The Structure of Conjugacy Closed Loops [*]

Kenneth Kunen [†]
University of Wisconsin, Madison, WI 53706, U.S.A.
kunen@math.wisc.edu

March 12, 1998

Abstract

We study structure theorems for the conjugacy closed (CC-) loops, a specific variety of G-loops (loops isomorphic to all their loop isotopes). These theorems give a description all such loops of small order. For example, if p and q are primes, $p < q$, and $q - 1$ is not divisible by p, then the only CC-loop of order pq is the cyclic group of order pq. For any prime $q > 2$, there is exactly one non-group CC-loop in order $2q$, and exactly three in order q^2. We also derive a number of equations valid in all CC-loops. By contrast, every equation valid in all G-loops is valid in all loops.

1 Introduction

A *quasigroup* is a system $\mathcal{Q} = (G, \cdot)$ such that G is a non-empty set and $\cdot$ is a binary function on G satisfying $\forall xy \exists ! z (xz = y)$ and $\forall xy \exists ! z (zx = y)$. In a quasigroup, we may name the z as a function of x, y and define *left division*, $\backslash$, and *right division*, $/$, by:

$$x \cdot (x \backslash y) = y \qquad (y/x) \cdot x = y \tag{1}$$

[*] 1991 Mathematics Subject Classification: Primary 20N05; Secondary 03C05, 08A05.

[†] Author supported by NSF Grants CCR-9503445 and DMS-9704520. The author is grateful to the referee for many helpful comments on the original draft of this paper.

By cancellation, and setting $y = xu$ or $y = ux$, we have also

$$x\backslash(x \cdot u) = u \qquad (u \cdot x)/x = u \tag{2}$$

As usual, equations written this way with variables are understood to be universally quantified. Quasigroups are often defined to be systems of the form $\mathcal{Q} = (G, \cdot, \backslash, /)$ satisfying (1) and (2); this lets us define the notion in a purely equational way, without existential quantifiers. A *loop* is a quasigroup which has an identity element, 1, satisfying $\forall x(x1 = 1x = x)$. See the books [1], [5], [16] for general background and references to the literature on quasigroups and loops.

There are probably no interesting results about the class of all loops, since it is too broad; for example, there are already 109 loops of order six [2]. However, there has been much study of specific classes of loops. Most well-known are the groups, which are the associative loops. For these, there are many structure theorems, which enable one to enumerate easily the groups of small orders; for example, there are only two groups of order six. In this paper, we look at structure theorems for conjugacy closed loops.

Definition 1.1 *A loop is* conjugacy closed *(or a* CC-loop*) iff it satisfies the two identities:*

$$RCC: \ z(yx) = ((zy)/z)(zx) \qquad\qquad LCC: \ (xy)z = (xz)(z\backslash(yz))$$

Actually, every quasigroup satisfying both these identities must be a loop; see Section 6. Clearly, every group is a CC-loop. The reason for the terminology "conjugacy closed" is explained in Remark 3.2.

The reader unfamiliar with previous work on these loops [10][11][17] may not see why this particular variety of loop is interesting. One motivation for studying CC-loops is that they arise naturally in the study of isotopy, and the CC-loops form a natural variety of G-loops (= isotopy-isomorphy loops), as we explain in Section 2, which collects some useful results and definitions from the literature. The other is that the CC-loops have a non-trivial structure theory, described in Section 4; see also Goodaire and Robinson [10], where the notion originated. Using this structure theory, one may compute the CC-loops of small order. For example, if p is an odd prime, we show (Theorem 4.15) that the only non-group CC-loop of order $2p$ is the one constructed by R. L. Wilson, Jr. [19]. For $p = 3$, this loop is displayed in Table 1. Also

Table 1: A CC-Loop

$\bullet$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	5	6	4
3	3	1	2	6	4	5
4	4	6	5	2	1	3
5	5	4	6	3	2	1
6	6	5	4	1	3	2

(Theorem 4.17), in order p^2, there are exactly three non-group CC-loops, constructed by the method of Goodaire and Robinson [10].

By another result of Wilson [18], the only G-loop, and hence the only CC-loop, of prime order p is the cyclic group of order p. We show (Theorem 4.17) that for CC-loops, the same is true for orders pq, where $p < q$ are primes with $q - 1$ not divisible by p. Note that for these pq, the fact that any *group* of order pq must be cyclic is an easy exercise in using the Sylow theorems. The structure theory for CC-loops uses combinatorial arguments similar to those used in the proof of the Sylow theorems.

If $p < q$ are primes and $q - 1$ is divisible by p, then in order pq, there are CC-loops which are not groups (see Corollary 3.3.1 of [10]), as well as non-abelian groups.

The Moufang loops, whose structure is already widely discussed in the literature [1][4], are always diassociative (that is, every two elements generate a group) by Moufang's Theorem. The CC-loops need not even be power associative (that is, every single element generates a group); for example, in Table 1, the single element 4 generates the whole loop. It is shown in [11] that the CC-loops which are diassociative (equivalently, Moufang) are the extra loops studied by Fenyves [7][8].

It might seem that the structure for non-power-associative loops might be intractable, but we show (Theorem 3.11) that in a CC-loop, $xy = 1$ implies that yx is in the nucleus. From this we shall conclude (Theorem 3.21) that either the loop is power associative or the nucleus is non-trivial. In particular (Corollary 4.6), this implies that if G is any finite CC-loop, then for *some* prime p dividing $|G|$, G has a subloop H isomorphic to the cyclic group of order p. In Table 1, $|G| = 6$, $p = 3$, and $H = \{1, 2, 3\}$; there are no subloops of order 2, as one might have hoped from group theory.

Our structure theory succeeds through the study of loop automorphisms. In a group, the inner automorphisms are related to failures of commutativity. In the same way, CC-loops possess a family of automorphisms related to failures of associativity. This is described in more detail in Section 2. In Section 3, we derive a number of equations and implications between equations used in the structure theory in Section 4. The division between these two sections is a bit arbitrary, but in general, the results of Section 3 hold for all CC-loops, whereas Section 4 uses counting arguments to prove theorems about finite CC-loops.

One might ask to what extent the results of this paper hold for G-loops in general. In Section 5 we show that every equation (in fact, every universal statement) true in all G-loops is true in all loops, so that we do not have any analog to the results in Section 3.

In developing this work, we have found it very useful to use the automated reasoning tools OTTER [15], programmed by W. W. McCune, and SEM [20], programmed by J. Zhang and H. Zhang. OTTER is used in deriving equations from other equations, and was instrumental in producing many of the results in Section 3. OTTER's proofs are simply sequences of fifty or so intermediate equations, and seem at first to have little intuitive content, but following the method of previous work [12][13][14], we have rephrased OTTER's proofs using more conceptual notions, such as the action of automorphisms. SEM is used to construct finite examples. For example, the CC-loops given in Table 1 and Example 2.20 were constructed using SEM. Once one has such an example, it is usually possible to describe it in a more conceptual way; for example, the loop in Table 1 can be recognized as the one already constructed by Wilson (see [19] or Theorem 4.15), and we have described the one in Example 2.20 as a semidirect product. We originally tried to use SEM to construct a non-group CC-loop of order 15, but this failed, proving that there was no such loop. We then found the proof in this paper (Theorem 4.17), which does not rely on a computer search and which generalizes to other orders of the form pq. Besides the results explicitly presented in this paper, OTTER and SEM were very useful for quick experimentation and for checking out (often false) conjectures.

2 Isotopy and G-Loops

Throughout this section, $(G, \cdot)$ always denotes a loop. The theory of isotopy lets us associate with $(G, \cdot)$ a number of permutation groups. One may then apply familiar methods from group theory to study G. We begin with the *autotopy group* (see [1], p. 112).

Definition 2.1 *$\mathcal{SYM}(G)$ is the group of all permutations of the set G; $I \in \mathcal{SYM}(G)$ is the identity element. $\mathcal{ATOP}(G, \cdot)$ is the set of triples (α, β, γ) in $(\mathcal{SYM}(G))^3$ such that*

$$\forall x, y, z \in G[x\alpha \cdot y\beta = (xy)\gamma]$$

It is easy to see that $\mathcal{ATOP}(G)$ is a subgroup of $(\mathcal{SYM}(G))^3$.

Definition 2.2 *Define $\mathcal{AUT}(G, \cdot), \mathcal{LII}(G, \cdot), \mathcal{RII}(G, \cdot), \mathcal{II}(G, \cdot)$ by:*

$$\begin{array}{rcl} \alpha \in \mathcal{AUT}(G, \cdot) & \Longleftrightarrow & (\alpha, \alpha, \alpha) \in \mathcal{ATOP}(G, \cdot) \\ \alpha \in \mathcal{LII}(G, \cdot) & \Longleftrightarrow & \exists \phi \in \mathcal{SYM}(G)[\,(\phi, \alpha, \alpha) \in \mathcal{ATOP}(G, \cdot)\,] \\ \alpha \in \mathcal{RII}(G, \cdot) & \Longleftrightarrow & \exists \psi \in \mathcal{SYM}(G)[\,(\alpha, \psi, \alpha) \in \mathcal{ATOP}(G, \cdot)\,] \\ \alpha \in \mathcal{II}(G, \cdot) & \Longleftrightarrow & \exists \phi, \psi \in \mathcal{SYM}(G)[\,(\phi, \psi, \alpha) \in \mathcal{ATOP}(G, \cdot)\,] \end{array}$$

So, $\mathcal{AUT}(G, \cdot)$ is the group of automorphisms of $(G, \cdot)$. Bryant and Schneider [2] called $\mathcal{II}(G, \cdot)$ the *group* of $(G, \cdot)$. It is immediate from the definitions that:

Lemma 2.3 *Each of the sets $\mathcal{AUT}(G, \cdot), \mathcal{LII}(G, \cdot), \mathcal{RII}(G, \cdot), \mathcal{II}(G, \cdot)$ is a subgroup of $\mathcal{SYM}(G)$. Furthermore,*
$\mathcal{AUT}(G, \cdot) \subseteq \mathcal{LII}(G, \cdot) \cap \mathcal{RII}(G, \cdot)$, and
$\mathcal{LII}(G, \cdot) \cup \mathcal{RII}(G, \cdot) \subseteq \mathcal{II}(G, \cdot)$.

Another family of elements of $\mathcal{SYM}(G)$ is given by left and right multiplications by elements of G:

Definition 2.4 *Define, for each $a \in G$, $L_a = L(a)$ and $R_a = R(a)$ in $\mathcal{SYM}(G)$ by:*

$$xL_a = a \cdot x \qquad\qquad xR_a = x \cdot a$$

These are related to the autotopy group by:

Lemma 2.5 *Suppose that* $(\alpha,\beta,\gamma) \in \mathcal{ATOP}(G,\cdot)$. *Let* $b = 1\beta^{-1}$ *and* $a = 1\alpha^{-1}$. *Then for all* x, y: $x\alpha = (xb)\gamma$, $y\beta = (ay)\gamma$, *and* $(xb)\gamma \cdot (ay)\gamma = (xy)\gamma$. *Thus,* $\alpha = R_b\gamma$, $\beta = L_a\gamma$, *and* $(R_b\gamma, L_a\gamma, \gamma) \in \mathcal{ATOP}(G,\cdot)$.

Proof: Use $b\beta = 1$ and then $a\alpha = 1$ in the definition (2.1) of $\mathcal{ATOP}$. □

Now, applying this lemma to the definition of $\mathcal{LII}, \mathcal{RII}, \mathcal{II}$:

Lemma 2.6 *If* $\alpha \in \mathcal{SYM}(G)$, *then:*

1. $\alpha \in \mathcal{II}(G,\cdot)$ *iff for some* $a, b \in G$: $(R_b\alpha, L_a\alpha, \alpha) \in \mathcal{ATOP}(G,\cdot)$, *in which case* $(ab)\alpha = 1$.
2. $\alpha \in \mathcal{LII}(G,\cdot)$ *iff for some* $b \in G$: $(R_b\alpha, \alpha, \alpha) \in \mathcal{ATOP}(G,\cdot)$, *in which case* b *must be* $1\alpha^{-1}$.
3. $\alpha \in \mathcal{RII}(G,\cdot)$ *iff for some* $a \in G$: $(\alpha, L_a\alpha, \alpha) \in \mathcal{ATOP}(G,\cdot)$, *in which case* a *must be* $1\alpha^{-1}$.

Corollary 2.7 $\mathcal{AUT}(G,\cdot) = \{\alpha \in \mathcal{LII}(G,\cdot) : 1\alpha = 1\} = \{\alpha \in \mathcal{RII}(G,\cdot) : 1\alpha = 1\}$.

For every loop, we may define the left nucleus (N_λ), the middle nucleus (N_μ), the right nucleus (N_ρ), and the center (Z):

Definition 2.8 *For any loop* $(G,\cdot)$ *and* $a \in G$:
$a \in N_\lambda(G,\cdot)$ *iff* $\forall x, y \in G\,[a(xy) = (ax)y]$
$a \in N_\mu(G,\cdot)$ *iff* $\forall x, y \in G\,[x(ay) = (xa)y]$
$a \in N_\rho(G,\cdot)$ *iff* $\forall x, y \in G\,[x(ya) = (xy)a]$
$a \in Z_0(G,\cdot)$ *iff* $\forall x \in G\,[xa = ax]$
$N(G,\cdot) = N_\lambda(G,\cdot) \cap N_\mu(G,\cdot) \cap N_\rho(G,\cdot)$.
$Z(G,\cdot) = N(G,\cdot) \cap Z_0(G,\cdot)$.

It will turn out (Lemma 2.15) that $Z_0(G,\cdot) = Z(G,\cdot)$ for CC-loops. It is easy to verify the following equivalents, in terms of autotopy.

Lemma 2.9 *For any loop* $(G,\cdot)$:
$N_\lambda(G,\cdot) = \{a \in G : (L_a, I, L_a) \in \mathcal{ATOP}(G,\cdot)\}$.
$N_\mu(G,\cdot) = \{a \in G : (R_a^{-1}, L_a, I) \in \mathcal{ATOP}(G,\cdot)\}$.
$N_\rho(G,\cdot) = \{a \in G : (I, R_a, R_a) \in \mathcal{ATOP}(G,\cdot)\}$.
$Z_0(G,\cdot) = \{a \in G : L_a = R_a\}$.

Corollary 2.7 can fail for $\mathcal{II}(G,\cdot)$; that is, one can have $\alpha \in \mathcal{II}(G,\cdot)$ and $1\alpha = 1$ without α being an automorphism of the loop, but such an α must be an automorphism of the nucleus.

Lemma 2.10 *Suppose that $\alpha \in \mathcal{II}(G,\cdot)$ and $1\alpha = 1$. Then:*

1. *If either $u \in N_\lambda$ or $v \in N_\rho$, then $u\alpha \cdot v\alpha = (uv)\alpha$.*
2. *$\alpha \restriction N_\lambda \in \mathcal{AUT}(N_\lambda,\cdot)$.*
3. *$\alpha \restriction N_\rho \in \mathcal{AUT}(N_\rho,\cdot)$.*

Proof: Fix a, b as in Lemma 2.6.1. So, $(xb)\alpha \cdot (ay)\alpha = (xy)\alpha$ for all x, y. Equivalently, $u\alpha \cdot v\alpha = ((u/b) \cdot (a\backslash v))\alpha$ for all u, v. Since $(ab)\alpha = 1 = 1\alpha$, $ab = 1$. Now suppose that $u \in N_\lambda$. Then $(ua)b = u(ab) = u$, so $ua = u/b$. Hence, $u\alpha \cdot v\alpha = ((ua) \cdot (a\backslash v))\alpha = (u \cdot (a(a\backslash v)))\alpha = (uv)\alpha$. The mirror of this argument works for $v \in N_\rho$.

So, α maps N_λ isomorphically onto its range. To prove (2), we need $(N_\lambda)\alpha = N_\lambda$. Now, if $u \in N_\lambda$, then applying (1), $(u\alpha \cdot (xb)\alpha) \cdot (ay)\alpha = (uxb)\alpha \cdot (ay)\alpha = (uxy)\alpha = u\alpha \cdot (xy)\alpha = u\alpha \cdot ((xb)\alpha \cdot (ay)\alpha)$. Since $(xb)\alpha$ and $(ay)\alpha$ can be arbitrary elements of G, this proves $u\alpha \in N_\lambda$, so $(N_\lambda)\alpha \subseteq N_\lambda$. Applying this argument to α^{-1} shows $(N_\lambda)\alpha = N_\lambda$. □

So far, this whole discussion could be vacuous, since it is not clear whether $\mathcal{II}(G,\cdot)$ contains anything besides the identity permutation, I. However, in G-loops, $\mathcal{LII}$ and $\mathcal{RII}$ are large enough to make Corollary 2.7 and Lemma 2.10 useful for producing automorphisms.

Definition 2.11 *A loop G is a* G-loop *iff for each $a, b \in G$, there is an $\alpha \in \mathcal{SYM}(G)$ such that $(R_b\alpha, L_a\alpha, \alpha) \in \mathcal{ATOP}(G,\cdot)$; that is, $(xb)\alpha \cdot (ay)\alpha = (xy)\alpha$ for all $x, y \in G$.*

This α will be in $\mathcal{II}(G,\cdot)$ by Lemma 2.6.1. Furthermore, the special cases where $a = 1$ or $b = 1$ will provide us with a supply of permutations in $\mathcal{LII}(G,\cdot)$ and $\mathcal{RII}(G,\cdot)$ by Lemma 2.6.2 and Lemma 2.6.3. Actually, by E. L. Wilson [17], being a G-loop is equivalent to these special cases:

Lemma 2.12 *A loop $(G, \cdot)$ is a G-loop iff both*

- *For each $b \in G$, there is a $\beta \in \mathcal{SYM}(G)$ such that $(R_b\beta, \beta, \beta) \in \mathcal{ATOP}(G, \cdot)$, and*
- *For each $a \in G$, there is a $\gamma \in \mathcal{SYM}(G)$ such that $(\gamma, L_a\gamma, \gamma) \in \mathcal{ATOP}(G, \cdot)$.*

Proof: For the non-trivial direction, fix $a, b \in G$. First fix $\beta \in \mathcal{LII}(G, \cdot)$ such that $b = 1\beta^{-1}$, so that $(xb)\beta \cdot y\beta = (xy)\beta$ for all x, y. Then, fix $\alpha \in \mathcal{RII}(G, \cdot)$ such that $(x)\gamma \cdot (cy)\gamma = (xy)\gamma$ for all x, y, where $c = (ab)\beta$. Let $\alpha = \beta\gamma$. Then for all x, y: $(xy)\alpha = ((xb)\beta \cdot y\beta)\gamma = (xb)\beta\gamma \cdot ((ab)\beta \cdot y\beta)\gamma = (xb)\beta\gamma \cdot ((ay)\beta)\gamma = (xb)\alpha \cdot (ay)\alpha$. □

Definition 2.11 has the following interpretation: Let $u = xb$ and $v = ay$, so that we have $u\alpha \cdot v\alpha = ((u/b) \cdot (a\backslash v))\alpha$. Thus, if we define a new product, $\circ$, so that $u \circ v = (u/b) \cdot (a\backslash v)$, then $\circ$ is another loop operation on G, with identity $a \cdot b$, and α is an isomorphism from $(G, \cdot)$ to $(G, \circ)$. This $\circ$ is called a *principal loop isotope*. That is, the G-loops are those loops which are isomorphic to all their principal loop isotopes, and $\alpha \in \mathcal{II}(G, \cdot)$ iff α is an Isomorphism onto a principal loop Isotope.

In a G-loop, Definition 2.11 "seems" to pair an $\alpha \in \mathcal{II}(G, \cdot)$ with an $(a, b) \in G^2$, but this "correspondence" is not a function. By Bryant and Schneider [1] and R. L. Wilson, Jr. [18], each α has $|N_\mu|$ corresponding (a, b), and each (a, b) has $|\mathcal{AUT}(G, \cdot)|$ corresponding α. Hence, $|G|^2 \cdot |\mathcal{AUT}(G, \cdot)| = |\mathcal{II}(G, \cdot)| \cdot |N_\mu|$. When $|G|$ is prime, this implies that $|N_\mu| = |G|$, so that G is a group. Unfortunately, if $|G|$ is not prime, this type of analysis does not yield much information for G-loops in general.

We now consider "natural G-loops", in which the β and γ from Lemma 2.12 have some simple definition. So, fix an $a \in G$, and consider the requirement that there be a $\gamma \in \mathcal{SYM}(G)$ such that $(\gamma, L_a\gamma, \gamma) \in \mathcal{ATOP}(G, \cdot)$. A group is a G-loop, since we may let γ be either L_a^{-1} or R_a^{-1}. It is natural to consider loops in which one of these choices works as well. The first is uninteresting, since it holds only in groups. If $\gamma = L_a^{-1}$, we have $(L_a^{-1}, L_aL_a^{-1}, L_a^{-1}) \in \mathcal{ATOP}(G, \cdot)$; equivalently, $(L_a, I, L_a) \in \mathcal{ATOP}(G, \cdot)$, so that $a \in N_\lambda(G, \cdot)$ (by Lemma 2.9). If this holds for all a, then G is a group. Now, if $\gamma = R_a^{-1}$, we have $(R_a^{-1}, L_aR_a^{-1}, R_a^{-1}) \in \mathcal{ATOP}(G, \cdot)$; equivalently, $(R_a, R_aL_a^{-1}, R_a) \in \mathcal{ATOP}(G, \cdot)$; translating this to an equation, we get precisely equation LCC from Definition 1.1.

Likewise, consider the requirement that for each $b \in G$, there be a $\beta \in \mathcal{SYM}(G)$ such that $(R_b\beta, \beta, \beta) \in \mathcal{ATOP}(G, \cdot)$. In groups, β could be either L_b^{-1} or R_b^{-1}. In any loop, if β is always R_b^{-1}, then the loop is a group, whereas if β is always L_b^{-1}, then we have each $(L_bR_b^{-1}, L_b, L_b) \in \mathcal{ATOP}(G, \cdot)$, which yields equation RCC. Hence:

Lemma 2.13 *A loop $(G, \cdot)$ is conjugacy closed iff both $R_a \in \mathcal{RII}(G, \cdot)$ and $L_a \in \mathcal{LII}(G, \cdot)$ for each $a \in G$. If $(G, \cdot)$ is conjugacy closed, then $(G, \cdot)$ is a G-loop, and both $(R_a, R_aL_a^{-1}, R_a)$ and $(L_aR_a^{-1}, L_a, L_a)$ are in $\mathcal{ATOP}(G, \cdot)$.*

We may now take various products from $\mathcal{RII}(G, \cdot)$ and $\mathcal{LII}(G, \cdot)$ to produce automorphisms. In particular, as in [10]:

Lemma 2.14 *If G is conjugacy closed, then for each $a, b \in G$, both $R_aR_bR_{ab}^{-1}$ and $L_aL_bL_{ba}^{-1}$ are automorphisms of G.*

Proof: By Lemma 2.13, $R_aR_bR_{ab}^{-1} \in \mathcal{RII}(G, \cdot)$. It is then an automorphism by Corollary 2.7. □

Note that in *every* loop, the associative law holds iff $R_aR_bR_{ab}^{-1} = I$ for all a, b. However, in CC-loops, the fact that these are automorphisms lets us use automorphism arguments to study non-associative CC-loops in the same way that inner automorphisms are used to study non-commutative groups. Every commutative CC-loop is a group; more generally, for any CC-loop, the three nuclei coincide [10] and contain Z_0 (see Definition 2.8).

Lemma 2.15 *For any CC-loop $(G, \cdot)$: $Z(G, \cdot) = Z_0(G, \cdot) \subseteq N(G, \cdot) = N_\lambda(G, \cdot) = N_\mu(G, \cdot) = N_\rho(G, \cdot)$.*

Proof: Apply Lemma 2.9 and Lemma 2.13, plus the fact that $\mathcal{ATOP}(G, \cdot)$ is a group. □

Definition 2.16 *For any $a \in G$, let $J_a = R_aL_a^{-1}$ and let $E_a = R_aR_{a\backslash 1}$.*

In a group, $E_a = I$ and J_a is an inner automorphism. In a CC-loop, E_a is an automorphism (by Lemma 2.14); J_a need not be an automorphism of the loop, but it does define an automorphism of the nucleus [10] (apply Lemma 2.10; note that $J_a \in \mathcal{II}(G, \cdot)$ and $1J_a = 1$).

Corollary 2.17 *For any CC-loop $(G, \cdot)$, let $N = N(G, \cdot)$. Then $E_a \in \mathcal{AUT}(G, \cdot)$, and $J_a \restriction N \in \mathcal{AUT}(N, \cdot)$, for each $a \in G$.*

Corollary 2.18 *For any CC-loop $(G, \cdot)$, if $|N(G, \cdot)| = 2$ then $Z(G, \cdot) = N(G, \cdot)$.*

Proof: Since the only automorphism of $N(G, \cdot)$ is the identity, it follows that for each $a \in G$, and each $x \in N(G, \cdot)$, $xL_a R_a^{-1} = x$, so $ax = xa$. □

Table 1 is an example of a CC-loop in which the nucleus has size 3 and the center has size 1. Nevertheless, we shall see later (Lemma 4.16) that the method of proof of Corollary 2.18 is useful for proving the center to be non-trivial in cases where the nucleus has size greater than two, if we have some further information about the orders of these J_a.

Some further examples of non-group CC-loops are described in Goodaire and Robinson [10]. In addition, the following, which is a modification of the semidirect product construction in groups, will be useful later as a source of counter-examples:

Lemma 2.19 *Suppose that $G = H \times A$, where $(H, +)$ and $(A, +)$ are abelian groups, and we define a product on G by*

$$(h, x) \cdot (k, y) = (h + k\theta_x + i_{x,y}\ ,\ x + y) \quad ,$$

where the θ_x, for $x \in A$, and the $i_{x,y}$, for $x, y \in A$, satisfy:

1. *Each θ_x is an automorphism of H and $\theta_{x+y} = \theta_x \theta_y$.*
2. *Each $i_{x,y}$ is an element of H and $i_{x,0} = i_{0,y} = 0$.*
3. *For each x, y, z :*

$$\begin{aligned} i_{y,z}\theta_x + i_{x,y+z} &= i_{x,y} - i_{y,x} + i_{x,z}\theta_y + i_{y,x+z} \\ i_{x,y} + i_{x+y,z} &= i_{x,z} + i_{y,z}\theta_x - i_{z,y}\theta_x + i_{x+z,y} \quad . \end{aligned}$$

Then G is a CC-loop. Furthermore, $\{h \in H : \forall y[h\theta_y = h]\} \times \{0\} \subseteq Z(G)$ and $H \times \{0\} \subseteq N(G)$.

Proof: Note that by item (1), we also have $\theta_{-x} = (\theta_x)^{-1}$ and $\theta_0 = I$. Using this plus item (2), it is easy to see that $(0,0)$ is the identity element of G. To prove that G is a loop, and to identify \ and /, we may solve the equation $(h,x)\cdot(k,y) = (\ell, z)$ for (k,x) or for (h,y) to obtain:

$$\begin{aligned}(h,x)\backslash(\ell,z) &= ((\ell - h - i_{x,z-x})\theta_{-x}\ ,\ z-x)\\ (\ell,z)/(k,y) &= (\ell - k\theta_{z-y} - i_{z-y,y}\ ,\ z-y)\end{aligned}$$

We compute the product of three elements as:

$$\begin{aligned}(h,x)\cdot[(k,y)\cdot(\ell,z)] &= (h + k\theta_x + \ell\theta_{x+y} + i_{y,z}\theta_x + i_{x,y+z}\ ,\ x+y+z)\\ [(h,x)\cdot(k,y)]\cdot(\ell,z) &= (h + k\theta_x + \ell\theta_{x+y} + i_{x,y} + i_{x+y,z}\ ,\ x+y+z)\ \ .\end{aligned}$$

Note that these are equal iff $i_{x,y} + i_{x+y,z} = i_{y,z}\theta_x + i_{x,y+z}$, which holds whenever at least one of x,y,z is 0 (applying item (2) and $\theta_0 = I$), so that $H \times \{0\} \subseteq N(G)$. Likewise, using the definition of $\cdot$, any element of the form $(h,0)$ is in the center iff $h\theta_y = h$ for all y.

Now, equations RCC and LCC require:

$$\begin{aligned}RCC:\ (h,x)\cdot[(k,y)\cdot(\ell,z)] &= [((h,x)(k,y))\,/\,(h,x)]\cdot[(h,x)(\ell,z)]\\ LCC:\ [(h,x)\cdot(k,y)]\cdot(\ell,z) &= [(h,x)(\ell,z)]\cdot[(\ell,z)\,\backslash\,((k,y)(\ell,z))]\end{aligned}$$

The right-hand side of these are:

$$\begin{aligned}RCC\ &:\ (h + k\theta_x + \ell\theta_{x+y} + i_{x,y} - i_{y,x} + i_{x,z}\theta_y + i_{y,x+z}\ ,\ x+y+z)\\ LCC\ &:\ (h + k\theta_x + \ell\theta_{x+y} + i_{x,z} + i_{y,z}\theta_x - i_{z,y}\theta_x + i_{x+z,y}\ ,\ x+y+z)\ \ .\end{aligned}$$

Thus, to get RCC and LCC, we need precisely item (3). □

Note that if $i_{x,y} = 0$ for all x,y, then G is a group, and the construction reduces to the standard semidirect product. The following use of Lemma 2.19 to get a non-group G will be useful later:

Example 2.20 *In Lemma 2.19, take $(H,+) \cong (A,+) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, where $H = \{0,p,q,s\}$ and $A = \{0,a,b,c\}$. Define θ_x and $i_{x,y}$ by:*

x	θ_x
0	I
a	I
b	(p,q)
c	(p,q)

$\longleftarrow y \longrightarrow$

	$i_{x,y}$	0	a	b	c
	0	0	0	0	0
$\uparrow$	a	0	p	0	q
x	b	0	p	0	p
$\downarrow$	c	0	0	s	0

Then $G = H \times A$ is a 16-element CC-loop satisfying the equation $(1/x) = (x \backslash 1)$, with a 4-element nucleus, $H \times \{0\}$, and a 2-element center, $\{0, s\} \times \{0\}$. This loop contains α, β such that $\alpha\alpha = 1$ but $\alpha(\alpha\beta) \neq \beta$ and $(\beta\alpha)\alpha \neq \beta$; furthermore, the cosets, $\langle\alpha\rangle \cdot \beta$ and $\langle\alpha\rangle \cdot \alpha\beta$, are neither equal nor disjoint.

Proof: G is a CC-loop by Lemma 2.19; the tedium of verifying item (3) there may be alleviated somewhat by noting that the equations are trivially true if one of x, y, z is 0, so that there are only $3^3 = 27$ cases to verify, not $4^3 = 64$. It is clear from the proof of Lemma 2.19 that an element (k, y) is in $N_\mu(G)$ iff $\forall xz[i_{x,y} + i_{x+y,z} = i_{y,z}\theta_x + i_{x,y+z}]$, which implies in particular $\forall z[i_{a,y} + i_{a+y,z} = i_{y,z} + i_{a,y+z}]$. For $y = a$ and $y = b$, this is refuted by $z = b$, and for $y = c$, this is refuted by $z = c$. Hence, the only possible elements of the nucleus have form $(k, 0)$, so $N(G) = H \times \{0\}$. Furthermore, $(k, 0)$ cannot be in the center unless $k\theta_y = k$ for all y, so $Z(G) = \{0, s\} \times \{0\}$.

The equation $(1/x) = (x\backslash 1)$ is immediate from the formulas for $/$ and $\backslash$ derived in the proof of Lemma 2.19.

Finally, let $\alpha = (0, c)$ and $\beta = (0, b)$. Then $\alpha\alpha = (0, 0)$, $\alpha\beta = (s, a)$ and $\alpha(\alpha\beta) = (s, b) \neq \beta$. Also, $\beta\alpha = (p, a)$ and $(\beta\alpha)\alpha = (s, b) \neq \beta$. Furthermore, $\langle\alpha\rangle \cdot \beta \,\cap\, \langle\alpha\rangle \cdot \alpha\beta = \{\beta, \alpha\beta\} \cap \{\alpha\beta, \alpha(\alpha\beta)\} = \{\alpha\beta\}$. □

3 Some Useful Equations

Throughout this section, $(G, \cdot)$ always denotes a conjugacy closed loop. We collect here a number of equations and implications between equations which G must satisfy. Often (but not always), it is more transparent to state and prove equations in terms of permutations. For example, in Lemma 2.14, the fact that $R_a R_b R_{ab}^{-1}$ is an automorphism could be expressed as the equation $(((xa)b)/ab) \cdot (((ya)b)/ab) = ((((xy)a)b)/ab)$ and then derived directly from equations LCC and RCC of Definition 1.1, but this derivation would be a bit messy and obscure. We begin by re-stating the definition of "conjugacy closed" in terms of conjugations.

Lemma 3.1 *For any x, y :*

1. $L_x^{-1} R_y L_x = R_x^{-1} R_{xy}$; $R_x^{-1} L_y R_x = L_x^{-1} L_{yx}$
2. $L_x^{-1} L_y L_x = L_{(xy)/x}$; $R_x^{-1} R_y R_x = R_{x\backslash(yx)}$
3. $L_x R_y L_x^{-1} = R_{x\backslash 1}^{-1} R_{x\backslash y}$; $R_x L_y R_x^{-1} = L_{1/x}^{-1} L_{y/x}$
4. $L_x L_y L_x^{-1} = L_{x\backslash(yx)}$; $R_x R_y R_x^{-1} = R_{(xy)/x}$

Proof: The equation RCC of Definition 1.1 asserts both $R_x L_z = L_z R_z^{-1} R_{zx}$ and $L_y L_z = L_z L_{(zy)/z}$; equivalently, $L_z^{-1} R_x L_z = R_z^{-1} R_{zx}$ and $L_z^{-1} L_y L_z = L_{(zy)/z}$. Renaming the variables, and applying also LCC, we get both (1) and (2). To obtain item (3), use the conjugations in item (1) to compute $L_x^{-1} R_{x\backslash 1}^{-1} R_{x\backslash y} L_x$ and $R_x^{-1} L_{1/x}^{-1} L_{y/x} R_x$. Item (4) is proved likewise from (2). □

Remark 3.2 The equations (2) of Lemma 3.1 are easily seen to be equivalent to RCC and LCC. Originally [10], a CC-loop was defined to be a loop in which the left and right multiplications were closed under conjugations – that is, for all x, y, there are u, v such that $L_x^{-1} L_y L_x = L_u$ and $R_x^{-1} R_y R_x = R_v$. But this requires that $u = (xy)/x$ and $v = x\backslash(yx)$, so we retrieve equations (2). Hence, our definition of CC-loop is equivalent to the original one.

Lemma 3.3 *If $cd = 1$, then $L_c^{-1} R_d L_c = R_c^{-1}$, $R_d^{-1} L_c R_d = L_d^{-1}$, and $E_c = R_c R_d = L_c^{-1} L_d^{-1} \in \mathcal{AUT}(G, \cdot)$. Furthermore, $J_c^{-1} = R_d L_c$ and $J_d = L_c R_d$.*

Proof: The first two equations are immediate from Lemma 3.1.1. These yield $L_c = R_d L_c R_c = R_d L_d^{-1} R_d^{-1}$; cancelling the R_d, we get $R_c R_d = L_c^{-1} L_d^{-1}$. $E_c \in \mathcal{AUT}(G, \cdot)$ by Corollary 2.17. □

Lemma 3.4 *For any x, y, $xy = yx$ iff $L_x L_y = L_y L_x$ iff $R_x R_y = R_y R_x$.*

Proof: By Lemma 3.1.2. □

Lemma 3.5 *For any x, y, $R_{xy} = R_x R_y$ iff $L_x R_y = R_y L_x$ iff $L_{xy} = L_y L_x$.*

Proof: By Lemma 3.1.1. □

Lemma 3.6 *For any x, y, $J_{xy} = J_x R_y L_x R_y^{-1} L_x^{-1} J_y$.*

Proof: By Lemma 3.1.1 and the definition of J. □

This lemma is most useful when the commutator, $R_y L_x R_y^{-1} L_x^{-1}$, disappears. That could happen in several ways. First, recall (Corollary 2.17) that J_x defines an automorphism of the nucleus. It follows that:

Corollary 3.7 *Let $N = N(G, \cdot)$. Then $J_x J_y \restriction N = J_{xy} \restriction N$.*

Thus, the map $x \mapsto J_x$ yields a homomorphism from G into $\mathcal{AUT}(N, \cdot)$. Next, we may consider subloops other than the nucleus.

Definition 3.8 *A subloop H of G is* nuclear *iff for all $h, k \in H$, $R_{hk} = R_h R_k$.*

Note that the nucleus is nuclear and that every nuclear subloop must be a group. In view of Lemma 3.5, the condition $R_{hk} = R_h R_k$ could have been replaced by $L_h R_k = R_k L_h$, or by $L_{hk} = L_k L_h$.

Lemma 3.9 *If H is a nuclear subloop of G, then $J_h J_k = J_{hk}$ for all $h, k \in H$, and J_d maps H isomorphically onto HJ_d for all $d \in G$.*

Proof: The first statement is immediate by Lemmas 3.6 and 3.5. By Lemma 2.13, $(R_d, J_d, R_d) \in \mathcal{ATOP}(G, \cdot)$, so for any x, y:

$$xd \cdot yJ_d = (xy) \cdot d$$

Let $c = 1/d$, so $cd = 1$. Then $J_d = L_c R_d$ by Lemma 3.3. So, if $h, k \in H$:

$$(hk)J_d = (c(hk)) \cdot d = ((ch)\ k) \cdot d = (ch)d \cdot kJ_d = hJ_d \cdot kJ_d$$

Hence, J_d restricted to H is an isomorphism. □

The next lemma is used only for the proof of the theorem which follows it.

Lemma 3.10 *If $cd = 1$, then the following equations hold; x denotes any element of G:*

$$\begin{array}{rcll}
R_{c^2}^{-1} & = & R_d L_d^2 L_c R_d L_c & (1) \\
L_{c^2} R_{c^2}^{-1} & = & R_d L_c L_d L_c R_d L_c & (2) \\
L_c R_{cx}^{-1} L_c^{-1} & = & R_x^{-1} R_d & (3) \\
R_d R_{(cx)d} R_d^{-1} & = & R_x & (4) \\
L_d L_c R_x L_c^{-1} L_d^{-1} & = & R_{(xc)d} & (5) \\
R_d L_c L_x R_c & = & L_{xc} & (6) \\
R_d L_c R_{c^2} & = & R_c L_c & (7) \\
R_d L_d R_{xd}^{-1} L_d^{-1} R_d^{-1} & = & R_x^{-1} R_c & (8) \\
L_d L_c R_x R_c L_c & = & L_c R_{xc} & (9) \\
R_c R_d L_d L_c & = & I & (10)
\end{array}$$

Proof: For (1), we apply Lemma 3.1.1 and then Lemma 3.3 three times to get $R_{c^2}^{-1} = L_c^{-1} R_c^{-1} L_c R_c^{-1} = R_d L_d R_d^{-1} R_c^{-1} L_c R_c^{-1} = R_d L_d^2 L_c L_c R_c^{-1} = R_d L_d^2 L_c R_d L_c$. For (2), first note by Lemma 3.3 that $R_d^{-1} L_c R_c^{-1} = L_c$; that is, $(c(x/d))/c = cx$. Hence, by Lemma 3.1.2, $L_c^{-1} L_{x/d} L_c = L_{cx}$. Now, since $1/d = c$, Lemma 3.1.3 implies $R_d L_x L_d^{-1} R_d^{-1} = L_c^{-1} L_{x/d} L_c$, so $R_d L_x L_d^{-1} R_d^{-1} = L_{cx}$. Setting $x = c$, we have $R_d L_c L_d^{-1} R_d^{-1} = L_{c^2}$, and (2) now follows by using the value of $R_{c^2}^{-1}$ from (1). Equation (3) is immediate from Lemma 3.1.3, since $c\backslash 1 = d$. For (4), apply Lemma 3.1.2 to get $R_d R_{d\backslash(xd)} R_d^{-1} = R_x$, but then $d\backslash(xd) = (cx)d$ because $R_d L_d^{-1} = L_c R_d$ by Lemma 3.3. For (5), Lemma 3.3 implies $R_c R_d L_d L_c = I$, so $c(d((xc)d)) = x$. Thus, by 3.1.1, $L_c^{-1} L_d^{-1} R_{(xc)d} L_d L_c = L_c^{-1} R_d^{-1} R_{d((xc)d)} L_c = R_{cd}^{-1} R_{c(d((xc)d))} = R_x$. For (6), apply 3.1.1 and then 3.3 to get $L_{xc} = L_c R_c^{-1} L_x R_c = R_d L_c L_x R_c$. For (7), apply 3.1.1 and then 3.3 to get $R_d L_c R_{c^2} = R_d L_c R_c L_c^{-1} R_c L_c = R_d R_d^{-1} R_c L_c = R_c L_c$. For (8), apply 3.1.3 and 3.1.4 to get $R_d L_d R_{xd}^{-1} L_d^{-1} R_d^{-1} = R_d R_{d\backslash(xd)}^{-1} R_{d\backslash 1} R_d^{-1} = R_x^{-1} R_{1/d}$. To prove (9), we rewrite it as $c(((c(dz))\,x)c) = (cz)(xc)$, which says the same as $L_{c(dz)} R_c L_c = R_c L_{cz}$. By 3.1.1 and 3.1.2, $R_c^{-1} L_{c(dz)} R_c L_c = L_c^{-1} L_{(c(dz))c} L_c = L(z L_d L_c R_c L_c R_c^{-1})$. But by Lemma 3.3, $L_d L_c R_c L_c R_c^{-1} = L_d L_c R_c R_d L_c = L_c$, so $R_c^{-1} L_{c(dz)} R_c L_c = L_{cz}$. Finally, equation (10) is immediate from Lemma 3.3. □

The following theorem is important because it gives us a supply of elements of the nucleus.

Theorem 3.11 *If $cd = 1$ then dc is in the nucleus.*

Proof: Fix c, d with $cd = 1$. By Lemma 3.1.4, $R_y^{-1} = R_x^{-1} R_{(xy)/x}^{-1} R_x$. Below, we shall take the right side of this equation with $x = c^2$, and apply Lemma 3.10 to derive $R_y^{-1} = R_{(dc)y}^{-1} R_{dc}$. This will imply that $R_{(dc)y} = R_{dc} R_y$ for every y, which implies that dc is in the (middle) nucleus. In the following chain of equalities, the comments on the right indicate the equation numbers from Lemma 3.10 used to derive the equality with the next line:

$$\begin{array}{ll}
R_y^{-1} = R_{c^2}^{-1} \cdot (R((c^2y)/c^2))^{-1} \cdot R_{c^2} = R_{c^2}^{-1} \cdot (R(yL_{c^2}R_{c^2}^{-1}))^{-1} \cdot R_{c^2} = & //1,2 \\
R_dL_d^2L_cR_dL_c \cdot (R(yR_dL_cL_dL_cR_dL_c))^{-1} \cdot R_{c^2} = & //3 \\
R_dL_d^2L_cR_d \cdot (R(yR_dL_cL_dL_cR_d))^{-1} \cdot R_dL_cR_{c^2} = & //4 \\
R_dL_d^2L_c \cdot (R(yR_dL_cL_d))^{-1} \cdot R_d^2L_cR_{c^2} = & //5 \\
R_dL_d \cdot (R(yR_dL_cL_dR_cR_d))^{-1} \cdot L_dL_cR_d^2L_cR_{c^2} = & //6,7 \\
R_dL_d \cdot (R(((dc)y)d))^{-1} \cdot L_dL_cR_dR_cL_c = & //8 \\
(R((dc)y))^{-1} \cdot R_cR_dL_dL_dL_cR_dR_cL_c = & //9 \\
R_{(dc)y}^{-1} \cdot R_cR_dL_dL_cR_{dc} = & //10 \\
R_{(dc)y}^{-1} \cdot R_{dc} & \square
\end{array}$$

Of course, it is possible that $cd = dc = 1$ (that is, $(1/c) = (c\backslash 1)$), in which case Theorem 3.11 tells us nothing, but in that case we shall see (Lemma 3.20 below) that the subloop generated by c is a group. First, some preliminaries:

Lemma 3.12 *If $cd = dc = 1$, then:*

1. $L_c^{-1}R_dL_c = R_c^{-1}$ *and* $R_c^{-1}L_dR_c = L_c^{-1}$.
2. $E_c = R_cR_d = (L_cL_d)^{-1} \in \mathcal{AUT}(G,\cdot)$, *and it commutes with each of* L_c, L_d, R_c, *and* R_d.
3. $L_c^{-1}R_cL_c = (R_c)^2R_d$ *and* $R_c^{-1}L_cR_c = (L_c)^2L_d$.
4. $R_{c^2} = (R_c)^3R_d$ *and* $L_{c^2} = (L_c)^3L_d$.
5. $J_c = L_dR_c$; $J_c^{-1} = R_dL_c$; $J_d = L_cR_d$; $J_d^{-1} = R_cL_d$.

Proof: (1), (2), and (5) follow from Lemmas 3.3 and Lemma 3.4. To prove (3): (2) implies $(R_c)^2R_d = L_c^{-1}L_d^{-1}R_c$; then use $L_d^{-1}R_c = R_cL_c$, which follows from (1). Then (4) follows from $L_c^{-1}R_cL_c = R_c^{-1}R_{c^2}$ (by Lemma 3.1.1), and (3). □

The commutation relations in this lemma give a pretty good description of the group generated by R_c, R_d, L_c, L_d in the case that $cd = dc = 1$. First, some general notation

Definition 3.13 *If $X \subseteq G$, then $\langle X\rangle$ is the subloop of G generated by X. If $x, y \in G$, then $\langle x\rangle = \langle\{x\}\rangle$ and $\langle x, y\rangle = \langle\{x, y\}\rangle$.*

Definition 3.14 *If $X \subseteq G$, then: $\mathcal{R}(X)$ is the subgroup of $\mathcal{RII}(G,\cdot)$ generated by all the R_a for $a \in X$; $\mathcal{L}(X)$ is the subgroup of $\mathcal{LII}(G,\cdot)$ generated by all the L_a for $a \in X$; $\mathcal{I}(X)$ is the subgroup of $\mathcal{II}(G,\cdot)$ generated by both the L_a and R_a for all $a \in X$.*

Lemma 3.15 *If H is a subloop of G, then both $\mathcal{R}(H)$ and $\mathcal{L}(H)$ are normal subgroups of $\mathcal{I}(H)$.*

Proof: By Lemma 3.1.1. □

Lemma 3.16 *If $X \subseteq G$, then $\mathcal{II}(\langle X \rangle) = \mathcal{II}(X)$.*

Proof: It is enough to show that $R_{xy}, R_{x\backslash y}, R_{y/x}, L_{xy}, L_{x\backslash y}, L_{y/x}$, are always in the subgroup generated by R_x, R_y, L_x, L_y. For R_{xy}, just apply Lemma 3.1.1. For $R_{x\backslash y}$, use 3.1.1 again to get that $L_x^{-1} R_{x\backslash y} L_x = R_x^{-1} R_y$, Then, for $R_{y/x}$, use 3.1.2, which implies $R_x^{-1} R_{y/x} R_x = R_{x\backslash y}$. □

We now describe $\mathcal{II}(\langle c \rangle) = \mathcal{II}(\{c\})$ in the case that $1/c = c\backslash 1$. Although this group is generated by L_c and R_c, it is simpler to express the group in terms of L_c, R_c, E_c, since E_c is in the center.

Lemma 3.17 *If $cd = dc = 1$, then the following hold; r, s, t, i, j, k, n are arbitrary integers:*

1. *E_c is in the center of $\mathcal{II}(\langle c \rangle)$.*
2. *$R_c^{-j} L_c^t R_c^j = E_c^{-jt} L_c^t$.*
3. *$E_c^r R_c^s L_c^t \cdot E_c^i R_c^j L_c^k = E_c^{r+i-jt} R_c^{s+j} L_c^{t+k}$.*
4. *$(E_c^r R_c^s L_c^t)^{-1} = E_c^{-st-r} R_c^{-s} L_c^{-t}$.*
5. *Every element of $\mathcal{II}(\langle c \rangle)$ is of the form $E_c^r R_c^s L_c^t$ for some r, s, t.*
6. *$\mathcal{II}(\langle c \rangle)$ is abelian iff $E_c = I$ iff $R_c L_c = L_c R_c$.*
7. *$J_c^n = E_c^{(n-1)n/2} R_c^n L_c^{-n}$.*
8. *$R_d = E_c R_c^{-1}$; $L_d = E_c^{-1} L_c^{-1}$.*

Proof: Items (1) and (8) are by Lemma 3.12.2. For item (2) in the case $j = t = 1$, apply 3.12.3 and 3.12.2. The rest follows by an easy computation. □

We next describe R_y and L_y for $y \in \langle c \rangle$ in the case that $1/c = c\backslash 1$.

Definition 3.18 *For any integer n, let $x^n = 1R_x^n$.*

So, $x^{n+1} = x^n \cdot x$ for all n, positive and negative. It turns out, by the next lemma, that if $1/c = c\backslash 1$ then all possible associations of c^n are equal.

Lemma 3.19 *If $1/c = c\backslash 1$, then the following hold; m, n are arbitrary integers:*

1. $R_{c^n} = E_c^{(n-1)n/2} R_c^n \;\; ; \;\; L_{c^n} = E_c^{-(n-1)n/2} L_c^n$.
2. $c^m \cdot c^n = c^{m+n}$.
3. $E_{c^n} = E_c^{n^2}$.
4. $J_{c^n} = E_c^{(n-1)n/2} J_c^n$.

Proof: By Lemma 3.1.1, $L_{c^{n+1}} = L_c R_c^{-1} L_{c^n} R_c$, so $L_{c^n} = R_c L_c^{-1} L_{c^{n+1}} R_c^{-1}$. Using this, the formula for L_{c^n} may be verified by induction for $n \geq 0$ (going up), and for $n \leq 0$ (going down), using the commutation relations in Lemma 3.17. Also by 3.1.1, $R_{c^{n+1}} = R_{c^n} L_{c^n}^{-1} R_c L_{c^n}$, from which the formula for R_{c^n} may be verified, using the formula for L_{c^n}. This proves (1)

Now, (2) is immediate from the definition of c^n, since $1E_c = 1$. By (2), c generates a cyclic sub*group*, so $c^n\backslash 1 = c^{-n}$. Items (3) and (4) are now immediate from the definitions of E and J, using Lemma 3.17 and (1). □

Lemma 3.20 *For any $c \in G$, the following are equivalent:*

1. *$\langle c \rangle$ is a group .*
2. *$1/c = c\backslash 1$.*
3. *$c \cdot c^2 = c^2 \cdot c$.*

Proof: (1) $\Rightarrow$ (3) is trivial, and (2) $\Rightarrow$ (1) is immediate from Lemma 3.19. To prove (3) $\Rightarrow$ (2), assume (3) and $cd = 1$; we must prove $dc = 1$. By (3) and RCC of Definition 1.1:

$$c \cdot (c^2 d) = (cc^2)/c = (c^2 c)/c = c^2$$

so $c^2 d = c$. Using this and LCC,

$$c = (cc)d = (cd)(d\backslash(cd)) = d\backslash 1$$

so $dc = 1$. □

It now follows immediately by Theorem 3.11 that:

Theorem 3.21 *If $N(G, \cdot) = \{1\}$, then $\langle x \rangle$ is a group for every x.*

If $\langle c \rangle$ is a group, then either $\langle c \rangle \cong \mathbb{Z}$ or $\langle c \rangle \cong \mathbb{Z}_m$ for some positive integer m (where, of course, $\mathbb{Z}$ and $\mathbb{Z}_m$ denote the additive groups of integers and integers modulo m). In the $\mathbb{Z}_m$ case:

Lemma 3.22 *If $\langle c \rangle \cong \mathbb{Z}_m$, then*

1. $E_c^m = I$
2. $R_c^{2m} = L_c^{2m} = J_c^{2m} = I$.
3. *If m is odd, then* $R_c^m = L_c^m = J_c^m = I$.
4. *If m is even, then* $R_c^m = L_c^m = J_c^m = E_c^{m/2}$.

Proof: Applying Lemma 3.19.1, $R_c = R_{c^{m+1}} = E_c^{(m+1)m/2} R_c^{m+1}$, so

$$E_c^{m(m+1)/2} R_c^m = I \qquad (1)$$

Again by 3.19.1,

$$I = R_{c^m} = E_c^{(m-1)m/2} R_c^m \qquad (2)$$

Dividing (1) by (2) yields $E_c^m = I$. Then, squaring (1) or (2) yields $R_c^{2m} = I$. Likewise, $L_c^{2m} = I$ and $J_c^{2m} = I$ (squaring Lemma 3.19.4 with $n = m$).

If m is odd, then $m \mid (m-1)m/2$, so (2) yields $R_c^m = I$, while if m is even, then $(m-1)m/2 \equiv m/2 \pmod{m}$, so $E_c^{\pm m/2} = R_c^{\pm m}$. Likewise for L_c and J_c. □

Note that Example 2.20 provides an example (where c is the element α) where $m = 2$ and R_c and L_c have order 4, not 2. We do have enough information about elements of order 2 to prove the following.

Lemma 3.23 *If $a^2 = b^2 = (ab)^2 = 1$, then $ab = ba$.*

Proof: Using *LCC* of Definition 1.1 with $x = y = ab$ and $z = b$, we have $b = [(ab)b] \cdot [b \backslash ((ab)b)]$. Then, since $L_b^2 = R_b^2$:

$$b = [b(ba)] \cdot [ba] \tag{1}$$

Using *RCC* of Definition 1.1 with $x = y = a$ and $z = b$, we have $b = [(ba)/b] \cdot [ba]$. Then, since $L_b R_b^{-1} = R_b L_b$ (by Lemma 3.12.1):

$$b = [b(ab)] \cdot [ba] \tag{2}$$

By (1), (2), and cancelling, $ba = ab$. □

Note that even in groups, no two of $a^2 = 1$, $b^2 = 1$, $(ab)^2 = 1$ is sufficient to derive $ab = ba$.

Corollary 3.24 *If $x^2 = 1$ for all x, then G is a commutative group.*

Proof: Since the center is contained in the nucleus (Lemma 2.15), every commutative CC-loop is a group. □

Actually, it is well-known that every commutative G-loop is a group, and it is also easy to check that the equation $x^2 = 1$ implies commutativity in G-loops.

Now, the last few results emphasized the situation where $\langle x \rangle$ is a group. If in fact every $\langle x, y \rangle$ is a group (that is, the loop is *diassociative*), then the loop is an *extra loop*, and we may appeal to some results already in the literature.

Definition 3.25 *G is* flexible *iff $R_x L_x = L_x R_x$ for every x.*

This is usually written as the equation, $x(yx) = (xy)x$. A flexible CC-loop is an extra loop [11], and hence a Moufang loop [7][8]. By Moufang's Theorem [1], every Moufang loop is diassociative. Hence:

Proposition 3.26 *G satisfies the flexible law iff G it is diassociative.*

In an extra loop, the square of every element is in the nucleus [8]; in particular, the nucleus is non-trivial (since if $x^2 = 1$ for all x, then G must be a group by Corollary 3.24). We do not know if a CC-loop must have a non-trivial nucleus.

Lemma 3.27 *For any c, the following are equivalent:*

1. $R_c L_c = L_c R_c$.
2. $E_c = I$.
3. $\langle c \rangle$ *is a nuclear subloop of* G.

Proof: (1)$\Rightarrow$(2): Let $d = c\backslash 1$, so $cd = 1$. Then $c(dc) = (cd)c = c$, so $dc = 1$. Then, applying Lemma 3.12.1, $R_d L_c = L_c R_c^{-1} = R_c^{-1} L_c$, so $R_d = R_c^{-1}$, whence $E_c = R_c R_d = I$.

(2)$\Rightarrow$(3): Let $d = c\backslash 1$, so $cd = 1$ and $E_c = R_c R_d$. Then $d = dE_c = (dc)d$, so $dc = 1$. Hence $\langle c \rangle$ is a group. By Lemma 3.19.1, $R_{c^n} = R_c^n$ for each n, which implies that $\langle c \rangle$ is nuclear.

(3)$\Rightarrow$(1): Since $\langle c \rangle$ is a group, let $d = c^{-1}$. By "nuclear", $I = R_{cd} = R_c R_d$, so applying Lemma 3.12.3, $R_c L_c = L_c (R_c)^2 R_d = L_c R_c$. □

Note that $(1/c) = (c\backslash 1)$ is not an equivalent. The CC-loop of Example 2.20 satisfies $(1/x) = (x\backslash 1)$ for every x but it is not an extra loop (since it is not diassociative).

Finally, the next two lemmas will be used to prove that certain elements which "should" be distinct (judging by group theory) really are distinct in CC-loops.

Lemma 3.28 *If A and C are subloops of G, with $A \cap C = \{1\}$ and $C \cong \mathbb{Z}_p$ for some prime p, then the elements ac for $a \in A$ and $c \in C$ are all distinct.*

Proof: Suppose we have $ac = a'c'$, with $a, a' \in A$, and $c, c' \in C$. We need to prove that $a = a'$ and $c = c'$. This is clear (using $A \cap C = \{1\}$) if any one of a, a', c, c' is 1, so assume none of them is. Then $c' = c^n$ for some n, and the case $n = 1$ is trivial, so assume $1 < n < p$, and we derive a contradiction.

By Lemma 3.1.1, $L_x R_{xy}^{-1} = R_y^{-1} L_x R_x^{-1}$, so $(xz)/(xy) = (x(z/y))/x$. So, $(xc^i)/(xc^j) = (xc^{i-j})/x = (xc^{i+k})/(xc^{j+k})$, for any integers i, j, k. Since $ac = a'c^n$, we have $a = (a'c^n)/c = (a'/c)c^n$ (applying Lemma 3.4), so $a/a' = ((a'/c)c^n)/((a'/c)c^1) = ((a'/c)c^{n+k})/((a'/c)c^{1+k})$ for any k. Using this, we show, by induction on $r \geq 0$, that $((a'/c)c^{1+r(n-1)}) \in A$. Now, fix r such that $r \cdot (n-1) \equiv -1 \pmod{p}$, and we have $a'/c \in A$, so $c \in A$, a contradiction. □

Lemma 3.29 *Suppose that $\langle c \rangle \cong \mathbb{Z}_p$ for some prime p, and $aE_c^iR_c^\ell = aE_c^jR_c^m$. Then $\ell \equiv m \pmod{p}$.*

Proof: It is sufficient to derive a contradiction from $aE_c^iR_c^\ell = a$ along with $0 < \ell < p$. If $p = 2$, this is easy (using $E_c = R_c^2$ and $E_c^2 = R_c^4 = I$), so assume $p > 2$.

If $i = 0$, then $aR_c^\ell = a$ plus $R_c^p = I$ yields $ac = aR_c = a$, a contradiction, so assume $0 < i < p$.

For any n with $0 < n < p$, fix $b \in \langle c \rangle$ such that $b^n = c$. Applying Lemma 3.19, $R_c = E_b^{(n-1)n/2}R_b^n$ and $E_c = E_b^{n^2}$, so

$$a = aE_c^iR_c^\ell = aE_b^{(2in^2+\ell n^2-\ell n)/2}R_b^{\ell n} \quad .$$

If (in $\mathbb{Z}_p$) $2i + \ell \neq 0$, we may choose $n = \ell/(2i + \ell)$, so that $aR_b^{\ell n} = a$, yielding a contradiction as in the $i = 0$ case.

If (in $\mathbb{Z}_p$) $2i + \ell = 0$, we have $aE_b^{in}R_b^{-2in} = a$, and we may choose $n = 1/i$, yielding $aE_bR_b^{-2} = a$, or $(ab^{-1})b = (ab)b$. Cancelling yields $b^{-1} = b$, a contradiction, since $p > 2$. □

4 Structure Theorems

Throughout this section, $(G, \cdot)$ always denotes a conjugacy closed loop. We use the general isotopy results in Section 2, together with the equations in Section 3 to analyze the structure of conjugacy closed loops.

We begin with some conditions which imply that the size of a subloop divides the size of the loop. Bruck ([1] p. 92) discusses such "Lagrange theorems" for loops in general.

Definition 4.1 *Let H be a subloop of G. H is a* characteristic *subloop iff every automorphism of G takes H into H. H is an* isolated *subloop iff H is nuclear and $HJ_x = H$ for all $x \in G$.*

In groups, "characteristic" has its usual meaning, while "isolated" is equivalent to "normal". We use "isolated" here because "normal" already has a somewhat different meaning [1] in loops. Note that the nucleus is both characteristic and isolated.

Lemma 4.2 *If H is either a nuclear or a characteristic subloop of G, then any two right cosets, Ha and Hb, are either equal or disjoint.*

Proof: It is sufficient to prove that $Ha = Hd$ for all $d \in Ha$, since then, if $Ha \cap Hb$ contains any element, d, we have $Ha = Hd = Hb$. So, fix $d = ha \in Ha$.

To prove $H(ha) \subseteq Ha$, fix $k(ha) \in H(ha)$. Let $x = (k(ha))/a$, so $k(ha) = xa$; we need to show that $x \in H$. If H is nuclear, then $x = kh \in H$. If H is characteristic, then note that $x/h = kR_{ha}R_a^{-1}R_h^{-1} \in H$, since $R_{ha}R_a^{-1}R_h^{-1} \in \mathcal{AUT}(G, \cdot)$ by Lemma 2.14. Hence, $x \in H$.

To prove $Ha \subseteq H(ha)$, fix $ka \in Ha$. Let $x = (ka)/(ha)$, so $ka = x(ha)$; we need to show that $x \in H$. If H is nuclear, then $x = kh^{-1} \in H$. If H is characteristic, note that $x = (((k/h)h)a)/(ha) \in H$ since $R_h R_a R_{ha}^{-1} \in \mathcal{AUT}(G, \cdot)$. □

Note that the conclusion to Lemma 4.2 fails for the CC-loop in Example 2.20. Even in cases where the cosets fail to be disjoint, one can sometime prove a Lagrange theorem by analyzing the orbits under right multiplication, using the following lemma and its corollary:

Lemma 4.3 *If H is a commutative subgroup of G and $|H| = p^n$, where p is a prime and n is finite, then $|\mathcal{R}(H)| = p^r$ and $|\mathcal{L}(H)| = p^\ell$ for some finite $r, \ell \geq n$.*

Proof: $\mathcal{R}(H)$ and $\mathcal{L}(H)$ are commutative groups (by Lemma 3.4), and are finitely generated (by definition), and the order of each of their generators is a power of p (by Lemma 3.22). Thus, $|\mathcal{R}(H)|$ and $|\mathcal{L}(H)|$ are powers of p. The R_a, for $a \in H$, are all distinct, which implies that $r \geq n$; likewise, $\ell \geq n$. □

Corollary 4.4 *If H is a commutative subgroup of G and $|H| = p^n$, where p is a prime and n is finite, then for each $b \in G$, the sizes of the sets $\{b\alpha : \alpha \in \mathcal{R}(H)\}$ and $\{b\alpha : \alpha \in \mathcal{L}(H)\}$ are both power of p and at least p^n.*

Proof: They are powers of p by Lemma 4.3, and they are at least p^n because the elements $bR_a = ba$, for $a \in H$, are all distinct. □

Theorem 4.5 *If G is finite and H is a subloop of G, then $|G|$ is divisible by $|H|$ if any of the following hold.*

1. *H is a group and the Sylow p-subgroups of H are commutative for each prime p.*

2. H is a nuclear subloop of G.

3. H is a characteristic subloop of G.

Proof: For (1), it is enough to prove this when H is an abelian p-group, in which case, the result follows from Corollary 4.4, since the size of each orbit under $\mathcal{R}(H)$ is divisible by $|H|$. For (2) and (3), the result is immediate by Lemma 4.2 □

A special case of (2) or of (3) is that $|G|$ is divisible by the size of the nucleus, but this fact is true in *all* loops [1].

Corollary 4.6 *If $1 < |G| < \infty$, then G contains an isomorphic copy of $\mathbb{Z}_p$ for some prime factor p of G.*

Proof: By Theorem 3.21 either the nucleus is non-trivial or every $\langle x \rangle$ is a group. □

Corollary 4.7 *If $|G| = p$, where p is prime, then $G \cong \mathbb{Z}_p$.*

Of course, by Wilson [18], this corollary is true of all G-loops.

As with normal subgroups of groups,

Lemma 4.8 *If H is an isolated subloop of G, then $aH = Ha$ for all $a \in G$.*

If a subloop H is both characteristic and isolated, then one can form a quotient G/H as follows. In general, for $S, T \subseteq H$, define their *set product*, $S \cdot T = \{st : s \in S \text{ and } t \in T\}$.

Lemma 4.9 *Suppose H is a characteristic and isolated subloop of G. Then $(Ha) \cdot (Hb) = H(ab)$ for every a, b.*

Proof: Since H is a characteristic subloop, the automorphism $R_x R_y R_{xy}^{-1}$ takes H to H, so, as in the proof of Lemma 4.2, $(Hx) \cdot y = H(xy)$ for any x, y. Likewise, $x \cdot (yH) = (xy)H$. Now, $H(ab) = (Ha)b \subseteq (Ha) \cdot (Hb)$. To prove equality, fix $h, k \in H$, and we prove $(ha) \cdot (kb) \in H(ab)$. Since $(Ha) \cdot (kb) = H(a(kb))$, fix $h' \in H$ such that $(ha) \cdot (kb) = h' \cdot (a \cdot (kb))$, and then, by Lemma 4.8, fix $k' \in H$ such that $kb = bk'$. Then $(ha) \cdot (kb) = h' \cdot (a \cdot (bk'))$. Now, $a(bk') \in a(bH) = H(ab)$, so fix $k'' \in H$ so that $a(bk') = k''(ab)$. Then, since H is nuclear, $(ha) \cdot (kb) = (h'k'') \cdot (ab) \in H(ab)$ □

Definition 4.10 *If H is a characteristic and isolated subloop of G, then $G/H = \{Ha : a \in G\}$; the product operation on G/H is set product.*

Lemma 4.11 *If H is a characteristic and isolated subloop of G, then G/H is a CC-loop and the map $x \mapsto Hx$ is a homomorphism from G onto G/H with kernel H.*

Lemma 4.13 will produce some examples of characteristic and isolated subloops.

Lemma 4.12 *Suppose that $\langle h \rangle \cong \mathbb{Z}_p$, p is prime, and $|G|$ is finite. Then there is a subloop $K \subseteq G$ such that $|K| \equiv |G| \pmod{p^2}$ and $\langle h \rangle$ is a nuclear subloop of K.*

Proof: Let $H = \langle h \rangle$, and let $K = \{x \in G : xE_h = x\}$. Then $H \subseteq K \subseteq G$. H is a nuclear subloop of K by Lemma 3.27. For any $b \in G$, let $O_b = \{b\alpha : \alpha \in \mathcal{R}(H)\}$ be the orbit of b under $\mathcal{R}(H)$. Since $E_h \in \mathcal{R}(H)$ and $\mathcal{R}(H)$ is commutative (Lemma 3.4), each O_b is either contained in or disjoint from K. Furthermore, by Corollary 4.4, $|O_b|$ is always a power of p. Now, suppose $b \notin K$, so $bE_h \neq b$. Then O_b contains $b, bh, (bh)h, \ldots, bR_h^{p-1}$, plus bE_h, all of which are distinct by Lemma 3.29, so $p^2 \mid |O_b|$. Hence, $|K| \equiv |G| \pmod{p^2}$. □

Now, we already know that p divides $|G|$; this lemma is trivial when $|G| \equiv p \pmod{p^2}$, since we could just take $K = \langle h \rangle$. When $|G| \leq p^2$, then K must equal G. We shall look in detail at the situation $|G| = p^2$ later.

Lemma 4.13 *If $\langle h \rangle \cong \mathbb{Z}_p$, where p is prime and $p^2 > |G|$, then $\langle h \rangle$ is a characteristic and isolated subgroup of G.*

Proof: It is nuclear by Lemma 4.12. To prove it is isolated, fix any $x \in G$, and let $K = \langle h \rangle J_x$; we must show that $K = \langle h \rangle$. Now $K \cong \langle h \rangle \cong \mathbb{Z}_p$ by Lemma 3.9. By Lemma 3.28, if $K \cap \langle h \rangle = \{1\}$, then $|G| \geq p^2$; hence, fix $a \neq 1$ in $K \cap \langle h \rangle$. But then $K = \langle a \rangle = \langle h \rangle$. The same argument shows that $\langle h \rangle$ is characteristic. □

The following theorem yields a weak version of the fact that the order of a finite *group* of exponent p is a power of p:

Theorem 4.14 *Suppose that $|G| = pm$, where p is prime and $m - 1$ is not divisible by p, and suppose that $\langle a \rangle \cong \mathbb{Z}_p$ for every $a \neq 1$. Then G contains an isomorphic copy of $\mathbb{Z}_p \times \mathbb{Z}_p$, and $|G|$ is divisible by p^2.*

Proof: That $|G|$ is divisible by p^2 is immediate by Theorem 4.5, once we produce the $\mathbb{Z}_p \times \mathbb{Z}_p$. To do that, first iterate Lemma 4.12 a finite number of times to produce a subloop $K \subseteq G$ such that $|K| \equiv |G| \pmod{p^2}$ and $\langle x \rangle$ is a nuclear subloop of K for *every* $x \in K$. Then, $E_x = I$ for every $x \in K$, so K is flexible, and hence diassociative (by Proposition 3.26). $|K| > p$ because $m - 1$ is not divisible by p. Fix $a, b \in K$ with $b \neq 1$ and $a \notin \langle b \rangle$. Then $H = \langle a, b \rangle$ is a group of exponent p, and has size greater than p, so it contains a copy of $\mathbb{Z}_p \times \mathbb{Z}_p$. □

What are the non-group CC-loops of order seven or less? By Wilson [18] (or Corollary 4.7), these cannot have prime order, and it is easy to see by inspection that all loops of order four are commutative, and hence groups if they are CC, so that leaves order six. In that case, we have the CC-loop from Table 1, and that is the only one, as is true in general for orders $2q$, where q is an odd prime, by the following theorem:

Theorem 4.15 *If q is an odd prime, then there are exactly three CC-loops of order $2q$, exactly two of which are groups.*

Proof: Assume $|G| = 2q$. Let $N = N(G, \cdot)$. Then $|N|$ divides $2q$

First note that $|N|$ cannot be 2: If $|N| = 2$, then N is also the center by Corollary 2.18. Say $N = \{1, c\}$. Fix a different from 1 and c. Note that $\langle a \rangle$ cannot be a group, since if $\langle a \rangle \cong \mathbb{Z}_n$, then $\langle a, c \rangle \cong \mathbb{Z}_n \times \mathbb{Z}_2$. By Theorem 4.5, $2n$ must divide $2q$, which means that $G \cong \mathbb{Z}_q \times \mathbb{Z}_2$, so $|N| = 2q$, a contradiction. Let $b = a \backslash 1$, so $ab = 1$. Then $ba \neq 1$ (by Lemma 3.20), but $ba \in N$ (by Theorem 3.11), so $ba = c$. Let $E_a = R_a R_b \in \mathcal{AUT}(G, \cdot)$ (see Lemma 3.3); note that $bE_a = cb$. Since E_a is an automorphism and c is in the center, $b^k E_a = (bE_a)^k = b^k c^k$ for each k (we are defining b^k by Definition 3.18). Now G/N is a CC-loop of size q and hence isomorphic to $\mathbb{Z}_q$, so $b^q \in N$. Since q is odd, $b^q E_a = b^q c$, which is impossible, since E_a is the identity on N.

So, $|N|$ is either 1, q, or $2q$.

Next, note that G has some subloop isomorphic to $\mathbb{Z}_q$: This is clear if $|N|$ is q or $2q$, so suppose that $|N| = 1$ (which will later turn out to be impossible). Then, by Theorems 3.21 and 4.5, each $\langle x \rangle$ is a group of some order dividing $2q$, and we cannot have that every x has order 2 (or G would be a boolean group (by Corollary 3.24) and hence have size a power of 2), so $\langle x \rangle \cong \mathbb{Z}_q$ for some x.

Now, fix a subloop H isomorphic to $\mathbb{Z}_q$. Then H is a a characteristic and isolated subgroup of G (by Lemma 4.13), and $G/H \cong \mathbb{Z}_2$ (by Lemma 4.11). There are now three cases:

Case 1: $x^2 = 1$ for all $x \notin H$. Then, for all $x \notin H$: $R_x^2 = L_x^2 = J_x^2 = E_x$, and $J_x \upharpoonright H \in \mathcal{AUT}(H)$ (by Lemmas 3.22 and 3.9). Fix some $c \notin H$ and some $h \in H$ with $h \neq 1$. Then the general element of G is of the form $h^n c^i$, with $n \in \mathbb{Z}_q$ and $i \in \mathbb{Z}_2$. Now fix $r \in \mathbb{Z}_q$ such that $hJ_c = h^r$, so $hc = ch^r$.

Now, consider an arbitrary element $x = h^n c \notin H$. Then $hx = xh^s$ for some s. But then $hx = h^{n+1}c = ch^{nr+r}$ and $xh^s = (h^n c)h^s = (ch^{nr})h^s = ch^{nr+s}$, so $r = s$. Thus, for all $x \notin H$, we have $J_x = J_c$, and hence $hE_x = h^{r^2}$.

To compute r: $h^{r^2} = hE_c = (hc)c = (hc)(ch^r h^{-r}) = (hc)((hc)h^{-r}) = (h^{-r})E_{hc} = h^{-r^3}$, so $r = -1$. Hence, for all $x \notin H$: $R_x^2 = L_x^2 = J_x^2 = E_x = I$, since E_x is the identity on $\langle \{x\} \cup H \rangle = G$. Hence, $E_x = I$ for all $x \in G$, since H is a nuclear subgroup.

Now we compute: $(h^m c)(h^n c) = (h^m c)(ch^{-n}) = (h^m c)((ch^{-m})h^{m-n}) = (h^m c)((h^m c)h^{m-n}) = (h^{m-n})E_{h^m c} = h^{m-n}$. Similarly:

$$\begin{array}{rcl} h^m \cdot h^n = h^{m+n} & \qquad & (h^m c) \cdot h^n = h^{m-n} c \\ h^m \cdot (h^n c) = h^{m+n} c & \qquad & (h^m c) \cdot (h^n c) = h^{m-n} \end{array}$$

which we recognize as the usual description of the non-abelian group of order $2q$ as a semidirect product of $\mathbb{Z}_q$ by $\mathbb{Z}_2$.

Case 2: $\langle x \rangle$ is a group for all $x \notin H$, but not all such x have order 2. Fix $c \notin H$ with $c^2 \neq 1$. Then the only possibility is that c has order $2q$, so that $\langle c \rangle = G \cong \mathbb{Z}_{2q}$.

Case 3: Neither Case 1 nor Case 2 holds. Then fix c such that $\langle c \rangle$ is not a group. Then $c \notin H$ but $c^2 \in H$; however, $c^2 \neq 1$. Let $h = c^2$; then $H = \langle h \rangle$. Let $d = c \backslash 1$, so that $cd = 1$. Now $dc \neq 1$ (otherwise, $\langle c \rangle$ would be a group by Lemma 3.20), but $dc \in H$ (since $G/H \cong \mathbb{Z}_2$), and $dc \in N$ (by Theorem 3.11). Hence, $N = H$.

As in Case 1, the general element of G is of the form $h^n c^i$, with $n \in \mathbb{Z}_q$ and $i \in \{0, 1\}$. Again, $J_c \upharpoonright H \in \mathcal{AUT}(H)$, but now we apply Corollary 3.7 to get $(J_c)^2 \upharpoonright H = (J_{c^2}) \upharpoonright H = I \upharpoonright H$. Now, $J_c \upharpoonright H$ cannot be the identity (since $c \backslash (c^2 \cdot c) = c^2$ would imply $c^2 \cdot c = c \cdot c^2$, making $\langle c \rangle$ a group by Lemma 3.20). Thus, the only possibility is that $hJ_c = h^{-1}$, so that $h^n c = ch^{-n}$. Now, using $H = N$ and $c^2 = h$, we easily compute:

$$\begin{array}{rcl} h^m \cdot h^n = h^{m+n} & \qquad & (h^m c) \cdot h^n = h^{m-n} c \\ h^m \cdot (h^n c) = h^{m+n} c & \qquad & (h^m c) \cdot (h^n c) = h^{1+m-n} \end{array}$$

It is also easy to verify that these equations indeed yield a CC-loop, which is then the only non-group CC-loop of order $2q$. $\square$

Regarding Case 3: Note that we have $x^2 = h$ for each $x \notin \langle h \rangle$, as might be expected from examining Table 1. To verify that this really defines a CC-loop, one may plug the equations directly into LCC and RCC, but it is simpler to just verify that $[G : N] = 2$, and then quote Theorem 3.1 of Goodaire and Robinson [10], which says that this implies the loop is CC. The actual construction of this loop is due to Wilson [19].

Next, consider CC-loops of order pq, where $p \leq q$ are odd primes, with $q - 1$ not divisible by p. In the case $p = q$, a non-group CC-loop of order p^2 was described in [10]. In the case $p < q$, we shall show there is none at all; since [10] already proved that any such loop must have a trivial nucleus, it is not surprising that we begin by proving that the nucleus is non-trivial.

Lemma 4.16 *Suppose that $|G| = pq$, where $p \leq q$ are odd primes and $q - 1$ is not divisible by p. If G is not a group, then $N(G, \cdot) = Z(G, \cdot)$, and is isomorphic to either $\mathbb{Z}_p$ or $\mathbb{Z}_q$.*

Proof: Consider the three possibilities for $N = N(G, \cdot)$.

If $N \cong \mathbb{Z}_q$, then G/N is a CC-loop of size p, so $G/N \cong \mathbb{Z}_p$. Then, in view of Corollary 3.7, every J_x defines an automorphism of N of order p. But, since p does not divide $q - 1$, the only such automorphism is the identity, so every J_x is the identity on N, which means that N is contained in the center. The same argument works if $N \cong \mathbb{Z}_p$.

Finally, suppose $N = \{1\}$. Then, by Theorems 3.21 and 4.5, each $\langle x \rangle$ is a group of order either p or q. Furthermore, the orders of these $\langle x \rangle$ cannot all be the same, or Theorem 4.14 would yield a contradiction; hence $p < q$ and some $\langle x \rangle$ have order p and some $\langle x \rangle$ have order q. Now, fix a with $\langle a \rangle \cong \mathbb{Z}_q$.

Then this $\langle a \rangle$ is characteristic and isolated by Lemma 4.13. In particular, $\langle a \rangle$ is nuclear, so by Lemma 3.9, each J_x defines an automorphism of $\langle a \rangle$. Furthermore, if $x \notin \langle a \rangle$, then $x^p = 1$, so $J_x^p = I$ by Lemma 3.22.3, so $J_x \restriction \langle a \rangle$ is the identity. Thus, a commutes with all elements of G, so that $a \in N(G)$ by Lemma 2.15, a contradiction . $\square$

The proof of the following theorem is patterned after Goodaire and Robinson [9][10], from which (1) is immediate, given Lemma 4.16.

Theorem 4.17 *Suppose that $p \leq q$ are odd primes and $q - 1$ is not divisible by p. Then*

1. *$p < q$: The only CC-loop of order pq is $\mathbb{Z}_{pq}$.*
2. *$p = q$: There are exactly three CC-loops of order p^2 besides $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Proof: Assume that G has order pq and is not a group. Do *not* assume $p \leq q$, but assume that $q-1$ is not divisible by p, and $p-1$ is not divisible by q, so that by Lemma 4.16, we may assume that $N = N(G, \cdot) = Z(G, \cdot) \cong \mathbb{Z}_q$. We shall now derive a multiplication table in the case $p = q$, and a contradiction in the case $p \neq q$.

Recall that x^k denotes $1R_x^k$, so $x^k \cdot x = x^{k+1}$. Note that G/N is a CC-loop of order p, and hence a group, so that for any x, i, j, there is a $y \in N = Z$ such that $x^i \cdot x^j = x^{i+j}y = yx^{i+j}$.

For now, fix any $b \notin N$. Then $b \cdot b^2 \neq b^3$, since otherwise $\langle b \rangle$ would be a group (by Lemma 3.20), which would imply that $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$. Let $c = (b \cdot b^2)/b^3$, so that $b \cdot b^2 = c \cdot b^3 = b^3 \cdot c$. Note that $c \in N$ and $c \neq 1$, so that $N = Z = \langle c \rangle$.

For any natural numbers r, s, define $\epsilon(r, s)$ in the field $\mathbb{Z}_q$ so that $b^r \cdot b^s = b^{r+s} \cdot c^{\epsilon(r,s)}$. Note that $\epsilon(0, s) = \epsilon(r, 0) = \epsilon(r, 1) = 0$ for any r, s, and our choice of c implies $\epsilon(1, 2) = 1$.

For any s, let $\alpha_s = R_b^s R_{b^s}^{-1} \in \mathcal{AUT}(G, \cdot)$ (applying Corollary 2.7). Note that $c\alpha_s = c$. Define $\delta(s) \in \mathbb{Z}_q$ so that $b\alpha_s = b^{s+1}/b^s = b \cdot c^{-\delta(s)}$. Since α_s is an automorphism, $b^r\alpha_s = b^{s+r}/b^s = b^r c^{-r\delta(s)}$. That is, we must have (in $\mathbb{Z}_q$), $\epsilon(r, s) = r \cdot \delta(s)$. Note that $\delta(0) = \delta(1) = 0$ and $\delta(2) = 1$.

Since $b^p \in N$, we have $b^p = b^p\alpha_2 = b^p c^{-p}$, which is impossible unless $p = q$, establishing (1) of the theorem.

We now proceed to examine the possibilities in order q^2. Fix $\mu \in \mathbb{Z}_q$ such that $b^q = c^\mu$. Every element of G is of the form $b^r c^i$ for some r, i, and this representation is unique if we take $0 \leq r < q$ and $i \in \mathbb{Z}_q$. We have a product on these elements defined by:

$$b^r c^i \cdot b^s c^j = \begin{cases} b^{r+s} \cdot c^{i+j+\epsilon(r,s)} & \text{if } r + s < q \\ b^{r+s-q} \cdot c^{i+j+\epsilon(r,s)+\mu} & \text{if } r + s \geq q \end{cases}$$

Furthermore, it is easy to see that these equations define a loop of size q^2 (based on the formal symbols $b^r c^i$). It remains to investigate what values of μ and the $\epsilon(r, s) = r \cdot \delta(s)$ really lead to a CC-loop, and what the possible isomorphism types are.

To verify that the loop is conjugacy-closed, we simply insert three loop elements into the equations LCC and RCC. A straightforward computation shows that LCC is automatically satisfied, and RCC reduces to:

$$s\,\delta(r) + t\,\delta(r+s) = t\,\delta(r) + s\,\delta(r+t) + t\,\delta(s) - s\,\delta(t) \qquad (R)$$

Setting $r = t = 1$ yields $\delta(1+s) = s + \delta(s)$, so $\delta(s) = s(s-1)/2 \pmod q$, and hence $\epsilon(r,t) = rt(t-1)/2 \pmod q$. It is easy to check that this expression satisfies (R). So, we have one CC-loop for every choice of $\mu \in \mathbb{Z}_q$.

Now, the choice of $b \notin N$ determined $c \in N$ and then μ. Let us now see what other values of μ could arise from a different choice, $\hat{b} \notin N$. This $\hat{b}$ defines $\hat{c}$ so that $\hat{b} \cdot \hat{b}^2 = \hat{b}^3 \cdot \hat{c}$, and then $\hat{\mu} \in \mathbb{Z}_q$ such that $\hat{b}^q = \hat{c}^{\hat{\mu}}$. Since the value of $\hat{\mu}$ only depends on which coset of the nucleus $\hat{b}$ lies in, we may as well assume that $\hat{b} = b^n$, where $1 \le n < q$. Then $\hat{b} \cdot \hat{b}^2 = b^{3n} c^{\epsilon(n,n)+\epsilon(n,2n)}$ and $\hat{b}^3 = \hat{b}^2 \cdot \hat{b} = b^{3n} c^{\epsilon(n,n)+\epsilon(2n,n)}$, so $\hat{c} = c^{\epsilon(n,2n)-\epsilon(2n,n)} = c^{n^3}$. Also, $\hat{b}^q = (b^n)^q = b^{nq} c^{\nu} = c^{n\mu} c^{\nu}$, where $\nu = \epsilon(n,n) + \epsilon(2n,n) + \ldots \epsilon((q-1)n,n) = (q(q-1)/2) \cdot n\delta(n) \equiv 0 \pmod q$. Thus, $\hat{\mu} = \mu/n^2$, so that the various possible values of μ obtainable from a given loop are all in the ratio of a perfect square in the field $\mathbb{Z}_q$. It follows that up to isomorphism, the three possibilities for μ are 0, 1 (equivalently, any non-zero square), and any non-square. □

If q is an odd prime and $\mu \in \mathbb{Z}_q$, let $C(q,\mu)$ denote the CC-loop of order q^2 constructed as above. For any loop, $(G, \cdot)$, we may form the mirror, $(G, \circ)$, by letting $x \circ y = y \cdot x$. A straightforward computation shows that for $q > 3$, the mirror of $C(q,\mu)$ is isomorphic to $C(q,-\mu)$, whereas for $q = 3$, the mirror of $C(q,\mu)$ is isomorphic to $C(q,-\mu+2)$.

5 G-loops

It is reasonable to ask to what extent the results of this paper generalize to G-loops. The results of this section put some limits on this. In Section 3, we collected a number of results true in all CC-loops. These were mainly equations, or else implications between equations, such as

$$\forall xyz[xy = yx \Rightarrow x(yz) = y(xz)] \qquad (1)$$

from Lemma 3.4. Here, we show that the only facts of this sort true in all G-loops are true in all loops.

An *equation* is an expression of the form $\sigma = \tau$, where σ and τ are terms composed of variables, 1, and the functions $\backslash, /, \cdot$. A *universal* sentence is a logical sentence of the form $\forall x_1 \cdots x_n \psi$, where ψ is an equation or a Boolean combination of equations. Thus, (1) above is a universal sentence.

Theorem 5.1 *If φ is a universal sentence true in all G-loops, then φ is true in all loops.*

Bruck [1] (p. 57) asked if one could find "necessary and sufficient conditions upon the loop G in order that" G be a G-loop. By Theorem 5.1, such conditions cannot be just universal statements. We do not know whether such conditions can be first-order. Of course, there are first-order logical statements true in all G-loops which are not true in all loops. An example of such a statement is

$$\forall xy[xy = yx] \;\Rightarrow\; \forall xyz[x(yz) = y(xz)] \tag{2}$$

But, by Theorem 5.1, for a general G-loop, one cannot pin down by a formula exactly which elements need to commute in order to conclude $x(yz) = y(xz)$.

In proving Theorem 5.1, note first that by the following lemma, it is sufficient to consider sentences about $\cdot$ and 1:

Lemma 5.2 *If φ is a universal sentence, then there is a universal sentence φ' such that φ' does not use $\backslash$ or $/$, and such that $[\varphi \iff \varphi']$ is true in all loops.*

Proof: Replace all occurrences of $\backslash$ and $/$, using the observation that in loops, $\psi(x/y)$ is equivalent to $\forall z[(zy = x) \;\Rightarrow\; \psi(z)]$. □

Let us call an *incomplete binary system* a pair $(G, \circ)$, where G is a nonempty set, $\circ : dom(\circ) \to G$ is a function, and $dom(\circ) \subseteq G \times G$. We use "$x \circ y = z$" to abbreviate "$(x, y) \in dom(\circ) \wedge x \circ y = z$". This incomplete binary system is an *incomplete loop* iff it contains an element 1 which makes the loop properties hold as far as $\circ$ is defined; more formally:

$$\begin{aligned}
&\forall x \in G[x \circ 1 = 1 \circ x = x] \\
&\forall xyz \in G[x \circ y = x \circ z \;\Rightarrow\; y = z] \\
&\forall xyz \in G[y \circ x = z \circ x \;\Rightarrow\; y = z]
\end{aligned}$$

Note that if $(G, \circ)$ is a *finite* incomplete loop and $dom(\circ)$ is all of $G \times G$, then $(G, \circ)$ is a loop. By a theorem of Evans, every finite incomplete loop may be extended to a loop on a possibly larger finite set:

Lemma 5.3 (Evans [6]) *If $(G, \circ)$ is an incomplete loop, then there is a loop $(H, *)$ such that $G \subseteq H$, $|H| \leq 2 \cdot |G|$, and $*$ agrees with $\circ$ wherever $\circ$ is defined.*

Now, any universal sentence which fails in some loop fails because of a finite number of elements – that is, because of some finite incomplete subloop. This incomplete subloop may then be extended to a finite loop, where the sentence still fails. Hence,

Lemma 5.4 *If φ is a universal sentence true in all finite loops, then φ is true in all loops.*

Definition 5.5 *A loop $(G, \cdot)$ is* saturated *iff*

- *G is countably infinite.*
- *Every finitely generated subloop of G is finite.*
- *Whenever $(K, *)$ is a finite loop, H is a subloop of K, and i is an injective homomorphism from H into G, there is an extension of i to an injective homomorphism from K into G.*

The notion of "saturated" is borrowed from model theory [3], but it has a somewhat different meaning there. Note in particular, with $H = \{1\}$, that a saturated loop contains isomorphic copies of all finite loops. So,

Lemma 5.6 *If the loop $(G, \cdot)$ is saturated, then every universal sentence true in $(G, \cdot)$ is true in all loops.*

Furthermore, the saturated loop is unique.

Lemma 5.7 *There is exactly one saturated loop, up to isomorphism.*

Lemma 5.8 *The saturated loop is a G-loop.*

Proof: It is sufficient to prove that every loop isotope of a saturated loop is saturated. □

Proof of Theorem 5.1: If φ is true in all G-loops, then it is true in the saturated loop, and hence in all loops. □

6 Concluding Remarks

We feel that we have demonstrated that CC-loops have a non-trivial structure, but we have not settled all possible questions. Following Theorems 4.15 and 4.17, one might try to characterize all CC-loops of sizes pq or p^3 (for primes p, q). A more general question is whether the nucleus must be non-trivial. In fact, as pointed out in [10], in all known examples the loop modulo the nucleus is a commutative group.

In another direction, one might try to develop a structure theory of G-loops. It is still unknown whether there is a non-group G-loop of order 15. Perhaps one might extend the results of Section 5 to show that "there is no structure theory", but it is not clear exactly what such a statement would mean.

We do not know whether it pays to study the consequences of LCC and RCC separately. Related to this, one might study LCC and RCC *quasigroups*. Note that in a quasigroup, RCC implies that there is a left identity (apply RCC with $zy = z$ to show that $yx = x$ for all x), so that every CC quasigroup is a loop.

References

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

[2] B. F. Bryant and H. Schneider, Principal loop-isotopes of quasigroups, *Canadian J. Math* 18 (1966) 120 – 125.

[3] C. C. Chang and H. J. Keisler, *Model Theory*, North-Holland, 1990.

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

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

[6] T. Evans, Embedding Incomplete Latin Squares, *Amer. Math. Monthly* 67 (1960) 958 – 961.

[7] F. Fenyves, Extra Loops I, *Publicationes Mathematicae Debrecen* 15 (1968) 235 – 238.

[8] F. Fenyves, Extra Loops II, *Publicationes Mathematicae Debrecen* 16 (1969) 187 – 192.

[9] E. G. Goodaire and D. A. Robinson, Loops Which Are Cyclic Extensions of Their Nuclei, *Compositio Math.* 45 (1982) 341 – 356.

[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] J. Hart and K. Kunen, Single Axioms for Odd Exponent Groups, *J. Automated Reasoning* 14 (1995) 383 – 412.

[13] K. Kunen, Moufang Quasigroups, *J. Algebra* 183 (1996) 231-234.

[14] K. Kunen, Quasigroups, Loops, and Associative Laws, *J. Algebra* 185 (1996) 194-204.

[15] W. W. McCune, OTTER 3.0 Reference Manual and Guide, Technical Report ANL-94/6, Argonne National Laboratory, 1994; available at URL: `http://www.mcs.anl.gov`

[16] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Heldermann Verlag, 1990.

[17] E. L. Wilson, A class of loops with the isotopy-isomorphy property, *Canadian J. Math* 18 (1966) 589 – 592.

[18] R. L. Wilson, Jr., Isotopy-isomorphy loops of prime order, *J. Algebra* 31 (1974) 117 – 119.

[19] R. L. Wilson, Jr., Quasidirect products of quasigroups, *Comm. Algebra* 3 (1975) 835 – 850.

[20] 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/`