STRUCTURAL INTERACTIONS OF CONJUGACY CLOSED LOOPS

ALEŠ DRÁPAL

Abstract. We study conjugacy closed loops by means of their multiplication groups. Let Q be a conjugacy closed loop, N its nucleus, A the associator subloop, and $\mathcal{L}$ and $\mathcal{R}$ the left and right multiplication group, respectively. Put $M = \{a \in Q;\ L_a \in \mathcal{R}\}$. We prove that the cosets of A agree with orbits of $[\mathcal{L}, \mathcal{R}]$, that $Q/M \cong (\operatorname{Inn} Q)/\mathcal{L}_1$ and that one can define an abelian group on $Q/N \times \mathcal{L}_1$. We also explain why the study of finite conjugacy closed loops can be restricted to the case of N/A nilpotent. Group $[\mathcal{L}, \mathcal{R}]$ is shown to be a subgroup of a power of A (which is abelian), and we prove that Q/N can be embedded into $\operatorname{Aut}([\mathcal{L}, \mathcal{R}])$. Finally, we describe all conjugacy closed loops of order pq.

Conjugacy closed loops have been defined independently by Soikis [15] and by Goodaire and Robinson [7][8]. More recent results concerning their structure have been obtained by Basarab [1], Kunen [10], Drápal [4] and by Kinyon, Kunen and Phillips [11].

This paper can be regarded as a sequel to [4] since its main concern rests in exploring how various features of conjugacy closed loops are manifested in their multiplication groups. We shall use several results of [11] and end by settling down the structure of conjugacy closed loops of order pq. Their study was initiated by Goodaire and Robinson in [7] and resumed by Kunen [10] who proved that if a nonassociative conjugacy closed loop of such order exists, then $q < p$ has to divide $p - 1$. Kunen also fully described the case $q = 2$. Here we shall prove that whenever q divides $p - 1$, then there can be constructed, up to isomorphism, exactly one nonassociative conjugacy closed loop of order pq. Its operation can be given by the formula

$$(i, r) \cdot (j, s) = (i + j\gamma^r + (1 - \gamma^r)(1 - \gamma^s),\ r + s),$$

where i and j are integers modulo p, r and s are integers modulo q and γ is a fixed integer whose multiplicative order modulo p is equal to q.

Unlike in [10], we shall not construct the loop by considering equalities of loop terms, but we shall derive it from knowledge of loop's multiplication group. To get the structure of the multiplication group we shall use various facts, some of which have appeared in [11] and [4], and some of which will be proved in this paper. In fact, we shall obtain quite a few structural results,

2000 *Mathematics Subject Classification.* Primary 20N05; Secondary 08A05.
Key words and phrases. Conjugacy closed loop, multiplication group, nucleus.
Supported by institutional grant MSM 0021620839.

and not all of them will be needed for the case pq. Before turning to their short overview, we shall list those properties of conjugacy closed loops that will be used throughout this paper without a further reference. All of them can be found in [4] or [11] (of course, some of them were proved earlier, e.g. in [7] or [1]). For general loop properties consult [3] or [2].

Conjugacy closed loops are those loops where both left and right translations are closed under conjugation. We shall usually denote a loop by Q, and for each $a \in Q$ we shall use L_a and R_a to denote the left translation $x \mapsto ax$ and the right translation $x \mapsto xa$, respectively. The mapping $R_a^{-1}L_a$ will be denoted by T_a. For $S \subseteq Q$ we shall write $L_{(S)}$ to denote the set $\{L_s;\ s \in S\}$. Similarly $R_{(S)}$.

Left translations L_x generate the *left multiplication group* $\mathcal{L}$, and the right translations R_x generate the *right multiplication group* $\mathcal{R}$. The group $\mathrm{Mlt}\, Q = \langle \mathcal{L}, \mathcal{R} \rangle$ is the *multiplication group* of Q. If Q is conjugacy closed, then

$$L_x L_y L_x^{-1} = L_{T_x(y)} \quad \text{and} \quad R_x R_y R_x^{-1} = R_{T_x^{-1}(y)}.$$

These identities imply further ones, from which we shall mention

$$L_x R_y R_z^{-1} L_x^{-1} = R_{xy} R_{xz}^{-1} \quad \text{and} \quad R_x L_y L_z^{-1} R_x^{-1} = L_{yx} L_{zx}^{-1}.$$

It is immediate that $\mathcal{L}$ and $\mathcal{R}$ are normal subgroups of $\mathrm{Mlt}\, Q$, for every conjugacy closed loop Q.

Mappings $L_{xy}^{-1} L_x L_y$ generate $\mathcal{L}_1$, in every loop Q. The latter mapping will be denoted by $L(x,y)$. Similarly, $R(x,y) = R_{yx}^{-1} R_x R_y$. If Q is conjugacy closed, then $L(x,y)$ and $R(x,y)$ are automorphisms of Q, the group $\mathcal{L}_1$ is abelian and coincides with $\mathcal{R}_1$, $L(x,y) = L(y,x)$ and $R(x,y) = R(y,x)$ for all $x, y \in Q$, and for every $x \in Q$ and every $\varphi \in \mathcal{L}_1$ we have $\varphi(x)/x \in N$ and $x\backslash\varphi(x) \in N$. Here N stands for the *nucleus* of Q (the set of elements which associate with all other elements of Q). If Q is conjugacy closed, then N is a normal subloop of Q and Q/N is an abelian group [1]. Furthermore, the mappings $L(x,y)$ and $R(x,y)$ depend only on the cosets xN and yN.

Generally, there are three nuclei N_λ, N_μ and N_ρ, where $N_\lambda = \{a \in Q;\ a(xy) = (ax)y \text{ for all } x, y \in Q\}$, and where N_μ and N_ρ are defined similarly by shifting the position of a. We have $N = N_\lambda = N_\rho = N_\mu$ in every conjugacy closed loop Q.

The stabilizer $(\mathrm{Mlt}\, Q)_1$ of the unit element is known as the *inner mapping group* of Q and will be denoted by $\mathrm{Inn}\, Q$. If Q is conjugacy closed, then there exists a surjective group homomorphism $\Lambda : \mathcal{L} \to \mathrm{Inn}\, Q$, $\Lambda(L_x) = T_x$ for all $x \in Q$. This homomorphism is identical on $\mathcal{L}_1$, and hence each element of $\mathrm{Inn}\, Q$ can be expressed as $T_x\varphi$, for some $x \in Q$ and $\varphi \in \mathcal{L}_1$. We also see that $\mathrm{Inn}\, Q$ is generated by mappings T_x, $x \in Q$ (which means that to prove the normality of a subloop U it suffices to show $T_x(u) \in U$ and $T_x^{-1}(u) \in U$, for all $x \in Q$ and $u \in U$).

For every loop Q denote by $A = A(Q)$ the least normal subloop such that Q/A is a group. $A(Q)$ is known as the *associator subgroup*. If Q is conjugacy closed, then $A \leq Z(N)$.

The most famous property of conjugacy closed loops seems to be the fact that they are G-loops, i.e., that every conjugacy closed loop Q is isomorphic to each of its isotopes. Now, $x \circ y = x/e \cdot f\backslash y$ defines such a (principal) isotope, fe is its unit and $\mathrm{Mlt}\, Q(\circ) = \mathrm{Mlt}\, Q$. The left and right multiplication groups coincide as well, and so $\mathcal{L}_1 = \mathcal{R}_1$ (which holds in every conjugacy closed loop) turns to $\mathcal{L}_{fe} = \mathcal{R}_{fe}$ (since $Q(\circ)$ is also conjugacy closed). We see that $\mathcal{L}_u = \mathcal{R}_u$ for all $u \in Q$, whenever Q is conjugacy closed.

In Section 1 we shall collect results that are true in a more general setting. Lemmas 1.1 and 1.5, Corollary 1.6 and Proposition 1.7 are easy group-theoretical facts. Lemma 1.2 is one of the basic loop-theoretical statements; the proof is included to make the paper dependendent only on [4] and [11]. Lemma 1.8 is another classical result of loop theory and Lemmas 1.4 and 1.9 are easy observations. Proposition 1.3 is the only statement of Section 1 that seems to be new. The basic nature of the proposition suggests that it had to be observed earlier. Nevertheless, I was not able to find a reference.

In Section 2 we shall show that the cosets of $A(Q)$, Q a conjugacy closed loop, coincide with the orbits of $[\mathcal{L}, \mathcal{R}]$. We shall also observe that the action of $\mathcal{R}$ on $\mathcal{L}$ by conjugation induces a subgroup of $\mathrm{Out}\, \mathcal{L} = \mathrm{Aut}\, \mathcal{L}/\mathrm{Inn}\, \mathcal{L}$ that is isomorphic to Q/N, and we shall relate the obtained automorphisms of $\mathcal{L}$ to $[\mathcal{L}, \mathcal{R}]$.

Section 3 is devoted to the proof of $Q/M \cong \mathrm{Inn}\, Q/\mathcal{L}_1$ and to the construction of an abelian group on $Q/N \times \mathcal{L}_1$. By M we mean a normal subloop of Q that consists of all $a \in Q$ with $L_a \in \mathcal{R}$. This subloop has been introduced in [4] and for conjugacy closed loops it seems to be of significant structural importance.

Section 4 discusses certain extensions of conjugacy closed loops that will be called *conical*. They can be constructed as quotients of semidirect products, and they correspond to situations when a conjugacy closed loop Q possesses a proper subloop P with $Q = PN$. In such a situation one can obtain Q as a conical extension of P, and that can be done only by means of group theory. Loops which possess no such proper subloop P will be called *conefree*. We shall show that N/A is nilpotent in every finite conefree conjugacy closed loop Q.

In Section 5 we shall prove that $[\mathcal{L}, \mathcal{R}]$ has to be an abelian group and that Q/N can be embedded into $\mathrm{Aut}\, [\mathcal{L}, \mathcal{R}]$, for every conjugacy closed loop Q. Furthermore, we shall make clear that $[\mathcal{L}, \mathcal{R}]$ can be embedded into a power A^r of the (abelian) group $A = A(Q)$, where $r \le |Q : N|$. If Q/N is a group of prime order, then one can even prove $r = 2$. This is used to identify the group G that has to be isomorphic to $\mathrm{Mlt}\, Q$ when Q is a nonassociative conjugacy closed loop of order pq. By considering automorphisms of G we finally come, in Section 6, to a formula that describes the binary operation of Q. The formula is not really novel: In [2, page 184] Belousov defined a nonassociative loop on $F^* \times F$, F a field, such that

$$(a, i) \cdot (b, j) = (ab,\ (a^{-1} - 1)(b^{-1} - 1)\rho + b^{-1}i + j),$$

where $\rho \in F^*$ is a parameter of the loop. Goodaire and Robinson observed in [7] that such loops are conjugacy closed (this property does not change when a^{-1} and b^{-1} are replaced by a and b, respectively). Every subgroup of F^* induces a subloop, and so a q-element subgroup of F^* yields a nonassociative conjugacy closed of order pq whenever F is a field of order p and q divides $p-1$. This paper proves, amongst others, that all such loops are mutually isomorphic.

1. Some general properties of loops and groups

We start by an easy lemma that does not seem to require a proof.

Lemma 1.1. *Let G be a transitive permutation group on Ω. Put $H = \langle G_\omega;\ \omega \in \Omega\rangle$. Then $H \trianglelefteq G$, and G/H acts regularly on orbits of H. Furthermore, if Δ is such a block of G that the action of G on the conjugate blocks of Δ has a regular image, then Δ is equal to a union of orbits of H.*

Lemma 1.2. *Let Q be a loop (or a quasigroup) and let $\sim$ be an equivalence on Q. If all $x, y \in Q$ with $x \sim y$ and all $u \in Q$ satisfy*

$$ux \sim uy,\ xu \sim yu,\ u\backslash x \sim u\backslash y \quad \textit{and} \quad x/u \sim y/u,$$

then $\sim$ is a congruence on Q.

Proof: The first two conditions imply that $\sim$ is compatible with the product. Hence $\cdot$ induces on $Q/{\sim}$ a binary operation with left and right division. It suffices to show that both divisions are always uniquely determined, i.e. that $Q/{\sim}$ is left and right cancellative. Now, if $ux \sim uy$, then $x = u\backslash(ux) \sim u\backslash(uy) = y$, and this establishes the left cancellativity. The rest is clear. □

Proposition 1.3. *Let Q be a loop and let $\mathcal{L}$ be its left multiplication group. Put $B = \langle \mathcal{L}_u;\ u \in Q\rangle$. Then the orbits of B coincide with the cosets of the associator subloop $A(Q)$.*

Proof: A loop is a group if and only if $\mathcal{L}$ is regular. Hence the image of the action of $\mathcal{L}$ on the cosets modulo $A(Q)$ has to be regular. These cosets consist of orbits of B, by Lemma 1.1. Suppose that the equivalence $\sim$ induced by these orbits is a congruence of the loop Q. Then the left multiplication group of $Q/\sim$ is regular, by Lemma 1.1, and so $Q/\sim$ is a group. If $Q/\sim$ is a group, then the orbits of B consist of cosets modulo $A(Q)$, and we see that the orbits and the cosets coincide.

If $x \sim y$, then clearly $ux \sim uy$ and $u\backslash x \sim u\backslash y$, for all $u \in Q$. From $x \sim y$ we also obtain that L_x and L_y act on the orbits of B in the same way. Therefore $xu \sim yu$. To see that $\sim$ is a congruence it remains to verify, by Lemma 1.2, that $x/u \sim y/u$. Now, $L_{x/u}$ and $L_{y/u}$ map u to the same orbit of B, and hence they act on the set of orbits identically. Thus $L_{x/u}(1) = x/u \sim y/u = L_{y/u}(1)$. □

It is worth noting that $\langle \mathcal{L}_u;\ u \in Q\rangle$ and $\langle \mathcal{R}_u;\ u \in Q\rangle$ have the same orbits. These orbits can be smaller than those of $\langle(\operatorname{Mlt} Q)_u;\ u \in Q\rangle$; take any nonabelian group Q. In fact, it is easy to see that the orbits of $\langle (\mathrm{Mlt}\, Q)_u;\ u \in Q\rangle$ yield the smallest congruence $\sim$ with $Q/{\sim}$ an abelian group.

Consider now a normal subloop S of a loop Q. Then $L_x \mapsto L_{xS}$ and $R_x \mapsto R_{xS}$ determine surjective homomorphisms of $\mathcal{L}$ and $\mathcal{R}$ to the left and right multiplication group of Q/S, respectively. Together they yield a surjective homomorphism $\mathrm{Mlt}\, Q \to \mathrm{Mlt}\,(Q/S)$. If Q/S is a group (i.e., if $S \geq A(Q)$), then $R_{xS} \mapsto xS$ is an isomorphism from the right multiplication group of Q/S to $(Q/S)^{op}$ (the opposite group). These facts lead to

Lemma 1.4. *Suppose that Q is a loop with a normal subloop S such that Q/S is a group. Then there exists a unique surjective homomorphism $\mathcal{R} \to (Q/S)^{op}$ that maps each $R_x\varphi$ to xS, for every $x \in Q$ and $\varphi \in \mathcal{R}_1$. The kernel of this homomorphism consists of all mappings $R_s\varphi$, where $\varphi \in \mathcal{R}_1$ and $s \in S$.*

We shall use the preceding lemma also for the left multiplication group. In that version $(Q/S)^{op}$ is replaced by Q/S. This is due to the fact that we compose mappings from the right to the left. The next three statements are easy observations concerning groups.

Lemma 1.5. *Let G be a group and let K be its subgroup. Let $\alpha_i \in \mathrm{Aut}\, G$ be such that $\alpha_3 = \alpha_2\alpha_1$, $1 \leq i \leq 3$. If there are two $i \in \{1, 2, 3\}$ such that $\alpha_i(x)x^{-1} \in K$ for all $x \in G$, then this condition holds for all $i \in \{1, 2, 3\}$.*

Proof: From $\alpha(x)x^{-1} \in K$ one gets $x\alpha(x)^{-1} \in K$, and setting $y = \alpha(x)$ yields $\alpha^{-1}(y)y^{-1} \in K$. We see that the condition is retained by the inverse automorphisms, and so it can be assumed that it holds for $i = 1, 2$. Then $\alpha_2\alpha_1(x)x^{-1} = \alpha_2(\alpha_1(x))\alpha_1(x)^{-1} \cdot \alpha_1(x)x^{-1} \in K$. □

Corollary 1.6. *Let G be a group, $K \leq G$ and $U \leq \mathrm{Aut}\, G$. If $U = \langle S\rangle$ and $\alpha(x)x^{-1} \in K$ for all $\alpha \in S$ and $x \in G$, then $\alpha(x)x^{-1} \in K$ for all $\alpha \in U$ and $x \in S$.*

Proposition 1.7. *Let G be a group, $K \trianglelefteq G$ and $U \leq \mathrm{Aut}\, G$. Assume $G = \langle X\rangle$ and $U = \langle S\rangle$. If $\alpha(x)x^{-1} \in K$ for all $\alpha \in S$ and $x \in X$, then $\alpha(x)x^{-1} \in K$ for all $\alpha \in U$ and $x \in G$.*

Proof: Consider $\alpha \in S$ and suppose that $x, y \in G$ satisfy $\alpha(x)x^{-1} \in K$ and $\alpha(y)y^{-1} \in K$. Then $\alpha(x^{-1})x = x^{-1}(\alpha(x)x^{-1})^{-1}x \in K$ and $\alpha(xy)(xy)^{-1} = (\alpha(x)x^{-1})(x(\alpha(y)y^{-1})x^{-1}) \in K$. We see that if $\alpha(x)x^{-1} \in K$ for all $x \in X$, then $\alpha(x)x^{-1} \in K$ for all $x \in G$. The rest follows from Corollary 1.6. □

A loop Q is called an *A_ℓ-loop*, if each $\varphi \in \mathcal{L}_1$ is an automorphism. Define *A_r-loops* symmetrically. A loop Q is said to be an *A-loop* exactly when $\mathrm{Inn}\, Q \leq \mathrm{Aut}\, Q$. A conjugacy closed loop is an A_ℓ-loop and an A_r-group, but it is not an A-loop, unless a group.

Lemma 1.8. *Let Q be an A_ℓ-loop. Then $\varphi L_x\varphi^{-1} = L_{\varphi(x)}$ for all $\varphi \in \mathcal{L}_1$ and $x \in Q$. Furthermore*

$$(L_x\varphi)(L_y\psi) = L_{x\varphi(y)}L(x, \varphi(y))\varphi\psi$$

whenever $x, y \in Q$ *and* $\varphi, \psi \in \mathcal{L}_1$.

Proof: We have $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in Q$. Hence $\varphi L_x = L_{\varphi(x)}\varphi$, and the rest is easy. □

The formula of the lemma allows us to regard $\mathcal{L}$ as a group on $Q \times \mathcal{L}_1$ with $(x, \varphi) \cdot (y, \psi) = (x\varphi(y), L(x, \varphi(y))\varphi\psi)$. This seems to have been observed for the first time by Sabinin [13].

Lemma 1.9. *Let* Q *be a loop with a nucleus* N*. Then* $(u, v) \mapsto L_u R_v$ *defines a surjective homomorphism* $N \times N \to L_{(N)} R_{(N)} \le \operatorname{Mlt} Q$*. Its kernel is equal to* $\{(u, u^{-1});\ u \in Z(Q)\}$.

Proof: Note that $L_u R_x = R_x L_u$ and $R_u L_x = L_x R_u$ for all $u \in N$ and $x \in Q$. The rest is immediate. □

2. The commutator of multiplication groups

Let Q be a conjugacy closed loop and let $\mathcal{L}$ and $\mathcal{R}$ be its left and right multiplication group, respectively. We have already defined $M = M(Q)$ as the set of all $a \in Q$ with $L_a \in \mathcal{R}$. This definition is left-right symmetric (since $\mathcal{L}_1 = \mathcal{R}_1$), and from Section 3 of [4] we know that $Z(\mathcal{L}) = \{R_a;\ a \in M\}$, $Z(\mathcal{R}) = \{L_a;\ a \in M\}$ and $\mathcal{L} \cap \mathcal{R} = Z(\mathcal{L})\mathcal{L}_1 = Z(\mathcal{R})\mathcal{R}_1$. The orbits of $\mathcal{L} \cap \mathcal{R}$ yield a congruence of Q and this congruence is determined by a corresponding normal subloop of Q. We see that this subloop is equal to M, and so we can state

Proposition 2.1. *The orbits of* $\mathcal{L} \cap \mathcal{R}$ *coincide with the cosets of the normal subloop* M.

The group $[\mathcal{L}, \mathcal{R}]$ is also a normal subgroup of $\operatorname{Mlt} Q$, and it is contained in $\mathcal{L} \cap \mathcal{R}$. The orbits of $[\mathcal{L}, \mathcal{R}]$ therefore constitute cosets of a normal subloop contained in M, and we shall see in Theorem 2.4 that this subloop is exactly the associator subloop $A = A(Q)$. Some easy calculations will be needed.

Lemma 2.2. *Let* $x, y \in Q$*. Then* $[L_x^{-1}, R_y^{-1}] = R_{xy} R_x^{-1} R_y^{-1} = L_x L_y L_{xy}^{-1}$ *and* $[L_x, R_y] = R_{x\backslash 1} R_{x\backslash y}^{-1} R_y = L_x^{-1} L_{x/y} L_{1/y}^{-1}$.

Proof: Proceed by direct computation, using the formulas in the introduction. □

Corollary 2.3. $\mathcal{L}_1 = \mathcal{R}_1 = \langle [L_x, R_y];\ x, y \in Q\rangle = \langle [R_x, L_y];\ x, y \in Q\rangle$.

Proof: With respect to Lemma 2.2 it clearly suffices to prove, say, that each $R_{xy}^{-1} R_y R_x$ is a product of some $[L_u, R_v]$. Turn $R_{xy}^{-1} R_y R_x$ to $R_y^{-1} R_{x\backslash y} R_x$ and observe that $[L_x, R_x] = R_{x\backslash 1} R_x$. Now, $[L_x, R_y] = (R_{x\backslash 1} R_x)(R_y^{-1} R_{x\backslash y} R_x)^{-1}$, by Lemma 2.2. □

Theorem 2.4. *Let* Q *be a conjugacy closed loop and denote by* $\mathcal{L}$ *and* $\mathcal{R}$ *the left and right multiplication group of* Q*, respectively. Then*

$$[\mathcal{L}, \mathcal{R}] = \langle \mathcal{L}_u;\ u \in Q\rangle = \langle \mathcal{R}_u;\ u \in Q\rangle$$

and the orbits of $[\mathcal{L},\mathcal{R}]$ *coincide with the cosets modulo the associator subloop* $A(Q)$*.*

Proof: We have $\mathcal{L}_u = \mathcal{R}_u$ for every $u \in Q$, and to prove $\langle \mathcal{L}_u;\, u \in Q\rangle \le [\mathcal{L},\mathcal{R}]$ it suffices to show $\mathcal{L}_1 \le [\mathcal{L},\mathcal{R}]$, since $[\mathcal{L},\mathcal{R}] \trianglelefteq \operatorname{Mlt} Q$. The inclusion follows from Corollary 2.3, and from Proposition 1.3 we see that it remains to prove $[\mathcal{L},\mathcal{R}] \le \langle \mathcal{L}_u;\, u \in Q\rangle$. Denote the latter group by B and note that every element of $\mathcal{L}$ (or $\mathcal{R}$) can be expressed as $L_x^{-1}\varphi$ (or $R_y^{-1}\psi$), where $\varphi,\psi \in \mathcal{L}_1 = \mathcal{R}_1$. Now, $[L_x^{-1}\varphi, R_y^{-1}\psi] = \varphi^{-1}L_x\psi^{-1}R_yL_x^{-1}\varphi R_y^{-1}\psi$. We need to show $L_x\psi^{-1}R_yL_x^{-1}\varphi R_y^{-1} \in B$, and we have $L_x\psi^{-1}L_x^{-1} \in \mathcal{L}_x$ and $R_y\varphi R_y^{-1} \in \mathcal{L}_y$. Hence it suffices to verify $L_xR_yL_x^{-1}R_y^{-1} = [L_x^{-1}, R_y^{-1}] \in B$. However, that follows from Corollary 2.3. □

We have seen that all elements of $[\mathcal{L},\mathcal{R}]$ map each coset of A onto itself. We shall now characterize all mappings from $\operatorname{Mlt} Q$ that have this property. This will involve the subloop of Q that equals the preimage of $Z(Q/A)$. Note that this subloop consists of all $x \in Q$ with $T_{xA} = \mathrm{id}_{Q/A}$. We have $T_a \in \mathcal{L}_1$ if and only if $a \in M$, by [4, Theorem 3.7], and so $T_{aA} = \mathrm{id}_{Q/A}$ for all $a \in M$. In other words, $M/A \le Z(Q/A)$.

Proposition 2.5. *Let* Q *be a conjugacy closed loop and put* $A = A(Q)$*. Groups* $[\mathcal{L},\mathcal{R}]\{T_x;\, xA \in Z(Q/A)\}$ *and* $\{\psi \in \operatorname{Mlt} Q;\ \psi(uA) = uA$ *for all* $u \in Q\}$ *coincide.*

Proof: The former group is surely contained in the latter, by Theorem 2.4. Let now ψ be an element of the latter group, $\psi(1) = a \in A$. Each element of $\operatorname{Inn} Q$ is equal to some $T_x\varphi$, $\varphi \in \mathcal{L}_1$, and so ψ can be expressed as $\mu T_x\varphi$, where $\mu \in [\mathcal{L},\mathcal{R}]$, $\mu(1) = a$ and $\varphi \in \mathcal{L}_1$. Now, $T_x\varphi = T_x\varphi T_x^{-1}T_x$ and $T_x\varphi T_x^{-1} \in [\mathcal{L},\mathcal{R}]$, again by Theorem 2.4. The rest consists in the direct observation that T_x fixes each coset of A if and only if $xA \in Z(Q/A)$. □

Group $[\mathcal{L},\mathcal{R}]$ is also of importance when studying outer automorphisms of $\mathcal{L}$ that are induced by $\mathcal{R}$. Let us first verify that the term outer automorphism is rightly chosen.

Proposition 2.6. *Let* Q *be a conjugacy closed loop and consider the action of* $\mathcal{R}$ *on* $\mathcal{L}$ *by conjugation. The kernel of this action is equal to* $R_{(N)} = \{R_a;\ a \in N\}$ *and the projection of the action's image to* $\operatorname{Out}\mathcal{L}$ *yields a group isomorphic to* Q/N*. The conjugation by* R_x*,* $x \in Q$*, gives an inner automorphism of* $\mathcal{L}$ *if and only if* $x \in N$ *(in which case it gives the identity).*

Proof: Consider $x \in Q$. We have $R_xL_yR_x^{-1} = L_{yx}L_x^{-1}$ for all $y \in Q$. Every conjugate of L_x in $\mathcal{L}$ is again a left translation, and so $L_{yx}L_x^{-1}$ has to equal some L_z, if R_x should induce an inner automorphism of $\mathcal{L}$. We shall see that this takes place if and only if $x \in N$. Indeed, from $L_{yx} = L_zL_x$ we get $z = y$, and $L_{yx} = L_yL_x$ for all $y \in Q$ if and only if $x \in N_\mu = N$. On the other hand, if $x \in N$, then $R_xL_yR_x^{-1} = L_{yx}L_x^{-1} = L_y$ for all $y \in Q$.

Every $\varphi \in \mathcal{R}_1$ induces an inner automorphism of $\mathcal{L}$, since $\mathcal{R}_1 = \mathcal{L}_1$. This automorphism is trivial if and only if $\varphi = \mathrm{id}_Q$. The automorphism induced by $R_x\varphi$ is inner if and only if $R_x \in \operatorname{Inn}\mathcal{L}$, i.e. exactly when $x \in N$. This makes clear the statement about the kernel of the action. The preimage of $\operatorname{Inn}\mathcal{L}$ is equal to $\{R_x\varphi;\ x \in N \text{ and } \varphi \in \mathcal{R}_1\}$ and this is the kernel of the action's projection to $\operatorname{Out}\mathcal{L}$. One gets the same kernel when mapping $\mathcal{R}$ to $Q/N = (Q/N)^{op}$, by $R_x\varphi \mapsto xN$ (see Lemma 1.4), and this yields the isomorphism between Q/N and the image of the projected action. □

Proposition 2.7. *Let Q be a conjugacy closed loop and put $A = A(Q)$. Fix $\gamma \in \mathcal{L} \cup \mathcal{R}$ and consider $\alpha \in \operatorname{Aut}\mathcal{L}$, $\alpha(\lambda) = \gamma\lambda\gamma^{-1}$ for all $\lambda \in \mathcal{L}$. If $\gamma \in \mathcal{R}$, then $\alpha(\lambda)\lambda^{-1} \in [\mathcal{L}, \mathcal{R}]$ for all $\lambda \in \mathcal{L}$. If $\gamma = L_x\varphi \in \mathcal{L}$, where $\varphi \in \mathcal{L}_1$ and $x \in Q$, then $\alpha(\lambda)\lambda^{-1} \in [\mathcal{L}, \mathcal{R}]$ for all $\lambda \in \mathcal{L}$ if and only if $xA \in Z(Q/A)$.*

Proof: We have $\alpha(\lambda)\lambda^{-1} = [\gamma^{-1}, \lambda^{-1}]$, and this makes clear the case $\gamma \in \mathcal{R}$. In the case $\gamma = L_x\varphi$ first note that $[\mathcal{L}, \mathcal{R}]$ is a normal subloop of $\mathcal{L}$. If $x = 1$, then $\gamma \in \mathcal{L}_1 = \mathcal{R}_1$, and so $\alpha(\lambda)\lambda^{-1} \in [\mathcal{L}, \mathcal{R}]$ for all $\lambda \in \mathcal{L}$. From Lemma 1.5 it hence follows that we need to investigate only the case $\gamma = L_x$. We shall show that then $\alpha(L_y^{-1})L_y \in [\mathcal{L}, \mathcal{R}]$, for all $y \in Q$, if and only if $xA \in Z(Q/A)$. Nothing else will be needed, by Proposition 1.7.

Now, $\alpha(L_y^{-1})L_y = [L_x^{-1}, L_y]$ is equal to $L_{w(y)}^{-1}$, where $w(y) = y\backslash((xy)/x)$, by [4, Proposition 4.4]. By Theorem 2.4 we are looking for x with $w(y) \in A$ for all $y \in Q$. Such x are clearly exactly those that satisfy $xA \in Z(Q/A)$. □

3. Structural isomorphisms

We start by two lemmas that are not really necessary for the subsequent text. Nevertheless they seem to be of interest of their own.

Lemma 3.1. *Let U be a subloop of a conjugacy closed loop Q. Then U is normal in Q if and only if $\langle L_u;\ u \in U\rangle \trianglelefteq \mathcal{L}$.*

Proof: We have $L_xL_uL_x^{-1} = L_{T_x(u)}$, $L_x^{-1}L_uL_x = L_{T_x^{-1}(u)}$ and $\operatorname{Inn}Q = \langle T_x;\ x \in Q\rangle$. If U is normal in Q, then $T_x(u) \in U$ for all $x \in Q$ and $u \in U$, and so $\langle L_u;\ u \in U\rangle \trianglelefteq \mathcal{L}$. To prove the converse we have to show that the normality of $\langle L_u;\ u \in U\rangle$ implies $T_x^{\pm 1}(u) \in U$ for all $u \in U$ and $x \in Q$. We have $L_{T_x^{\pm 1}(u)} \in \langle L_u;\ u \in U\rangle$ and it is clear that $L_y \in \langle L_u;\ u \in U\rangle$, $y \in Q$, if and only if $y \in U$. □

Lemma 3.2. *Let U be a nuclear subloop of a conjugacy closed loop Q. Consider groups $L_{(U)} = \{L_u;\ u \in U\}$, $R_{(U)} = \{R_u;\ u \in U\}$ and $L_{(U)}R_{(U)} = \{L_uR_v;\ u, v \in U\}$. If any of them is normal in $\operatorname{Mlt}Q$, then all are normal. This holds if and only if U is a normal subloop of Q.*

Proof: The sets $L_{(U)}$, $R_{(U)}$ and $L_{(U)}R_{(U)}$ are really groups, by Lemma 1.9. The subloop U is contained in the nucleus, and so $\mathcal{R}$ centralizes $L_{(U)}$. Hence $L_{(U)} \trianglelefteq \operatorname{Mlt}Q$ if and only if $L_{(U)} \trianglelefteq \mathcal{L}$. A large part of the lemma thus follows from Lemma 3.1 and from its symmetric version. It remains to prove that $L_{(U)}R_{(U)} \trianglelefteq \operatorname{Mlt}Q$ implies the normality of U in Q. But this is also clear since the orbit of $L_{(U)}R_{(U)}$ containing 1 equals U. □

Theorem 3.3. *Let Q be a conjugacy closed loop. Denote by $\mathcal{L}$ its left multiplication group and put $M = \{a \in Q;\ R_a \in \mathcal{L}\}$. Then there exists a (unique) isomorphism $Q/M \cong \operatorname{Inn} Q/\mathcal{L}_1$ sending each xM, $x \in Q$, to $T_x\mathcal{L}_1$.*

Proof: We have $A(Q) \le M$, and hence there exists a surjective homomorphism $\mathcal{L} \to Q/M$ that maps each $L_x\varphi$, $\varphi \in \mathcal{L}_1$ and $x \in Q$, to xM. Its kernel consists of all $L_x\varphi$ with $x \in M$. (This follows from the symmetric version of Lemma 1.4.)

Consider also the homomorphism $\pi\Lambda : \mathcal{L} \to \operatorname{Inn} Q/\mathcal{L}_1$, where π is the natural projection modulo $\mathcal{L}_1$. Now, $T_x \in \mathcal{L}_1 \le \mathcal{L}$ if and only if $R_x \in \mathcal{L}$, i.e., if and only if $x \in M$. We see that both homomorphisms have the same kernel and the rest is clear. □

Theorem 3.4. *Let Q be a conjugacy closed loop. The operation*

$$(xN, \varphi) \cdot (yN, \psi) = (xyN,\ L(x, y)\, \varphi\psi)$$

defines an abelian group on $Q/N \times \mathcal{L}_1$. This group is the image of the surjective homomorphism $\mathcal{L} \to Q/N \times \mathcal{L}_1$ that maps $L_x\varphi$ to (xN, φ), for each $x \in Q$ and $\varphi \in \mathcal{L}_1$. The kernel of this homomorphism is equal to $L_{(N)} = \{L_a;\ a \in N\}$.

Proof: The operation is well defined since the value of $L(x, y)$ depends only on xN and yN. The group $L_{(N)}$ is clearly normal in $\mathcal{L}$. Identify $\mathcal{L}$ with $Q \times \mathcal{L}_1$ by means of Lemma 1.8. Every $\varphi \in \mathcal{L}_1$ is a nuclear automorphism, which implies that $xN = \varphi(x)N$ for all $x \in N$. Hence $L(x, \varphi(y)) = L(x, y)$, and the factorization over $L_{(N)}$ yields the formula of the theorem. Group Q/N is abelian and $L(x, y) = L(y, x)$ for all $x, y \in Q$. □

Corollary 3.5. *Let Q be a conjugacy closed loop. Then $L(x, yz)L(y, z) = L(xy, z)L(x, y)$, for all $x, y, z \in Q$.*

Proof: The group of Theorem 3.4 contains $\mathcal{L}_1$ as its subgroup and Q/N is the corresponding quotient. Mappings $L(x, y)$ appear in the formula of the theorem in the rôle of a factor system. Therefore they satisfy the standard factor system equality (which is responsible for the associativity of the group). □

We shall finish this section by collecting several easy facts about mappings T_x. Some of them can be found in [7], [10] and [11].

Lemma 3.6. *Let Q be a conjugacy closed loop. Then*

(i) *$T_xT_y = L(x, y)T_{xy}$ for all $x, y \in Q$;*
(ii) *$a \in N$ if and only if $T_xT_a = T_{xa}$ for all $x \in Q$;*
(iii) *$a \in N$ if and only if $T_aT_x = T_{ax}$ for all $x \in Q$;*
(iv) *$T_xT_y(a) = T_{xy}(a)$ for all $x, y \in Q$ and all $a \in N$;*
(v) *$T_a(xy) = T_a(x)T_a(y)$ for all $a \in N$ and $x, y \in Q$.*

Proof: Point (i) can be obtained by applying Λ to $L_xL_y = L(x, y)L_{xy}$. The condition of (ii) (or (iii)) is hence equivalent to $L(x, a) = \mathrm{id}_Q$ (or $L(a, x) =$

id_Q), for all $x \in Q$, respectively, and that holds exactly when $a \in N$. Point (iv) follows from (i) because N is normal and $L(x,y)$ fixes elements of N pointwise. For (v), use direct computation or [4, Theorem 2.10]. □

Corollary 3.7. *Let U be a nuclear subloop of a conjugacy closed loop Q (i.e., $U \le N$). Then U is normal in Q if and only if $T_x(u) \in U$ for all $x \in Q$ and $u \in U$.*

Proof: Only the converse implication is needed. To get it we have to show that the condition implies $T_x^{-1}(u) \in U$, for all $x \in Q$ and $u \in U$. However, $T_x^{-1}(a) = T_{x\backslash 1}(a)$ for every $a \in N$, by point (iv) of Lemma 3.6. □

Corollary 3.8. **[Kunen]** *Map each $x \in Q$ to the permutation $a \mapsto T_x(a)$ of N. This mapping constitutes a homomorphism $Q \to \mathrm{Aut}\, N$, for every conjugacy closed loop Q.*

4. Conical construction

Proposition 4.1. *Let Q be a conjugacy closed loop, G a group and $\tau : Q \to \mathrm{Aut}\, G$ a homomorphism. The binary operation*

$$(g,x) \cdot (h,y) = (g\tau_x(h), xy)$$

defines a conjugacy closed loop on $G \times Q$. The loop satisfies

$$\begin{aligned} (h,y)/(g,x) &= (h\tau_{y/x}(g^{-1}), y/x), \\ (g,x)\backslash(h,y) &= (\tau_x^{-1}(g^{-1}h), x\backslash y), \\ ((g,x)(h,y))/(g,x) &= (g\tau_x(h)\tau_{(yx)/x}(g^{-1}), (xy)/x) \quad \textit{and} \\ (g,x)\backslash((h,y)(g,x)) &= (\tau_x^{-1}(g^{-1}h\tau_y(g)), x\backslash(yx)). \end{aligned}$$

The nucleus of the loop is equal to $\{(g,a);\ g \in G \text{ and } a \in N\}$.

Proof: The formulas of the proposition are easy to verify. For conjugacy closedness one needs to show

$$\begin{aligned} L_{(g,x)}L_{(h,y)}L^{-1}_{(g,x)} &= L_{((g,x)(h,y))/(g,x)} \quad \text{and} \\ R_{(g,x)}R_{(h,y)}R^{-1}_{(g,x)} &= R_{(g,x)\backslash((h,y)(g,x))}, \end{aligned}$$

for all $(g,x),(h,y) \in G \times Q$. This is not difficult and can be done in a straightforward manner. However, one can refrain from doing so since our construction is a special case of a general construction of the semidirect product for conjugacy closed loops. The general construction is described in Section 9 of [11].

For $g,h,k \in G$ and $x,y,z \in Q$ one obtains

$$\begin{aligned} (g,x) \cdot (h,y)(k,z) &= (g\tau_x(h)\tau_{xy}(hk), x \cdot yz) \quad \text{and} \\ (g,x)(h,y) \cdot (k,z) &= (g\tau_x(h)\tau_{xy}(hk), xy \cdot z). \end{aligned}$$

It is hence clear that (g,x) belongs to the nucleus if and only if $x \in N$. □

The loop of Proposition 4.1 will be denoted by $S(G,Q,\tau)$.

Lemma 4.2. *Assume* $x \equiv y \bmod A(Q)$. *Then* $(h,y)/(g,x) = (hg^{-1}, y/x)$ *for all* $g,h \in G$. *Furthermore,* $(g,y)/(g,x) = (1,y/x)$ *and* $(g,x)\backslash(g,y) = (1, x\backslash y)$, *for all* $g \in G$.

Proof: The last equality holds for all $x, y \in Q$. To get the first one note that $\operatorname{Ker}\tau$ contains $A(Q)$. This means that $\tau_{y/x}$ is the identity whenever $x \equiv y \bmod A(Q)$. □

Proposition 4.3. *Put* $S = S(G,Q,\tau)$, *where* $\tau : Q \to \operatorname{Aut} G$ *is a homomorphism,* G *a group and* Q *a conjugacy closed loop. Then* $A(S) = \{(1,a);\ a \in A(Q)\}$.

Proof: The associator subloop $A(S)$ is the least normal subloop of S that contains all $(\alpha\cdot\beta\gamma)/(\alpha\beta\cdot\gamma)$, where $\alpha,\beta,\gamma \in S$. Assume $\alpha = (g,x)$, $\beta = (h,y)$ and $\gamma = (k,z)$. Then $(\alpha\cdot\beta\gamma)/(\alpha\beta\cdot\gamma) = (1, (x\cdot yz)/(xy\cdot z))$, by Lemma 4.2, and we see that $A(S)$ contains $\{(1,a);\ a \in A(Q)\}$. It suffices to show that the latter subloop is normal in S. Now, $T^{-1}_{(g,x)}(1,a) = (\tau_x^{-1}(g^{-1}g), T_x^{-1}(a)) = (1, T_x^{-1}(a))$ belongs to the subloop whenever a belongs to $A(Q)$. We are done, by the symmetrical version of Corollary 3.7. □

Proposition 4.4. *Let* Q *be a conjugacy closed loop with nucleus* N *and let* G *be a group such that* $G \cap Q = N$. *Suppose that* $\tau : Q \to \operatorname{Aut} G$ *satisfies*

(1) $\tau_x(a) = T_x(a)$ *for all* $a \in N$ *and* $x \in Q$, *and*
(2) $\tau_a(g) = aga^{-1}$ *for all* $a \in N$ *and* $g \in G$.

Put $\varDelta = \{(a^{-1},a);\ a \in N\}$. *Then* $\varDelta$ *is a normal subloop of* $S = S(G,Q,\tau)$, $(a^{-1},a)(b^{-1},b) = ((ab)^{-1}, ab)$ *for all* $a,b \in N$ *and* $(g,a) \equiv (ga,1) \bmod \varDelta$ *for all* $(g,a) \in G \times N$.

Denote by π *the natural projection* $S \to S/\varDelta$. *It is injective on both* $G\times 1$ *and* $1\times Q$, *and* $\pi(1\times Q)$ *is a proper subloop of* $S/\varDelta$ *if and only if* N *is a proper subgroup of* G. *The nucleus* $N(S/\varDelta)$ *is equal to* $N(S)/\varDelta = \pi(N(S)) = \pi(G\times 1)$, *and the associator* $A(S/\varDelta)$ *is equal to* $A(S)\varDelta/\varDelta = \pi(1\times A(Q))$.

Proof: We have $(a^{-1},a)(b^{-1},b) = (a^{-1}\tau_a(b^{-1}), ab) = (a^{-1}ab^{-1}a^{-1}, ab) = ((ab)^{-1}, ab)$, for all $a,b \in N$. By Proposition 4.1, $T^{-1}_{(g,x)}(a^{-1},a)$ is equal to $(\tau_x^{-1}(g^{-1}a^{-1}\tau_a(g)), T_x^{-1}(a))$, and so $T^{-1}_{(g,x)}(a^{-1},a) = (\tau_x^{-1}(g^{-1}a^{-1}aga^{-1}), T_x^{-1}(a)) = (T_x^{-1}(a^{-1}), T_x^{-1}(a))$ for all $a \in N$, $g \in G$ and $x \in Q$. We have verified that $\varDelta$ forms a normal (nuclear) subloop of S.

The nucleus of S is the semidirect product $S(G,N,\tau)$, by Proposition 4.1. Thus $(g,a)(a,a^{-1}) = (g\tau_a(a),1) = (ga,1)$ for all $g \in G$ and $a \in N$, and $(g,a) \equiv (ga,1) \bmod \varDelta$, as required.

We have $(h,1)/(g,1) = (hg^{-1},1)$ and $(1,y)/(1,x) = (1,y/x)$ for all $g,h \in G$ and $x,y \in Q$. The results of the division are in $\varDelta$ if and only if $h = g$ or $y = x$, respectively. This means that π is injective on both subloops $G\times 1$ and $1 \times Q$.

We also have $(a,a^{-1})(1,x) = (a, a^{-1}x)$ for all $a \in N$ and $x \in Q$. Hence $\varDelta(1\times Q) = \{(a,x);\ a \in N \text{ and } x \in Q\}$. Since $\pi(1\times Q) = S/\varDelta$ if and only if $\varDelta(1\times Q) = S$, we see that this takes place if and only if $N = G$.

To compute the nucleus first note that each surjective homomorphism of loops moves the nucleus into the nucleus. Hence $N(S/\Delta)$ contains $N(S)/\Delta$ and we only need to show that $(g,x)\Delta \notin N(S/\Delta)$ for each $x \in Q \setminus N$. Consider such an x and find $y,z \in Q$ with $u = (x \cdot yz)/(xy \cdot z) \neq 1$. Then $((g,x)\cdot(1,y)(1,z))/((g,x)(1,y)\cdot(1,z)) = (g, x\cdot yz)/(g, xy\cdot z) = (1,u)$, by Lemma 4.2. The element $(1,u)$ does not belong to Δ, and so $(g,x)\Delta \notin N(S/\Delta)$.

Let us finally consider the associator subloop. In every surjective homomorphism of loops the image of the associator subloop contains the associator subloop of the image. We hence have $A(S/\Delta) \geq \pi(1 \times A(Q))$. The equality follows from the injectivity of π on $1 \times Q$ and from the fact that in any loop the associator subloop contains the associator subloop of each of its subloops. □

We shall denote S/Δ by $\mathrm{Cone}\,(G,Q,\tau)$. This loop will be called the *conical extension* of Q by G (by means of τ).

Recall that in every loop Q the product $PU = UP$ forms a subloop of Q whenever U is a normal subloop of Q and P is also a subloop (not necessarily normal). If $U = N$ and $Q = NP$, then for every $a \in N_\mu(P)$ one clearly has $(bx)(a \cdot yc) = (bx \cdot a)(yc)$ for all $x,y \in P$ and $b,c \in N$. This implies $N_\mu(P) = P \cap N_\mu(Q)$.

Lemma 4.5. *Let Q be a conjugacy closed loop with a subloop P. Suppose that $Q = PN$. The nucleus of P is then equal to $N \cap P$. Denote by τ the homomorphism $P \to \mathrm{Aut}\,N$, $x \mapsto \tau_x$, $\tau_x(a) = T_x(a)$ for all $x \in P$ and $a \in N$. Set $S = S(N,P,\tau)$ and denote by π the mapping $S \to Q$, $(a,x) \mapsto ax$. Then π is a surjective homomorphism of loops and* $\mathrm{Ker}\,\pi = \{(b^{-1},b);\ b \in P \cap N\}$.

Proof: The equality $N(P) = N \cap P$ follows from the remark preceding the lemma. Consider $a,b \in N$ and $x,y \in P$. Then $(a,x)\cdot(b,y) = (a \cdot ((xb)/x), xy)$, and so $\pi((a,x)\cdot(b,y)) = a\cdot(((xb)/x)x)y = a(x\cdot by) = ax\cdot by = \pi(a,x)\cdot\pi(b,y)$. We see that π is really a homomorphism. Now, $ax = 1$ if and only if $x \in P \cap N$ and $x = a^{-1}$. □

In the situation of Lemma 4.5 we have

(1) $\tau_x(a) = T_x(a)$ for all $a \in N \cap P$ and $x \in P$, and
(2) $\tau_a(g) = aga^{-1}$ for all $a \in N \cap P$ and $g \in N$.

This means that π of the lemma induces an isomorphism $\mathrm{Cone}\,(N,P,\tau) \cong Q$. We record it as

Theorem 4.6. *Let Q be a conjugacy closed loop with such a subloop P that $Q = PN$. For every $x \in P$ define $\tau_x \in \mathrm{Aut}\,N$ by $\tau_x(a) = (xa)/x$. Then there exists an isomorphism* $\mathrm{Cone}\,(N,P,\tau) \cong Q$.

Every conjugacy closed loop Q that possesses a subloop P with $Q = PN$ can be thus regarded as a conical extension of P.

Let us recapitulate the steps needed for a construction of such an extension. One can start from the action of N on N by conjugation. Since $A \leq Z(N)$, this action gives a homomorphism

$$\tau_0 : N/A \to \operatorname{Aut} N, \quad \tau_0(aA)(b) = aba^{-1}.$$

To get a conical extension one needs to enlarge τ_0 to a homomorphism

$$\tau_1 : Q/A \to \operatorname{Aut} N, \quad \tau_1(aA) = \tau_0(aA) \text{ for all } \quad a \in N.$$

This is still not sufficient, since we need a homomorphism $Q/A \to \operatorname{Aut} G$, where $N \trianglelefteq G$. Thus τ_1 has to be further extended to $\tau_2 : Q/A \to \operatorname{Aut} G$, in such a way that

(1) $\tau_2(xA)(a) = \tau_1(xA)(a)$ for all $x \in Q$ and $a \in N$, and
(2) $\tau_2(aA)(g) = aga^{-1}$ for all $g \in G$ and $a \in N$.

One then puts $\tau(x) = \tau_2(xA)$ for all $x \in Q$.

Conical extensions can be thus obtained by appropriate extensions of inner automorphisms of N. From the structural point of view the more interesting conjugacy closed loops are those that cannot be constructed in a clear way from smaller ones by means of group theory. The conical extension can be applied whenever a loop Q has a proper subloop P with $Q = PN$. Call Q *conefree* if it possesses no such subloop.

Theorem 4.7. *Let Q be a finite conefree conjugacy closed loop. Let $N = N(Q)$ be its nucleus and $A = A(Q)$ its associator subloop. Then N/A is a nilpotent group.*

Proof: Consider all subloops P of Q that contain A and have the property that P/A is a maximal subgroup of Q/A. Each such P contains N, since otherwise Q would not be conefree. Denote by F the intersection of all possible P. Then F/A is the Frattini subgroup of Q/A, and so it is nilpotent. We know that F contains N, and nothing more is needed. □

5. Embeddings

Proposition 5.1. *Let Q be a conjugacy closed loop. Then $L_a\varphi = \varphi L_a$ for all $a \in N$ and $\varphi \in \mathcal{L}_1$.*

Proof: Group $\mathcal{L}_1$ is generated by mappings $L(x, y)$. These mappings depend only on xN and yN, and so $L_a L(x, y)L_a^{-1} = L(T_a(x), T_a(y)) = L(x, y)$, by point (v) of Lemma 3.6. □

We see that $\mathcal{L}$ contains $L_{(N)} \times \mathcal{L}_1$ as its subgroup. In fact, this can be proved for all A_ℓ-loops in which N is a normal subloop (some other results of this paper generalize to A_ℓ-loops as well).

Corollary 5.2. *Let Q be a conjugacy closed loop. Then $L_a\psi = \psi L_a$ for all $a \in N$ and $\psi \in [\mathcal{L}, \mathcal{R}]$.*

Proof: We can assume $\psi \in \mathcal{L}_u$, for some $u \in Q$, by Theorem 2.4. Then $\psi = L_v^{-1}\varphi L_v$ for $v = 1/u$ and some $\varphi \in \mathcal{L}_1$. Furthermore, $L_a\psi L_a^{-1} = L_v^{-1}L_vL_aL_v^{-1}\varphi L_vL_a^{-1}L_v^{-1}L_v = L_v^{-1}L_{T_v(a)}\varphi L_{T_v(a)}^{-1}L_v = L_v^{-1}\varphi L_v = \psi$. □

Lemma 5.3. *Let Q be a conjugacy closed loop and let Γ be a coset modulo N. Then N acts regularly on Γ by left translations. Denote by J the image of this action, and denote by I the image of the action of $[\mathcal{L},\mathcal{R}]$ on Γ. Then $I \cong A(Q)$, $I \le Z(J)$ and the orbits of I coincide with those cosets of $A(Q)$ that lie in Γ.*

Proof: We know that the orbits of I have to coincide with the cosets modulo $A(Q)$ that are contained in Γ, by Theorem 3.4. The properties we wish to show are retained by conjugation by L_u, $u \in Q$, and so we can assume $\Gamma = N$. Then J becomes the regular action of N on itself by left translations, and the centralizer of J is the group of right translations. We know, by Corollary 5.2, that I is a subgroup of this centralizer. Because the centralizer is a regular permutation group, I is fully determined by any of its orbits. One such orbit is equal to $A = A(Q)$ and $A \le Z(N)$. The rest is clear. □

Theorem 5.4. *Let Q be a conjugacy closed loop and let $\mathcal{L}$ and $\mathcal{R}$ be its left and right multiplication groups, respectively. Furthermore, let N be its nucleus and let A be its associator subloop. Then there exists $r \le |Q : N|$, such that $[\mathcal{L},\mathcal{R}]$ can be embedded into the product of r copies of A.*

Proof: We have observed in Lemma 5.3 that by restricting all permutations of $[\mathcal{L},\mathcal{R}]$ to a coset modulo N one obtains a semiregular permutation group that is isomorphic to A. We can hence map $[\mathcal{L},\mathcal{R}]$ to a product of such permutation groups, each coordinate corresponding to a coset of N. □

Corollary 5.5. *The group $[\mathcal{L},\mathcal{R}]$ is abelian, in every conjugacy closed loop Q.*

Proposition 5.6. *Let Q be a conjugacy closed loop and consider the action of $\mathcal{L}$ on $[\mathcal{L},\mathcal{R}]$ by conjugation. The kernel of this action is equal to $\{L_a\varphi;\ a \in N$ and $\varphi \in \mathcal{L}_1\}$ (which is the normalizer of $\mathcal{L}_1$ in $\mathcal{L}$).*

Proof: We have $\mathcal{L}_1 \le [\mathcal{L},\mathcal{R}]$, by Theorem 3.4, and so in our action $\mathcal{L}_1$ acts trivially, by Corollary 5.5. From Lemma 5.3 we see that each L_a, $a \in N$, acts trivially as well. On the other hand, $\mathcal{L}_1$ fixes pointwise exactly the elements of N, and hence for every $x \in Q \setminus N$ there exists $\varphi \in \mathcal{L}_1$ with $L_x\varphi \ne \varphi L_x$. □

The action of Proposition 5.6 can be regarded as an action of Q/N on $[\mathcal{L},\mathcal{R}]$ (cf. Lemma 1.4), and so we can state

Corollary 5.7. *There exists an embedding of Q/N to* $\operatorname{Aut}[\mathcal{L},\mathcal{R}]$*, in every conjugacy closed loop Q.*

From Theorem 5.4 and Corollary 5.7 we see that Q/N can be embedded into $\operatorname{Aut} A^r$, for some $r \le |Q : N|$. It seems that quite a lot can be done to downsize r. However, in this paper we shall not go beyond Corollary 5.9 (see below).

Proposition 5.8. *Let Q be a conjugacy closed loop and let $A = A(Q)$ be its associator subloop. Then L_a and R_a belong to $[\mathcal{L}, \mathcal{R}]$, for every $a \in A$, and $[\mathcal{L}, \mathcal{R}] = \{L_a\varphi;\ a \in A \text{ and } \varphi \in \mathcal{L}_1\} \cong L_{(A)} \times \mathcal{L}_1$.*

Proof: For every $a \in A$ there must exist $\psi \in [\mathcal{L}, \mathcal{R}]$ with $\psi(1) = a$, by Theorem 3.4. Now, $\psi = L_a\varphi$ for some $\varphi \in \mathcal{L}_1 \leq [\mathcal{L}, \mathcal{R}]$. Hence $L_a \in [\mathcal{L}, \mathcal{R}]$. The expression of ψ as $L_a\varphi$ is unique, and the rest follows easily. □

Corollary 5.9. *Let Q be a conjugacy closed loop with $|Q : N|$ a prime number. Then $\mathcal{L}_1$ embeds into $A = A(Q)$ and $[\mathcal{L}, \mathcal{R}] \cong A \times \mathcal{L}_1$ embeds into $A \times A$.*

Proof: Every $\varphi \in \mathcal{L}_1$ fixes all elements of N pointwise. The points fixed by φ form a subloop of Q because φ is an automorphism. Since we assume that there is no subloop between N and Q, $\mathcal{L}_1$ has to act on $Q \setminus N$ semiregularly, and so $\mathcal{L}_1$ embeds into A, by Lemma 5.3. The isomorphism $[\mathcal{L}, \mathcal{R}] \cong A \times \mathcal{L}_1$ follows from Proposition 5.8. □

Recall that the orbits of $\mathcal{L} \cap \mathcal{R}$ correspond to the cosets of $M = \{a \in Q;\ L_a \in \mathcal{R}\}$, by Proposition 2.1. Since $(\mathcal{L} \cap \mathcal{R})_1 = [\mathcal{L}, \mathcal{R}]_1 = \mathcal{L}_1$, we immediately obtain

Lemma 5.10. *Let Q be a conjugacy closed loop. Then $|M : A(Q)| = |(\mathcal{L} \cap \mathcal{R}) : [\mathcal{L}, \mathcal{R}]|$.*

Lemma 5.11. *Let Q be a nonassociative conjugacy closed loop of order pq. Then one of the primes, say p, is equal to the order of N, and also to the order of $\mathcal{L}_1$. We have $N = M = A$, $[\mathcal{L}, \mathcal{R}] = \mathcal{L} \cap \mathcal{R} \cong N \times N$, and $\mathcal{L}/\mathcal{L} \cap \mathcal{R} \cong \operatorname{Inn} Q/\mathcal{L}_1$ is of order q. Furthermore, $|\mathcal{L}| = p^2q = |\mathcal{R}|$, $|\operatorname{Mlt} Q| = p^2q^2$ and $|\operatorname{Inn} Q| = pq$. The group $\operatorname{Inn} Q$ is elementary abelian if $p = q$, and nonabelian if $p \neq q$. In the latter case q divides $p - 1$.*

Proof: We have $1 \lneq A \leq M \leq N \lneq Q$, and so $A = M = N$. Assume $|N| = p$. Then $[\mathcal{L}, \mathcal{R}] = \mathcal{L} \cap \mathcal{R} \cong N \times N$ and $|\mathcal{L}_1| = p$, by Lemma 5.10 and Corollary 5.9. In every conjugacy closed loop $\mathcal{L}/\mathcal{L} \cap \mathcal{R} \cong \mathcal{L}\mathcal{R}/\mathcal{R} \cong (\operatorname{Inn} Q)\mathcal{R}/\mathcal{R} \cong (\operatorname{Inn} Q)/\mathcal{L}_1$, since $(\operatorname{Inn} Q) \cap \mathcal{R} = \mathcal{R}_1 = \mathcal{L}_1$. Also $(\operatorname{Inn} Q)/\mathcal{L}_1 \cong Q/N$, by Theorem 3.4. This resolves the group orders and it remains to prove that $\operatorname{Inn} Q$ cannot be cyclic. Now, nontrivial $\operatorname{Inn} Q$ is never cyclic, for every loop Q, by [9] (see also [12] and [6]). We shall observe that this can be seen also directly, without resorting to the general theorem. If $\operatorname{Inn} Q$ were cyclic, a generator φ of $\mathcal{L}_1$ would equal ψ^q for some $\psi \in \operatorname{Inn} Q$. This cannot happen if $q = p$ since ψ fixes 1 and moves points within the cosets of N (recall that Q/N is an abelian group). Assume $p \neq q$ and note that φ acts regularly in each coset Γ modulo N, $\Gamma \neq N$. This means that ψ has to act as a p-cycle on each such coset Γ, and so ψ^p is a permutation of order q that fixes all points outside N. In such a situation it is easy to deduce that $|\operatorname{Inn} Q|$ has to be divided by q^2, which is a contradiction. □

Proposition 5.12. *Let Q be a nonassociative conjugacy closed loop of order pq, q dividing $p-1$. Then $Z(Q)=1$. Furthermore, consider the group*

$$\begin{aligned} G = \langle x,y,u,v; \quad & x^p = y^p = u^q = v^q = 1,\ xy = yx,\ uv = vu, \\ & xv = vx,\ yu = uy,\ uxu^{-1} = x^\gamma,\ vyv^{-1} = y^\gamma\rangle, \end{aligned}$$

where $\gamma^q \equiv 1 \bmod p$, $\gamma \not\equiv 1 \bmod p$. For all nontrivial $a,b \in N$ there exists an isomorphism $\Phi : G \to \operatorname{Mlt} Q$ such that $x \mapsto L_a$, $y \mapsto R_b$, $\Phi(\langle x,y,u\rangle) = \mathcal{L}$ and $\Phi(\langle x,y,v\rangle) = \mathcal{R}$.

Proof: Facts established in Lemma 5.11 will be used without further reference. The nonabelian group $\operatorname{Inn} Q$ moves points within the cosets of N. Therefore no L_a, $a \in N$ nontrivial, commutes with $\psi \in \operatorname{Inn} Q$ if $|\psi| = q$. Hence $a \notin Z(Q)$ and $Z(Q)=1$. Consider now a Sylow q-subgroup of $\operatorname{Mlt} Q$. It intersects both $\mathcal{L}$ and $\mathcal{R}$ in a q-element subgroup, and we shall choose generators of these subgroups and denote them by u and v, respectively. Groups $\langle u\rangle$ and $\langle v\rangle$ are different, as $|\mathcal{L} \cap \mathcal{R}| = p^2$. We see that $\langle u,v\rangle$ is elementary abelian, of order q^2. Now, $Z(\mathcal{L}) = R_{(N)}$ and $Z(\mathcal{R}) = L_{(N)}$, by Theorem 3.7 and Corollary 3.8 of [4]. Hence u commutes with all R_b, $b \in N$, and v commutes with all L_a, $a \in N$. However, u cannot commute with L_a, $a \in N$ nontrivial, since $\mathcal{L}$ would be abelian. The rest is clear since we can replace u and v by their appropriate powers, respectively. □

6. Conjugacy closed loops of order pq

Lemma 6.1. *Let Q be a loop with an element a.*

(i) *If $a \in N_\mu \cap N_\rho$, then $L_{xa}^{-1} R_a L_x = L_a^{-1} R_a$ for all $x \in Q$; and*
(ii) *If $a \in N_\mu \cap N_\lambda$, then $R_{ax}^{-1} L_a R_x = R_a^{-1} L_a$ for all $x \in Q$.*

Proof: We shall prove point (i). Consider $c \in Q$ and put $d = L_{xa}^{-1} R_a L_x(c)$. Then $(xa)d = (xc)a$, and hence $x(ad) = x(ca)$, by $a \in N_\mu \cap N_\rho$. We obtain $ad = ca$, and so $d = L_a^{-1} R_a(c)$. □

Lemma 6.2. *Let Q be a loop, a an element of Q, and K a normal subloop of Q.*

(i) *If $K \le N_\mu \cap N_\rho$, then $L_{xa}^{-1} R_a L_x(c) = L_a^{-1} R_a(c)$ for all $c \in K$ and $x \in Q$.*
(ii) *If $K \le N\mu \cap N_\lambda$, then $R_{ax}^{-1} L_a R_x(c) = R_a^{-1} L_a(c)$ for all $c \in K$ and $x \in Q$.*

Proof: We shall prove point (i). The element $d = L_{xa}^{-1} R_a L_x(c)$ belongs to K, as $L_{xa}^{-1} R_a L_x \in \operatorname{Inn} Q$. Therefore from $(xa)d = (xc)a$ and $c,d \in N_\rho \cap N_\mu$ one obtains $x(ad) = x(ca)$ and $ad = ca$. The latter fact means $d = L_a^{-1} R_a(c)$. □

Lemma 6.3. *A loop Q is conjugacy closed if and only if $L_{xa}^{-1} R_a L_x = L_a^{-1} R_a$ and $R_{ax}^{-1} L_a R_x = R_a^{-1} L_a$, for all $a,x \in Q$.*

Proof: This is one of the standard facts concerning conjugacy closed loops. See [5, Lemma 2.1] or [11, Lemma 2.4]. □

For the rest of this section G will mean the group from Proposition 5.12, and by H we shall denote its subgroup $\langle xy^{-1}, uv\rangle$. Then $(uv)(xy^{-1})(uv)^{-1}$ equals $(xy^{-1})^{\gamma}$, and we see that H is a nonabelian group of order pq.

An element $x^i v^r$, $0 \le i < p$ and $0 \le r < q$, belongs to H if and only if $i = r = 0$. Indeed, $(x^i v^r)(xy^{-1})(x^i v^r)^{-1} = xy^{-\gamma^r}$ implies that $x^i v^r \notin H$ for all $r \ne 0$. Clearly, $H \cap \langle x, y\rangle = \langle xy^{-1}\rangle$, and so $x^i \in H$ exactly when $i = 0$.

Put $\Omega = \{(i, r);\ 0 \le i < p \text{ and } 0 \le r < q\}$.

Lemma 6.4. *The set $\{x^i v^r;\ (i, r) \in \Omega\}$ is a complete system of left coset representatives modulo H. Furthermore,*

$$\begin{array}{rclrcl} x(x^i v^{-r} H) & = & x^{i+1} v^{-r} H, & y(x^i v^{-r})H & = & x^{i+\gamma^r} v^{-r} H, \quad \textit{and} \\ u(x^i v^{-r} H) & = & x^{\gamma i} v^{-(r+1)} H, & v(x^i v^{-r})H & = & x^i v^{-(r-1)} H. \end{array}$$

Proof: If $x^i v^r H = x^j v^s H$, then $x^{i-j} v^{r-s} \in H$. However, that means $i = j$ and $r = s$, by considerations above. The system of representatives is complete since $|G : H| = pq = |\Omega|$. Now, $yx^i v^{-r} = x^i v^{-r} v^r y v^{-r} = x^i v^{-r} y^{\gamma^r} = x^{i+\gamma^r} v^{-r} (xy^{-1})^{-\gamma^r}$ and $ux^i v^{-r} = x^{\gamma i} u v^{-r} = x^{\gamma i} v^{-(r+1)}(uv)$. The rest is clear. □

Identify now $x^i v^{-r} H$ with (i, r). This identification yields an action of G on Ω, where

$$\begin{array}{rclrcl} x\,(i,r) & = & (i+1, r), & y\,(i,r) & = & (i+\gamma^r, r), \quad \text{and} \\ u\,(i,r) & = & (\gamma i, r+1), & v\,(i,r) & = & (i, r-1). \end{array}$$

The action of the powers of the generators is easy to compute and we get

$$\begin{array}{rclrcl} x^j\,(i,r) & = & (i+j, r), & y^j\,(i,r) & = & (i+j\gamma^r, r), \quad \text{and} \\ u^s\,(i,r) & = & (\gamma^s i, r+s), & v^s\,(i,r) & = & (i, r-s), \end{array}$$

for all integers j and s.

The action of G on Ω is equivalent, by construction, to the action of G on the left cosets of H. The stabilizer of $G_{(0,0)}$ is hence equal to H. The generators of H are xy^{-1} and uv. Clearly,

$$(xy^{-1})^j\,(i,r) \;=\; (i + j(1-\gamma^r), r) \quad \text{and} \quad (uv)^s\,(i,r) \;=\; (\gamma^s i, r),$$

for all integers j and s.

Lemma 6.5. *Assume $1 \le i < p$. Then $G_{(0,0),(i,0)} = \langle xy^{-1}\rangle$. Furthermore, if $w\,(0,0)$ and $w\,(i,0)$ are known for some $w \in G$, then w is completely determined by $w\,(j,s)$, for any $(j,s) \in \Omega$, $s \ne 0$.*

Proof: The set $\{(j, 0);\ 0 \le j < p\}$ is a block of G. The permutation uv fixes only one point of this block, i.e. the point $(0, 0)$. Since all q-element subgroups of H are conjugate, the same property must be fulfilled by all elements of H that are of order q. Hence $H_{(i,0)} = \langle xy^{-1}\rangle$. For the rest it suffices to show that $w \in H_{(i,0)}$ is completely determined by $w\,(j,s)$,

$s \neq 0$. However, that follows from the fact that $\langle xy^{-1}\rangle$ acts semiregularly on $\{(j,s) \in \Omega;\ s \neq 0\}$. □

Corollary 6.6. *Let Q be a loop on Ω with $\operatorname{Mlt} Q \le G$. Suppose that $(i,0)\cdot(j,s) = (i+j,s)$ and $(j,s)\cdot(i,0) = (j+i\gamma^s,s)$ for all $(j,s) \in \Omega$ and all i, $0 \le i < p$. Then Q is completely determined by any value $(i_1,r_1)\cdot(i_2,r_2)$, where $(i_k,r_k) \in \Omega$ and $r_k \neq 0$, for $k \in \{1,2\}$.*

Proof: This is an immediate consequence of Lemma 6.5, since $(i_1,r_1)\cdot(i_2,r_2)$ determines $L_{(i_1,r_1)}$, and the subsequent knowledge of $(i_1,r_1)\cdot(i,r)$ determines $R_{(i,r)}$, for all $(i,r) \in \Omega$, $r \neq 0$. □

Lemma 6.7. *Let Q be a loop on Ω with $\operatorname{Mlt} Q \le G$, and such that $(0,0)$ is its unit element. Suppose that $\mathcal{L} \le \langle x,y,u\rangle$ and $\mathcal{R} \le \langle x,y,v\rangle$. Then Q is conjugacy closed and $\Gamma = \{(i,0);\ 0 \le i < p\}$ is contained in the nucleus.*

Proof: The set Γ is a block of G, and hence a normal subloop of Q. We have $\mathcal{L}_{(0,0)} \le \langle xy^{-1}\rangle$, and this implies $\Gamma \le N_\rho$ as xy^{-1} fixes all elements of Γ. Similarly, $\Gamma \le N_\lambda$. Furthemore, $\mathcal{L} \cap \mathcal{R} = \langle x,y\rangle$, and so $[\mathcal{L},\mathcal{R}] \cap H \le \langle xy^{-1}\rangle$ as well. Thus $[L_\alpha, R_\beta]$ fixes Γ pointwise, for all $\alpha,\beta \in Q$, and hence $\Gamma \le N_\mu$.

Consider now mappings $L^{-1}_{(j,s)\cdot(i,r)}R_{(i,r)}L_{(j,s)}$ and $L^{-1}_{(i,r)}R_{(i,r)}$, for some (i,r) and (j,s) from Ω, where $r \neq 0$. These mappings agree on Γ, by point (i) of Lemma 6.2. However, they also agree on (i,r), since this point is fixed by both of them. Hence they agree everywhere, by Lemma 6.5. For the rest use Lemma 6.1, Lemma 6.3 and the left-right symmetry. □

Proposition 6.8. *Let Q be a nonassociative conjugacy closed loop of order pq, q dividing $p-1$. Then there exists an isomorphism $\Phi : G \cong \operatorname{Mlt} Q$ with $\Phi(H) = \operatorname{Inn} Q$ that fulfils conditions of Proposition 5.12. In addition one can assume that either $\Phi(u)$ or $\Phi(u(xy^{-1})^{(1-\gamma)/\gamma})$ is a left translation of Q.*

Proof: The automorphisms of G that normalize each of the subgroups $\langle x\rangle$, $\langle y\rangle$, $\langle x,y,u\rangle$ and $\langle x,y,v\rangle$ form a subgroup of $\operatorname{Aut} G$, and this subgroup will be denoted by B. We have $\operatorname{Inn} G \le B$, since all these subgroups are normal.

For any choice of $i,j \in \{1,\dots,p-1\}$ the defining relations of G remain valid when x is replaced by x^i, and y by y^j. Hence there exists $\alpha = \alpha_{i,j} \in B$ such that $\alpha(x) = x^i$, $\alpha(y) = y^j$, $\alpha(u) = u$ and $\alpha(v) = v$.

Let us consider an isomorphism $\Phi : G \cong \operatorname{Mlt} Q$ that fulfils conditions of Proposition 5.12. We shall first look for $\alpha \in B$ such that $\Phi\alpha$ maps H upon $\operatorname{Inn} Q$, and then replace Φ by $\Phi\alpha$. The centre of $\langle x,y,u\rangle$ is equal to $\langle y\rangle$, and $Z(\mathcal{L}) = \{R_a;\ a \in Q\}$. In our situation $M = N = A$, by Lemma 5.11, and $(\operatorname{Inn} Q) \cap (\mathcal{L} \cap \mathcal{R}) = \mathcal{L}_1 = \mathcal{R}_1$. Since $\Phi(\langle x,y\rangle) = \mathcal{L} \cap \mathcal{R}$, we see that $\Phi^{-1}(\mathcal{L}_1)$ is a proper subgroup of $\langle x,y\rangle$ which is different from both $\langle x\rangle$ and $\langle y\rangle$. Thus it equals $\langle xy^{-j}\rangle$ from some j, $1 \le j < p$. Setting $\alpha = \alpha_{1,j}$ yields $(\Phi\alpha)^{-1}(\mathcal{L}_1) = \alpha^{-1}(\langle xy^{-j}\rangle) = \langle xy^{-1}\rangle$. We can hence assume $\Phi(xy^{-1}) \in \mathcal{L}_1$.

The normalizer of $\langle xy^{-1}\rangle$ in G is equal to $\langle x,y,uv\rangle$, which is a group of order p^2q. Consider $\psi \in \operatorname{Inn} Q$ of order q. Then $\psi\mathcal{L}_1\psi^{-1} = \mathcal{L}_1$, as $\mathcal{L}_1 \trianglelefteq \operatorname{Inn} Q$. Therefore $\Phi^{-1}(\psi) \in \langle x,y,uv\rangle$. All q-element subgroups of

$\langle x, y, uv\rangle$ are mutually conjugated in $\langle x, y, uv\rangle$, and hence there exists $\alpha \in B$ such that $(\Phi\alpha)^{-1}(\psi)$ is a power of uv, and $\alpha(\langle xy^{-1}\rangle) = \langle xy^{-1}\rangle$. Hence $(\Phi\alpha)(uv) \in \operatorname{Inn} Q$ and $(\Phi\alpha)(xy^{-1}) \in \operatorname{Inn} Q$, which implies $(\Phi\alpha)(H) = \operatorname{Inn} Q$. We can assume $\Phi(H) = \operatorname{Inn} Q$.

Note that $\alpha_{j,j}(H) = H$ for any $j \in \{1, \dots, p-1\}$. We can thus replace Φ by $\Phi\alpha_{j,j}$ without violating the condition $\Phi(H) = \operatorname{Inn} Q$.

The preimage of each left translation is an element of $\langle x, y, u\rangle$. The left translations form a complete set of representatives for the left cosets of $\mathcal{L}_1$ in $\mathcal{L}$, and hence their preimages form a complete set of representatives for left cosets modulo $\langle xy^{-1}\rangle$ in $\langle x, y, u\rangle$. Let u_1 be the representative of $u\langle xy^{-1}\rangle$. Then either $u_1 = u$, or $u_1 = u(xy^{-1})^j = \alpha_{j,j}(uxy^{-1})$, for some j, $1 \le j < p$. We see that either $\Phi(u)$ is a left translation of Q, or that $\Phi(u(xy^{-1})^{(1-\gamma)/\gamma})$ can be assumed to be a left translation of Q, when Φ is replaced by $\Phi\alpha_{i,i}$, for an appropriate $i \in \{0, \dots, p-1\}$. □

Theorem 6.9. *Let Q be a nonassociative conjugacy closed loop of order pq, where $q < p$ are primes. Such a loop exists if and only if q divides $p-1$, and then it is determined uniquely up to isomorphism.*

If q divides $p-1$ and γ is an integer with $\gamma^q \equiv 1 \bmod p$, $\gamma \not\equiv 1 \bmod p$, then Q is isomorphic to a loop on $\{(i,r);\ 0 \le i < p$ and $0 \le r < q\}$, where

$$(i,r)\cdot(j,s) = (i + j\gamma^r + (1-\gamma^r)(1-\gamma^s),\ r+s)$$

for all elements (i,r) and (j,s) of the underlying set.

Proof: We shall use the isomorphism $\Phi : G \to \operatorname{Mlt} Q$ constructed in Proposition 6.8. The isomorphism maps x to some R_a, $a \in M = N$, as $x \in Z(\langle x, y, u\rangle)$. A symmetric argument shows that $\Phi(y)$ is a left translation. From $\Phi(xy^{-1}) \in \operatorname{Inn} Q$ we obtain $\Phi(y) = L_a$.

Group $\langle x, v\rangle$ is abelian of order pq, and $x^i v^r$ is of exponent p if and only if $r \equiv 0 \bmod q$. Since $\mathcal{R}_1$ is of exponent p, we see that $\Phi(x^i v^r) \in \mathcal{R}$ is fixed point free when $x^i v^r \ne 1$. This means that $\Phi(\langle x, v\rangle)$ is a regular abelian permutation group, and that each element of Q has a unique expression as $\Phi(x^i v^{-r})(1)$, where $0 \le i < p$ and $0 \le r < q$. Denote this element by $[i,r]$, and note that $[i,0] = \Phi(x^i)(1) = L_a^i(1) = a^i$. We also have $[i,0]\cdot[j,s] = a^i(a^j[0,s]) = a^{i+j}[0,s] = [i+j, s]$, and $[j,s]\cdot[i,0] = a^j[0,s]a^i = \Phi(x^j y^i v^{-s})(1)$.

This can be turned into

$$[j,s]\cdot[i,0] = [j + i\gamma^s, s],$$

since $y^i v^{-s} = v^{-s} y^{i\gamma^s} = x^{i\gamma^s} v^{-s}(x^{-1}y)^{i\gamma^s}$, and $\Phi(x^{-1}y) \in \operatorname{Inn} Q$.

From $\Phi(xy^{-1}), \Phi(uv) \in \operatorname{Inn} Q$ we get

$$\Phi(u)(1) = \Phi(v^{-1})(1) = [0,1] = \Phi(u(xy^{-1})^j)(1),$$

for every $j \in \{0, \dots, p-1\}$.

This means that $[0,1]\cdot[0,1]$ is equal to $\Phi(u(xy^{-1})^j v^{-1})(1)$, when j is such that $\Phi(u(xy^{-1})^j)$ is a left translation. Now, $ux^j y^{-j} v^{-1} = x^{j\gamma} u y^{-j} v^{-1} =$

$x^{j\gamma}y^{-j}v^{-2}(uv) = x^{j\gamma}v^{-2}y^{-j\gamma^2}(uv) = x^{j(\gamma-\gamma^2)}v^{-2}(xy^{-1})^{j\gamma^2}(uv)$. We assume $j \in \{0, (1-\gamma)/\gamma\}$, by Proposition 6.8, and so $[0,1]\cdot[0,1] = [\eta, 2]$, where $\eta \in \{0, (1-\gamma)^2\}$.

We have proved $\Phi(x)[i,r] = [1,0][i,r] = [i+1,r]$ and $\Phi(y)[i,r] = [i+\gamma^r, r]$. We also have $\Phi(u)[i,r] = \Phi(ux^iv^{-r})(1) = \Phi(x^{\gamma i}v^{-(r+1)}(uv)(1) = [\gamma i, r+1]$ and $\Phi(v)[i,r] = \Phi(x^iv^{-(r-1)})(1) = [i, r-1]$.

We see that the bijection $[i,r] \mapsto (i,r)$ induces an isomorphism of Q upon such a loop on Ω that fulfils the assumptions of Corollary 6.6. The loop on Ω satisfies, in addition, $(0,1)\cdot(0,1) = (\eta,2)$. However, that means that the loop is uniquely determined, by Corollary 6.6.

Consider first the group operation $(i,r)\cdot(j,s) = (i+j\gamma^r, r+s)$. Then $L_{(i,r)} = x^iu^r$ and $R_{(j,s)} = v^{-s}y^j$. The multiplication group of this group is contained in G, and $(0,1)\cdot(0,1) = (0,2)$. The case $\eta = 0$ thus yields an associative conjugacy closed loop Q.

Consider now the loop described in the theorem. This loop satisfies $(0,1)\cdot(0,1) = (1-\gamma)^2$. We shall verify that the left and right translations belong to $\langle x,y,u\rangle$ and $\langle x,y,v\rangle$, respectively.

Now, $(xy^{-1})^{\gamma^{-r}-1}$ sends $(j,s)\in\Omega$ to $(j+(\gamma^{-r}-1)(1-\gamma^s),\ s)$, and this is sent by x^iu^r to $(i+\gamma^rj+(1-\gamma^r)(1-\gamma^s),\ r+s)$. We have verified that $L_{(i,r)} = x^iu^r(xy^{-1})^{\gamma^{-r}-1}$ for all $(i,r)\in\Omega$. In particular, $L_{(0,1)} = u(xy^{-1})^{(1-\gamma)/\gamma}$ as $\gamma^{-1}-1 = (1-\gamma)/\gamma$.

The mapping $(xy^{-1})^{1-\gamma^s}y^j$ sends $(i,r)\in\Omega$ to $(i+j\gamma^r+(1-\gamma^s)(1-\gamma^r),\ r)$, and we see that $R_{(j,s)} = v^{-s}(xy^{-1})^{\gamma^s-1}y^j$, for all $(j,s)\in\Omega$.

We have now two loops on Ω: one defined by the formula of the theorem, and the other one which is isomorphic to the loop Q. Both of them satisfy the assumptions of Corollary 6.6, and coincide on $(0,1)\cdot(0,1)$. They are thus identical, again by Corollary 6.6.

Note that up to now we have not proved that the loop is really conjugacy closed. However, that follows from Lemma 6.7. □

7. Conclusions

We have demonstrated that the structure of conjugacy closed loops is reflected substantially in their multiplication groups. We also used multiplication groups to describe the structure of conjugacy closed loops of order pq.

It might be worth repeating the stages involved in the procedure of determining the uniqueness of the pq-loops:

(1) Identify isomorphism types of $G \cong \operatorname{Mlt} Q$ and of $\operatorname{Inn} Q$.
(2) Gather enough partial information about the multiplication table of Q to be able to reconstruct the rest only from knowledge of one further product.
(3) By using automorphisms of G limit the choices for the result of such a product.
(4) For each of the choices compute the loop.

The last stage was not included in the paper for the sake of brevity, since the proof can rely on the uniqueness property, and so one can just verify that the found loop operation satisfies the assumptions of the earlier stages.

The above strategy might work in many further cases. However, the ongoing research on conjugacy closed loops indicates that more potent methods will be available soon. Using these methods one will be able to show the uniqueness and existence of many conjugacy closed loops in a more direct way. The approach via multiplication groups often requires a lot of laborous computations, but it can bring insight into loops where there seem to be no structural properties from which to start. When a class of loops is better understood, then the machinery of multiplication groups may prove to be too heavy. On the other hand, they can still generate interesting problems. One of them can be derived from the results of this paper: Let Q be a nonassociative conjugacy closed loop of order pq, and let $\mathcal{L}$ and $\mathcal{R}$ be the left and right multiplication group of Q, respectively. Suppose that there is another loop with the same underlying set and same left and right multiplication groups. From Theorem 6.9 and Lemma 6.7 we see that such a loop is isomorphic to Q. It seems desirable to find examples of other loops where $\mathcal{L}$ and $\mathcal{R}$ determine the structure of the loop uniquely up to isomorphism.

References

[1] A. S. Basarab, Klass LK-lup, *Matematicheskie issledovanija* **120** (1991), 3–7.

[2] V. D. Belousov, Osnovy teorii kvazigrupp i lup, Nauka, Moskva, 1967.

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

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

[5] A. Drápal, *Multiplication groups of finite loops that fix at most two points*, J. Algebra **235** (2001), 154–175.

[6] A. Drápal, *Orbits of inner mapping groups*, Monatsh. Math. **134** (2002), 191–206.

[7] 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.

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

[9] T. Kepka and M. Niemenmaa, *On loops with cyclic inner mapping groups*, Arch. Mat. (Basel) **60** (1993), 233–236.

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

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

[12] M. Niemenmaa and T.Kepka, *On multiplication group of loops*, J. Algebra **135** (1990), 112-122.

[13] Lev V. Sabinin, *Geometrija lupp*, Matematicheskie zametki **12** (1972), 605–616.

[14] Lev V. Sabinin, Smooth Quasigroups and Loops, Kluwer Academic Publishers, 1999.

[15] L. R. Soikis, O specialnych lupach, in *Voprosy teorii kvazigrupp i lup* (V. D. Belousov, ed.), Akademia Nauk Moldav. SSR, Kishinev, 1970, pp. 122-131.

Dept. of Mathematics, Charles University, Sokolovská 83, 186 75 Praha 8, Czech Rep.

E-mail address: `drapal@karlin.mff.cuni.cz`