section 4, we show that if a Bol loop which satisfies these conditions is minimally non-Moufang, then it is minimally nonassociative as well. Since, as earlier noted, a minimally non-Moufang Bol loop can be generated by two elements, it is natural to investigate two-generator nilpotent class two Bol loops. This we do in Section 5.

2 Commutator and Associator Identities

Throughout the rest of this paper, we assume that B is a Bol loop which is nilpotent of class two, hence, all commutators and associators in B are central.

For any $x, y, z \in B$, not only do we have $xy = yx(x, y)$ and $(xy)z = [x(yz)](x, y, z)$ but also, since commutators and associators are central, $yx = xy(x, y)^{-1}$ and $x(yz) = [(xy)z](x, y, z)^{-1}$. In particular, $(y, x) = (x, y)^{-1}$. Furthermore, if c is any central element in B, $(xc, y) = (x, yc) = (x, y)$, and $(xc, y, z) = (x, yc, z) = (x, y, zc) = (x, y, z)$. Since commutators are central, this means that $(xy, z) = (yx(x, y), z) = (yx, z)$ and similarly, $(xy, z, w) = (yx, z, w)$, and so on. Also, if n is any element in the nucleus of B, then

$$(2.1) \qquad \begin{aligned}(nx, y, z) = (xn, y, z) = (x, ny, z) = (x, yn, z)\\ = (x, y, nz) = (x, y, zn) = (x, y, z).\end{aligned}$$

We use these results implicitly, without further comment, in establishing a number of basic identities.

Lemma 2.1 *For all $x, y, z, w \in B$, $(xy, z, w)(x, y, zw) = (x, y, z)(y, z, w)(x, yz, w)$.*

Proof This follows from

$$\begin{aligned}(xy \cdot z)w &= (x \cdot yz)w(x, y, z)\\ &= x(yz \cdot w)(x, y, z)(x, yz, w)\\ &= x(y \cdot zw)(x, y, z)(x, yz, w)(y, z, w)\\ &= (xy \cdot zw)(x, y, z)(x, yz, w)(y, z, w)(x, y, zw)^{-1}\\ &= (xy \cdot z)w(x, y, z)(x, yz, w)(y, z, w)(x, y, zw)^{-1}(xy, z, w)^{-1}.\end{aligned}$$

If we now cancel $(xy \cdot z)w$ and multiply both sides by $(xy, z, w)(x, y, zw)$, we get the desired result. ∎

https://doi.org/10.4153/CJM-2007-012-7 Published online by Cambridge University Press

Lemma 2.2 *For all $x, y, z \in B$, $(x, z, y) = (x, y, z)^{-1}$.*

Proof Suppose that $(x, y, z) = s$. Set $a = (yz)^{-1}$ and $b = xy \cdot z = [x \cdot yz]s = sx \cdot yz$. Then, using the right power alternative identity, $x = s^{-1}ba$. Repeated use of the Bol identity and the centrality of s gives

$$\begin{aligned} xz \cdot y &= (s^{-1}ba \cdot z)y = (ba \cdot z)ys^{-1} \\ &= \{[(xy \cdot z)a]z\}ys^{-1} && \text{substituting for } b \\ &= [(xy)(za \cdot z)]ys^{-1} && \text{using the Bol identity} \\ &= x\{[y(za \cdot z)]y\}s^{-1} && \text{using the Bol identity again} \\ &= x\{[(yz \cdot a)z]y\}s^{-1} && \text{and a third time} \\ &= x(zy)s^{-1} && \text{since } a = (yz)^{-1}. \end{aligned}$$

Thus, $(x, z, y) = s^{-1} = (x, y, z)^{-1}$, as required. ∎

Lemma 2.3 *For all $x, y, z \in B$ and for any integer n, $(x, y, zy^n) = (x, y, z)$ and $(x, zy^n, y) = (x, z, y)$.*

Proof By the Bol identity, the definition of associator, the centrality of associators and Lemma 2.2,

$$\begin{aligned} (xy \cdot z)y = x(yz \cdot y) &= [(x \cdot yz)y](x, yz, y)^{-1} = [(x \cdot yz)(x, yz, y)^{-1}]y \\ &= [(x \cdot yz)(x, y, yz)]y. \end{aligned}$$

After cancelling y, we obtain $(xy)z = (x \cdot yz)(x, y, yz)$, so, by centrality of (y, z) and the definition of the associator of x, y and z, $(x, y, zy) = (x, y, yz) = (x, y, z)$.

For n a positive integer, the first identity of the lemma now follows from right power alternativity and induction. That is,

$$(x, y, zy^n) = (x, y, zy^{n-1} \cdot y) = (x, y, zy^{n-1}) = \cdots = (x, y, z).$$

For n a negative integer, say $n = -m$, $(x, y, z) = (x, y, zy^n \cdot y^m) = (x, y, zy^n)$.

The second identity of the lemma now follows by Lemma 2.2. That is,

$$(x, zy^n, y) = (x, y, zy^n)^{-1} = (x, y, z)^{-1} = (x, z, y).$$ ∎

Note that since commutators are central, we can also write the identities in Lemma 2.3 in the form $(x, y, y^n z) = (x, y, z)$ and $(x, y^n z, y) = (x, z, y)$.

Lemma 2.4 *For all $x, y, z \in B$ and for any integers m and n, $(x, y^m, z^n) = (x, y, z)^{mn}$.*

https://doi.org/10.4153/CJM-2007-012-7 Published online by Cambridge University Press

Proof We first use induction on n to prove the result in the special case that $m = 1$ and $n > 0$.

Setting $w = z$ in Lemma 2.1 and using right alternativity and Lemma 2.3, we get $(x, y, z^2) = (x, y, z)(x, yz, z) = (x, y, z)(x, y, z) = (x, y, z)^2$.

Suppose that $(x, y, z^k) = (x, y, z)^k$. Setting $z = w^k$ in Lemma 2.1, we get

$$(xy, w^k, w)(x, y, w^{k+1}) = (x, y, w^k)(y, w^k, w)(x, yw^k, w).$$

Using right power alternativity, and then replacing w by z, this becomes $(x, y, z^{k+1}) = (x, y, z^k)(x, yz^k, z)$. Applying the induction hypothesis and Lemma 2.3, this becomes $(x, y, z^{k+1}) = (x, y, z)^k(x, y, z) = (x, y, z)^{k+1}$, as required.

Setting $w = z^{-1}$ in Lemma 2.1, we get

$$(xy, z, z^{-1})(x, y, zz^{-1}) = (x, y, z)(y, z, z^{-1})(x, yz, z^{-1}).$$

Using right power alternativity, this becomes $1 = (x, y, z)(x, yz, z^{-1})$. If we now use Lemma 2.3, we get $1 = (x, y, z)(x, yz \cdot z^{-1}, z^{-1}) = (x, y, z)(x, y, z^{-1})$, so that $(x, y, z^{-1}) = (x, y, z)^{-1}$.

In n is a negative integer, say $n = -m$, then

$$(x, y, z^n) = (x, y, (z^{-1})^m) = (x, y, z^{-1})^m = [(x, y, z)^{-1}]^m = (x, y, z)^{-m} = (x, y, z)^n.$$

Finally, using Lemma 2.2,

$$(x, y^m, z^n) = (x, y^m, z)^n = (x, z, y^m)^{-n} = (x, z, y)^{-mn} = (x, y, z)^{mn},$$

as required. ∎

Lemma 2.5 *For any x, y, and $z \in B$, $(xy, y, z) = (x, y, z)(y, y, z)$ and $(xy, z, y) = (x, z, y)(y, z, y)$.*

Proof Setting $w = y^{-1}$ in Lemma 2.1, we get

$$(xy, z, y^{-1})(x, y, zy^{-1}) = (x, y, z)(y, z, y^{-1})(x, yz, y^{-1}).$$

Applying first Lemma 2.4 and then Lemma 2.3, this becomes $(xy, z, y)^{-1}(x, y, z) = (x, y, z)(y, z, y)^{-1}(x, z, y)^{-1}$. Cancelling (x, y, z), and using Lemma 2.2, we get the first identity of the lemma.

The second identity follows by applying Lemma 2.2. ∎

Corollary 2.6 *For any x, y, $z \in B$, and any integer n, $(xy^n, y, z) = (x, y, z)(y, y, z)^n$ and $(xy^n, z, y) = (x, z, y)(y, z, y)^n$.*

Proof If $n = 0$, the result is obvious.

If $n > 0$, the result follows from successive applications of Lemma 2.5.

If $n < 0$, say $n = -m$, then, by successive applications of the result for $m > 0$, we can peel off one y at a time. That is, $(x, y, z) = (xy^n \cdot y^m, y, z) = (xy^n, y, z)(y, y, z)^m$, so that $(xy^n, y, z) = (x, y, z)(y, y, z)^{-m} = (x, y, z)(y, y, z)^n$, as required.

As in the proof of the second identity in Lemma 2.5, the second identity of the corollary now follows by application of Lemma 2.2. ∎

https://doi.org/10.4153/CJM-2007-012-7 Published online by Cambridge University Press

Corollary 2.7 *For any $y, z \in B$ and any integer n, $(y^n, y, z) = (y, y, z)^n$. In particular, $(y^{-1}, y, z) = (y, y, z)^{-1}$.*

Proof Set $x = 1$ in Corollary 2.6. ∎

Lemma 2.8 *For any $x, y, z \in B$,*

$$(x, y, zx) = (x, y, z)(x, yz, x)(x, x, z) \quad \textit{and} \quad (x, zx, y) = (x, z, y)(x, x, yz)(x, z, x).$$

Proof Setting $w = x$ in Lemma 2.1, we get

$$(xy, z, x)(x, y, zx) = (x, y, z)(y, z, x)(x, yz, x),$$

which, by the centrality of (x, y), becomes

$$(yx, z, x)(x, y, zx) = (x, y, z)(y, z, x)(x, yz, x).$$

Applying Lemma 2.5, this becomes

$$(y, z, x)(x, z, x)(x, y, zx) = (x, y, z)(y, z, x)(x, yz, x).$$

Cancelling (y, z, x) and multiplying both sides by $(x, x, z) = (x, z, x)^{-1}$, we get the first identity of the lemma.

The second identity follows by applying Lemma 2.2. ∎

We now turn our attention to some identities involving commutators.

Lemma 2.9 *For any $x, y \in B$ and every integer n, $(x, y^n) = (x, y)^n (y, x, y)^{n(n-1)}$ and $(x^n, y) = (x, y)^n (x, x, y)^{n(n-1)}$.*

Proof We establish the first identity by induction on n, $n > 0$. The result clearly holds for $n = 0$ and $n = 1$.

Suppose $(x, y^k) = (x, y)^k (y, x, y)^{k(k-1)}$. We wish to find (x, y^{k+1}). Since

$$\begin{aligned} xy^{k+1} &= (xy^k)y = (y^k x)y(x, y^k) = y^k(xy)(y^k, x, y)(x, y^k) \\ &= y^k(yx)(x, y)(y^k, x, y)(x, y^k) \\ &= y^{k+1}x(y^k, y, x)^{-1}(x, y)(y^k, x, y)(x, y^k), \end{aligned}$$

we see that $(x, y^{k+1}) = (y^k, y, x)^{-1}(x, y)(y^k, x, y)(x, y^k)$.

Applying Lemma 2.2, Corollary 2.7 and the induction hypothesis, this becomes

$$\begin{aligned} (x, y^{k+1}) &= (y, x, y)^k (x, y)(y, x, y)^k (x, y)^k (y, x, y)^{k(k-1)} \\ &= (x, y)^{k+1} (y, x, y)^{k(k+1)}, \end{aligned}$$

as required. We now prove the result for $n < 0$.

https://doi.org/10.4153/CJM-2007-012-7 Published online by Cambridge University Press

We begin with $n = -1$. Let $w = (x, y^{-1})$. Then $xy^{-1} = (y^{-1}x)w$. Multiplying both sides on the left by y, $y(xy^{-1}) = y(y^{-1}x)w$, and so

$$(yx)y^{-1}(y, x, y^{-1})^{-1} = (yy^{-1})xw(y, y^{-1}, x)^{-1}.$$

Applying Lemma 2.4, we get $(yx)y^{-1}(y, x, y) = xw(y, y, x)$. Now multiply both sides by $y(y, y, x)$. We get $yx = (xy)w(y, y, x)^2$, so that $(y, x) = w(y, y, x)^2$ and so $(x, y^{-1}) = w = (y, x)(y, y, x)^{-2} = (x, y)^{-1}(y, x, y)^2 = (x, y)^{-1}(y, x, y)^{(-1)(-2)}$. Thus the result holds for $n = -1$.

Now let $n = -m$, and let $z = y^{-1}$, so that $z^m = y^{-m} = y^n$. Then, since $m > 0$, and using Lemma 2.4 and Corollary 2.7,

$$\begin{aligned}(x, z^m) &= (x, z)^m(z, x, z)^{m(m-1)} = (x, y^{-1})^m(y^{-1}, x, y^{-1})^{m(m-1)} \\ &= (x, y^{-1})^m(y, x, y)^{m(m-1)}.\end{aligned}$$

But we saw above that $(x, y^{-1}) = (x, y)^{-1}(y, x, y)^2$, so that

$$\begin{aligned}(x, y^n) = (x, z^m) &= (x, y)^{-m}(y, x, y)^{2m}(y, x, y)^{m(m-1)} \\ &= (x, y)^n(y, x, y)^{m(m+1)} = (x, y)^n(y, x, y)^{(-m)(-m-1)} \\ &= (x, y)^n(y, x, y)^{n(n-1)},\end{aligned}$$

as required. This proves the first identity.

For the second,

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

as required. ∎

Corollary 2.10 *For any $x, y \in B$ and any integers m and n,*

$$(x^m, y^n) = (x, y)^{mn}(x, x, y)^{mn(m-1)}(y, x, y)^{mn(n-1)}.$$

Proof By Lemma 2.9 and Lemma 2.4,

$$\begin{aligned}(x^m, y^n) &= (x^m, y)^n(y, x^m, y)^{n(n-1)} \\ &= [(x, y)^m(x, x, y)^{m(m-1)}]^n(y, x, y)^{mn(n-1)} \\ &= (x, y)^{mn}(x, x, y)^{mn(m-1)}(y, x, y)^{mn(n-1)}.\end{aligned}$$

∎

Lemma 2.11 *For any $x, y \in B$ and any integer n, $(xy^n, y) = (x, y)(y, x, y)^n$.*

https://doi.org/10.4153/CJM-2007-012-7 Published online by Cambridge University Press

Proof For $n = 0$, the result is obvious.

For $n > 0$, we again proceed by induction on n. We have

$$\begin{aligned}(xy)y &= [y(xy)](xy, y) = [(yx)y](xy, y)(y, x, y)^{-1}\\ &= [(xy)y](y, x)(xy, y)(y, x, y)^{-1},\end{aligned}$$

so $(y, x)(xy, y)(y, x, y)^{-1} = 1$, hence $(xy, y) = (y, x)^{-1}(y, x, y) = (x, y)(y, x, y)$ and the result holds for $n = 1$.

Suppose it holds for $n = k$, that is, $(xy^k, y) = (x, y)(y, x, y)^k$. Then using right alternativity, the result for $n = 1$, Lemma 2.3, and the induction hypothesis,

$$\begin{aligned}(xy^{k+1}, y) &= ([xy^k]y, y) = (xy^k, y)(y, xy^k, y)\\ &= (xy^k, y)(y, x, y) = (x, y)(y, x, y)^{k+1},\end{aligned}$$

as required.

For $n < 0$, say $n = -m$, $(x, y) = ([xy^n]y^m, y) = (xy^n, y)(y, xy^n, y)^m = (xy^n, y)(y, x, y)^m$, so $(xy^n, y) = (x, y)(y, x, y)^{-m} = (x, y)(y, x, y)^n$. ■

Lemma 2.12 *For all $x, y, z \in B$,*

$$\begin{aligned}(xz, y) &= (x, y)(z, y)(y, x, z)(x, z, y)^2,\\ (x, yz) &= (x, y)(x, z)(x, z, y)(y, x, z)^2.\end{aligned}$$

Proof We have

$$\begin{aligned}xz \cdot y &= (x \cdot zy)(x, z, y)\\ &= (x \cdot yz)(z, y)(x, z, y)\\ &= (xy \cdot z)(z, y)(x, z, y)(x, y, z)^{-1}\\ &= (xy \cdot z)(z, y)(x, z, y)^2 \qquad \text{by Lemma 2.2}\\ &= (yx \cdot z)(x, y)(z, y)(x, z, y)^2\\ &= (y \cdot xz)(x, y)(z, y)(y, x, z)(x, z, y)^2,\end{aligned}$$

which gives the first identity of the lemma. For the second identity,

$$\begin{aligned}(x, yz) &= (yz, x)^{-1} = [(y, x)(z, x)(x, y, z)(y, z, x)^2]^{-1}\\ &= (x, y)(x, z)(x, z, y)(y, x, z)^2,\end{aligned}$$

as required. ■

Theorem 2.13 *For any $x, y \in B$ and any integers m, n, p and q,*

$$(x^m y^n, x^p y^q) = (x, y)^{mq-np}(x, x, y)^r(y, y, x)^s,$$

where $r = (mq - np)(m + p - 1)$ and $s = (np - mq)(n + q - 1)$.

https://doi.org/10.4153/CJM-2007-012-7 Published online by Cambridge University Press

Proof By Lemma 2.12,

$$(x^m y^n, x^p y^q) = (x^m, x^p y^q)(y^n, x^p y^q)(x^p y^q, x^m, y^n)(x^m, y^n, x^p y^q)^2.$$

Applying Lemma 2.9 and Lemma 2.4, the right side becomes

$$(x, x^p y^q)^m (x, x, x^p y^q)^{m(m-1)} \cdot (y, x^p y^q)^n (y, y, x^p y^q)^{n(n-1)} (x^p y^q, x, y)^{mn} (x^m, y, x^p y^q)^{2n}.$$

By Lemma 2.3, this is equal to

$$(x, x^p y^q)^m (x, x, y^q)^{m(m-1)} (y, x^p y^q)^n (y, y, x^p)^{n(n-1)} (x^p y^q, x, y)^{mn} (x^m, y, x^p)^{2n}.$$

Now, using Lemma 2.4, this becomes

$$(x, x^p y^q)^m (x, x, y)^{qm(m-1)} (y, x^p y^q)^n (y, y, x)^{pn(n-1)} (x^p y^q, x, y)^{mn} (x^m, y, x)^{2pn}.$$

Application of Corollary 2.6 and Corollary 2.7 reduces this to

$$(x, x^p y^q)^m (x, x, y)^{qm(m-1)} \cdot (y, x^p y^q)^n (y, y, x)^{pn(n-1)} (x, x, y)^{pmn} (y, x, y)^{qmn} (x, y, x)^{2mpn}.$$

Collecting like terms, this becomes

$$(x, x^p y^q)^m (y, x^p y^q)^n (x, x, y)^{qm(m-1)-pmn} (y, y, x)^{pn(n-1)-qmn}.$$

We now apply the second identity in Lemma 2.12 together with right alternativity. We obtain

$$[(x, y^q)(x, y^q, x^p)(x^p, x, y^q)^2]^m \cdot [(y, x^p)(y, y^q, x^p)]^n (x, x, y)^{qm(m-1)-pmn} (y, y, x)^{pn(n-1)-qmn}.$$

Again applying Lemma 2.9 and Lemma 2.4, this becomes

$$[(x, y)^q (y, x, y)^{q(q-1)} (x, y, x)^{pq} (x^p, x, y)^{2q}]^m \cdot [(y, x)^p (x, y, x)^{p(p-1)} (y, y, x)^{pq}]^n (x, x, y)^{qm(m-1)-pmn} (y, y, x)^{pn(n-1)-qmn}.$$

Applying Corollary 2.7 and collecting like terms, we finally obtain

$$(x^m y^n, x^p y^q) = (x, y)^{mq-np} (x, x, y)^{(mq-np)(m+p-1)} (y, y, x)^{(np-mq)(n+q-1)},$$

as required. ∎

https://doi.org/10.4153/CJM-2007-012-7 Published online by Cambridge University Press

Theorem 2.14 *For any $x, y \in B$ and any integers m, n, p, and q,*

$$(x^m y^n)(x^p y^q) = x^{m+p} y^{q+n} (y,x)^{np} (x,x,y)^{-np(p-1)-mp(q+2n)} (y,y,x)^{np(n+q-1)}.$$

Proof Let $z = (x^m y^n)(x^p y^q)$. Then

$$\begin{aligned} zy^n &= x^m\{[y^n(x^p y^q)]y^n\} && \text{Bol identity} \\ &= x^m\{[(x^p y^q)y^n]y^n\}(y^n, x^p y^q) \\ &= x^m[x^p y^{q+2n}](x,y)^{-np}(x,x,y)^{-np(p-1)}(y,y,x)^{np(n+q-1)} \\ &&& \text{right power alternativity (twice) and Theorem 2.13} \\ &= x^{m+p} y^{q+2n}(y,x)^{np}(x,x,y)^{-np(p-1)}(y,y,x)^{np(n+q-1)}(x^m, x^p, y^{q+2n})^{-1} \\ &= x^{m+p} y^{q+2n}(y,x)^{np}(x,x,y)^{-np(p-1)-mp(q+2n)}(y,y,x)^{np(n+q-1)} \end{aligned}$$

using, at the last step, Lemma 2.4 and Corollary 2.7. Now multiply both sides of the equation on the right by y^{-n} to get the desired result. ∎

Theorem 2.15 *For any $x, y \in B$ and any integers m, n, p, q, r, and s,*

$$(x^m y^n, x^p y^q, x^r y^s) = (x,x,y)^{m(ps-qr)}(y,y,x)^{n(qr-ps)}.$$

Proof

$$\begin{aligned} &[(x^m y^n)(x^p y^q)](x^r y^s) \\ &\quad = (x^{m+p} y^{n+q})(x^r y^s)(y,x)^{np}(x,x,y)^{-np(p-1)-mp(q+2n)}(y,y,x)^{np(n+q-1)} \\ &\quad = (x^{m+p+r} y^{n+q+s})(y,x)^{np+nr+qr}(x,x,y)^{t}(y,y,x)^{u}, \end{aligned}$$

where $t = -np(p-1) - mp(q+2n) - (n+q)r(r-1) - (m+p)r(s+2(n+q))$ and $u = np(n+q-1) + (n+q)r(n+q+s-1)$.

Similarly,

$$\begin{aligned} &(x^m y^n)[(x^p y^q)(x^r y^s)] \\ &\quad = (x^m y^n)(x^{p+r} y^{q+s})(y,x)^{qr}(x,x,y)^{-qr(r-1)-pr(s+2q)}(y,y,x)^{qr(q+s-1)} \\ &\quad = (x^{m+p+r} y^{n+q+s})(y,x)^{np+nr+qr}(x,x,y)^{v}(y,y,x)^{w}. \end{aligned}$$

where $v = -qr(r-1) - pr(s+2q) - n(p+r)(p+r-1) - m(p+r)(q+s+2n)$ and $w = qr(q+s-1) + n(p+r)(n+q+s-1)$.

Cancelling common terms, we see that

$$(x^m y^n, x^p y^q, x^r y^s) = (x,x,y)^{t-v}(y,y,x)^{u-w},$$

https://doi.org/10.4153/CJM-2007-012-7 Published online by Cambridge University Press

where

$$\begin{aligned} t - v &= -np(p-1) - mp(q+2n) - (n+q)r(r-1) \\ &\quad - (m+p)r(s+2(n+q)) - [-qr(r-1) - pr(s+2q) \\ &\quad - n(p+r)(p+r-1) - m(p+r)(q+s+2n)] \\ &= m(ps-qr), \end{aligned}$$

and

$$\begin{aligned} u - w &= np(n+q-1) + (n+q)r(n+q+s-1) \\ &\quad - [qr(q+s-1) + n(p+r)(n+q+s-1)] \\ &= n(qr-ps). \end{aligned}$$

■

Before we conclude this section, we record two other interesting results:

Lemma 2.16 *For all $x, y, z \in B$, $(x, y, z)^2(y, z, x)^2(z, x, y)^2 = 1$.*

Proof Switching x and z in Lemma 2.12, we obtain

$$(zx, y) = (z, y)(x, y)(y, z, x)(z, x, y)^2.$$

But since $(xz, y) = (zx, y)$, setting the right-hand side of this last equation equal to the right-hand side of the equation in Lemma 2.12 and cancelling (x, y) and (z, y), we get $(y, z, x)(z, x, y)^2 = (y, x, z)(x, z, y)^2$. Bringing everything to the left-hand side of the equation and applying Lemma 2.2, we get the desired result. ■

Lemma 2.17 *For all $x, y, z \in B$, $(xz, y)(yx, z)(zy, x) = (x, z, y)(y, x, z)(z, y, x)$.*

Proof Using cyclic permutations of the variables in Lemma 2.12, we obtain

$$\begin{aligned} (xz, y) &= (x, y)(z, y)(y, x, z)(x, z, y)^2, \\ (yx, z) &= (y, z)(x, z)(z, y, x)(y, x, z)^2, \\ (zy, x) &= (z, x)(y, x)(x, z, y)(z, y, x)^2. \end{aligned}$$

Multiplying these together and cancelling commutators that are inverses of each other, we get $(xz, y)(yx, z)(zy, x) = (x, z, y)^3(y, x, z)^3(z, y, x)^3$. But, by Lemma 2.16, $(x, z, y)^2(y, x, z)^2(z, y, x)^2 = 1$, so the desired conclusion follows. ■

https://doi.org/10.4153/CJM-2007-012-7 Published online by Cambridge University Press

3 Centrality of Squares

In this section, B will represent a Bol loop which is centrally nilpotent of class 2 and in which the square of every associator is 1. As noted above, this condition is a generalization of the assumption that there is a unique nontrivial commutator, associator.

Applying the added condition that associators square to 1, Lemma 2.2 becomes

Corollary 3.1 *For all $x, y, z \in B$, $(x, z, y) = (x, y, z)$.*

The next theorem is interesting because Moufang loops with squares in the nucleus have appeared at various points in the literature. These so-called *extra* loops were first identified by F. Fenyves and later characterized as precisely those loops which satisfy the identity $(xy \cdot z)x = x(y \cdot zx)$ [CR].

Theorem 3.2 *For any $x \in B$, $x^2 \in N(B)$.*

Proof Let y and z be any elements of B. By Lemma 2.4 and Corollary 3.1, $(y, x^2, z) = (y, z, x^2) = (y, z, x)^2 = 1$, so $x^2 \in N_\mu(B) = N_\rho(B)$.

To see that $x^2 \in N_\lambda(B)$, put $y = x$ in Lemma 2.1. This gives $(x^2, z, w)(x, x, zw) = (x, x, z)(x, z, w)(x, xz, w)$. By Corollary 3.1 and Lemma 2.8,

$$\begin{aligned}(x, xz, w) &= (x, w, zx) = (x, w, z)(x, wz, x)(x, x, z)\\ &= (x, z, w)(x, x, wz)(x, x, z).\end{aligned}$$

Thus, $(x^2, z, w)(x, x, zw) = (x, x, z)^2(x, z, w)^2(x, x, wz) = (x, x, wz)$, and so $x^2 \in N_\lambda(B)$, as required. ∎

Corollary 3.3 *For any $x, y, z \in B$, and any integers m, n and r*

$$\begin{aligned}(x^m, y^n, z^r) &= \begin{cases} 1 & \text{if } mnr \equiv 0 \pmod 2 \\ (x, y, z) & \text{otherwise} \end{cases}\\ &= (x, y, z)^{mnr}.\end{aligned}$$

Proof Since squares are in the nucleus of B, it follows from equation (2.1) that we can reduce the exponents m, n and r modulo 2. The result is then obvious. ∎

We also obtain the following simplifications of results from Section 2.

Corollary 3.4 *For any $x, y \in B$ and any integers m, n, p and q,*

$$(x^m y^n, x^p y^q) = (x, y)^{mq-np}(x, x, y)^{mp(n+q)}(y, y, x)^{nq(m+p)}.$$

Proof By Theorem 2.13, $(x^m y^n, x^p y^q) = (x, y)^{qm-pn}(x, x, y)^r(y, y, x)^s$, where $r = (mq - np)(m + p - 1)$ and $s = (np - mq)(n + q - 1)$. But $m(m - 1)$ is even as is $p(p - 1)$, so modulo 2, $r \equiv mpq - npm \equiv mp(q - n) \equiv mp(n + q)$. Similarly, $s \equiv npq - mqn \equiv nq(p + m) \pmod 2$. ∎

https://doi.org/10.4153/CJM-2007-012-7 Published online by Cambridge University Press

Corollary 3.5 *For any $x, y \in B$ and any integers m, n, p and q,*

$$(x^m y^n)(x^p y^q) = x^{m+p} y^{q+n} (y,x)^{np} (x,x,y)^{mpq} (y,y,x)^{npq}.$$

Proof By Theorem 2.14,

$$(x^m y^n)(x^p y^q) = x^{m+p} y^{q+n} (y,x)^{np} (x,x,y)^{-np(p-1)-mp(q+2n)} (y,y,x)^{np(n+q-1)}.$$

But, again, $p(p-1) \equiv n(n-1) \equiv 0 \pmod 2$, and $-mp(q+2n) \equiv mpq \pmod 2$, so the result follows. ■

Turning our attention to commutators, we also get

Corollary 3.6 *For any $x, y \in B$ and any integers m and n, $(x^m, y^n) = (x,y)^{mn}$.*

Proof By Corollary 2.10, $(x^m, y^n) = (x,y)^{mn}(x,x,y)^{mn(m-1)}(y,x,y)^{mn(n-1)}$. But, for any integers m and n, both $m(m-1)$ and $n(n-1$ are even, and so

$$(x,x,y)^{mn(m-1)}(y,x,y)^{mn(n-1)} = 1.$$ ■

Corollary 3.7 *For all $x, y, z \in B$, $(xz, y) = (x,y)(z,y)(y,x,z)$.*

Proof Since $(x,z,y)^2 = 1$, this is an immediate consequence of Lemma 2.12. ■

If we now add the additional assumption that commutators also square to 1, that is, that B' is a central elementary Abelian 2-group, then we obtain

Theorem 3.8 *If B is a Bol loop with B' a central elementary Abelian 2-group, then squares are central in B. That is, for all $x \in B$, $x^2 \in \mathcal{Z}(B)$.*

Proof By Theorem 3.2, squares are in the nucleus. That they are in the centre follows from Corollary 3.6 and the fact that commutators have square 1. ■

It is extremely rare for the loop ring of a loop to satisfy any interesting identity other than associativity. For example, a commutative loop ring must be associative (with mild restrictions on characteristic) [Pa] and a right alternative loop ring must be alternative in characteristic different from 2 [Ku]. That loops exist with a loop ring that is right, but not left, alternative came to light only in 1994 [GR1]. Later, it was shown that one class of loops with this property are those Bol loops with a unique commutator/associator [GR2]. This suggests a further study of such loops. Here we offer one property.

Corollary 3.9 *If B is a Bol loop in which there is a unique nontrivial commutator/associator s, then squares are central in B.*

Proof By [GR1], s is central and $s^2 = 1$, so Theorem 3.8 applies. ■

https://doi.org/10.4153/CJM-2007-012-7 Published online by Cambridge University Press

4 Minimally Non-Moufang Bol Loops

We apply the results of Section 3 to investigate minimally non-Moufang Bol loops.

Theorem 4.1 *Let B be a finite Bol loop which is nilpotent of class two and in which all associators square to* 1.[2] *Suppose that B is minimally non-Moufang in the sense that it is not Moufang, but every proper subloop of B is Moufang. Then every proper subloop of B is associative.*

Proof Since B is Bol but not Moufang, it is not left alternative, that is, there exist elements $x, y \in B$ with $(x, x, y) \neq 1$. The subloop $\langle x, y\rangle$ generated by x and y is not Moufang, so it cannot be proper. Thus $B = \langle x, y\rangle$. In what follows, we will use $\mathcal{Z}$ for $\mathcal{Z}(B)$.

Since all commutators and associators of B are central, $B/\mathcal{Z}$ is an Abelian group that can be generated by two elements, (but not by one, else it is easy to see that B is a group). We have $B/\mathcal{Z} = \langle \mathcal{Z}x\rangle \times \langle \mathcal{Z}y\rangle$. Thus, every element of B can be represented in the form $zx^m y^n$, where $z \in \mathcal{Z}$.

If the result is false, there is a subloop K of B of minimal order which is Moufang, but not associative. Thus, there exist $a, b, c \in K$ with $(a, b, c) \neq 1$. Say $a = z_1 x^m y^n$, $b = z_2 x^p y^q$ and $c = z_3 x^r y^s$. By Theorem 2.15,

$$(a, b, c) = (x, x, y)^{m(ps-qr)}(y, y, x)^{n(qr-ps)}.$$

Since a, b and c do not associate, $(x, x, y)^{m(ps-qr)}(y, y, x)^{n(qr-ps)} \neq 1$. Then, since $(x, x, y)^2 = (y, y, x)^2 = 1$, we must have $ps - qr \equiv 1 \equiv qr - ps \pmod 2$ and $(a, b, c) = (x, x, y)^m (y, y, x)^n$.

Now, since K is Moufang, $(b, b, c) = 1$. But

$$\begin{aligned}(b, b, c) &= (x^p y^q, x^p y^q, x^r y^s) = (x, x, y)^{p(ps+qr)}(y, y, x)^{q(ps+qr)}\\ &= (x, x, y)^p (y, y, x)^q,\end{aligned}$$

so $(x, x, y)^p (y, y, x)^q = 1$. Similarly, $(c, b, c) = 1$, so

$$\begin{aligned}(c, b, c) &= (x^r y^s, x^p y^q, x^r y^s) = (x, x, y)^{r(ps+qr)}(y, y, x)^{s(ps+qr)}\\ &= (x, x, y)^r (y, y, x)^s,\end{aligned}$$

and $(x, x, y)^r (y, y, x)^s = 1$.

Thus $(x, x, y)^p = (y, y, x)^q$ and $(x, x, y)^r = (y, y, x)^s$. Since $(x, x, y)^2 = 1$, $(x, x, y)^p = 1$ or (x, x, y) (according as p is even or odd), and $(x, x, y)^r = 1$ or (x, x, y) (according as r is even or odd). Since $(x, x, y) \neq 1$, $(x, x, y)^p = 1 = (x, x, y)^r$ would imply that p and r are both even. But this is not possible, since $ps + qr \equiv 1 \pmod 2$. Suppose p is odd (the case where r is odd is analogous). Then, $(y, y, x)^q = (x, x, y)^p = (x, x, y) \neq 1$, so q is odd, $q \equiv p \pmod 2$, and $(y, y, x) = (x, x, y) \neq 1$. Now, since $(y, y, x)^s = (x, x, y)^r$, $s \equiv r \pmod 2$. But then $ps + qr \equiv ps + ps \equiv 0 \pmod 2$, a contradiction.

We have shown that no such K can exist; that is, every proper subloop of B is associative. ∎

[2] All we really need is that $(x, x, y)^2 = 1$ for all $x, y \in B$.

https://doi.org/10.4153/CJM-2007-012-7 Published online by Cambridge University Press

5 Two-Generator Bol Loops

As we have seen, an MNM Bol loop must be generated by two elements. In this section, we consider the structure of finite 2-generator Bol loops which are nilpotent of class two. If B is generated by x and y, then by Theorem 2.13 and Theorem 2.15, all commutators and associators in B can be expressed in the form $r^\alpha s^\beta t^\gamma$, where $r = (x, y)$, $s = (x, x, y)$ and $t = (y, y, x)$ are central. Thus every element in B can be expressed in the form $x^p y^q r^\alpha s^\beta t^\gamma$. Theorem 2.14 tells us how to multiply two such elements, so that multiplication in B is completely determined once we know $|x|$, $|y|$, $|r|$, $|s|$ and $|t|$. By Theorem 2.15, if we do not want B to be associative, then s and t cannot both be 1. Without loss of generality, we may assume that $s \neq 1$.

This observation forms the basis for the construction of a new class of Bol loops. The construction in the case that $r^2 = s^2 = t^2 = 1$ is described in [CG1].

References

[B] G. Bol, *Gewebe und Gruppen.* Math. Ann. **114**(1937), no. 1, 414–431.

[CG1] O. Chein and E. G. Goodaire, *A new construction of Bol loops of order 8k.* J. Algebra **287**(2005), no. 1, 103–122.

[CG2] ———, *Moufang loops with a unique nonidentity commutator (associator, square).* J. Algebra **130** (1990), no. 2, 369–384.

[CG3] ———, *Minimally nonassociative commutative Moufang loops.* Results Math. **39** (2001), no. 1-2, 11–17.

[CG4] ———, *Minimally nonassociative Moufang loops with a unique nonidentity commutator are ring alternative.* Comment. Math. Univ. Carolin. **43** (2002), no. 1, 1–8.

[CG5] ———, *Minimally nonassociative nilpotent Moufang loops.* J. Algebra **268** (2003), no. 1, 327–342.

[CR] O. Chein and D. A. Robinson, *An "extra" law for characterizing Moufang loops.* Proc. Amer. Math. Soc. **33** (1972), 29–32.

[G] E. G. Goodaire, *Units in right alternative loop rings.* Publ. Math. Debrecen **59** (2001), no. 3–4, 353–362.

[GR1] E. G. Goodaire and D. A. Robinson, *A class of loops with right alternative loop rings.* Comm. Algebra **22** (1995), no. 14, 5623–5634.

[GR2] ———, *A construction of loops which admit right alternative loop rings.* Results Math. **59** (1996), no. 1-2, 56–62.

[KO] M. J. Kallaher and T. G. Ostrom, *Fixed point free linear groups, rank three planes and Bol quasifields.* J. Algebra **18** (1971), 159–178.

[Ku] K. Kunen, *Alternative loop rings.* Comm. Algebra **26** (1998), no. 2, 557–564.

[MM] G. A. Miller and H. C. Moreno, *Non-abelian groups in which every subgroup is abelian.* Trans. Amer. Math. Soc. **4**(1903), no. 4, 398–404.

[Pa] L. J. Paige, *A theorem on commutative power associative loop algebras.* Proc. Amer. Math. Soc. **6**(1955), 279–280.

[Pf] H. O. Pflugfelder, *Quasigroups and Loops. Introduction.* Heldermann Verlag, Berlin, 1990.

[S] W. R. Scott, *Group Theory.* Prentice-Hall, Inc., 1964.

Temple University
Philadelphia, PA 19122
U.S.A.
e-mail: orin@temple.edu

Memorial University of Newfoundland
St. John's, NF
A1C 5S7
e-mail: edgar@math.mun.ca

https://doi.org/10.4153/CJM-2007-012-7 Published online by Cambridge University Press