The structure of extra loops

Michael K. Kinyon and Kenneth Kunen

Abstract

The Sylow theorems hold for finite extra loops, as does P. Hall's theorem for finite solvable extra loops. Every finite nonassociative extra loop Q has a nontrivial center, $Z(Q)$. Furthermore, $Q/Z(Q)$ is a group whenever $|Q| < 512$. Loop extensions are used to construct an infinite nonassociative extra loop with a trivial center and a nonassociative extra loop Q of order 512 such that $Q/Z(Q)$ is nonassociative. There are exactly 16 nonassociative extra loops of order $16p$ for each odd prime p.

1. Introduction

Definition 1.1. A loop Q is an *extra loop* iff Q is both conjugacy closed (a CC-loop) and a Moufang loop.

Lemma 1.2. A loop Q is an extra loop iff Q satisfies one (equivalently all) of the following equations:
1. $(x \cdot yz) \cdot y = xy \cdot zy$.
2. $yz \cdot yx = y \cdot (zy \cdot x)$.
3. $(xy \cdot z) \cdot x = x \cdot (y \cdot zx)$.

Extra loops were first introduced via these equations by Fenyves [11, 12], who proved the equivalence of (1)(2)(3). Goodaire and Robinson [18] showed that Definition 1.1 is equivalent, and this definition is often more useful in practice, since one may combine results in the literature on CC-loops and on Moufang loops to prove theorems about extra loops.

Moufang loops are discussed in standard texts [3, 4, 24] on loop theory. In particular, these loops are diassociative by Moufang's Theorem.

2000 Mathematics Subject Classification:20N05
Keywords:extra loop, Moufang loop, conjugacy closed loop
The second author was partially supported by NSF Grant DMS-0097881

CC-loops were introduced by Goodaire and Robinson [17, 18], and independently (with different terminology) by Сойкис [26]. Further discussion can be found in [9, 10, 20, 21].

If Q is an extra loop and $N = N(Q)$ is the nucleus of Q, then N is a normal subloop of Q and Q/N is a boolean group (see Fenyves [12]). Besides leading to the result of Chein and Robinson that extra loops are exactly those Moufang loops with squares in the nucleus [8], Fenyves's result suggests that one might provide a detailed structure theory for finite extra loops. A start on such a theory was made in [20], where it was shown that if Q is a finite nonassociative extra loop, then $|N|$ is even and $|Q : N| \geqslant 8$, so that $16 \mid |Q|$. The five nonassociative Moufang loops of order 16 are all extra loops (see Chein [5], p. 49). Among these five is the Cayley loop (1845), which is the oldest known example of a nonassociative loop.

The Cayley loop is usually described by starting with the octonion ring ($\mathbb{R}^8$), and restricting the multiplication to $\{\pm e_i : 0 \leqslant i \leqslant 7\}$, where the e_i are the standard basis vectors. Restricting to $\mathbb{R}^8\backslash\{0\}$ or to S^7 does not yield an extra loop (it is Moufang, but not CC). In fact, by Nagy and Strambach ([23], Corollary 2.5, p. 1043), there are no nonassociative connected smooth extra loops. There are also no nonassociative connected compact extra loops, since Q/N is boolean, and hence totally disconnected.

The main results of this paper are listed in the abstract. After we review basic facts about extra loops in §, we characterize the nuclei of nonassociative extra loops in §. The Sylow theorems are proved in §, and P. Hall's theorem is proved in §. The center is discussed in §. In §, we consider loop extensions and describe the two examples mentioned in the abstract. In § we analyze the nonassociative extra loops of order $16p$, for p an odd prime, and show that the number of such loops is independent of p; it follows that this number is 16, since by [16], there are 16 such loops of order 48.

2. Basic facts

We collect some facts from the literature. In particular, we point out that an extra loop yields four boolean groups which help elucidate the loop structure. One is the quotient by the nucleus:

Lemma 2.1. Let Q be an extra loop with nucleus $N = N(Q)$.

1. For each $x \in Q$, $x^2 \in N$.

2. Q/N is a boolean group.

3. Every finite subloop of Q of odd order is contained in N.

4. Every element of Q of finite odd order is contained in N.

The lemma, particularly (1), is due to Fenyves [12]. Considered as a Moufang or CC-loop, an extra loop has a normal nucleus, so (2) follows from (1) and the fact that a Moufang or CC-loop of exponent 2 is a boolean group. (3) follows from (2) (since $Q \to Q/N$ maps the subloop to $\{1\}$), and (4) follows from (3).

Corollary 2.2. Every finite extra loop has the Lagrange property; that is, the order of every subloop divides the order of the loop.

This follows from the fact that Q/N is a group, so that both Q/N and N have the Lagrange property; see Bruck [4], §V.2, Lemma 2.1. This corollary holds for all CC-loops Q, because Basarab [2] has shown that Q/N is an abelian group; see also [20] for an exposition of Basarab's proof, and see [9] for related results.

Another boolean group is generated by the associators:

Definition 2.3. For x, y, z in a loop Q, define the *associator* $(x, y, z) \in Q$ by $(x \cdot yz)(x, y, z) = xy \cdot z$. Let $A(Q)$ be the subloop of Q generated by all the associators.

In an extra loop Q, $A(Q) \leqslant N(Q)$, since $Q/N(Q)$ is a group. Furthermore, by §5 of [20], we have:

Lemma 2.4. In any extra loop Q:

1. (x, y, z) is invariant under all permutations of the set $\{x, y, z\}$.

2. $(x, y, z) = (ux, vy, wz)$ for all $x, y, z \in Q$ and $u, v, w \in N(Q)$.

3. $(x, y, z) = (x^{-1}, y, z)$.

4. (x, y, z) commutes with each of x, y, z.

5. $A(Q) \leqslant Z(N(Q))$ and $A(Q)$ is a boolean group.

Note that Lemma 2.4 shows that the associator (x, y, z) determines a totally symmetric mapping from $(Q/N)^3$ into $A(Q)$.

If $|Q| < 512$, then Theorem 6.6 will show that $A(Q) \leqslant Z(Q)$ (equivalently, $Q/Z(Q)$ is a group); this fails for some Q of order 512; see Example . For any finite nonassociative extra loop, $|Z(Q) \cap A(Q)| \geqslant 2$ (see Theorem 6.1).

The properties we have listed for associators actually characterize extra loops:

Lemma 2.5. Suppose that Q is a loop with the following properties:

1. Q is flexible, that is, $(x, y, x) = 1$ for all $x, y \in Q$.
2. Every associator is in the nucleus.
3. The square of every associator is 1.
4. (x, y, z) is invariant under all permutations of {x,y,z}.
5. (x, y, z) commutes with each of x, y, z.

Then Q is an extra loop.

Proof. $x\cdot[y\cdot zx] = x\cdot yz\cdot x\cdot(y,z,x) = [xy\cdot z](x,y,z)x(y,z,x) = [xy\cdot z]\cdot x$. □

The third boolean group is the right inner mapping group, which turns out in this case to coincide with the left inner mapping group (see 2.7(5) below). We use the following notation.

Definition 2.6. For any loop Q, the *left translations* L_x and *right translations* R_y are defined by: $xy = xR_y = yL_x$. The *right* and *left multiplication groups* are, respectively

$$\mathrm{RMlt} = \mathrm{RMlt}(Q) = \langle R_y : y \in Q\rangle \quad \text{and} \quad \mathrm{LMlt} = \mathrm{LMlt}(Q) = \langle L_x : x \in Q\rangle.$$

For $S \subset Q$, set $R(S) := \{R_x : x \in S\}$. The *right* and *left inner mapping groups* are, respectively,

$$\begin{aligned} \mathrm{RMlt}_1 &= \mathrm{RMlt}_1(Q) = \{g \in \mathrm{RMlt} : 1g = 1\} \ \text{ and} \\ \mathrm{LMlt}_1 &= \mathrm{LMlt}_1(Q) = \{g \in \mathrm{LMlt} : 1g = 1\}. \end{aligned}$$

Also for $x, y \in Q$, define

$$R(x,y) := R_x R_y R_{xy}^{-1} \qquad \text{and} \qquad L(x,y) := L_x L_y L_{yx}^{-1}.$$

It is easily seen that $R(x,y) \in \mathrm{RMlt}_1$ and that RMlt_1 is the group generated by $\{R(x,y) : x, y \in Q\}$; likewise for the $L(x,y)$ and LMlt_1.

Lemma 2.7. For any extra loop Q:

1. All permutations in RMlt_1 and LMlt_1 are automorphisms of Q.
2. $R(x,y)R(u,v) = R(u,v)R(x,y)$.

3. $L(x, y) = R(x, y) = L(y, x) = R(y, x)$
4. $R(x, y)^2 = I$.
5. $\mathrm{RMlt}_1 = \mathrm{LMlt}_1$ is a boolean group.
6. $zR(x, y) = z(x, y, z)$.

(1) is due to Goodaire and Robinson [17], and (2),(3) are from [20]; these are true for all CC-loops. (4) is also from [20], and (5) is immediate from (2),(3),(4). Also, [20] shows that $zL(y, x) = z(x, y, z)^{-1}$ holds in all CC-loops, so (6) follows, using (3) and Lemma 2.4.

Besides the left and right inner mappings, we have the middle inner mappings $T_x = R_x L_x^{-1}$. In any CC-loop, the group generated by the middle inner mappings coincides with the group generated by all inner mappings [9].

Lemma 2.8. In any extra loop Q with $N = N(Q)$ and $A = A(Q)$:

1. $T_a \in \mathrm{Aut}(Q)$ iff $a \in N(Q)$.
2. For each $x \in Q$, $\mathcal{T}(x) := T_x{\restriction}N \in \mathrm{Aut}(N)$.
3. $\mathcal{T} : Q \to \mathrm{Aut}(N)$ is a homomorphism.
4. Each T_x maps A onto A, so that $A \trianglelefteq Q$ and Q/A is a group.
5. Each $(T_x)^2$ is the identity on A.

(1) is from [9], and holds for all CC-loops. (2) is due to Goodaire and Robinson [17], and (3) is from [21]. Both are true for all CC-loops. $(A)T_x = A$ is due to Fook [13], and is true for all Moufang loops; see also Lemma 6.2 below. Note that by the remark preceding the lemma, to prove that A is normal, it is sufficient to show that $(A)T_x = A$. (5) follows from (3) and (4), since $x^2 \in N$, so T_{x^2} is the identity on A by Lemma 2.4.

Our last boolean group is related to two of the others. In an extra loop Q with $A = A(Q)$, set

$$A^* := \{g \in \mathrm{RMlt} : xg \in Ax,\ \forall x \in Q\}$$

Note that this subgroup of RMlt is the kernel of the natural homomorphism $\mathrm{RMlt}(Q) \to \mathrm{RMlt}(Q/A); g \mapsto (Ax \mapsto Axg)$, and so $A^* \trianglelefteq \mathrm{RMlt}(Q)$.

Lemma 2.9. Let Q be an extra loop. Then $A^* = \mathrm{RMlt}_1(Q) \cdot R(A)$, a direct product. Hence A^* is a boolean group.

Proof. Obviously $R(A) \leqslant A^*$, and conversely, if $R_a \in A^*$, then $a \in A$. By Lemma 2.7(6), $\mathrm{RMlt}_1 \leqslant A^*$. If $g \in A^*$, write $g = hR_a$ for $h \in \mathrm{RMlt}_1$, $a = 1g$. Since $h \in A^*$, $R_a \in A^*$, and so $A^* = \mathrm{RMlt}_1 \cdot R(A)$. Since $A \leqslant N(Q)$ and $\mathrm{RMlt}_1 \leqslant \mathrm{Aut}(Q)$, the product $\mathrm{RMlt}_1 \cdot R(A)$ is direct. Since $A \leqslant N(Q)$, $R(A)$ is a boolean group (an isomorphic copy of A), and so A^* is a boolean group by Lemma 2.7(5). □

3. The nucleus

We describe which groups can be nuclei of nonassociative extra loops.

Proposition 3.1. For a group G, the following are equivalent:

1. $Z(G)$ contains an element of order 2.
2. There is a nonassociative extra loop Q with $G = N(Q)$.
3. There is an extra loop Q with $G = N(Q)$, $|Q : G| = 8$, and $Z(Q) = Z(G)$.

Proof. (2) → (1) is by Lemma 2.4. Now, assume (1) and we shall prove (3). Fix $-1 \in Z(G)$ of order 2, and let $C = \{\pm 1, \pm e_1 \cdots \pm e_7\}$ be the 16-element Cayley loop. In the extra loop $G \times C$, let $M = \{(1,1), (-1,-1)\}$. Note that M is a normal subloop. Let $Q = (G \times C)/M$. □

4. Sylow Theorems

We begin by remarking that for extra loops, two possible definitions of "p-loop" are equivalent. For Moufang loops, the following result is due to Glauberman and Wright [14, 15]. It also holds for power-associative CC-loops, as follows easily from ([20], Coro. 3.2, 3.4).

Lemma 4.1. If Q is a finite extra loop and p is a prime, then the following are equivalent:

1. $|Q|$ is a power of p.
2. The order of every element of Q is a power of p.

Definition 4.2. Let π be a set of primes. A finite loop Q is a *π-loop* if the set of prime factors of $|Q|$ is a subset of π. If $|Q|$ has prime factorization $|Q| = \Pi_p p^{i_p}$, then a *Hall π-subloop* of Q is a subloop of order $\Pi_{p\in\pi} p^{i_p}$. If

$\pi = \{p\}$, than a Hall π-subloop is called a *Sylow p-subloop*. Let $\mathrm{Syl}_p(Q)$ denote the set of all Sylow p-subloops of Q, and let $\mathrm{Hall}_\pi(Q)$ denote the set of all Hall π-subloops of Q.

Of course, in general, Sylow p-subloops and Hall π-subloops need not exist. But for extra loops, Sylow p-subloops do exist and satisfy the familiar Sylow Theorems for groups (Theorem 4.5 below). In §, we will show that Hall π-subloops exist for solvable extra loops and satisfy P. Hall's Theorem for groups (Theorem 5.3). As a preliminary to both theorems:

Lemma 4.3. Let π be a set of primes with $2 \in \pi$, and let Q be a finite extra loop with $A = A(Q)$.

1. If P is a Hall π-subloop of Q, then $A \leqslant P$.
2. If G is a Hall π-subgroup of $\mathrm{RMlt}(Q)$, then $A^* \leqslant G$.

Proof. Since $A \trianglelefteq Q$ and is a boolean group, AP is a subloop of Q of order $|A||P|/|A \cap P|$, and so AP is a π-subloop of Q. By the Lagrange property (Corollary 2.2), Hall π-subloops are maximal π-subloops, and so $AP = P$, establishing (1). The proof for (2) is similar. □

Next we need a minor refinement of the Sylow Theorems for groups. For a finite group G, let $O^p(G)$ denote the subgroup generated by all elements of order prime to p ([1], p. 5). Note that $O^p(G) \trianglelefteq G$.

Lemma 4.4. Assume that G is a finite group, p is prime, and $P, Q \in \mathrm{Syl}_p(G)$. Then $Q = x^{-1}Px$ for some $x \in O^p(G)$.

Proof. If $|G| = p^m j$, where $p \nmid j$, then $|O^p(G)| = p^\ell j$, where $0 \leqslant \ell \leqslant m$. Also $|P \cap O^p(G)| = p^\ell$, since $P \cap O^p(G) \in \mathrm{Syl}_p(O^p(G))$ ([1], (6.4)). Thus $|P \cdot O^p(G)| = |P||O^p(G)|/|P \cap O^p(G)| = p^m j = |G|$, and so $G = P \cdot O^p(G)$. Finally, by the usual Sylow Theorem, let $Q = y^{-1}Py$, where $y = ux$, with $u \in P$ and $x \in O^p(G)$. But then $Q = x^{-1}Px$. □

Theorem 4.5. Suppose that Q is a finite extra loop and $|N(Q)| = p^m r$, where p is prime and $p \nmid r$. Then

1. $|\mathrm{Syl}_p(Q)| = 1 + kp$, where $1 + kp \mid r$.
2. If S is a p-subloop of Q, then there exists $P \in \mathrm{Syl}_p(Q)$ containing S.
3. If $P_1, P_2 \in \mathrm{Syl}_p(Q)$, then there exists $x \in N(Q)$ such that $P_1 T_x = P_2$, so that P_1 and P_2 are isomorphic.

Proof. For $p > 2$: By Lemma 2.1(3), every p-subloop is contained in N, so the Sylow Theorems for groups can be applied to N.

For $p = 2$: The natural homomorphism $[\cdot] : Q \to Q/A; x \mapsto [x]$ yields a map $[\cdot] : P \mapsto P/A$ from the set of 2-subloops P of Q with $A \leqslant P$ to the set of 2-subgroups of Q/A. If $P/A \in \mathrm{Syl}_2(Q/A)$, then $P \in \mathrm{Syl}_2(Q)$, and so by Lemma 4.3, $[\cdot]$ yields a $1-1$ correspondence between $\mathrm{Syl}_2(Q)$ and $\mathrm{Syl}_2(Q/A)$. One can now apply the Sylow Theorems to the group Q/A. To get $x \in N(Q)$ in (3), we apply Lemma 4.4 to Q/A to get $P_1T_x = P_2$, where $[x] \in O^2(Q/A)$. Now $x = x_1 \cdots x_n$ where the order of each $[x_i]$, say t_i, is odd. Then $x_i = a_i z_i$, where $a_i = x_i^{t_i} \in A$ and $z_i = x_i^{1-t_i} \in N$ since $1 - t_i$ is even. Thus each $x_i \in N$, and so $x \in N$. Finally, that P_1 and P_2 are isomorphic follows from Lemma 2.8(1). □

Next we relate the Sylow p-subloops of an extra loop Q to the Sylow p-subgroups of the right multiplication group $\mathrm{RMlt}(Q)$.

Theorem 4.6. Let Q be an extra loop with $\mathrm{RMlt} = \mathrm{RMlt}(Q)$.

1. If $g \in \mathrm{RMlt}$ has odd order, then $g = R_a$ for some $a \in N(Q)$.
2. $O^2(\mathrm{RMlt}) \leqslant R(N(Q))$.
3. Each subgroup of RMlt of odd order is isomorphic to a subgroup of $N(Q)$.
4. $S \mapsto R(S)$ is a $1-1$ correspondence between the subloops of Q of odd order and the subgroups of RMlt of odd order.

Proof. For $g \in \mathrm{RMlt}$, write (uniquely) $g = hR_a$, where $a = 1g$ and $h \in \mathrm{RMlt}_1$. Note that $hR_ah = R_{ah}$ because $h \in \mathrm{Aut}(Q)$ and $h^2 = I$ (Lemma 2.7(1)(5)). From this plus induction, $g^{2k} = (R_{ah}R_a)^k$ and $g^{2k+1} = hR_a(R_{ah}R_a)^k$ for $k \geqslant 0$. Now, the Moufang identity $R_xR_yR_x = R_{xyx}$ plus induction yields $R_x(R_yR_x)^k = R_{x(yx)^k}$. Thus, $g^{2k+1} = hR_u$, where $u = a \cdot (ah \cdot a)^k$. If $g^{2k+1} = I$ then $h = I$ and $1 = u = a^{2k+1}$, so $a \in N(Q)$ by Lemma 2.1(4). This establishes (1), and the rest follows from (1) and Lemma 2.1(3). □

Theorem 4.7. Let Q be an extra loop. Then $P \mapsto \mathrm{RMlt}_1 \cdot R(P)$ is a $1 - 1$ correspondence between the 2-subloops of Q containing A and the 2-subgroups of $\mathrm{RMlt}(Q)$ containing A^*.

Note that in the theorem, $\mathrm{RMlt}_1 \cdot R(P)$ is not a direct product of subgroups, but is rather a factorization of a group into a subgroup and a subset. The multiplication in this group is given by $hR_a \cdot kR_b = hkR(ak, b)R_{ak\cdot b}$.

Proof. If $A \leqslant P \leqslant Q$, then certainly $A^* \leqslant \mathrm{RMlt}_1 \cdot R(P)$ by Lemma 2.9. Conversely, suppose G is a 2-subgroup of RMlt with $A^* \leqslant G$, and set $P = 1G$, the orbit of G through $1 \in Q$. Each $g \in G$ can be uniquely written as $g = hR_a$ for some $h \in \mathrm{RMlt}_1$, $a = 1g \in P$, and since $\mathrm{RMlt}_1 \leqslant G$, we have $G = \mathrm{RMlt}_1 \cdot R(P)$. $|P|$ is a power of 2, so what remains is to show that P is a subloop. For $a, b \in P$, $R_aR_b = R(a,b)R_{ab}$, and so $ab \in P$ as $R(a,b) \leqslant G$. Similarly, $a \in P$ implies $a^{-1} \in P$, which completes the proof. □

Corollary 4.8. Let Q be a finite extra loop, and let p be a prime. Then $\mathrm{Syl}_p(Q)$ is in a $1-1$ correspondence with $\mathrm{Syl}_p(\mathrm{RMlt}(Q))$.

Proof. If $p > 2$, then Theorem 4.6 yields that $P \mapsto R(P)$ is a $1-1$ correspondence between $\mathrm{Syl}_p(Q)$ and $\mathrm{Syl}_p(\mathrm{RMlt})$.

If $p = 2$, then Theorem 4.7 and Lemma 4.3(2) yield that $P \mapsto \mathrm{RMlt}_1 \cdot R(P)$ is a $1-1$ correspondence between $\mathrm{Syl}_p(Q)$ and $\mathrm{Syl}_p(\mathrm{RMlt})$. □

5. Solvability and Hall π-subloops

Recall that a loop Q is *solvable* if there exists a normal series

$$1 = Q_0 \trianglelefteq Q_1 \trianglelefteq \cdots \trianglelefteq Q_m = Q$$

of subloops Q_i such that each factor Q_{i+1}/Q_i is an abelian group.

Theorem 5.1. An extra loop Q is solvable if and only if $N = N(Q)$ is solvable.

Proof. Since solvability is inherited by subloops, the solvability of Q implies the solvability of N. Conversely, if $1 = N_0 \trianglelefteq \cdots \trianglelefteq N_m = N$ is a normal series for N, then $1 = N_0 \trianglelefteq \cdots \trianglelefteq N_m \trianglelefteq Q$ is a normal series for Q, since Q/N is an abelian group. □

By Proposition 3.1 and the fact that the nucleus of a nonassociative extra loop has index at least 8, the smallest nonsolvable nonassociative extra loop has order 960.

Corollary 5.2. Let Q be an extra loop of order p^aq^b, where p, q are primes. Then Q is solvable.

Proof. Since $|N(Q)| = p^cq^d$, the result follows from Burnside's p^aq^b-Theorem for groups ([1], (35.13)) and Theorem 5.1. □

This theorem and its corollary actually hold for CC-loops Q because Q/N is an abelian group by Basarab [2] (or see [9, 20]). However, the Sylow theorems and P. Hall's Theorem (cf. [1], (18.5)) can fail in CC-loops, since the 6-element nonassociative CC-loop does not have a subloop of order 2. P. Hall's Theorem for extra loops is:

Theorem 5.3. Let Q be a finite solvable extra loop and π a set of primes. Then

1. Q has a Hall π-subloop.
2. If $P_1, P_2 \in \mathrm{Hall}_\pi(Q)$, then there exists $x \in Q$ such that $P_1 T_x = P_2$.
3. Any π-subloop of Q is contained in some Hall π-subloop of Q.

The proof is similar to that of the Sylow Theorem 4.5.

Proof. For $2 \notin \pi$: If S is any π-subloop of Q, then the natural homomorphism $Q \to Q/N$ takes S onto a π-subloop of a boolean group, so that $S \leqslant N$.

The result then follows from P. Hall's Theorem applied to the solvable group N (Theorem 5.1).

For $2 \in \pi$: The natural homomorphism $[\cdot] : Q \to Q/A$ yields a map $[\cdot] : P \mapsto P/A$ from the set of π-subloops P of Q with $A \leqslant P$ to the set of π-subgroups of Q/A. If $P/A \in \mathrm{Hall}_\pi(Q/A)$, then $P \in \mathrm{Hall}_\pi(Q)$, and so by Lemma 4.3, $[\cdot]$ restricts to a $1-1$ correspondence between $\mathrm{Hall}_\pi(Q)$ and $\mathrm{Hall}_\pi(Q/A)$. Now apply P. Hall's Theorem to the solvable group Q/A. □

6. The center

Theorem 6.1. If Q is a nonassociative extra loop and $A(Q)$ is finite, then $|Z(Q) \cap A(Q)| > 1$.

Proof. Applying Lemma 2.8, define $\mathcal{T}' : Q \to \mathrm{Aut}(A)$ by $\mathcal{T}'(x) = T_x{\restriction}A$. By Lemma 2.4, $\mathcal{T}'(x) = I$ for $x \in N$. Thus, via $\mathcal{T}'$, the boolean group Q/N acts on the boolean group A. Since $|A|$ is even and the size of each orbit is a power of 2, there must be some $a \in A\backslash\{1\}$ which is fixed by this action. Then $a \in Z(Q)$. □

This can fail when $A(Q)$ is infinite; see Example .

Lemma 6.2. In an extra loop,

$$(x, y, zt) = (x, y, tz) = (x, y, z) \cdot (x, y, t)T_z = (x, y, z)T_t \cdot (x, y, t).$$

Proof. Applying Lemma 2.7, we have $zR(x,y) = z(x,y,z)$, $tR(x,y) = t(x,y,t)$, and $zR(x,y) \cdot tR(x,y) = (zt)R(x,y) = zt \cdot (x,y,zt)$, so

$$z(x,y,z) \cdot t(x,y,t) = zt \cdot (x,y,zt) \quad .$$

Since associators are in the nucleus, we get $(x,y,z)T_t \cdot (x,y,t) = (x,y,zt)$. Also, $(x,y,tz) = (x,y,zt)$ by Lemma 2.4, since Q/N is abelian> Therefore $tz \in Nzt$. □

Since $(x,y,t)T_z = (x,y,z) \cdot (x,y,zt)$, we have, in the case of extra loops, another proof of Fook's result (Lemma 2.8.3) that $(A)T_z = A$. Lemma 6.2 yields:

Lemma 6.3. In an extra loop, z commutes with (x,y,t) iff t commutes with (x,y,z) iff $(x,y,z)(x,y,t) = (x,y,zt)$.

Lemma 6.4. If Q is an extra loop, with $a = (x,y,z)$, then
$a \in Z(\langle \{x,y,z\} \cup N \rangle)$, and $A(\langle \{x,y,z\} \cup N \rangle) = \{1,a\}$.

Proof. $a \in N$ implies that T_a is an automorphism of Q (Lemma 2.8), so that $\{s \in Q : sa = as\}$ is a subloop of Q, and this subloop contains all elements of $\{x,y,z\} \cup N$ by Lemma 2.4, which also implies that $(u,v,w) \in \{1,a\}$ for all $u,v,w \in \{x,y,z\} \cup N$. Then $A(\langle \{x,y,z\} \cup N \rangle) \subseteq \{1,a\}$ follows by using Lemma 6.2. □

Lemma 6.5. If Q is an extra loop, then $|A(Q) : A(Q) \cap Z(Q)| \notin \{2,4,8\}$.

Proof. Set $Z = A(Q) \cap Z(Q)$, and define $\mathcal{T}' : Q \to \mathrm{Aut}(A)$, as in the proof of Theorem 6.1. Assume that $|A : Z| > 1$. Fix $e_1, e_2, e_3 \in Q$ with $(e_1,e_2,e_3) \notin Z$, and then fix $e_4 \in Q$ such that $(e_1,e_2,e_3)\mathcal{T}'(e_4) \neq (e_1,e_2,e_3)$. Define

$$q_1 := (e_2,e_3,e_4) \quad q_2 := (e_1,e_3,e_4) \quad q_3 := (e_1,e_2,e_4) \quad q_4 := (e_1,e_2,e_3).$$

By Lemmas 6.3 and 2.4, $q_i\mathcal{T}'(e_j) = q_i$ iff $j \neq i$. Now, let $q_S = \prod_{i \in S} q_i$ for $S \subseteq \{1,2,3,4\}$, and observe that $q_S\mathcal{T}'(e_j) = q_S$ iff $j \notin S$, so that the q_S are all in distinct cosets of Z. Thus, $|A : Z| \geqslant 16$. □

Theorem 6.6. If Q is a finite extra loop with some associator not contained in $Z(Q)$, then $|A(Q)| \geqslant 32$ and $|Q : N(Q)| \geqslant 16$, so that $512 \mid |Q|$.

Proof. $|Q : N| \geqslant 16$ follows from Lemma 6.4. $|A(Q) \cap Z(Q)| \geqslant 2$ follows from Theorem 6.1, so $|A(Q)| \geqslant 32$ follows from Lemma 6.5, so $512 \mid |Q|$. □

The "512" is best possible; see Example . The construction there is suggested by the proof of Lemma 6.5. We shall get $A(Q) = N(Q) = \langle q_0, q_1, q_2, q_3, q_4 \rangle$, of order 32, $Q/N = \langle [e_1], [e_2], [e_3], [e_4] \rangle$, of order 16, and $Z(Q) = \{1, q_0\}$.

7. Extension

Say we are given an abelian group $(G,+)$ and a boolean group $(B,+)$, and we wish to construct all extra loops Q such that $G \trianglelefteq Q$, $G \leqslant N(Q)$, and $Q/G \cong B$. We may view this as an extension problem; see [7] §II.3, p. 35.

Assuming that we already have Q, let $\pi : Q \to B$ be the natural quotient map. By the Axiom of Choice, we can assume that B is a section; that is, B is a subset of Q and $\pi \restriction B$ is the identity function. Then for $a, b \in B$, we have the loop product $a \cdot b$ from Q and the abelian group sum $a + b \in B$. Since $a \cdot b$ and $a + b$ are in the same left coset of G, there is a function $\psi : B \times B \to G$ with $a \cdot b = (a+b)\psi(a,b)$. We may assume that the identity element of B is the 1 of Q, so that $\psi(1,a) = \psi(a,1) = 1$. Each $T_a \restriction G \in \mathrm{Aut}(G)$. Also, the map $x \mapsto T_x \restriction G$ is a homomorphism from Q to $\mathrm{Aut}(G)$, and is the identity map on G (since G is abelian), so it defines a homomorphism: $B \to \mathrm{Aut}(G)$. Every element of Q is in some left coset of G, so it can be expressed uniquely in the form au, with $a \in B$ and $u \in G$. Since $G \leqslant N(Q)$, we can compute the product of two elements of this form as $au \cdot bv = ab \cdot uT_b v = (a+b) \cdot \psi(a,b)(uT_b)v$. In particular, for $b \in B$, $b^2 = b \cdot b = (b+b) \cdot \psi(b,b) = \psi(b,b)$.

Turning this around, and converting to additive notation,

Definition 7.1. Suppose we are given:

1. An abelian group $(G,+)$ and a boolean group $(B,+)$.
2. A map $\psi : B \times B \to G$ with $\psi(0,a) = \psi(a,0) = 0$.
3. A homomorphism, $a \mapsto \tau_a$, from B to $\mathrm{Aut}(G)$.

Then $B \ltimes^{\psi}_{\tau} G$ denotes the set $B \times G$ given the product operation:

$$(a,u) \cdot (b,v) = (a+b,\ \psi(a,b) + u\tau_b + v).$$

$B \ltimes_{\tau} G$ denotes $B \ltimes^{\psi}_{\tau} G$ in the case that $\psi(a,b) = 0$ for all a, b.

Then $B \ltimes_{\tau} G$ is a group, and is the usual semidirect product.

Lemma 7.2. $B \ltimes^{\psi}_{\tau} G$ is always a loop with identity element $(0,0)$. The map $u \mapsto (0,u)$ is an isomorphism from G onto $\{0\} \times G \trianglelefteq B \ltimes^{\psi}_{\tau} G$.

Proof. We can solve the equations $(a,u) \cdot (b,v) = (c,w)$ for (b,v) or (a,u):

$$(a,u)\backslash(c,w) = (a+c,\ w - \psi(a,a+c) - u\tau_a\tau_c)$$
$$(c,w)/(b,v) = (b+c,\ w\tau_b - \psi(b+c,b)\tau_b - v\tau_b).$$

Here, we have simplified the expression using the facts that B is boolean and the map $b \mapsto \tau_b$ is a homomorphism. This proves that $B \ltimes_\tau^\psi G$ is a loop. $\{0\} \times G$ is a normal subloop because the map $(a, u) \mapsto a$ is a homomorphism. □

It is fairly easy to calculate, in terms of ψ and τ, what is required for $B \ltimes_\tau^\psi G$ to satisfy various properties, such as the inverse property, the Moufang law, etc. In the case of extra loops, we shall use the conditions of Lemma 2.5 on the associators; some of these conditions can be verified immediately:

Lemma 7.3. Let $Q = B \ltimes_\tau^\psi G$. Then $A(Q) \leqslant \{0\} \times G \leqslant N(Q)$.

Proof. To compute the associators, we solve:

$$[(a,u) \cdot (b,v)(c,w)] \;\cdot\; \big((a,u),(b,v),(c,w)\big) \;=\; (a,u)(b,v) \cdot (c,w).$$

First, we compute both associations:

$$\begin{aligned}
(a,u) \cdot (b,v)(c,w) &= (a,u)(b+c,\ \psi(b,c) + v\tau_c + w) \\
&= (a+b+c,\ \psi(a,b+c) + u\tau_b\tau_c + \psi(b,c) + v\tau_c + w) \\
(a,u)(b,v) \cdot (c,w) &= (a+b,\ \psi(a,b) + u\tau_b + v) \cdot (c,w) \\
&= (a+b+c,\ \psi(a+b,c) + \psi(a,b)\tau_c + u\tau_b\tau_c + v\tau_c + w).
\end{aligned}$$

So,

$$\big((a,u),(b,v),(c,w)\big) \;=\; \big(0,\ \psi(a+b,c) + \psi(a,b)\tau_c - \psi(a,b+c) - \psi(b,c)\big).$$

Observe that this depends only on a, b, c, and has value 0 if any of a, b, c are 0, so that $\{0\} \times G \leqslant N(Q)$, and all $(x, y, z) \in \{0\} \times G$. □

We now consider in more detail the case when both B and G are boolean. We shall in fact start with τ and the desired associator map $\alpha : B^3 \to G$, where $\big(0, \alpha(a,b,c)\big)$ denotes the intended value of $\big((a,u),(b,v),(c,w)\big)$ for some (any) $u, v, w \in G$. We plan to construct ψ from α and τ. This is useful because α is determined by its values on a basis for B. We need to assume some conditions on α suggested by Lemmas 6.2 and 2.4:

Lemma 7.4. Suppose that G and B are boolean groups and E is a basis for B. Let $\tau \in \mathrm{Hom}(B, \mathrm{Aut}(G))$, and assume that $\alpha : E^3 \to G$ satisfies the equations:

H1. $(\alpha(a_1, b, c))\tau_{a_2} + \alpha(a_2, b, c) = \alpha(a_1, b, c) + (\alpha(a_2, b, c))\tau_{a_1}$,

H2. $(\alpha(a, b_1, c))\tau_{b_2} + \alpha(a, b_2, c) = \alpha(a, b_1, c) + (\alpha(a, b_2, c))\tau_{b_1}$,

H3. $(\alpha(a, b, c_1))\tau_{c_2} + \alpha(a, b, c_2) = \alpha(a, b, c_1) + (\alpha(a, b, c_2))\tau_{c_1}$,

F1. $(\alpha(a, b, c))\tau_a = \alpha(a, b, c)$,

F2. $(\alpha(a, b, c))\tau_b = \alpha(a, b, c)$,

F3. $(\alpha(a, b, c))\tau_c = \alpha(a, b, c)$.

Then α extends uniquely to a map $\overline{\alpha} : B^3 \to G$ satisfying these same equations for all elements of B, together with

P1. $\overline{\alpha}(a_1 + a_2, b, c) = (\overline{\alpha}(a_1, b, c))\tau_{a_2} + \overline{\alpha}(a_2, b, c)$,

P2. $\overline{\alpha}(a, b_1 + b_2, c) = (\overline{\alpha}(a, b_1, c))\tau_{b_2} + \overline{\alpha}(a, b_2, c)$,

P3. $\overline{\alpha}(a, b, c_1 + c_2) = (\overline{\alpha}(a, b, c_1))\tau_{c_2} + \overline{\alpha}(a, b, c_2)$.

If α is symmetric, then the same holds for $\overline{\alpha}$. If in addition, α satisfies $\alpha(a, a, b) = 0$ for all $a, b \in E$, then $\overline{\alpha}(a, a, b) = 0$ for all $a, b \in B$.

Proof. First, fix $a, b \in E$, and consider the map $\varphi : E \to B \ltimes_\tau G$ defined by $\varphi(c) = (c, \alpha(a, b, c))$. H3 says that $\varphi(c_1)\varphi(c_2) = \varphi(c_2)\varphi(c_1)$, and F3 says that each $(\varphi(c))^2 = 1$. It follows that φ extends uniquely to a homomorphism $\varphi' : B \to B \ltimes_\tau G$; then $\varphi'(c) = (c, \alpha'(a, b, c))$.

Doing this for every $a, b \in E$, we get $\alpha' : E \times E \times B \to G$, which is the unique extension of α satisfying H3,F3,P3. But then it is easily seen that α' satisfies H1,H2,F1,F2 also. α' is computed inductively using P3; the purpose of φ was just to prove that this computation yields a well-defined function.

Repeating this on the second coordinate yields $\alpha'' : E \times B \times B \to G$, which is the unique extension of α satisfying H2,H3,F2,F3,P2,P3. Doing it again yields $\overline{\alpha}$.

If α is symmetric, then the symmetry of $\overline{\alpha}$ follows from the uniqueness of $\overline{\alpha}$. Finally, assume in addition that $\alpha(a, a, b) = 0$ holds on E. First, for each $e \in E$, note that $\{b \in B : \overline{\alpha}(e, e, b) = 0\}$ is a subgroup of B, so that $\overline{\alpha}(e, e, b) = 0$ for all $b \in B$. Then, for each fixed $b \in B$, $\{a \in B : \overline{\alpha}(a, a, b) = 0\}$ is a also a subgroup, so that $\overline{\alpha}(a, a, b)$ for all $a, b \in B$. □

We now analyze the special case that in $Q = B \ltimes_\tau^\psi G$, the elements of $E \times \{0\}$ all have order 2 and all commute with each other. We can then use α to compute the correct ψ. Observe first:

Lemma 7.5. In an extra loop Q, suppose that the elements $x_1, x_2, \ldots, x_n$ all pairwise commute. Let π be a permutation of the set $\{1, 2, \ldots, n\}$. Then $x_1 \cdot x_2 \cdot \cdots \cdot x_n = x_{\pi(1)} \cdot x_{\pi(2)} \cdot \cdots \cdot x_{\pi(n)}$, where both products are right-associated.

Proof. It is sufficient to prove $x \cdot yz = y \cdot xz$ when $xy = yx$, and this follows by $x \cdot yz = xy \cdot z \cdot (x, y, z) = yx \cdot z \cdot (x, y, z) = y \cdot xz$. □

Thus, if the elements of $E \times \{0\}$ all commute, then the value of a right-associated product from $E \times \{0\}$ must be independent of the order in which that product is taken. This will simplify the form of ψ. If the elements of $E \times \{0\}$ also have order 2 in Q, then it is easy to say what properties α must satisfy:

Theorem 7.6. Suppose that we are given boolean groups G and B, with $E \subset B$ a basis for B. Suppose that we also have $\tau \in \mathrm{Hom}(B, \mathrm{Aut}(G))$ and a map $\alpha : E^3 \to G$ satisfying:

1. α is invariant under permutations of its arguments,
2. $\alpha(e_1, e_1, e_2) = 0$,
3. $(\alpha(e_1, e_2, e_3))\tau_{e_4} + \alpha(e_1, e_2, e_4) = \alpha(e_1, e_2, e_3) + (\alpha(e_1, e_2, e_4))\tau_{e_3}$.

Then there is a unique $\psi : B \times B \to G$ satisfying:

a. $\psi(0, a) = \psi(a, 0) = 0$ for all $a \in B$,

b. $Q := B \ltimes_\tau^\psi G$ is an extra loop,

c. In Q, whenever $e_1, e_2, e_3 \in E$, we have

$$(e_1, 0) \cdot (e_1, 0) = 0, \quad (e_1, 0) \cdot (e_2, 0) = (e_2, 0) \cdot (e_1, 0),$$

and the associator $\big((e_1, 0), (e_2, 0), (e_3, 0)\big) = \big(0, \alpha(e_1, e_2, e_3)\big)$,

d. $\psi(e, b) = 0$ whenever $e \in E$.

Condition (d) expresses the intent that the elements of the section be right-associated products from E.

Proof. Note that (1 – 3) implies that $(\alpha(e_1, e_2, e_3))\tau_{e_1} = \alpha(e_1, e_2, e_3)$.

By Lemma 7.4, α extends uniquely to a symmetric map $\overline{\alpha} : B^3 \to G$ satisfying the conditions Hi, Fi, Pi there. For the uniqueness part of the theorem, we note that assuming that $B \ltimes_\tau^\psi G$ is an extra loop, this $\overline{\alpha}$ must indeed yield the associator; that is, by condition (c) and Lemma 6.2, we have:

$$\big((a,u),(b,v),(c,w)\big) = \big(0, \overline{\alpha}(a,b,c)\big).$$

Then, by the computation in the proof of Lemma 7.3, we get:

$$\overline{\alpha}(a,b,c) = \psi(a+b,c) + \psi(a,b)\tau_c + \psi(a,b+c) + \psi(b,c).$$

Consider the case where $a = e \in E$. Then condition (d) implies that $\psi(e,b) = \psi(e,b{+}c) = 0$, so we get $\psi(e{+}b,c) = \psi(b,c){+}\overline{\alpha}(e,b,c)$. Repeating this, we see that for $e_1,\dots,e_n \in E$,

$$\psi(e_1 + \cdots + e_n, c) \ = \ \sum_{j=1}^{n} \overline{\alpha}\big(e_j,\ \sum_{k<j} e_k,\ c\big). \tag{$*$}$$

For example,

$$\begin{aligned} \psi(e_1+e_2,c) &= \overline{\alpha}(e_2,e_1,c) \\ \psi(e_1+e_2+e_3,c) &= \overline{\alpha}(e_2,e_1,c) + \overline{\alpha}(e_3,e_1+e_2,c) = \\ &\qquad \overline{\alpha}(e_2,e_1,c) + (\overline{\alpha}(e_3,e_1,c))\tau_{e_2} + \overline{\alpha}(e_3,e_2,c) \end{aligned}$$

This proves the uniqueness of ψ. To prove existence, one can take $(*)$ as a definition of ψ (after proving that it is well-defined), and then prove that it yields an extra loop with the correct associators.

To prove that it is well-defined, fix c and define, $\Psi_n = \Psi_n^{(c)} : E^n \to B$ for $n \geqslant 1$ so that

$$\begin{aligned} \Psi_1(e) &= 0. \\ \Psi_{n+1}(e_0,e_1,\dots,e_n) &= \Psi_n(e_1,\dots,e_n) + \overline{\alpha}(e_0, e_1+\cdots+e_n, c). \end{aligned}$$

It is easy to see that $\Psi_2(e,e) = 0$ and $\Psi_{n+2}(e,e,e_1,\dots,e_n) = \Psi_n(e_1,\dots,e_n)$. We need to prove that each Ψ_n is invariant under permutations of its arguments. Then, it will be unambiguous to define $\psi(e_1+\cdots+e_n,c) = \Psi_n^{(c)}(e_1,\dots,e_n)$. To prove invariance under permutations, we induct on n; for the induction step, it is sufficient to prove that $\Psi_{n+2}(e,e',e_1,\dots,e_n) = \Psi_{n+2}(e',e,e_1,\dots,e_n)$, and this follows from the fact that

$$\begin{aligned} \overline{\alpha}(e,e'+b,c) + \overline{\alpha}(e',b,c) &= (\overline{\alpha}(e,e',c))\tau_b + \overline{\alpha}(e,b,c) + \overline{\alpha}(e',b,c) \\ &= \overline{\alpha}(e',e+b,c) + \overline{\alpha}(e,b,c). \end{aligned}$$

Now that we have ψ defined, we need to check that our given $\overline{\alpha}(a,b,c)$ is really the true associator. Use $\big(0,(a,b,c)\big)$ to denote $\big((a,u),(b,v),(c,w)\big)$ for some (any) $u,v,w \in G$; then, as in the proof of Lemma 7.3,

$$(a,b,c) = \psi(a+b,c) + \psi(a,b)\tau_c + \psi(a,b+c) + \psi(b,c).$$

We prove $\overline{\alpha}(a,b,c) = (a,b,c)$ by induction on the number of basis elements needed to add up to a. If $a = 0$, then $\overline{\alpha}(a,b,c) = (a,b,c) = 0$. For the induction step, note that $\overline{\alpha}(e+a,b,c) - \overline{\alpha}(a,b,c) = \overline{\alpha}(e,b,c)\tau_a$, which is the same as $(e+a,b,c) - (a,b,c)$, since using $\psi(e+b,c) = \psi(b,c) + \overline{\alpha}(e,b,c)$, we get:

$$(e+a,b,c) - (a,b,c) = \overline{\alpha}(e,a+b,c) + \overline{\alpha}(e,a,b)\tau_c + \overline{\alpha}(e,a,b+c) =$$

$$\overline{\alpha}(e,b,c)\tau_a + \overline{\alpha}(e,a,c) + \overline{\alpha}(e,a,b)\tau_c + \overline{\alpha}(e,a,b)\tau_c + \overline{\alpha}(e,a,c) = \overline{\alpha}(e,b,c)\tau_a\,.$$

Now that we have identified $\overline{\alpha}(a,b,c)$ as the associator, it is easy to prove that Q is an extra loop by verifying the conditions in Lemma 2.5. (2) and (3) are clear from Lemma 7.3. (1) (Q is flexible) holds because $\overline{\alpha}(a,b,a) = 0$, and (4) holds because $\overline{\alpha}$ is symmetric. For (5), we must check that $\big(0,\overline{\alpha}(a,b,c)\big)$ commutes with (a,u), and this follows from the fact that $(\overline{\alpha}(a,b,c))\tau_a = \overline{\alpha}(a,b,c)$. □

We now describe three examples.

If $|G| = 2$ and $|B| = 8$ (so $E = \{e_1,e_2,e_3\}$), there is only one nonassociative option. $\alpha(e_1,e_2,e_3)$ must be the non-identity element of G, and each τ_x must be I. This extra loop of order 16 is the opposite extreme from the Cayley loop (where the elements outside the nucleus have order 4 and anticommute).

Example 7.7. There is an extra loop Q of order 512 such that $Q/Z(Q)$ is nonassociative.

Proof. Let $E = \{e_1,e_2,e_3,e_4\}$ and $G = \langle q_0,q_1,q_2,q_3,q_4\rangle$, so that $|Q| = 512$. Define τ so that $q_0\tau_{e_k} = q_0$ and $q_j\tau_{e_k} = q_j + \delta_{j,k}q_0$ for $j,k \in \{1,2,3,4\}$; then $Z(Q)$ will be $\{(0,0),(q_0,0)\}$. Define α so that $\alpha(e_i,e_j,e_k) = q_\ell$ whenever $i,j,k,\ell \in \{1,2,3,4\}$ are distinct. □

The ψ of this example was first found using McCune's program Mace4 [22], and the abstract discussion of this section was then obtained by reverse engineering.

Example 7.8. There is an infinite nonassociative extra loop Q with $Z(Q) = \{1\}$.

Proof. Let B be any infinite boolean group, and we use a wreath product construction. B acts on $(\mathbb{Z}_2)^B$ by permuting the indices; that is, for $u : B \to \mathbb{Z}_2$, let $((u)\tau_a)(b) = u(a+b)$. Let $G = \{u \in (\mathbb{Z}_2)^B : |u^{-1}\{1\}| < \aleph_0\}$; so G is a direct sum of $|B|$ copies of $\mathbb{Z}_2$ (and is hence isomorphic to B, since $\dim(B) = |B|$). Since B is infinite, $B \ltimes_\tau G$ (and hence also $B \ltimes_\tau^\psi G$) will have trivial center.

Let E be a basis for B. For $e_1, e_2, e_3 \in E$, let $\alpha(e_1, e_2, e_3) = 0$ unless e_1, e_2, e_3 are distinct, in which case $\alpha(e_1, e_2, e_3)$ is the element of $G \leqslant (\mathbb{Z}_2)^B$ which is 1 on the 8 members of $\langle e_1, e_2, e_3\rangle$ and 0 elsewhere. To verify condition (3), we let $u = (\alpha(e_1, e_2, e_3))\tau_{e_4} + \alpha(e_1, e_2, e_4)$ and let $v = \alpha(e_1, e_2, e_3) + (\alpha(e_1, e_2, e_4))\tau_{e_3}$, and consider cases: If $e_1 = e_2$, then $u = v = 0$, so assume that $e_1 \neq e_2$. If $e_3 \in \{e_1, e_2\}$, then $u = v = \alpha(e_1, e_2, e_4)$, and if $e_4 \in \{e_1, e_2\}$, then $u = v = \alpha(e_1, e_2, e_3)$, so assume also that $\{e_3, e_4\} \cap \{e_1, e_2\} = \emptyset$. If $e_3 = e_4$ then $u = v = 0$. In the remaining case, e_1, e_2, e_3, e_4 are all distinct; then both u, v are 1 on the 16 members of $\langle e_1, e_2, e_3, e_4\rangle$ and 0 elsewhere. □

8. Semidirect Products

The loop $B \ltimes_\tau^\psi G$ from Definition 7.1 is not really a semidirect product, since it need not contain an isomorphic copy of B. If we delete the ψ, we get a true semidirect product. Following Robinson [25]:

Definition 8.1. Let B, G be loops, and assume that $\tau \in \mathrm{Hom}(B, \mathrm{Aut}(G))$. Then $B \ltimes_\tau G$ denotes the set $B \times G$ given the product operation:

$$(a, u) \cdot (b, v) = (ab,\ (u)\tau_b \cdot v).$$

We write $B \ltimes G$ when τ is clear from context.

It is easily verified that $B \ltimes G$ is a loop, with identity element $(1, 1)$, but $B \ltimes G$ need not inherit all the properties satisfied by B and G. The general situation for extra loops was discussed in [25]. Here, we consider only an easy special case:

Lemma 8.2. Assume that $\tau \in \mathrm{Hom}(B, \mathrm{Aut}(G))$, B is an extra loop, and G is a group. Then $B \ltimes_\tau G$ is an extra loop, and the inverse is given by $(a, u)^{-1} = (a^{-1}, (u^{-1})\tau_{a^{-1}})$.

Proof. Note that $(a, u) \cdot (a^{-1}, (u^{-1})\tau_{a^{-1}}) = (1, 1)$. We verify the extra loop equation $(xy \cdot z) \cdot x = x \cdot (y \cdot zx)$, setting $x = (a, u)$, $y = (b, v)$, $z = (c, w)$:

$$\begin{aligned} ((a,u)(b,v) \cdot (c,w)) \cdot (a,u) &= \bigl((ab \cdot c) \cdot a,\ (u)\tau_{bca} \cdot (v)\tau_{ca} \cdot (w)\tau_a \cdot u\bigr) \\ (a,u) \cdot ((b,v) \cdot (c,w)(a,u)) &= \bigl(a \cdot (b \cdot ca),\ (u)\tau_{bca} \cdot (v)\tau_{ca} \cdot (w)\tau_a \cdot u\bigr) \end{aligned}$$

These are clearly equal, since B is an extra loop. In writing these equations, we used the facts that G is associative, and that $\mathrm{Aut}(G)$ is associative and τ is a homomorphism, so that the notation τ_{bca} is unambiguous, even though $b \cdot ca$ need not equal $bc \cdot a$. □

Of course, the same reasoning will work for other equations which are weakenings of the associative law; for example, if B is Moufang and G is a group, then $B \ltimes G$ is Moufang.

In some cases, we can prove that every extra loop of a given order is a semidirect product:

Lemma 8.3. Suppose that Q is a finite extra loop and $N = N(Q)$ is abelian. Then Q is isomorphic to $B \ltimes_\tau G$, where $B \in \mathrm{Syl}_2(Q)$, $G = O^2(N)$, $\tau_a = T_a{\restriction}G$, and each $(\tau_a)^2 = I$.

Proof. Say $|Q| = 2^n r$, where r is odd, so $|B| = 2^n$. Then $|N| = 2^m r$ for some $m \leqslant n$, and $|B \cap N| = 2^m$. Since N is abelian, it is an internal direct sum of $B \cap N$ and $G = O^2(N)$, which must have order r. Then $Q = BG$, since $B \cap G = \{1\}$. Furthermore, each T_a maps G to G because $T_a \in \mathrm{Aut}(N)$ and G is a characteristic subgroup of N. Then $Q \cong B \ltimes_\tau G$ follows. Also, $(\tau_a)^2 = \tau_{a^2} = I$ because $a^2 \in N$, which is abelian. □

Lemma 8.4. Suppose that Q is a nonassociative extra loop of order $16p$, where p is an odd prime. Then $N(Q) \cong \mathbb{Z}_2 \times \mathbb{Z}_p$.

Proof. $|Q : N| \geqslant 8$ because any $\langle \{x, y\} \cup N \rangle$ is associative, and $Z(N)$ contains an element of order 2 by Lemma 2.4, so $|N| = 2p$ and N cannot be the dihedral group, so N must be $\mathbb{Z}_2 \times \mathbb{Z}_p$. □

Combining Lemmas 8.3 and 8.4, we see that such Q must be of the form $B \ltimes_\tau \mathbb{Z}_p$, where B is one of the five extra loops of order 16 and each $\tau_a \in \{1, -1\} \leqslant \mathrm{Aut}(\mathbb{Z}_p)$; this is because $(\tau_a)^2 = I$, and the only element of $\mathrm{Aut}(\mathbb{Z}_p)$ of order 2 is the map $u \mapsto -u$. We shall now show that the number of such loops is independent of p. Obviously, $\mathrm{Hom}(B, \{1, -1\})$ does not depend on p, but different homomorphisms can result in isomorphic loops, so we must show that for $\tau, \sigma \in \mathrm{Hom}(B, \{1, -1\})$, the question of whether $B \ltimes_\tau \mathbb{Z}_p \cong B \ltimes_\sigma \mathbb{Z}_p$ does not depend on p:

Lemma 8.5. If B is a finite extra 2-loop and $\tau, \sigma \in \mathrm{Hom}(B, \{1, -1\})$, say $\tau \sim \sigma$ iff there is an $\alpha \in \mathrm{Aut}(B)$ with $\tau = \alpha\sigma$. Let p be an odd prime. Then, identifying $\{1, -1\} \leqslant \mathrm{Aut}(\mathbb{Z}_p)$, $B \ltimes_\tau \mathbb{Z}_p \cong B \ltimes_\sigma \mathbb{Z}_p$ iff $\tau \sim \sigma$.

Proof. If $\tau = \alpha\sigma$, then define $\Phi : B \ltimes_\tau \mathbb{Z}_p \to B \ltimes_\sigma \mathbb{Z}_p$ by $(a, u)\Phi = ((a)\alpha, u)$. To verify that Φ is an isomorphism, use

$$\begin{aligned} ((a,u) \cdot_\tau (b,v))\Phi &= (ab,\ (u)\tau_b + v)\Phi \ = \ ((ab)\alpha,\ (u)\tau_b + v) \\ (a,u)\Phi \cdot_\sigma (b,v)\Phi &= ((a)\alpha, u) \cdot_\sigma ((b)\alpha, v) \ = \ ((a)\alpha \cdot (b)\alpha,\ (u)\sigma_{(b)\alpha} + v), \end{aligned}$$

and these are equal because τ_b (i.e., $(b)\tau$) is the same as $\sigma_{(b)\alpha}$ (i.e., $(b)\alpha\sigma$).

Conversely, suppose we are given an isomorphism $\Phi : B \ltimes_\tau \mathbb{Z}_p \to B \ltimes_\sigma \mathbb{Z}_p$. Then $\Phi(B \times \{0\}) \in \mathrm{Syl}_2(B \ltimes_\sigma \mathbb{Z}_p)$. But also $(B \times \{0\}) \in \mathrm{Syl}_2(B \ltimes_\sigma \mathbb{Z}_p)$, and $\mathrm{Aut}(B \ltimes_\sigma \mathbb{Z}_p)$ acts transitively on the set of Sylow 2-subloops by Theorem 4.5. Thus, composing Φ with an automorphism, we may assume WLOG that $\Phi(B \times \{0\}) = B \times \{0\}$. Also, $\Phi(\{1\} \times \mathbb{Z}_p) = \{1\} \times \mathbb{Z}_p$ because $\{1\} \times \mathbb{Z}_p$ is the only subloop of $B \ltimes_\sigma \mathbb{Z}_p$ isomorphic to $\mathbb{Z}_p$. So, we have $(a, 0)\Phi = ((a)\alpha, 0)$ and $(1, u)\Phi = (1, (u)\beta)$ for some $\alpha \in \mathrm{Aut}(B)$ and $\beta \in \mathrm{Aut}(\mathbb{Z}_p)$. Since $(a, u) = (a, 0) \cdot (1, u)$, we also have $(a, u)\Phi = ((a)\alpha, (u)\beta)$. Furthermore, the map $(c, w) \mapsto (c, (w)\beta^{-1})$ is an automorphism of $B \ltimes_\sigma \mathbb{Z}_p$, since $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ is abelian. Composing Φ with this automorphism, we may assume WLOG that $\beta = I$, so that $(a, u)\Phi = ((a)\alpha, u)$. Then, since Φ is an isomorphism, we have:

$$((ab)\alpha, (u)\tau_b + v) = ((a,u) \cdot_\tau (b,v))\Phi = (a,u)\Phi \cdot_\sigma (b,v)\Phi = ((ab)\alpha, (u)\sigma_{(b)\alpha} + v),$$

so $\tau = \alpha\sigma$. □

It follows now that the number of nonassociative extra loops of order $16p$ is independent of p. In the case $p = 3$, that number is already known to be 16, since Goodaire, May, and Raman [16], following the classification of Chein [6], have listed all nonassociative Moufang loops of order less than 64. From Appendix E of [16], we find that 16 of the Moufang loops of order 48 are extra loops.

Theorem 8.6. For each odd prime p, there are exactly 16 nonassociative extra loops of order $16p$.

9. Conclusion

Although this paper has focused on extra loops, many of the lemmas hold more generally for CC-loops. For example, if Q is a CC-loop, then by

Басараб [2], Q/N is an abelian group. Of course, Q/N need not be boolean, but if Q is power-associative, then Q/N has exponent 12. Also, if Q is power-associative, nonassociative, and finite, then $|Q|$ is divisible by either 16 or 27. These results on power-associative CC-loops will appear elsewhere [19].

Acknowledgement. We would like to thank M. Aschbacher for suggesting the proof of Lemma 4.4, which is somewhat shorter than our original proof.

References

[1] **M. Aschbacher**; *Finite Group Theory*, Second edition, Cambridge University Press.

[2] **A. S. Basarab**: *A class of LK-loops*, (Russian), Mat. Issled. **120** (1991),3−7.

[3] **V. D. Belousov**: *Foundations of the theory of quasigroups and loops*, (Russian), Izdat. "Nauka", Moscow, 1967.

[4] **R. H. Bruck**: *A Survey of Binary Systems*, Springer-Verlag, 1971.

[5] **O. Chein**: *Moufang loops of small order, I*, Trans. Amer. Math. Soc. **188** (1974), 31 − 51.

[6] **O. Chein**: *Moufang loops of small order*, Mem. Amer. Math. Soc. **13** (1978), no. 197.

[7] **O. Chein, H. O. Pflugfelder, and J. D. H. Smith**, eds., *Quasigroups and Loops: Theory and Applications*, Heldermann Verlag, 1990.

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

[9] **A. Drápal**: *Conjugacy closed loops and their multiplication groups*, J. Algebra **272** (2004), 838 − 850.

[10] **A. Drápal**: *Structural interactions of conjugacy closed loops*, preprint

[11] **F. Fenyves**: *Extra loops I*, Publ. Math. Debrecen **15** (1968), 235 − 238.

[12] **F. Fenyves**: *Extra loops II*, Publ. Math. Debrecen **16** (1969), 187 − 192.

[13] **L. Fook**: *The devil and the angel of loops*, Proc. Amer. Math. Soc. **54** (1976), 32 − 34.

[14] **G. Glauberman**: *On loops of odd order. II*, J. Algebra **8** (1968), 393 − 414.

[15] **G. Glauberman and C. R. B. Wright**: *Nilpotence of finite Moufang 2-loops*, J. Algebra **8** (1968), 415 − 417.

[16] **E. G. Goodaire, S. May and M. Raman**: *The Moufang Loops of Order Less Than 64*, Nova Science Publishers, NY, 1999.

[17] **E. G. Goodaire and D. A. Robinson**: *A class of loops which are isomorphic to all loop isotopes*, *Canadian J. Math.* **34** (1982), 662 – 672.

[18] **E. G. Goodaire and D. A. Robinson**: *Some special conjugacy closed loops*, Canadian Math. Bull. **33** (1990), 73 – 78.

[19] **M. K. Kinyon and K. Kunen**: *Power-Associative, Conjugacy Closed Loops*, (*in preparation*).

[20] **M. K. Kinyon, K. Kunen and J. D. Phillips**: *Diassociativity in conjugacy closed loops*, Comm. Algebra **32** (2004), 767 – 786.

[21] **K. Kunen**: *The structure of conjugacy closed loops*, Trans. Amer. Math. Soc. **352** (2000), 2889 – 2911.

[22] **W. W. McCune**: *Mace 4.0 Reference Manual and Guide*, Argonne National Laboratory Technical Memorandum ANL/MCS-TM-264,2003, available at: `http://www.mcs.anl.gov/AR/mace4/`

[23] **P. T. Nagy and K. Strambach**: *Loops as invariant sections in groups, and their geometry*, Canad. J. Math. **46** (1994), 1027 – 1056.

[24] **H. O. Pflugfelder**: *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **8**, Heldermann Verlag, Berlin, 1990.

[25] **D. A. Robinson**: *Holomorphy theory of extra loops*, Publ. Math. Debrecen **18** (1971), 59 – 64 (1972).

[26] **L. R. Soĭkis**: *The special loops*, (Rusian), Questions of the Theory of Quasigroups and Loops, Izdat. Otdel Akad. Nauk Moldav. SSR, Kishinev, 1970, 122 – 131.

Received April 22, 2004

Michael K. Kinyon
Department of Mathematical Sciences
Indiana University South Bend
South Bend, IN 46634 USA
e-mail: mkinyon@iusb.edu
http://mypage.iusb.edu/~mkinyon

Kenneth Kunen
Department of Mathematics
University of Wisconsin
Madison, WI 57306 USA
e-mail: kunen@math.wisc.edu
http://www.math.wisc.edu/~kunen