Mathematical Proceedings of the Cambridge Philosophical Society

VOL. 84 NOVEMBER 1978 PART 3

Math. Proc. Camb. Phil. Soc. (1978), **84**, 377
Printed in Great Britain

Finite Bol loops

BY R. P. BURN
Homerton College, Cambridge

(*Received* 23 *December* 1977)

In this paper, we prove that, for any prime p, a Bol loop of order $2p$ or of order p^2 is necessarily a group, and we show that there exist exactly six non-associative Bol loops of order 8.

The author is indebted to his colleague, Stuart Plunkett, for checking, with a computer, that the sets of permutations obtained in Theorem 6 actually satisfy the conditions of Theorem 1.

For the definition of a loop, the reader should consult Bruck(4). In (1), Albert defines a right multiplication R_a as a permutation of a loop $(L, .)$,

$$R_a : x \to x.a.$$

We will call the set $\{R_a | a \in L\}$ the right regular representation of $(L, .)$ or briefly, the representation of L. When discussing loops of order 5 and 6 in (2), Albert uses the properties of a representation which we will name

PROPOSITION 1. *A set,* Π, *of permutations on a set* L *is the representation of a loop* $(L, .)$ *if and only if* (*a*) $1 \in \Pi$, (*b*) Π *is transitive on* L, (*c*) *if* $\alpha, \beta \in \Pi$, *and* $\alpha\beta^{-1}$ *fixes one element of* L, *then* $\alpha = \beta$.

A loop $(L, .)$ has a unique representation Π. However, a collection of permutations Π, satisfying the conditions of Proposition 1, is generally the representation of more than one loop, since Π does not determine the operation on L uniquely. In fact, if Π is given, exactly one operation on L is implied by each choice of identity in L. If $a, b \in L$, then Π is the right regular representation of $(L, .)$ if the operation . is defined by

$$a.b = aR_b,$$

where R_b is the unique element of Π mapping the identity in L to b.

https://doi.org/10.1017/S0305004100055213 Published online by Cambridge University Press

For any predetermined $a, b \in L$, a *principal isotope* $(L, \times)$ of a loop $(L, .)$ is defined by

$$x \times y = X . Y, \quad \text{where} \quad X . a = x \quad \text{and} \quad b . Y = y.$$

Now if $R_y^{\times}$ is a right multiplication of $(L, \times)$,

$$R_y^{\times} = R_a^{-1} R_Y.$$

This leads to

PROPOSITION 2. *If* $\{R_x | x \in L\}$ *is the representation of* $(L, .)$, *then the representation of any principal isotope of* $(L, .)$ *is* $\{R_a^{-1} R_x | x \in L\}$ *for some given* $a \in L$.

For a finite loop L of order n, there may be n^2 non-isomorphic principal isotopes. These n^2 loops have at most n distinct representations as the identity in the loop is not determined by the representation.

Clearly, a loop is a group if and only if its representation is closed under composition of permutations. An immediate consequence of Proposition 2, which was pointed out by Albert in (1), is that if one principal isotope of a loop $(L, .)$ is a group then the loop $(L, .)$ is an isomorphic group.

Definition. A loop $(L, .)$ is called a *Bol loop* if

$$[(a.b).c].b = a.[(b.c).b] \quad \text{for all} \quad a, b, c \in L.$$

As an immediate consequence of the definition we have

THEOREM 1. *If* Π *is the representation of a loop* L, *then* L *is a Bol loop if and only if* $\alpha, \beta \in \Pi$ *implies* $\alpha\beta\alpha \in \Pi$.

THEOREM 2. *If* Π *is the representation of a Bol loop and* $\alpha \in \Pi$, *then* $\alpha^n \in \Pi$ *for* $n \in Z$.

Proof. From Theorem 1, $\alpha . 1 . \alpha = \alpha^2 \in \Pi$, and $\alpha . \alpha . \alpha = \alpha^3 \in \Pi$, so by induction $\alpha^n \in \Pi$ for all positive n. Now if Π is the representation of a Bol loop $(L, .)$ with identity e, and if $\alpha = R_a$, L contains a unique element a' such that $a . a' = e$. Now, $eR_a R_{a'} R_a = a$, so, from Theorem 1, $R_a R_{a'} R_a = R_a$, and so $R_{a'} = R_a^{-1}$. Thus Π contains the inverse of each of its elements, and the proof is complete.

The property that a representation contains the inverses of each of its elements characterizes the representations of loops with the right inverse property, and this leads to a proof of the familiar characterization of Bol loops as those loops for which every principal isotope is a loop with the right inverse property ((7), theorem 3·1). For if $\alpha, \beta \in \Pi$, then, by Proposition 2, $\alpha^{-1}\beta$ belongs to the representation of a principal isotope. But, if this representation contains all its inverses, $(\alpha^{-1}\beta)^{-1} = \alpha^{-1}\gamma$ for some $\gamma \in \Pi$, and so $\alpha\beta^{-1}\alpha = \gamma$, and if this holds for all principal isotopes Π is the representation of a Bol loop. Conversely if Π is the representation of a Bol loop, then $\alpha, \beta, \gamma \in \Pi$ implies $\beta\alpha^{-1}\gamma\alpha^{-1}\beta \in \Pi$ and so the representation of the principal isotope containing $\alpha^{-1}\beta$ and $\alpha^{-1}\gamma$ also contains $(\alpha^{-1}\beta)\,(\alpha^{-1}\gamma)\,(\alpha^{-1}\beta)$ and so is the representation of a Bol loop.

THEOREM 3. *If* Π *is a representation of a finite Bol loop and* $\alpha \in \Pi$, *then* α *is a product of disjoint cycles of equal length.*

https://doi.org/10.1017/S0305004100055213 Published online by Cambridge University Press

Proof. If the shortest cycle in α is of length m, then α^m fixes at least m symbols. But by Theorem 2 and Proposition 1, $\alpha^m = 1$. So α consists wholly of m-cycles.

It is plain now that both the order of each element of Π and the number of disjoint cycles of which each element consists divide the order of the original loop.

COROLLARY 1. *The order of an element of a finite Bol loop divides the order of the loop.*

(This is a strengthened form of theorem V·1·2 in (4).)

COROLLARY 2. *A Bol loop of prime order is a cyclic group.*

Before tackling our main theorems, we establish a lemma.

LEMMA. *If R_a and R_b are right multiplications of a Bol loop and $R_a^2 = R_b^2 = 1$, then $R_a R_b = R_b R_a$ if and only if $aR_b = bR_a$.*

Proof. Let $1 = R_e$. If $R_a R_b = R_b R_a$, then $aR_b = aR_a R_b R_a = eR_b R_a = bR_a$. If $aR_b = bR_a$, then $aR_b = eR_b R_a = aR_a R_b R_a$, and so, by Theorem 1 and Proposition 1, $R_b = R_a R_b R_a$, and so $R_a R_b = R_b R_a$.

Since the statement of this lemma does not involve the identity in the loop, it implies that if α and β are two commuting elements of order 2 in the representation of a Bol loop, and $\alpha = (pq)(rs)\ldots$, then either $\beta = (pr)(qs)\ldots$ or $\beta = (ps)(qr)\ldots$, but, if α and β do not commute, then neither of these two possibilities for β can occur.

THEOREM 4. *If p is a prime number, then a Bol loop of order $2p$ is a group.*

Proof. Since any loop of order 4 is a group, we will only consider odd primes p. We will consider a Bol loop L with representation Π. If $\alpha \in \Pi$, from Theorem 3, the order of α is $1, 2, p$ or $2p$.

Case (i). Π *contains an element of order* $2p$. From Theorem 2, Π is the representation of a cyclic group of order $2p$.

Case (ii). Π *contains an element of order* p, *but no element of order* $2p$, If α is an element of order p in Π, then so are $\alpha^2, \alpha^3, \ldots, \alpha^{p-1}$. Each of these permutations consists of two p-cycles and the group generated by α has two orbits each of length p. If β is another element of order p in Π, then, since $p \geqslant 3$, each of the p-cycles which constitute β contains at least two symbols from the same orbit of $\langle\alpha\rangle$. Thus, for some integer k, $\alpha^k\beta^{-1}$ fixes a symbol, and so, from Proposition 1, $\alpha^k\beta^{-1}$ is the identity. This proves that Π contains exactly $p-1$ elements of order p.

The p elements of $\Pi \setminus \langle\alpha\rangle$ have order 2. Let γ be one such element. By Theorem 1, $\alpha\gamma\alpha \in \Pi$. If $\alpha\gamma\alpha \in \langle\alpha\rangle$, then $\gamma = \alpha^k$ for some integer k. Therefore $\alpha\gamma\alpha \in \Pi \setminus \langle\alpha\rangle$, and so is of order 2. Thus $(\alpha\gamma\alpha)^{-1} = \alpha\gamma\alpha$, and so $\gamma = \alpha^2\gamma\alpha^2$. Clearly $\gamma = \alpha^{2k}\gamma\alpha^{2k}$, but α is of odd order, so $\gamma = \alpha\gamma\alpha$, and so $\gamma = \alpha^n\gamma\alpha^n$ for all integers n. The $p-1$ distinct equations here determine γ uniquely from one of its transpositions, and since $\alpha^n\gamma = \gamma\alpha^{-n}$ the representation that we obtain is that of the dihedral group D_p.

Case (iii). Π *contains no element of order* p. Here Π consists of the identity and $2p-1$ elements of order 2. If α and β are elements of Π distinct from 1, then each consists of an odd number p of transpositions. If α and β are distinct, they may not commute, for if they did, by the lemma, they would have to have a transposition in common and

https://doi.org/10.1017/S0305004100055213 Published online by Cambridge University Press

this would contradict Proposition 1. Since $\alpha\beta = \alpha^{-1}\beta$, it belongs to a representation of a principally isotopic Bol loop by Proposition 2, and is therefore of order 1, 2, p or $2p$. The product $\alpha\beta$ may not have order 1 if α and β are distinct. The product $\alpha\beta$ may not have order 2 if α and β do not commute. So the product $\alpha\beta$ has order p or $2p$, but, in these cases, the loop L has a cyclic or dihedral group of order $2p$ as a principal isotope by cases (i) and (ii), and L itself is an isomorphic group.

THEOREM 5. *If p is a prime number, then a Bol loop of order p^2 is a group.*

Proof. Any loop of order 4 is a group, so we need only establish the theorem for odd primes p.

Let L be a Bol loop of order p^2 and let Π be its representation. From Theorem 3, every element of Π other than the identity is either a single cycle of length p^2 or else consists of p cycles of length p. If Π contains an element of order p^2, Π is a cyclic group by Theorem 2 and so L is a cyclic group.

If Π does not contain an element of order p^2, Π consists of the identity and p^2-1 elements of order p. In this case, by Theorem 1 and a theorem of Glauberman (theorem 15 in (6)), Π generates a p-group $\langle\Pi\rangle$ which has non-trivial centre. Let γ be an element of order p in the centre of this group, and let $\alpha \in \Pi$. If $x = x\gamma$, then $x\alpha = x\gamma\alpha = x\alpha\gamma$, so that, if γ fixes one element of L, $\gamma = 1$, since Π is transitive on L. Thus γ consists of p disjoint cycles of length p.

We now show that either $\alpha(\neq 1)$ and γ have the same orbits, or else the intersection of each orbit of α with an orbit of γ is a singleton.

If G is an orbit of γ and its p elements are not distributed with one each in each orbit of α, then at least two elements x and y (say) of G belong to the same orbit of α. Thus $x\gamma^i = y$ and $x\alpha^j = y$ for some i, j. In this case, $x(\gamma^i\alpha^{-j}) = x$, so $x(\gamma^i\alpha^{-j})^n = x$ for all integers n, and $x\gamma^{in} = x\alpha^{jn}$. Thus γ and α have an orbit in common. Now the p elements of any other orbit of γ are contained in $p-1$ orbits of α and so the same argument may be applied again. Thus the orbits of γ and the orbits of α are identical. The argument proves more, because we can choose n so that $jn \equiv 1 \pmod{p}$ and then $x\gamma^{in} = x\alpha$ and so each cycle of α is a power of a cycle of γ. By Proposition 1, there are at most $p-1$ elements of Π with this property, so that, for p^2-p elements of Π, the orbits have singleton intersection with the orbits of γ.

Let α be an element of Π with the same orbits as γ and let $\beta \in \Pi \setminus \langle\alpha\rangle$. We may label the elements of L and arrange the cycles of γ so that

$$\gamma = (a_1 b_1 c_1 \dots m_1)(a_2 b_2 c_2 \dots m_2) \dots (a_p b_p c_p \dots m_p),$$

and

$$\beta = (a_1 a_2 a_3 \dots a_p)(b_1 \dots)(c_1 \dots) \dots (m_1 \dots).$$

Then

$$b_1\beta^k = b_1\gamma^{-1}\beta^k\gamma = a_1\beta^k\gamma = a_{1+k}\gamma = b_{1+k}$$

and

$$c_1\beta^k = c_1\gamma^{-2}\beta^k\gamma^2 = a_1\beta^k\gamma^2 = a_{1+k}\gamma^2 = c_{1+k},$$

etc., with addition modulo p. So

$$\beta = (a_1 a_2 a_3 \dots a_p)(b_1 b_2 b_3 \dots b_p)(c_1 c_2 c_3 \dots c_p) \dots (m_1 m_2 m_3 \dots m_p).$$

Now

$$\alpha = (a_1 b_1 \dots m_1)^{k_1}(a_2 b_2 \dots m_2)^{k_2} \dots (a_p b_p \dots m_p)^{k_p}$$

https://doi.org/10.1017/S0305004100055213 Published online by Cambridge University Press

for some integers k_i, with $0 < k_i < p$. We now relabel the elements of L using the set $Z_p \times Z_p$ as follows:

$$a_i \to (i, 0),$$

$$b_i \to (i, 1),$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot$$

$$m_i \to (i, p-1).$$

Then $$\beta: (x, y) \to (x+1, y),$$

and $$\alpha: (x, y) \to (x, y + k_x),$$

so $$\beta^r \alpha^s \beta^r: (x, y) \to (x + 2r, y + sk_{x+r}),$$

and, since these p^2 permutations are distinct, they exhaust Π. Now

$$\alpha\beta^2\alpha: (x, y) \to (x+2, y + k_x + k_{x+2}),$$

and by Theorems 1 and 2, $\alpha\beta^2\alpha = \beta^r\alpha^s\beta^r$ for some r, s, and then

$$(x+2, y + k_x + k_{x+2}) = (x + 2r, y + sk_{x+r}) \quad \text{and} \quad r = 1.$$

For some s, $k_x + k_{x+2} = sk_{x+1}$ for all x. We may treat this as a recurrence relation for a sequence of integers with the condition $k_x \equiv k_{x+p} \pmod{p}$.

The auxiliary equation for this relation is $m^2 - sm + 1 = 0$. This has equal roots if and only if $s^2 = 4$. If $s = -2$, $m = -1$ and then $k_x = (Ax + B)(-1)^x$ for all x. But this contradicts $k_x \equiv k_{x+p}$ since p is odd, so $s \neq -2$. If $s = 2$, $m = 1$ and then

$$k_x = Ax + B.$$

Now $A \equiv 0$, since, if not, $k_{-B/A}$ (with $-B/A$ evaluated mod p) is zero and this is inadmissible. If $A \equiv 0$, k_x is constant. If the auxiliary equation has distinct roots, m_1, m_2, then $k_x = A(m_1)^x + B(m_2)^x$. But $m^p \equiv m \pmod{p}$ and so $k_{x+p-1} \equiv k_x \equiv k_{x+p}$, and again k_x is constant. In any case, the conditions imply that k_x is a constant function of x and this in turn makes α a power of γ. Therefore the group generated by α and β is precisely the group generated by γ and β, namely the elementary abelian group of order p^2. This completes the proof of Theorem 5.

Theorems 4 and 5 together with the previously known fact that Bol loops of prime order are cyclic groups establish that the smallest orders for which a non-associative Bol loop may occur are 8 and 12. Two non-associative Bol loops of order 8 have already appeared in the literature. Bol's paper (3) contains one due to Zassenhaus. Robinson (7) mentions Zassenhaus' loop and lists another. The theorem which follows incorporates an exhaustive search for Bol loops of order 8 and establishes that in addition to the groups there are exactly six non-isomorphic right Bol loops. In Theorem 6, Π_5 is the representation of Zassenhaus' loop and Π_6 is the representation of Robinson's loop. At least one non-associative Bol loop of order 12 exists, the smallest Moufang loop (5).

https://doi.org/10.1017/S0305004100055213 Published online by Cambridge University Press

THEOREM 6. *A Bol loop of order* 8 *which is not a group has one of the six following representations*:

Π_1
(1)
(1234) (5678)
(13) (24) (57) (68)
(1432) (5876)
(1537) (2648)
(1638) (2547)
(1735) (2846)
(1836) (2745)

Π_2
(1)
(1234) (5678)
(13) (24) (57) (68)
(1432) (5876)
(1537) (2648)
(16) (25) (38) (47)
(1735) (2846)
(18) (27) (36) (45)

Π_3
(1)
(1234)(5678)
(13) (24) (57) (68)
(1432) (5876)
(1537) (2846)
(16) (25) (38) (47)
(1735) (2648)
(18) (27) (36) (45)

Π_4
(1)
(1234) (5678)
(13) (24) (57) (68)
(1432) (5876)
(15) (26) (37) (48)
(16) (27) (38) (45)
(17) (28) (35) (46)
(18) (25) (36) (47)

Π_5
(1)
(1234) (5678)
(13) (24) (57) (68)
(1432) (5876)
(15) (26) (37) (48)
(16) (25) (38) (47)
(17) (28) (35) (46)
(18) (27) (36) (45)

Π_6
(1)
(12) (34) (56) (78)
(13) (25) (47) (68)
(14) (23) (58) (67)
(15) (26) (37) (48)
(16) (24) (38) (57)
(17) (28) (35) (46)
(18) (27) (36) (45)

Proof. If Π is the representation of a Bol loop of order 8, then, by Theorem 3, the elements of Π have order 1, 2, 4, or 8.

Case (i). Π *contains an element of order* 8. By Theorem 2, Π is the representation of the cyclic group C_8.

For the rest of the proof we will presume that Π is the representation of a Bol loop $\{1, 2, 3, 4, 5, 6, 7, 8\}$ containing no element of order 8. We denote the right multiplication mapping 1 to x by R_x. By Theorem 2, elements of order 4 occur in pairs in Π.

Case (ii). Π *contains six elements of order* 4. Let the six elements of order 4 be α, α^3, $\beta, \beta^3, \gamma, \gamma^3$. Since the square of any such element is of order 2, $\alpha^2 = \beta^2 = \gamma^2$ since Π contains 8 elements in all. Without loss of generality take $\alpha = R_2 = (1234)(5678)$, then $R_3 = \alpha^2$ and $R_4 = \alpha^3$. If $R_5 = (15ab)(\ldots)$, $R_5^2 = \alpha^2$ so $a = 3$ and $b = 7$. Moreover $R_5 = (1537)(2p4q)$, where $\{p, q\} = \{6, 8\}$. Now $R_7 = R_5^3 = (1735)(2q4p)$. The same argument also shows that $R_6 = (1638)(2x4y)$ and $R_8 = R_6^3 = (1836)(2y4x)$, where $\{x, y\} = \{5, 7\}$. The conditions on p, q, x and y may be met in four ways:

If $p = 8, q = 6, x = 5, y = 7$, Π is the regular representation of the quaternion group.

If $p = 6, q = 8, x = 5, y = 7$, Π is Π_1.

If $x = 7$ and $y = 5$, two further cases arise which are isomorphic to Π_1 under repeated conjugation by (13) (265) (487).

https://doi.org/10.1017/S0305004100055213 Published online by Cambridge University Press

Case (iii). Π *contains four elements of order* 4. Without loss of generality take

$$R_2 = (1234)(5678), \quad \text{then} \quad R_3 = R_2^2 \quad \text{and} \quad R_4 = R_2^3.$$

Again, without loss of generality, suppose R_5 is of order 4, $R_5 = (15ab)(\ldots)$. Since $R_5 R_x^{-1}$ has no fixed symbols for $x = 1, 2, 3$ or 4, $a = 2, 3$ or 4. Thus $R_5^2 = R_x$ for $x = 2, 3$ or 4 and in fact $R_5^2 = R_3$, so $R_5 = (1537)(2p4q)$, where $\{p, q\} = \{6, 8\}$. Also $R_7 = R_5^3$ and this is again of order 4. So R_6 and R_8 have order 2. To avoid $3R_6 R_x^{-1} = 3$ for $x \neq 6$, we must have $3R_6 = 8$ and similarly $3R_8 = 6$. So

$$R_6 = (16)(38)(2x)(4y) \quad \text{and} \quad R_8 = (18)(36)(2y)(4x).$$

The conditions $\{p, q\} = \{6, 8\}$ and $\{x, y\} = \{5, 7\}$ give just four cases.

If $p = 6, q = 8, x = 7, y = 5$, Π is the representation of the group $C_4 \times C_2$.

If $p = 6, q = 8, x = 5, y = 7$, then Π is Π_2.

If $p = 8, q = 6, x = 5, y = 7$, then Π is Π_3.

If $p = 8, q = 6, x = 7, y = 5$, then Π is isomorphic to Π_3 under conjugation by (15823764).

The representations Π_2 and Π_3 are not isomorphic, as the elements of order 4 in Π_2 commute with each other, while, in Π_3, $R_2 R_5 \neq R_5 R_2$.

Case (iv). Π *contains two elements of order* 4. Without loss of generality take

$$R_2 = (1234)(5678), \quad \text{then} \quad R_3 = R_2^2 \quad \text{and} \quad R_4 = R_2^3.$$

Since R_5 is of order 2, let $R_5 = (15)(2a)(3b)(4c)$. Now $5R_5 R_3 R_5 = b$, and $b = 6$, 7 or 8. So $R_5 R_3 R_5 = R_3$ and $b = 7$. Thus $R_5 = (15)(2a)(37)(4c)$, and a similar argument shows that $R_7 = (17)(2f)(35)(4g)$, so $\{a, c\} = \{f, g\} = \{6, 8\}$, and again that

$$R_6 = (16)(2x)(38)(4y) \quad \text{and} \quad R_8 = (18)(2y)(36)(4x).$$

The conditions $\{a, c\} = \{6, 8\}$ and $\{x, y\} = \{5, 7\}$ give just four cases.

If $a = 8, c = 6, x = 5, y = 7$, then Π is the representation of the dihedral group D_4.

If $a = 6, c = 8, x = 7, y = 5$, then Π is Π_4.

If $a = 6, c = 8, x = 5, y = 7$, then Π is Π_5.

If $a = 8, c = 6, x = 7, y = 5$, then Π is isomorphic to Π_5 under conjugation by (15263748).

The sets Π_4 and Π_5 are not isomorphic as all five elements of order 2 in Π_4 commute with the elements of order 4, while only three of the elements of order 2 in Π_5 do this.

Case (v). Π *contains seven elements of order* 2. If there are two elements in Π, distinct from each other and the identity, which commute with all elements of Π, let these be R_2 and R_3. Taking $R_2 = (12)(34)(56)(78)$, from the lemma $R_3 = (13)(24)(5a)(6b)$ and without loss of generality we may take $a = 7$ and $b = 8$. Now R_4 commutes with R_2 and R_3, so by the lemma $R_4 = (14)(23)(58)(67)$. Repeated use of the lemma gives R_5, R_6, R_7 and R_8 uniquely, so Π must be the regular representation of the group $C_2 \times C_2 \times C_2$, since this group is abelian and the representation has been completely determined by the supposition of commutativity.

We therefore know that, in any other Bol loop of this type, there cannot be more

https://doi.org/10.1017/S0305004100055213 Published online by Cambridge University Press

than one element, distinct from the identity, which commutes with all the others. We now suppose therefore that $R_2R_3 \neq R_3R_2$. Then if $R_2 = (12)(34)(56)(78)$,

$$R_3 = (13)(2x)(4y)(pq)$$

by the lemma. Since $\{5, 6\} \neq \{p, q\} \neq \{7, 8\}$, we may, without loss of generality, take $R_3 = (13)(25)(47)(68)$. Then

$$R_2R_3R_2 = (16)(24)(38)(57) = R_6 \quad \text{and} \quad R_3R_2R_3 = (17)(28)(35)(46) = R_7.$$

If we now suppose that $R_4R_2 = R_2R_4$, then $R_4 = (14)(23)(58)(67)$ using the lemma and considering the images of 5 under R_2 and R_6. Now

$$R_3R_4R_3 = (15)(26)(37)(48) = R_5$$

and the only transpositions remaining for R_8 are $(18)(27)(36)(45)$. Here Π is Π_6.

If on the other hand $R_4R_2 \neq R_2R_4$, then $R_4 = (14)(2x)(3y)(cd)$ by the lemma. By considering R_3, R_6 and R_7, neither x or y may be 5 or 8, so $(cd) = (58)$. If $x = 7$ and $y = 6$, $R_2R_4R_2(R_3R_4R_3)^{-1}$ fixes 1 and moves 2, which contradicts Proposition 1. Thus we must have $x = 6$ and $y = 7$, and now $R_2R_4R_2 = (15)(23)(48)(67) = R_5$ and the only transpositions remaining for R_8 are $(18)(27)(36)(45)$. In this case, Π is isomorphic to Π_6 under conjugation by $(132)(45)(678)$.

THEOREM 7. *If a representation of a loop is closed under conjugation by its own elements, then the loops derived from the representation by distinct choices of the identity are isomorphic.*

Proof. Let the loop $(L, .)$ with identity e have representation $\Pi = \{R_x | x \in L\}$, and the loop $(L, \times)$ with identity f have the same representation $\Pi = \{S_x | x \in L\}$. Under the conditions of the theorem,

$$fR_f^{-1}R_xR_f = x.f = fS_{x.f}$$

implies that

$$R_f^{-1}R_xR_f = S_{x.f}.$$

Now R_f is an isomorphism of $(L, .)$ onto $(L, \times)$ since

$$\begin{aligned} R_f : x.y &\to (x.y).f \\ &= eR_xR_yR_f \\ &= fR_f^{-1}R_xR_fR_f^{-1}R_yR_f \\ &= fS_{x.f}S_{y.f} \\ &= (x.f) \times (y.f). \end{aligned}$$

COROLLARY. *For each of the sets Π_i, $i = 1, 2, 3, 4, 5, 6$, listed in Theorem 6, the eight right Bol loops for which Π_i is the regular representation are isomorphic.*

Proof. When R_f is of order 2, the condition for a Bol loop in Theorem 1 is equivalent to the condition for isomorphic loops in Theorem 7. This establishes the corollary for Π_6.

https://doi.org/10.1017/S0305004100055213 Published online by Cambridge University Press

It remains to establish the result when R_f is of order 4. In Π_i, $i = 1, 2, 3, 4, 5$, the square of each element of order 4 is R_3, so

$$R_f^{-1} R_x R_f = R_f^{-2} R_f R_x R_f = R_3 R_f R_x R_f = R_3 R_y$$

for some y.

If R_y is the identity, $R_3 R_y = R_3$.

If R_y is of order 4, then $R_3 R_y = (R_y)^3$, and by Theorem 2 this completes the proof in the case of Π_1.

If R_y is of order 2, particular cases need to be checked.

In Π_2 and Π_3, we have $R_3 R_6 = R_8$ and $R_3 R_8 = R_6$.

In Π_4 and Π_5, we have $R_3 R_5 = R_7$, $R_3 R_6 = R_8$, $R_3 R_7 = R_5$ and $R_3 R_8 = R_6$. The proof is complete.

It is interesting to note that the loops with representations Π_1, Π_3 and Π_4 in Theorem 6 are pairwise principal isotopes, as are the loops with representations Π_2, Π_5 and Π_6.

REFERENCES

(1) Albert, A. A. Quasigroups I. *Trans. Amer. Math. Soc.* **54** (1943), 507–519.
(2) Albert, A. A. Quasigroups II. *Trans. Amer. Math. Soc.* **55** (1944), 401–419.
(3) Bol, G. Gewebe und Gruppen. *Math. Ann.* **114** (1937), 414–431.
(4) Bruck, R. H. *A survey of binary systems* (Berlin, Springer–Verlag, 1958).
(5) Chein, O. and Pflugfelder, H. O. The smallest Moufang loop. *Arch. Math.* **22** (1971), 573–576.
(6) Glauberman, G. On loops of odd order II. *J. Algebra* **8** (1968), 393–414.
(7) Robinson, D. A. Bol loops. *Trans. Amer. Math. Soc.* **123** (1966), 341–354.

https://doi.org/10.1017/S0305004100055213 Published online by Cambridge University Press

https://doi.org/10.1017/S0305004100055213 Published online by Cambridge University Press