# Diassociativity in Conjugacy Closed Loops

Michael K. Kinyon, Kenneth Kunen,* and J.D. Phillips†

February 18, 2003

**Abstract**

Let $Q$ be a conjugacy closed loop, and $N(Q)$ its nucleus. Then $Z(N(Q))$ contains all associators of elements of $Q$. If in addition $Q$ is diassociative (i.e., an extra loop), then all these associators have order 2. If $Q$ is power-associative and $|Q|$ is finite and relatively prime to 6, then $Q$ is a group. If $Q$ is a finite non-associative extra loop, then $16 \mid |Q|$.

## 1 Introduction

The notion of a conjugacy closed loop (CC-loop) is due to Goodaire and Robinson [10], and independently to Сойкис [18], with somewhat different terminology. Following, approximately, [10]:

**Definition 1.1** *A loop* $(Q, \cdot)$ *is* conjugacy closed *(or a* CC-loop*) if and only if there are functions* $f, g : Q \times Q \to Q$ *such that for all* $x, y, z$*:*

$$RCC: \; x \cdot yz = f(x,y) \cdot xz \qquad\qquad LCC: \; zy \cdot x = zx \cdot g(x,y) \quad .$$

As usual, define the left and right multiplications by $xy = xR_y = yL_x$, so that $R_y$ and $L_x$ are permutations of the set $Q$. Using these, we can express "CC-loop" in terms of conjugations:

**Lemma 1.2** *A loop* $Q$ *is a CC-loop if and only if there exist functions* $f, g : Q \times Q \to Q$ *such that*

$$L_x^{-1} L_y L_x = L_{f(x,y)} \qquad \textit{and} \qquad R_x^{-1} R_y R_x = R_{g(x,y)}.$$

*Author supported by NSF Grant DMS-0097881

†email addresses: mkinyon@iusb.edu, kunen@math.wisc.edu, phillipj@wabash.edu

*Proof.* $RCC$ and $LCC$ assert that $L_y L_x = L_x L_{f(x,y)}$ and $R_y R_x = R_x R_{g(x,y)}$. □

Thus, in a CC-loop, the left multiplications are closed under conjugation and the right multiplications are closed under conjugation; hence the name "conjugacy-closed".

These loops have a number of interesting properties, surveyed in Sections 2 and 3; for example, by [10], the left and right inner mappings are automorphisms. These properties allow a rather detailed structural analysis to be made; in particular, all CC-loops of orders $p^2$ and $2p$ (for primes $p$) are known (see [13]). This paper yields additional structural information about CC-loops — especially for the ones which are *power-associative* (that is, each $\langle x \rangle$ is a group) or *diassociative* (that is, each $\langle x, y \rangle$ is a group).

It is shown in [11] that the CC-loops which are diassociative (equivalently, Moufang) are the extra loops studied by Fenyves [8, 9]. By [9], if $Q$ is an extra loop, then $Q/N(Q)$ is a boolean group (where $N(Q)$ is the nucleus). It is immediate that a finite extra loop of odd order is a group. We show here (Corollary 8.7) that a finite power-associative CC-loop of order relatively prime to 6 is a group. The "6" cannot be improved, since there are non-associative power-associative CC-loops of order 16 (e.g., the Cayley loop) and of order 27 (see Section 10) (we do not know if there are ones of order divisible by 6 but not by 4 or 9). Also, one cannot drop the "power-associative", since by [10], there are non–power-associative CC-loops of order $p^2$ for every odd prime $p$.

More generally, we show that every power-associative CC-loop satisfies a weakening of diassociativity — namely, $\langle x, y \rangle$ is a group whenever $x$ is a cube and $y$ is a square. Then, if $|Q|$ is relatively prime to 6, every element must be a sixth power by the Lagrange property, so that $Q$ is diassociative, and hence an extra loop of odd order, and hence a group. Of course, we must verify that the Lagrange property really holds for CC-loops, since it can fail for loops in general. This is easy to do (see Corollary 3.2) using the result of Басараб [2]. He showed that for any CC-loop, $Q/N(Q)$ is an abelian group (this answers a question from [10]); we include a proof of this here (see Theorem 3.1), since it is fairly short using the notion of autotopy (see Белоусов [3] II§3 or Bruck [5] VII§2), together with some facts about the autotopies of CC-loops proved by Goodaire and Robinson (see [10] and Section 2).

We also establish two theorems about general CC-loops. First, whenever $S \subseteq Q$ and $S$ *associates* in the sense that $x \cdot yz = xy \cdot z$ holds for all $x, y, z \in S$, we prove that $\langle S \rangle$ also associates, and hence is a group (see Corollary 6.4). Second (see Theorems 7.8 and 7.10), we use this fact to show that $\langle b, c^2 \rangle$ and $\langle b^2, c \rangle$ are groups whenever $\langle b \rangle$ and $\langle c \rangle$ are groups and $c$ satisfies $c \cdot ((xc)\backslash 1) = x \backslash 1$ (such $c$ are called *WIP elements*; see Definition 2.17).

Finally, in a power-associative CC-loop, we show that all cubes are WIP elements (see Section 8), so that the subloop generated by a square and a cube always is a group.

Our investigations were aided by the computer programs OTTER, developed by McCune [14], and SEM, developed by J. Zhang and H. Zhang [19].

# 2 Background

Let $Q$ be a loop. We shall reformulate the notion of CC-loop in terms of autotopisms, the definition of which we now recall.

**Definition 2.1** *Let* $\mathrm{Sym}(Q)$ *denote the group of all permutations of the set* $Q$*, and let* $I$ *denote the identity element of* $\mathrm{Sym}(Q)$*. A triple* $(\alpha, \beta, \gamma) \in (\mathrm{Sym}(Q))^3$ *is an* autotopism *of* $Q$ *if* $y\alpha \cdot z\beta = (yz)\gamma$ *for all* $y, z \in Q$*. Let* $\mathrm{Atop}(Q)$ *denote the set of all autotopisms of* $Q$*.*

It is easy to see that $\mathrm{Atop}(Q)$ is a subgroup of $(\mathrm{Sym}(Q))^3$.

**Lemma 2.2** *A loop* $Q$ *is a CC-loop if and only if there exist mappings* $F, G : Q \to \mathrm{Sym}(Q)$ *such that*

$$(F_x, L_x, L_x) \qquad \text{and} \qquad (R_x, G_x, R_x)$$

*are in* $\mathrm{Atop}(Q)$*. In this case,* $F_x$ *and* $G_x$ *are given by:* $yF_x = f(x, y)$ *and* $yG_x = g(x, y)$ *(see Definition 1.1).*

We shall also use the division and the left and right inverse permutations:

**Definition 2.3** *In any loop* $Q$*, define permutations* $\rho$ *and* $\lambda$*, along with* $D_x$ *for* $x \in Q$*, by:*

$$y\lambda = 1/y \qquad y\rho = y\backslash 1 \qquad yD_x = y\backslash x \quad .$$

*We write* $y^\lambda, y^\rho$ *for* $y\lambda, y\rho$*, respectively; when these values are the same, they are denoted by* $y^{-1}$*. If* $y^\lambda = y^\rho$ *for* all $y$*, we let* $J = \lambda = \rho$*.*

Note that $yD_x^{-1} = x/y$, $\rho = D_1$, and $\lambda = D_1^{-1}$. These permutations are used in the following explicit expressions for $F_x$ and $G_x$, which are obtained from Definition 1.1:

**Lemma 2.4** *For all* $z$ *in a CC-loop,*

$$F_x = R_z L_x R_{xz}^{-1} = D_z L_x D_{xz}^{-1} \qquad \text{and} \qquad G_x = L_z R_x L_{zx}^{-1} = D_z^{-1} R_x D_{zx}.$$

*In particular,*

$$\begin{array}{rcccccccc} f(x,y) &=& (xy)/x &=& x\cdot yx^\rho &=& x/(xy^\rho) &=& [x(y\backslash x^\rho)]^\lambda \\ F_x &=& L_xR_x^{-1} &=& R_{x^\rho}L_x &=& \rho L_xD_x^{-1} &=& D_{x^\rho}L_x\,\lambda \end{array}$$

$$\begin{array}{rcccccccc} g(x,y) &=& x\backslash(yx) &=& x^\lambda y\cdot x &=& (y^\lambda x)\backslash x &=& [(x^\lambda/y)x]^\rho \\ G_x &=& R_xL_x^{-1} &=& L_{x^\lambda}R_x &=& \lambda R_xD_x &=& D_{x^\lambda}^{-1}R_x\,\rho \end{array}$$

*Proof.* $F_x = R_zL_xR_{xz}^{-1}$ is immediate from $RCC$. Replacing the $z$ in $RCC$ by $y\backslash z$ we obtain $xz = f(x,y)\cdot x(y\backslash z)$, which yields $F_x = D_zL_xD_{xz}^{-1}$. The rest of the expressions for $F_x$ are obtained by setting $z$ to equal either 1 or $x^\rho$. The expressions for $G_x$ are likewise obtained from $LCC$. □

**Corollary 2.5** *In every CC-loop,* $F_xG_x = G_xF_x = I$.

The following lemma lists some additional conjugation relations among the left and right translations; (3) and (4) are from [13], Lemma 3.1:

**Lemma 2.6** *In any CC-loop:*

1. $L_xL_yL_x^{-1} = L_{g(x,y)}$ $\qquad R_xR_yR_x^{-1} = R_{f(x,y)}$
2. $x\cdot g(x,y)z = y\cdot xz$ $\qquad zf(x,y)\cdot x = zx\cdot y$
3. $L_x^{-1}R_yL_x = R_x^{-1}R_{xy} = R_{y/x^\rho}R_x^{-1}$ $\qquad R_x^{-1}L_yR_x = L_x^{-1}L_{yx} = L_{x^\lambda\backslash y}L_x^{-1}$
4. $L_xR_yL_x^{-1} = R_{x^\rho}^{-1}R_{x\backslash y} = R_{yx^\rho}R_{x^\rho}^{-1}$ $\qquad R_xL_yR_x^{-1} = L_{x^\lambda}^{-1}L_{y/x} = L_{x^\lambda y}L_{x^\lambda}^{-1}$

*Proof.* For (1), use Lemma 1.2 and Corollary 2.5. (2) is equivalent to (1). For the first equality of (3), use Lemma 2.4 and Corollary 2.5 to get

$$R_xL_x^{-1}R_zL_x = G_xR_zL_x = F_x^{-1}R_zL_x = R_{xz} \quad .$$

For the second one, use (1) and Lemma 2.4 to get $R_xR_{y/x^\rho}R_x^{-1} = R_{f(x,y/x^\rho)} = R_{xy}$. For the first equality of (4), use Lemma 2.4 with $z$ replaced by $x\backslash z$ to obtain $R_{x^\rho}L_xR_z = R_{x\backslash z}L_x$. For the second equality, use Lemmas 1.2 and 2.4: $R_{x^\rho}^{-1}R_{x\backslash y}R_{x^\rho} = R_{g(x^\rho,x\backslash y)} = R_{yx^\rho}$. □

The left nucleus ($N_\lambda$), the middle nucleus ($N_\mu$), the right nucleus ($N_\rho$), and the nucleus ($N$) are defined by:

**Definition 2.7** *Let $Q$ be a loop.*

$$\begin{array}{rcl} N_\lambda(Q) &:=& \{a\in Q : \forall x,y\in Q\,[\,a\cdot xy = ax\cdot y\,]\} \\ N_\mu(Q) &:=& \{a\in Q : \forall x,y\in Q\,[\,xa\cdot y = x\cdot ay\,]\} \\ N_\rho(Q) &:=& \{a\in Q : \forall x,y\in Q\,[\,x\cdot ya = xy\cdot a\,]\} \\ N(Q) &:=& N_\lambda(Q)\cap N_\mu(Q)\cap N_\rho(Q) \end{array}$$

It is easy to verify the following equivalents, in terms of autotopy.

**Lemma 2.8** *For any loop $Q$:*

1. $N_\lambda(Q) = \{a \in Q : (L_a, I, L_a) \in \mathrm{Atop}(Q)\}$.
   $N_\mu(Q) = \{a \in Q : (R_a^{-1}, L_a, I) \in \mathrm{Atop}(Q)\}$.
   $N_\rho(Q) = \{a \in Q : (I, R_a, R_a) \in \mathrm{Atop}(Q)\}$.
2. *If* $(\alpha, I, \gamma) \in \mathrm{Atop}(Q)$*, then* $\alpha = \gamma$*,* $1\alpha \in N_\lambda(Q)$ *and* $\alpha = L_{1\alpha}$.

*Proof.* For (2), $x\alpha \cdot y = (xy)\gamma$, so taking $y = 1$ gives $\alpha = \gamma$. Then let $a = 1\alpha$ and $x = 1$ to obtain $ay = y\alpha$, so that $ax \cdot y = a \cdot xy$. □

**Definition 2.9** *For any loop $Q$,* $Z(Q) = \{x \in N(Q) : \forall y[xy = yx]\}$,

By Goodaire and Robinson [10]:

**Theorem 2.10** *In any CC-loop $Q$,* $N(Q) = N_\lambda(Q) = N_\mu(Q) = N_\rho(Q)$ *and* $N(Q)$ *is a normal subloop of $Q$. Also,* $Z(Q) = \{x \in Q : \forall y[xy = yx]\}$*, so that every commutative CC-loop is a group.*

Autotopies are useful for producing automorphisms:

**Lemma 2.11** *In any loop $Q$, if* $1\alpha = 1$ *and either* $(\alpha, \beta, \alpha) \in \mathrm{Atop}(Q)$ *or* $(\beta, \alpha, \alpha) \in \mathrm{Atop}(Q)$*, then* $\alpha = \beta$ *and $\alpha$ is an automorphism.*

*Proof.* If $(\alpha, \beta, \alpha) \in \mathrm{Atop}(Q)$, we have $x\alpha \cdot y\beta = (xy)\alpha$. Setting $x = 1$ yields $\alpha = \beta$. □

Following Bruck [5] §IV.1, define the generators of the right and left inner mapping groups by:

**Definition 2.12** $R(x, y) := R_x R_y R_{xy}^{-1}$ *and* $L(x, y) := L_x L_y L_{yx}^{-1}$.

**Lemma 2.13 ([10])** *In any CC-loop,* $R(x, y)$ *and* $L(x, y)$ *are automorphisms for all* $x, y$.

*Proof.* By Lemma 2.2, $(R(x, y), G_x G_y G_{xy}^{-1}, R(x, y)) \in \mathrm{Atop}(Q)$. Now apply Lemma 2.11. □

The following definitions will be useful in Sections 7 and 8:

**Definition 2.14** $E_x = R(x, x^\rho) = R_x R_{x^\rho}$.

**Definition 2.15** *$a$ is a* power-associative *element if $\langle a\rangle$ is a group. A loop is* power-associative *iff every element is power-associative.*

By ([13], Lemma 3.20):

**Lemma 2.16** *Let $Q$ be a CC-loop. The following are equivalent for an element $a \in Q$: (i) $a$ is power-associative; (ii) $1/a = a\backslash 1$; (iii) $a \cdot aa = aa \cdot a$. In particular, $Q$ is power-associative if and only if $\rho = \lambda$.*

Following Osborn [15]:

**Definition 2.17** *$c$ is a* WIP element *(briefly: $c$ is WIP) iff $\lambda R_c \rho = L_c^{-1}$. A loop has the* weak inverse property *iff every element is WIP.*

For convenience, we collect the following easy equivalents of WIP.

**Lemma 2.18** *In any loop, each of the following four equations is equivalent to the statement that $c$ is a WIP element:*

$$\begin{array}{cc} \lambda R_c \rho = L_c^{-1} & \rho L_c \lambda = R_c^{-1} \\ R_c \rho L_c = \rho & L_c \lambda R_c = \lambda \end{array}$$

# 3 $Q/N(Q)$

**Theorem 3.1 (Басараб [2])** *For a CC-loop $Q$, $Q/N(Q)$ is an abelian group.*

*Proof.* By Goodaire and Robinson [10], every CC-loop is a G-loop; that is, it is isomorphic to all its loop isotopes. In particular, for any element $v$, the isotope $(Q;\circ)$ defined by $x \circ y = x \cdot (v\backslash y)$ satisfies $RCC$:

$$x \cdot (v\backslash(y \cdot (v\backslash z))) = h(x,y,v) \cdot (v\backslash(x \cdot (v\backslash z))) \quad ,$$

where $h : Q^3 \to Q$. Replacing $z$ by $vz$, this simplifies to:

$$x \cdot (v\backslash(y \cdot z)) = h(x,y,v) \cdot (v\backslash(x \cdot z)) \quad .$$

We may set $z = 1$ to get $h(x,y,v) = (x(v\backslash y))/(v\backslash x)$, so we have

$$x \cdot (v\backslash(y \cdot z)) = [(x(v\backslash y))/(v\backslash x)] \cdot [v\backslash(x \cdot z)] \quad ,$$

which implies that $(L_v^{-1} L_x R_{v\backslash x}^{-1},\ L_x L_v^{-1},\ L_v^{-1} L_x) \in \mathrm{Atop}(Q)$ for all $x$ and $v$. Since also $(F_v F_x^{-1},\ L_v L_x^{-1},\ L_v L_x^{-1}) \in \mathrm{Atop}(Q)$ by Lemma 2.2, we have

$$(F_v F_x^{-1} L_v^{-1} L_x R_{v\backslash x}^{-1},\ I,\ L_v L_x^{-1} L_v^{-1} L_x) \in \mathrm{Atop}(Q) \quad .$$

Then, by Lemma 2.8, $1\, F_v F_x^{-1} L_v^{-1} L_x R_{v\backslash x}^{-1} = (x(v\backslash 1))/(v\backslash x) \in N_\lambda(Q)$. Applying Theorem 2.10, $Q/N(Q)$ is a CC-loop satisfying the additional equation $(x(v\backslash 1))/(v\backslash x) = 1$, or $xv^\rho = v\backslash x$. Hence, in $Q/N(Q)$, we have (using Lemma 2.4) $f(v,y) = v \cdot yv^\rho = y$, so that $RCC$ becomes $x \cdot yz = y \cdot xz$. Setting $z = 1$, we get $xy = yx$, so that $Q/N(Q)$ is commutative and satisfies the associative law, $x \cdot zy = xz \cdot y$. □

This is roughly the proof in [2], although Басараб studies in more detail those loops $Q$ such that $Q$ and all its loop isotopes satisfy $RCC$.

Recall that a finite loop has the *weak Lagrange property* if the order of any subloop divides the order of the loop, and a finite loop has the *strong Lagrange property* if every subloop has the weak Lagrange property [16]. In general if $H$ is a normal subloop of $Q$, and $H$ and $Q/H$ both have the strong Lagrange property, then so does $Q$ (see Bruck [5], §V.2, Lemma 2.1; see also [7]). It is now immediate from Theorem 3.1 that:

**Corollary 3.2** *Every finite CC-loop has the strong Lagrange property.*

**Corollary 3.3** *If $Q$ is a finite power-associative CC-loop and $|Q|$ is relatively prime to $n$, then every element of $Q$ is an $n^{\text{th}}$ power.*

The following Cauchy property is also immediate from Theorem 3.1:

**Corollary 3.4** *If $Q$ is a finite power-associative CC-loop and $|Q|$ is divisible by a prime $p$, then $Q$ contains an element of order $p$.*

Also, the fact that finite $p$-groups have non-trivial centers generalizes to:

**Corollary 3.5** *If $Q$ is a CC-loop of order $p^n$ for some prime $p$ and $n > 0$, then*

1. *$|Z(Q)| = p^r$, where $r \neq 0$ and $r \neq n-1$.*
2. *For all $m \leq n$, $Q$ has a normal subloop of order $p^m$.*

*Proof.* For (1): Let $N$ be the nucleus. For $x \in Q$, let $T_x = R_x L_x^{-1}$. By [10], each $T_x \restriction N$ is an automorphism of $N$. Furthermore, if we define $\mathcal{T} : Q \to \mathrm{Aut}(N)$ by $\mathcal{T}(x) = T_x \restriction N$, then $\mathcal{T}$ is a homomorphism by [13], Corollary 3.7. Thus, $\mathcal{T}(Q)$ is a subgroup of $\mathrm{Sym}(N)$, and $|\mathcal{T}(Q)|$ is a power of $p$, so the size of each orbit is a power of $p$. Since $|N| = p^\ell$ for some $\ell > 0$, there must be at least $p$ elements $y$ whose orbit is a singleton (equivalently, $y \in Z(Q)$). Hence $r \neq 0$.

If $r \geq n-1$, then $Q = \langle Z(Q) \cup \{a\}\rangle$ for any $a \neq Z(Q)$, but then $Q$ is commutative, so $r = n$.

For (2): Let $P$ be a subgroup of $Z(Q)$ of order $p$. Then the $m = 1$ case is immediate, using $P$, and the case $1 < m \leq n$ follows by applying induction to $Q/P$. □

# 4 Associators and Inner Mappings

**Definition 4.1** *In a loop $Q$,* associators *are denoted by:*

$$(x, y, z) := (x \cdot yz) \setminus (xy \cdot z) \qquad [x, y, z] := (x \cdot yz) \,/\, (xy \cdot z) \quad .$$

Since the two notions of "associator" are mirrors of each other, we concentrate on $(x, y, z)$ in the following:

**Lemma 4.2** *In any loop $Q$ with nucleus $N$, if $a \in N$, then*

*(i)* $(ax, y, z) = (x, y, z)$
*(ii)* $(xa, y, z) = (x, ay, z)$
*(iii)* $(x, ya, z) = (x, y, az)$
*(iv)* $(x, y, za) = a^{-1}(x, y, z)a$

*In addition, if $N$ is normal in $Q$, then*

*(v)* $(xa, y, z) = (x, y, z)$
*(vi)* $(x, ya, z) = (x, y, z)$
*(vii)* $a^{-1}(x, y, z)a = (x, y, z)$

*Proof.* (i)-(iv) are straightforward consequences of the definitions. Now assume $N$ is normal in $Q$. Then for $u \in Q$, $ua = bu$ for some $b \in N$. Thus (v) follows from (i), (vi) follows from (ii) and (v), and (vii) follow from (iv), (iii), and (vi). □

Theorem 3.1 implies that associators are nuclear, so we have:

**Corollary 4.3** *The nucleus of a nonassociative CC-loop has a nontrivial center which contains the subgroup generated by the associators.*

**Theorem 4.4** *In a CC-loop, the associators $(x, y, z)$ and $[x, y, z]$ are invariant under all permutations of the set $\{x, y, z\}$.*

*Proof.* It is enough to prove that $(x, y, z) = (y, x, z)$ and $(x, y, z) = (x, z, y)$, since the transpositions $(x\ y)$ and $(y\ z)$ generate $\mathrm{Sym}(\{x, y, z\})$.

For $(x, y, z) = (y, x, z)$: $x \cdot yz = f(x, y) \cdot xz$ by $RCC$ and $xy \cdot z = f(x, y)x \cdot z$ by Lemma 2.4, so $(x, y, z) = (f(x, y), x, z)$. By Theorem 3.1, there exists $a \in N$ such that $f(x, y) = ay$, so $(f(x, y), x, z) = (ay, x, z) = (y, x, z)$ by Lemma 4.2(i).

For $(x, y, z) = (x, z, y)$: Apply a similar argument, using $LCC$. □

**Lemma 4.5** *In a CC-loop,*

$$zL(y,x) = z(x,y,z)^{-1} \qquad xR(y,z) = [x,y,z]^{-1}x \quad .$$

*Proof.* We have:

$$(x \cdot yz)(x,y,z) = (xy \cdot z) \qquad [x,y,z](xy \cdot z) = (x \cdot yz) \quad .$$

Since associators are nuclear, this can be rewritten as

$$\{z(x,y,z)\}L(y,x) = z \qquad \{[x,y,z]x\}R(y,z) = x \quad .$$

Now use the fact that $L(y,x)$ and $R(y,z)$ are automorphisms which fix all elements of the nucleus. □

Applying Theorem 4.4:

**Corollary 4.6** *In a CC-loop, $L(x,y) = L(y,x)$ and $R(x,y) = R(y,x)$.*

Furthermore, the $L(x,y)$ and $R(u,v)$ all commute with each other; more generally, they commute with all nuclear automorphisms:

**Definition 4.7** *Let $Q$ be a loop with nucleus $N$. An automorphism $\alpha$ of $Q$ is* nuclear *iff $x\alpha \in xN$ for each $x \in Q$. $N\mathrm{Aut}(Q)$ is the set of nuclear automorphisms of $Q$.*

**Lemma 4.8** *$N\mathrm{Aut}(Q)$ is a normal subgroup of $\mathrm{Aut}(Q)$.*

**Theorem 4.9** *Let $Q$ be a CC-loop. Then $Z(N\mathrm{Aut}(Q))$ contains all $R(x,y)$ and $L(x,y)$.*

*Proof.* The $R(x,y)$ and $L(x,y)$ are automorphisms by Lemma 2.13 and nuclear by Theorem 3.1. Now, if $\alpha$ is nuclear, we have, using Lemma 4.5,

$$zL(y,x)\alpha = \{z(x,y,z)^{-1}\}\alpha = z\alpha \cdot (xa,yb,zc)^{-1} = z\alpha \cdot (x,y,z)^{-1} \quad ,$$

where $a,b,c \in N(Q)$, whereas

$$z\alpha L(y,x) = (z\alpha) \cdot (x,y,z\alpha)^{-1} = (z\alpha) \cdot (x,y,zd)^{-1} = z\alpha \cdot (x,y,z)^{-1} \quad ,$$

where $d \in N(Q)$. □

**Corollary 4.10** *In a CC-loop, the group generated by all the automorphisms $R(x,y)$ and $L(x,y)$ is abelian.*

# 5 Extra Loops

In this section we offer some characterizations of extra loops, i.e., Moufang CC-loops, which do not seem to be in the literature. We then apply the results of the previous section to extra loops.

A loop has the *right inverse property* (RIP) iff it satisfies $x/y = xy^{\phi}$ for some mapping $\phi$. The *left inverse property* (LIP) is similarly defined, and if either of these properties holds, then $\phi = \rho = \lambda$. A loop has the *anti-automorphic inverse property* (AAIP) iff it satisfies $(xy)^{\rho} = y^{\rho}x^{\rho}$. This is equivalent to $(xy)^{\lambda} = y^{\lambda}x^{\lambda}$, and these conditions imply $\rho = \lambda$. A loop satisfying any three of RIP, LIP, and AAIP satisfies the third, and is said to have the *inverse property* (IP) [5].

**Lemma 5.1** *In every CC-loop,* $(x \cdot yx^{\rho}) \cdot xy^{\rho} = x$ *and* $y^{\lambda}x \cdot (x^{\lambda}y \cdot x) = x$*.*

*Proof.* This follows immediately from Lemma 2.4. □

**Lemma 5.2** *In a CC-loop, each of the RIP, LIP, and AAIP is sufficient for the IP.*

*Proof.* If RIP holds, then using Lemma 5.1, we have $x \cdot yx^{-1} = x(xy^{-1})^{-1}$. Cancelling and replacing $y$ with $y^{-1}$ gives AAIP. Similarly, LIP implies AAIP. In Lemma 5.1, $yx^{\rho}$ and $x^{\lambda}y$ can be arbitrary elements of the loop, so if AAIP holds, then $xz \cdot z^{-1} = z^{-1} \cdot zx = x$, which are RIP and LIP, respectively. □

A loop is said to have the *right alternative property* (RAP) iff it satisfies $xy \cdot y = xy^2$. The *left alternative property* (LAP) is similarly defined. A loop is said to be *flexible* iff it satisfies $x \cdot yx = xy \cdot x$.

**Lemma 5.3** *In a CC-loop, each of the RAP and LAP is sufficient for flexibility.*

*Proof.* If RAP holds, then using *RCC* and Lemma 2.4, $x \cdot yx = f(x,y)x^2 = f(x,y)x \cdot x = xy \cdot x$. □

It is known that each of the IP and flexibility is sufficient for a CC-loop to be an extra loop [11]. Lemmas 5.2 and 5.3 give us additional conditions.

**Theorem 5.4** *Each of the following is sufficient for a CC-loop to be an extra loop: (i) RIP, (ii) LIP, (iii) AAIP, (iv) RAP, (v) LAP.*

The nucleus of an extra loop contains every square [9]. However, there are non-extra CC-loops $Q$ in which all squares are in the nucleus; such $Q$ can both be power-associative and have the weak inverse property; see Section 10.

**Lemma 5.5** *In a CC-loop,* $z(x,y,z)^{-1} = (x,y,z^\lambda)z$.

*Proof.* Applying the automorphism $L(y,x)$ to the equation $z^\lambda z = 1$, and using Lemma 4.5, we get $z^\lambda(x,y,z^\lambda)^{-1} \cdot z(x,y,z)^{-1} = 1 = z^\lambda z$. The result now follows because associators are in the nucleus. □

**Lemma 5.6** *Let* $Q$ *be a CC-loop such that* $N(Q)$ *contains every square. For* $i = 1,2,3$, *choose* $\epsilon_i \in \{I, \rho, \lambda\}$. *Then* $(x,y,z) = (x\epsilon_1, y\epsilon_2, z\epsilon_3)$. *Hence* $L(y,x) = L(y\epsilon_1, x\epsilon_2)$.

*Proof.* Note that $z^2 z^\lambda = z^\rho z^2 = z$ (since $z^2 z^\lambda z = z^2$). Then, Lemma 4.2 implies $(x,y,z) = (x,y,z^\lambda) = (x,y,z^\rho)$. The remainder follows from Theorem 4.4 and Lemma 4.5. □

**Theorem 5.7** *Let* $Q$ *be an extra loop.*

1. $L(x,y) = R(x,y) = L(y,x) = R(y,x)$ *and* $L(x,y)^2 = I$.
2. $(x,y,z) = [x,y,z]$ *and* $(x,y,z)^2 = 1$, *so that the subgroup of* $N(Q)$ *generated by the associators is a boolean group.*
3. *Each* $(x,y,z)$ *commutes with* $x$, $y$, *and* $z$.

*Proof.* (1) In Moufang loops, $R(x^{-1}, y^{-1}) = L(x,y) = L(y,x)^{-1}$ (see [5], Lemma VII.5.4). Now apply Corollary 4.6 and Lemma 5.6.

(2) In diassociative loops, $(x,y,z)^{-1} = [z^{-1}, y^{-1}, x^{-1}]$. Now, apply (1), along with Theorem 4.4 and Lemmas 4.5 and 5.6.

(3) This follows from (2), Lemmas 5.5 and 5.6, and Theorem 4.4. □

Hence, the nucleus of a nonassociative extra loop must contain elements of order 2.

**Corollary 5.8** *If* $Q$ *is a finite nonassociative extra loop, then* $16 \mid |Q|$.

*Proof.* Since the order of $N = N(Q)$ is even, and $Q/N$ is a boolean group, it is sufficient to show that $|Q : N| \geq 8$. Choose $a \notin N = N_\mu$, and then choose $b$ such that $R(a,b) \neq I$ (that is, $(xa)b \neq x(ab)$ for some $x$). Then $N < \text{fix}(R(a,b)) < Q$, since $a, b \in \text{fix}(R(a,b))$. Next, note that $\langle N \cup \{a\} \rangle = Na = aN$, and that $b \neq aN$ (otherwise $R(a,b)$ would be $I$), so $N < aN < \text{fix}(R(a,b)) < Q$, so $|Q : N| \geq 8$. □

# 6 Subgroups of CC-loops

Here, we show that some subloops of CC-loops are groups.

**Definition 6.1** *A triple of subsets $(A, B, C)$ of a loop $Q$* associates *iff $x \cdot yz = xy \cdot z$ whenever $x \in A$, $y \in B$, and $z \in C$. A subset $S$ of $Q$* associates *iff $(S, S, S)$ associates.*

Applying Theorem 4.4,

**Lemma 6.2** *In a CC-loop, the property "$(A, B, C)$ associates" is invariant under all permutations of the set $\{A, B, C\}$.*

By modifiying an argument of Bruck and Paige [6] for A-loops:

**Lemma 6.3** *In a CC-loop, if $(A, B, C)$ associates then $(\langle A\rangle, \langle B\rangle, \langle C\rangle)$ associates.*

*Proof.* For each $b \in B$ and $c \in C$, the map $R_b R_c R_{bc}^{-1}$ is an automorphism (see Lemma 2.13) and is the identity on $A$, so it is the identity on $\langle A\rangle$, which implies that $(\langle A\rangle, B, C)$ associates. By Lemma 6.2, we may apply this argument two more times to prove that $(\langle A\rangle, \langle B\rangle, \langle C\rangle)$ associates. □

**Corollary 6.4** *In a CC-loop, if $S$ associates, then $\langle S\rangle$ associates, and is hence a group.*

# 7 WIP Elements

Throughout this section, $(Q, \cdot)$ always denotes a CC-loop. By [13], power-associative elements $x$ satisfy a number of additional properties. In this section, we shall derive some further properties of these $x$ and their associated $E_x$ when $x$ is also a WIP element (see Definitions 2.14, 2.15, and 2.17).

Whenever $x$ is power-associative, all elements of the group generated by $L_x$ and $R_x$ are of the form $E_x^r R_x^s L_x^t$ for some $r, s, t \in \mathbb{Z}$. This is immediate from the following lemma, which is taken from Lemmas 3.17 and 3.19 of [13]:

**Lemma 7.1** *If $x$ is power-associative, then for all $r, s, t, i, j, k, n \in \mathbb{Z}$, the following hold:*

1. *$E_x$ commutes with $L_x$ and $R_x$.*
2. *$R_x^{-j} L_x^t R_x^j = E_x^{-jt} L_x^t$.*

3. $E_x^r R_x^s L_x^t \cdot E_x^i R_x^j L_x^k = E_x^{r+i-jt} R_x^{s+j} L_x^{t+k}$.
4. $R_{x^n} = E_x^{(n-1)n/2} R_x^n$
5. $L_{x^n} = E_x^{-(n-1)n/2} L_x^n$.
6. $E_{x^n} = E_x^{(n^2)}$.

**Lemma 7.2** *In a CC-loop, if $c$ is a power-associative WIP element, then for each $n \in \mathbb{Z}$, $c^n$ is a WIP element.*

*Proof.* Let $m = (n-1)n/2$. Applying Lemma 7.1, we have

$$R_{c^n} \rho L_{c^n} = E_c^m R_c^n \rho E_c^{-m} L_c^n = R_c^n \rho L_c^n = \rho \quad .$$

We are using the fact that $E_c$ commutes with $\rho$ (because it is an automorphism) and with $R_c$ (by Lemma 7.1(1)). □

**Lemma 7.3** *In a CC-loop, if $c$ is a power-associative WIP element, then the following hold:*

$$\begin{array}{cc} D_c = L_{c^{-1}}\, \rho & D_c^{-1} = R_{c^{-1}}\, \lambda \\ \lambda L_c \rho = R_c^{-1} & \rho R_c \lambda = L_c^{-1} \\ L_c \rho R_c = \rho & R_c \lambda L_c = \lambda \end{array}$$

*Proof.* Note that since $y D_c = y \backslash c$ and $y D_c^{-1} = c/y$, the equations in the right column are mirrors of the ones in the left, so we need only prove one from each row. For the first row, use $c \cdot g(c,y)z = y \cdot cz$ (see Lemma 2.6), and set $z = g(c,y)^\rho$ to get $c = y \cdot cg(c,y)^\rho = y \cdot c(c^{-1}y \cdot c)^\rho$ (see Lemma 2.4). Since $R_c \rho L_c = \rho$, we get $c = y \cdot (c^{-1}y)^\rho$, which implies $D_c = L_{c^{-1}}\, \rho$.

For the second row, apply both equations in the first row to $c^{-1}$, which is also WIP, to get $L_c \rho = D_{c^{-1}} = \rho R_c^{-1}$. The third row restates the second. □

Lemmas 2.18 and 7.3 provide conjugation relations which, together with Lemma 7.1, show that whenever $c$ is power-associative and WIP, all elements of the group generated by $L_c$, $R_c$, and $\rho$ are of the form $\alpha E_c^r R_c^s L_c^t$ for some $r, s, t \in \mathbb{Z}$, and some $\alpha \in \langle \rho \rangle$. It is also easy to see now that if $c$ is a power-associative WIP element, then each of $R_c, L_c$ commutes with each of $\lambda^2, \rho^2$.

**Lemma 7.4** *In a CC-loop, $x(yz \cdot x) = (x^\lambda \backslash y) \cdot zx$ and $(x \cdot yz)x = xy \cdot (z/x^\rho)$.*

*Proof.* By Lemmas 2.2 and 2.4 and Corollary 2.5, $(R_x, G_x, R_x)(F_x, L_x, L_x) = (L_{x^\lambda}^{-1}, R_x, R_x L_x)$ is an autotopism. Thus $x(yz \cdot x) = (x^\lambda \backslash y) \cdot zx$ for all $y, z$. □

**Lemma 7.5** *In a CC-loop, if $c$ is a power-associative WIP element and $x$ is arbitrary, then $x \cdot (x E_c^{-1} \cdot c) = x^2 \cdot c$.*

*Proof.* We have $x^2 = (x^\lambda\backslash c^{-1}) \cdot cx = (x/c) \cdot cx$ using Lemma 7.4 and $D_{c^{-1}} = \rho R_c^{-1}$. Thus $x^2 \cdot c = ((x/c) \cdot cx) \cdot c = (x/c)c \cdot g(c, cx) = x \cdot x L_c L_{c^{-1}} R_c = x \cdot (x E_c^{-1} \cdot c)$ by $LCC$, Lemma 2.4, and Lemma 7.1(5). □

**Lemma 7.6** *In a CC-loop, if $b$ and $c$ are power-associative, then $\langle b, c\rangle$ is a group if and only if $cE_b = c$ and $bE_c = b$. If $c$ is also a WIP element, then $cE_b = c$ iff $bE_c = b$.*

*Proof.* If $\langle b, c\rangle$ is a group, then obviously $cE_b = c$ and $bE_c = b$. Conversely, to prove that $\langle b, c\rangle$ is a group, it is sufficient, by Corollary 6.4, to show that $\{b, c\}$ associates; that is, $(x, y, z) = 1$ whenever $x, y, z \in \{b, c\}$. However, since $\langle c\rangle$ and $\langle b\rangle$ are groups and the associators are invariant under permutations (Theorem 4.4), it is sufficient to show that $b^2 \cdot c = b \cdot bc$ and $c^2 \cdot b = c \cdot cb$. By Lemma 7.1(5), these equations are equivalent to $cE_b = c$ and $bE_c = b$, respectively.

Now if $c$ is a WIP element, then Lemmas 7.5 and 7.1(5) give $bE_c^{-1} \cdot c = cL_{b^2} L_b^{-1} = b \cdot cE_b^{-1}$. Thus $bE_c = b$ if and only if $cE_b = c$. □

**Lemma 7.7** *In a CC-loop, if $c$ is power-associative and WIP, then $E_c^2 = I$.*

*Proof.* In Lemma 7.4, set $x = c$, $y = c\backslash u$, and $z = (c\backslash u)^\rho$ to obtain $c^2 = u((c\backslash u)^\rho / c^{-1})$; equivalently, $D_{c^2} = L_c^{-1} \rho R_{c^{-1}}^{-1}$. Now, applying Lemmas 7.3 and 7.1, we get $D_{c^2} = L_{c^{-2}}\, \rho = L_c^{-2} E_c^{-3} \rho$ and $L_c^{-1} \rho R_{c^{-1}}^{-1} = L_c^{-1} L_{c^{-1}} \rho = L_c^{-2} E_c^{-1} \rho$. so that $E_c^{-3} = E_c^{-1}$ . □

**Theorem 7.8** *In a CC-loop, if $c$ is WIP, and if $b$ and $c$ are power-associative, then $\langle b, c^2\rangle$ is a group.*

*Proof.* By Lemmas 7.1(6) and 7.7, $bE_{c^2} = bE_c^4 = b$. Now apply Lemma 7.6 to $c^2$, which is WIP by Lemma 7.2. □

**Lemma 7.9** *In a CC-loop, if $c$ is WIP, and if $b$ and $c$ are power-associative, then $cE_b^2 = c$.*

*Proof.* Lemma 7.5 implies $b^{-1} \cdot (b\backslash(b^2 \cdot c)) = b^{-1} \cdot (bE_c^{-1} \cdot c)$. Now $L_b^2 L_b^{-1} L_{b^{-1}} = E_b^{-2}$ by Lemma 7.1(5), and $bE_c^{-1} R_c = bR_{c^{-1}}^{-1} = b\lambda D_c = b^{-1}\backslash c$ by Lemmas 7.1(4) and 7.3. Therefore $cE_b^{-2} = b^{-1} \cdot (b^{-1}\backslash c) = c$. □

**Theorem 7.10** *In a CC-loop, if $c$ is WIP, and if $b$ and $c$ are power-associative, then $\langle b^2, c\rangle$ is a group.*

*Proof.* By Lemmas 7.1(6) and 7.9, $cE_{b^2} = cE_b^4 = c$. Now apply Lemma 7.6. □

Applying either Theorem 7.8 or 7.10 we see that a power-associative WIP CC-loop in which every element is a square must be a group. Then, applying the Lagrange property (Corollary 3.2), we get:

**Corollary 7.11** *A finite power-associative WIP CC-loop of odd order is a group.*

This corollary is not really new. In [1], Басараб shows that a loop satisfies Wilson's identity iff it is a "generalized Moufang loop" with squares in the nucleus. Then Goodaire and Robinson [11] showed that a loop satisfies Wilson's identity iff it is a WIP CC-loop. Thus, in fact, all squares are nuclear in a WIP CC-loop, so that $Q/N(Q)$ is a boolean group. We give an example in Section 10 of a power-associative WIP CC-loop of order 16 in which $|Q/N(Q)| = 4$; this is not an extra loop (that is, some $\langle b, c\rangle$ fails to be a group), so that Theorems 7.8 and 7.10 are best possible.

# 8 Power-Associative CC-loops

Throughout this section, $(Q, \cdot)$ always denotes a power-associative CC-loop. We shall derive some further results beyond Lemma 7.1. In particular, every cube is a WIP element (see Definition 2.17), and each $E_x^6 = I$ (see Definition 2.14).

**Lemma 8.1** $R_x L_x = D_{x^{-1}} D_x$ *and* $L_x R_x = (D_x D_{x^{-1}})^{-1}$.

*Proof.* By Lemma 2.4 and Corollary 2.5, $I = G_x F_x = D_{x^{-1}}^{-1} R_x \rho \cdot \rho L_x D_x^{-1} = D_{x^{-1}}^{-1} R_x L_x D_x^{-1}$, and $I = F_x G_x = D_{x^{-1}} L_x \lambda \cdot \lambda R_x D_x = D_{x^{-1}} L_x R_x D_x$. □

Note that this lemma requires that power-associativity hold in $Q$, not just that the particular element $x$ is power-associative, since we needed $\rho^2 = I$, or equivalently, $\rho = \lambda$; see Lemma 2.16.

Compare the following lemma with Lemma 5.1.

**Lemma 8.2** $(x \cdot xy) \cdot y^{-1}x^{-1} = x$ *and* $x^{-1}y^{-1} \cdot (yx \cdot x) = x$.

*Proof.* We compute

$$\begin{aligned}
L_x^2 &= E_x R_{x^{-1}} L_x^2 R_x && \text{(Lemma 7.1)}\\
&= E_x F_x D_{x^{-1}}^{-1} D_x^{-1} && \text{(Lemmas 2.4 and 8.1)}\\
&= E_x F_x G_x J R_x^{-1} D_x^{-1} && \text{(Lemma 2.4)}\\
&= E_x J R_x^{-1} D_x^{-1} && \text{(Corollary 2.5)}\\
&= J E_x R_x^{-1} D_x^{-1} && \text{(Lemma 2.13)}\\
&= J R_{x^{-1}} D_x^{-1} && \text{(Lemma 7.1(4))}
\end{aligned}$$

Thus $x \cdot xy = x/(y^{-1}x^{-1})$ or $(x \cdot xy) \cdot y^{-1}x^{-1} = x$, as claimed. □

**Lemma 8.3** *$y^{-1} \cdot (yR_x^3) = x^3$ and $(yL_x^3) \cdot y^{-1} = x^3$.*

*Proof.* By Lemma 2.6, $R_x^{-1}L_uR_x = L_{x^{-1}\backslash u}L_x^{-1}$, so $R_xL_{y^{-1}} = L_{x^{-1}y^{-1}}R_xL_x$. Thus, $y^{-1} \cdot (yR_x^3) = (yx \cdot x)R_xL_{y^{-1}} = (yx \cdot x)L_{x^{-1}y^{-1}}R_xL_x = xR_xL_x = x^3$ by Lemma 8.2. □

**Theorem 8.4** *In a power-associative CC-loop, every cube is a WIP element.*

*Proof.* From Lemmas 7.1(4,5) and 8.3, $E_x^3L_{x^3} = L_x^3 = JD_{x^3}^{-1}$ and $E_x^{-3}R_{x^3} = R_x^3 = JD_{x^3}$. Thus $I = JE_x^3L_{x^3}JE_x^{-3}R_{x^3} = JL_{x^3}JR_{x^3}$, by Lemma 7.1. Therefore $JL_{x^3}J = R_{x^3}^{-1}$, that is, $x^3$ is a WIP element. □

**Corollary 8.5** *For each $b, c$ in a power-associative CC-loop, $\langle b, c^6\rangle$ and $\langle b^2, c^3\rangle$ are groups.*

*Proof.* $c^3$ is WIP, so apply Theorems 7.8 and 7.10. □

The examples in Section 10 show that some $\langle b^2, c^2\rangle$ can fail to be a group (see Table 1), and so can some $\langle b^3, c^3\rangle$ (see Table 2).

**Corollary 8.6** *If $Q$ is a power-associative CC-loop in which every element is a sixth power, then $Q$ is a group.*

*Proof.* $Q$ is diassociative, and hence an extra loop. However, in an extra loop, all squares are in the nucleus [9], and so $Q = N(Q)$ is a group. □

Then, applying the Lagrange property (Corollary 3.2), we get:

**Corollary 8.7** *If $Q$ is a finite power-associative CC-loop of order relatively prime to 6, then $Q$ is a group.*

In a power-associative CC-loop, Lemma 7.1(6), Theorem 8.4, and Lemma 7.7 imply $E_x^{18} = E_{x^3}^2 = I$. We conclude this section with an improvement of this.

**Lemma 8.8** *In a power-associative CC-loop, $x^2 = y \cdot ((x^{-1}y)^{-1} \cdot x)$ and $x^2 = (x \cdot (yx^{-1})^{-1}) \cdot y$. Thus $D_{x^2} = L_{x^{-1}}JR_x$ and $D_{x^2}^{-1} = R_{x^{-1}}JL_x$.*

*Proof.* In Lemma 7.4, set $y = x^{-1}u$ and $z = (x^{-1}u)^{-1}$ to get $x^2 = u \cdot ((x^{-1}u)^{-1} \cdot x)$. □

**Theorem 8.9** *Every power-associative CC-loop satisfies $E_x^6 = I$ for all $x$.*

*Proof.*

$$\begin{array}{rcll} E_x^{-3} L_x^6 & = & L_{x^2}^3 & \text{(Lemma 7.1(5))} \\ & = & J D_{x^6}^{-1} & \text{(Lemma 8.3)} \\ & = & J R_{x^{-3}} J L_{x^3} & \text{(Lemma 8.8)} \\ & = & L_{x^{-3}}^{-1} L_{x^3} & \text{(Theorem 8.4)} \\ & = & E_x^6 L_x^3 E_x^{-3} L_x^3 & \text{(Lemma 7.1(5))} \\ & = & E_x^3 L_x^6 & \text{(Lemma 7.1(1))} \end{array}$$

Rearranging, we have $E_x^6 = I$. □

# 9 Semidirect Products

This standard construction from group theory generalizes to loops. We follow Goodaire and Robinson [12].

**Definition 9.1**

1. *Let $A, K$ be loops, and assume that $\varphi : A \to \mathrm{Sym}(K)$ satisfies $\varphi_{1_A} = I$ and $(1_K)\varphi_a = 1_K$ for all $a \in A$. The* external semidirect product $A \ltimes_\varphi K$ *is the set $A \times K$ with the binary operation*

$$(a, x)(b, y) := (ab,\ (x)\varphi_b \cdot y).$$

   *for $a, b \in A$, $x, y \in K$. We write $A \ltimes K$ when $\varphi$ is clear from context.*

2. *A loop $Q$ is an* internal semidirect product *of subloops $A$ and $K$ if $K$ is normal in $Q$, $Q = AK$, $A \cap K = \{1\}$, and each of $(K, A, K)$, $(A, A, K)$, and $(A, K, Q)$ associates.*

The external semidirect product $A \ltimes K$ is clearly a loop with left and right division operations given, respectively, by

$$\begin{array}{rcl} (a, x)\backslash(b, y) & = & (a\backslash b,\ [(x)\varphi_{a\backslash b}]\backslash y) \\ (a, x)/(b, y) & = & (a/b,\ (x/y)\varphi_b^{-1}) \end{array}$$

The following comes from [12], Thms. 2.3 and 2.4.

**Proposition 9.2**

1. *If $Q = A \ltimes K$ is an external semidirect product of loops $A$ and $K$, then $Q$ is isomorphic to the internal semidirect product of the subloops $A \times \{1\}$ and $\{1\} \times K$.*

2. *If a loop $Q$ is an internal semidirect product of subloops $A$ and $K$, then $Q$ is isomorphic to an external semidirect product $A \ltimes_\varphi K$, where $\varphi : A \to \mathrm{Sym}(K)$ is defined by: $\varphi_a = R_a L_a^{-1} \restriction K$.*

For CC-loops, the notion of semidirect product is much closer to its group-theoretic specialization than for arbitrary loops. Recall from Definition 4.7 the notion of a nuclear automorphism.

**Lemma 9.3** *Let $Q$ be a CC-loop which is an internal semidirect product of subloops $A$ and $K$, and define $\varphi : A \to \mathrm{Sym}(K)$ by $\varphi_a := R_a L_a^{-1} \restriction K$ for each $a \in A$. Then $\varphi(A) \subseteq N\mathrm{Aut}(K)$, and $\varphi : A \to N\mathrm{Aut}(K)$ is a homomorphism.*

*Proof.* Since $(A, K, Q)$ associates, we apply Lemma 6.2 repeatedly in what follows without explicit reference. (In CC-loops, the conditions that $(K, A, K)$ and $(A, A, K)$ associate are redundant.) For $x, y \in K$, $a \in A$,

$$a \cdot (xy)\varphi_a = x \cdot ya = x(a \cdot (y)\varphi_a) = xa \cdot (y)\varphi_a = (a \cdot (x)\varphi_a) \cdot (y)\varphi_a.$$

Thus $(xy)\varphi_a = (x)\varphi_a \cdot (y)\varphi_a$, and so $\varphi_a \in \mathrm{Aut}(K)$. Now for each $x \in K$, $a \in A$, Theorem 3.1 implies there exists $c \in N(Q)$ such that $(x)\varphi_a = xc$. But since $(x)\varphi_a \in K$, we have $c \in K \cap N(Q) \subseteq N(K)$. Thus $\varphi_a \in N\mathrm{Aut}(K)$. Finally, for $a, b \in A$, $x \in K$, we compute

$$ab \cdot (x)\varphi_{ab} = xa \cdot b = (a \cdot (x)\varphi_a)b = a((x)\varphi_a \cdot b) = a(b \cdot (x)\varphi_a\varphi_b).$$

Thus $(x)\varphi_{ab} = (x)\varphi_a\varphi_b$. This completes the proof. □

We take notational advantage of Lemma 9.3 as follows: if $A \ltimes K$ is a CC-loop, then we set $x^a := (x)\varphi_a$ for $x \in K$, $a \in A$. Note that $x^{a^\lambda} = x^{a^\rho} = (x)\varphi_a^{-1}$.

We now prove that the necessary conditions for a semidirect product to be a CC-loop given in Lemma 9.3 are also sufficient (Theorem 9.4). This generalizes D.A. Robinson's characterization of when $A \ltimes K$ is an extra loop in the case where $A$ is a group [17].

**Theorem 9.4** *Let $A, K$ be CC-loops, and $\varphi \in \mathrm{Hom}(A, \mathrm{Aut}(K))$. Then the following are equivalent:*

1. *$A \ltimes_\varphi K$ is a CC-loop.*
2. *$\varphi_b \in N\mathrm{Aut}(K)$ for all $b \in A$.*
3. *The triples*

$$\mathcal{U}(x, b) := (L_{x^b} R_x^{-1}, L_x, L_{x^b}) \qquad \text{and} \qquad \mathcal{V}(x, b) := (R_x, R_{x^b} L_x^{-1}, R_{x^b})$$

*are in $\mathrm{Atop}(K)$ for all $x \in K$ and $b \in A$.*

*Proof.* For (2) $\leftrightarrow$ (3): Fix $x \in K$ and $b \in A$. We have $\mathcal{L}_x := (L_x R_x^{-1}, L_x, L_x) \in$ Atop$(K)$ by Lemmas 2.2 and 2.4. Hence, $\mathcal{U}(x,b)\mathcal{L}_x^{-1} = (L_{x^b} L_x^{-1}, I, L_{x^b} L_x^{-1})$. Now if $\mathcal{U}(x,b) \in$ Atop$(K)$, then by Lemma 2.8(2), $1 L_{x^b} L_x^{-1} = x\backslash(x^b) \in N(K)$, so that $\varphi_b$ is a nuclear automorphism. Conversely, if $\varphi_b$ is nuclear, fix $k \in N(K)$ such that $x^b = xk$. Then $L_{x^b} L_x^{-1} = L_k$, and so $\mathcal{U}(x,b)\mathcal{L}_x^{-1} = (L_k, I, L_k) \in$ Atop$(K)$ by Lemma 2.8(1). Thus $\mathcal{U}(x,b) \in$ Atop$(K)$ since Atop$(K)$ is a group. A similar argument shows the equivalence of $\varphi_b \in N$Aut$(K)$ and $\mathcal{V}(x,b) \in$ Atop$(K)$.

For (1) $\leftrightarrow$ (3): Fix $(a,x),(b,y),(c,z) \in A \ltimes K$, and write out the two sides of $RCC$ in $A \ltimes K$ using $f(u,v) = (uv)/u$ (Lemma 2.4) in $K$. The left side is

$$(a,x)\cdot(b,y)(c,z) = (a\cdot bc,\ x^{bc}\cdot y^c z) \quad .$$

The right side is

$$[((a,x)(b,y))/(a,x)]\cdot(a,x)(c,z) = (f(a,b)\cdot ac,\ [(x^{bc}y^c)/(x^c)]\cdot x^c z) \quad .$$

Equating the $K$-components, replacing $z$ by $z^c$ and then applying the automorphism $\varphi_c^{-1}$, we get $x^b \cdot yz = [(x^b y)/x]\cdot xz$. Thus $A \ltimes K$ satisfies $RCC$ iff each $\mathcal{U}(x,b) \in$ Atop$(K)$.

Likewise, we can write out the two sides of $LCC$ in $A \ltimes K$ using $g(u,v) = u\backslash(vu)$ in $K$. The left side is

$$(c,z)(b,y)\cdot(a,x) = (cb\cdot a,\ z^{ba}y^a\cdot x) \quad .$$

The right side is

$$(c,z)(a,x)\cdot[(a,x)\backslash((b,y)(a,x))] = (ca\cdot g(a,b),\ (z^{ba}x^{a\backslash(ba)})[x^{a\backslash(ba)}\backslash(y^a x)]) \quad .$$

Equating the $K$-components, replacing $x$ by $x^{b^\lambda a}$, $z$ by $z^{b^\lambda}$, and then applying the automorphism $\varphi_a^{-1}$, we get $zy\cdot x^d = zx\cdot[x\backslash(yx^d)]$ where $d = b^\lambda$. Thus $A \ltimes K$ satisfies $LCC$ iff every $\mathcal{V}(x,d) \in$ Atop$(K)$. $\square$

We remark that the implication (1) $\to$ (2) follows directly from Lemma 9.3. However, the proof of Theorem 9.4 has the advantage of offering a characterization of when $A \ltimes_\varphi Q$ satisfies $RCC$ or $LCC$ alone, while our proof of Lemma 9.3 relies on Theorem 3.1. We also remark that in proving (1) $\leftrightarrow$ (3), the arguments for $LCC$ and $RCC$ are similar, but we could not simply say that the $LCC$ case follows from the $RCC$ case "by mirror symmetry", since there is an asymmetry in the definition of $A \ltimes Q$.

Theorem 9.4 suggests that a natural definition of *holomorph* for a CC-loop $Q$ is $N$Aut$(Q) \ltimes_\varphi Q$, where $\varphi$ is the identity map. (This differs slightly from the usage in §5 of Bruck [4].) If $Q$ is a group, then $N$Aut$(Q) =$ Aut$(Q)$, and $N$Aut$(Q) \ltimes_\varphi Q$ reduces to the usual definition of holomorph in group theory.

# 10 Examples

| • | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 1 | 1 | 2 | 0 | 4 | 5 | 3 | 7 | 8 | 6 | 10 | 11 | 9 | 13 | 14 | 12 | 16 | 17 | 15 | 19 | 20 | 18 | 22 | 23 | 21 | 25 | 26 | 24 |
| 2 | 2 | 0 | 1 | 5 | 3 | 4 | 8 | 6 | 7 | 11 | 9 | 10 | 14 | 12 | 13 | 17 | 15 | 16 | 20 | 18 | 19 | 23 | 21 | 22 | 26 | 24 | 25 |
| 3 | 3 | 4 | 5 | 6 | 7 | 8 | 0 | 1 | 2 | 12 | 13 | 14 | 16 | 17 | 15 | 11 | 9 | 10 | 22 | 23 | 21 | 24 | 25 | 26 | 20 | 18 | 19 |
| 4 | 4 | 5 | 3 | 7 | 8 | 6 | 1 | 2 | 0 | 13 | 14 | 12 | 17 | 15 | 16 | 9 | 10 | 11 | 23 | 21 | 22 | 25 | 26 | 24 | 18 | 19 | 20 |
| 5 | 5 | 3 | 4 | 8 | 6 | 7 | 2 | 0 | 1 | 14 | 12 | 13 | 15 | 16 | 17 | 10 | 11 | 9 | 21 | 22 | 23 | 26 | 24 | 25 | 19 | 20 | 18 |
| 6 | 6 | 7 | 8 | 0 | 1 | 2 | 3 | 4 | 5 | 15 | 16 | 17 | 11 | 9 | 10 | 13 | 14 | 12 | 26 | 24 | 25 | 18 | 19 | 20 | 22 | 23 | 21 |
| 7 | 7 | 8 | 6 | 1 | 2 | 0 | 4 | 5 | 3 | 16 | 17 | 15 | 9 | 10 | 11 | 14 | 12 | 13 | 24 | 25 | 26 | 19 | 20 | 18 | 23 | 21 | 22 |
| 8 | 8 | 6 | 7 | 2 | 0 | 1 | 5 | 3 | 4 | 17 | 15 | 16 | 10 | 11 | 9 | 12 | 13 | 14 | 25 | 26 | 24 | 20 | 18 | 19 | 21 | 22 | 23 |
| 9 | 9 | 10 | 11 | 12 | 13 | 14 | 16 | 17 | 15 | 18 | 19 | 20 | 22 | 23 | 21 | 24 | 25 | 26 | 0 | 1 | 2 | 5 | 3 | 4 | 8 | 6 | 7 |
| 10 | 10 | 11 | 9 | 13 | 14 | 12 | 17 | 15 | 16 | 19 | 20 | 18 | 23 | 21 | 22 | 25 | 26 | 24 | 1 | 2 | 0 | 3 | 4 | 5 | 6 | 7 | 8 |
| 11 | 11 | 9 | 10 | 14 | 12 | 13 | 15 | 16 | 17 | 20 | 18 | 19 | 21 | 22 | 23 | 26 | 24 | 25 | 2 | 0 | 1 | 4 | 5 | 3 | 7 | 8 | 6 |
| 12 | 12 | 13 | 14 | 15 | 16 | 17 | 10 | 11 | 9 | 21 | 22 | 23 | 26 | 24 | 25 | 20 | 18 | 19 | 4 | 5 | 3 | 8 | 6 | 7 | 1 | 2 | 0 |
| 13 | 13 | 14 | 12 | 16 | 17 | 15 | 11 | 9 | 10 | 22 | 23 | 21 | 24 | 25 | 26 | 18 | 19 | 20 | 5 | 3 | 4 | 6 | 7 | 8 | 2 | 0 | 1 |
| 14 | 14 | 12 | 13 | 17 | 15 | 16 | 9 | 10 | 11 | 23 | 21 | 22 | 25 | 26 | 24 | 19 | 20 | 18 | 3 | 4 | 5 | 7 | 8 | 6 | 0 | 1 | 2 |
| 15 | 15 | 16 | 17 | 9 | 10 | 11 | 13 | 14 | 12 | 24 | 25 | 26 | 18 | 19 | 20 | 22 | 23 | 21 | 8 | 6 | 7 | 2 | 0 | 1 | 3 | 4 | 5 |
| 16 | 16 | 17 | 15 | 10 | 11 | 9 | 14 | 12 | 13 | 25 | 26 | 24 | 19 | 20 | 18 | 23 | 21 | 22 | 6 | 7 | 8 | 0 | 1 | 2 | 4 | 5 | 3 |
| 17 | 17 | 15 | 16 | 11 | 9 | 10 | 12 | 13 | 14 | 26 | 24 | 25 | 20 | 18 | 19 | 21 | 22 | 23 | 7 | 8 | 6 | 1 | 2 | 0 | 5 | 3 | 4 |
| 18 | 18 | 19 | 20 | 21 | 22 | 23 | 26 | 24 | 25 | 0 | 1 | 2 | 5 | 3 | 4 | 6 | 7 | 8 | 9 | 10 | 11 | 13 | 14 | 12 | 16 | 17 | 15 |
| 19 | 19 | 20 | 18 | 22 | 23 | 21 | 24 | 25 | 26 | 1 | 2 | 0 | 3 | 4 | 5 | 7 | 8 | 6 | 10 | 11 | 9 | 14 | 12 | 13 | 17 | 15 | 16 |
| 20 | 20 | 18 | 19 | 23 | 21 | 22 | 25 | 26 | 24 | 2 | 0 | 1 | 4 | 5 | 3 | 8 | 6 | 7 | 11 | 9 | 10 | 12 | 13 | 14 | 15 | 16 | 17 |
| 21 | 21 | 22 | 23 | 24 | 25 | 26 | 20 | 18 | 19 | 3 | 4 | 5 | 6 | 7 | 8 | 2 | 0 | 1 | 13 | 14 | 12 | 16 | 17 | 15 | 9 | 10 | 11 |
| 22 | 22 | 23 | 21 | 25 | 26 | 24 | 18 | 19 | 20 | 4 | 5 | 3 | 7 | 8 | 6 | 0 | 1 | 2 | 14 | 12 | 13 | 17 | 15 | 16 | 10 | 11 | 9 |
| 23 | 23 | 21 | 22 | 26 | 24 | 25 | 19 | 20 | 18 | 5 | 3 | 4 | 8 | 6 | 7 | 1 | 2 | 0 | 12 | 13 | 14 | 15 | 16 | 17 | 11 | 9 | 10 |
| 24 | 24 | 25 | 26 | 18 | 19 | 20 | 23 | 21 | 22 | 6 | 7 | 8 | 1 | 2 | 0 | 4 | 5 | 3 | 17 | 15 | 16 | 10 | 11 | 9 | 14 | 12 | 13 |
| 25 | 25 | 26 | 24 | 19 | 20 | 18 | 21 | 22 | 23 | 7 | 8 | 6 | 2 | 0 | 1 | 5 | 3 | 4 | 15 | 16 | 17 | 11 | 9 | 10 | 12 | 13 | 14 |
| 26 | 26 | 24 | 25 | 20 | 18 | 19 | 22 | 23 | 21 | 8 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 16 | 17 | 15 | 9 | 10 | 11 | 13 | 14 | 12 |

Table 1: A Power-Associative CC-Loop

The example in Table 1 is a power-associative CC-loop of order 27 and exponent three. $Z(Q) = N(Q) = \{0, 1, 2\}$, and $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ is a normal subloop. Note that $|Z(Q)| = 3$ is required for non-associative CC-loops of order 27 by Corollary 3.5.

This loop also has the Automorphic Inverse Property (AIP); that is, $J \in \mathrm{Aut}(Q)$.

The example in Table 2 is a power-associative CC-loop of order 16. The loop must have the weak inverse property because $3 \nmid 16$, so every element is a cube (see Theorem 8.4). It is not diassociative because $4 \cdot (8 \cdot 4) \neq (4 \cdot 8) \cdot 4$; also, $Q = \langle 4, 8 \rangle$. $Z(Q) = N(Q) = \{0, 1, 2, 3\}$, so all squares are in the nucleus.

| $\bullet$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 1 | 1 | 2 | 3 | 0 | 5 | 6 | 7 | 4 | 9 | 10 | 11 | 8 | 13 | 14 | 15 | 12 |
| 2 | 2 | 3 | 0 | 1 | 6 | 7 | 4 | 5 | 10 | 11 | 8 | 9 | 14 | 15 | 12 | 13 |
| 3 | 3 | 0 | 1 | 2 | 7 | 4 | 5 | 6 | 11 | 8 | 9 | 10 | 15 | 12 | 13 | 14 |
| 4 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 12 | 13 | 14 | 15 | 10 | 11 | 8 | 9 |
| 5 | 5 | 6 | 7 | 4 | 1 | 2 | 3 | 0 | 13 | 14 | 15 | 12 | 11 | 8 | 9 | 10 |
| 6 | 6 | 7 | 4 | 5 | 2 | 3 | 0 | 1 | 14 | 15 | 12 | 13 | 8 | 9 | 10 | 11 |
| 7 | 7 | 4 | 5 | 6 | 3 | 0 | 1 | 2 | 15 | 12 | 13 | 14 | 9 | 10 | 11 | 8 |
| 8 | 8 | 9 | 10 | 11 | 15 | 12 | 13 | 14 | 0 | 1 | 2 | 3 | 7 | 4 | 5 | 6 |
| 9 | 9 | 10 | 11 | 8 | 12 | 13 | 14 | 15 | 1 | 2 | 3 | 0 | 4 | 5 | 6 | 7 |
| 10 | 10 | 11 | 8 | 9 | 13 | 14 | 15 | 12 | 2 | 3 | 0 | 1 | 5 | 6 | 7 | 4 |
| 11 | 11 | 8 | 9 | 10 | 14 | 15 | 12 | 13 | 3 | 0 | 1 | 2 | 6 | 7 | 4 | 5 |
| 12 | 12 | 13 | 14 | 15 | 11 | 8 | 9 | 10 | 6 | 7 | 4 | 5 | 3 | 0 | 1 | 2 |
| 13 | 13 | 14 | 15 | 12 | 8 | 9 | 10 | 11 | 7 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 14 | 14 | 15 | 12 | 13 | 9 | 10 | 11 | 8 | 4 | 5 | 6 | 7 | 1 | 2 | 3 | 0 |
| 15 | 15 | 12 | 13 | 14 | 10 | 11 | 8 | 9 | 5 | 6 | 7 | 4 | 2 | 3 | 0 | 1 |

Table 2: A Power-Associative WIP CC-Loop

These examples were found by the program SEM [19]. As usual, once one is given such an example, it is easy to write a very short program (in, e.g., C or java or python) to verify the claimed properties for it.

# References


[1] А. С. Басараб, Об одном классе $G$-луп, *Математические Исследования* Том 3, Вып. 2 (8) (1968) 72–77.

[2] А. С. Басараб, Класс LK-луп, *Математические Исследования* Вып. 120 (1991) 3–7.

[3] В. Д. Белоусов, *Основы Теории Квазигрупп и Луп*, Издательство «Наука», Москва, 1967.

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

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

[6] R. H. Bruck and L. J. Paige, Loops whose inner mappings are automorphisms, *Ann. of Math.* (2) (1956) 308–323.

[7] O. Chein, M. K. Kinyon, A. Rajah, and P. Vojtěchovský, Loops and the Lagrange property, to appear in *Results Math.*

[8] F. Fenyves, Extra loops I, *Publ. Math. Debrecen* 15 (1968) 235–238.

[9] F. Fenyves, Extra loops II, *Publ. Math. Debrecen* 16 (1969) 187–192.

[10] 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.

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

[12] E. G. Goodaire and D. A. Robinson, Semi-direct products and Bol loops, *Demonstratio Math.* 27 (1994) 573–588.

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

[14] W.W. McCune, *OTTER 3.0 Reference Manual and Guide*, Technical Report ANL-94/6, Argonne National Laboratory, 1994; or see: `http://www-fp.mcs.anl.gov/division/software/`

[15] J. M. Osborn, Loops with the weak inverse property, *Pacific J. Math.* 10 (1960) 295–304.

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

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

[18] Л. Р. Сойкис, О Специальных лупах, in *Вопросы Теории Квазигрупп и Луп* (В. Д. Белоусов , ed.), Редакц.-Издат. Отдел Акад. Наук Молдав. ССР, Кишинев, 1970, pp. 122–131.

[19] J. Zhang and H. Zhang, SEM: a system for enumerating models, *Proc. 14th Int.. Joint Conf. on AI (IJCAI-95)*, Montréal, 1995, pp. 298 – 303; available at URL: `http://www.cs.uiowa.edu/~hzhang/`