G-Loops and Permutation Groups

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

August 26, 1999

Abstract

A G-loop is a loop which is isomorphic to all its loop isotopes. We apply some theorems about permutation groups to get information about G-loops. In particular, we study G-loops of order pq, where $p < q$ are primes and $p \nmid (q-1)$. In the case $p = 3$, the only G-loop of order $3q$ is the group of order $3q$. The notion "G-loop" splits naturally into "left G-loop" plus "right G-loop". There exist non-group right G-loops and left G-loops of order n iff n is composite and $n > 5$.

1 Introduction

An important concept in the theory of loops is that of *isotopy*, and a *G-loop* is a loop which is isomorphic to all its loop isotopes. All the relevant definitions are given in Section 2, which stresses the algebraic point of view. These concepts also occur naturally in geometry, since isotopic loops correspond to the same 3-net; see Bruck [2], and Barlotti and Strambach [1].

R. L. Wilson, Jr. [13] showed that there are no non-group G-loops of prime order. It has remained open whether there are such loops in all composite orders greater than 5, although many of these orders have been handled by Wilson [14] and Goodaire and Robinson [6]. Here, we provide some information about orders of the form pq, where $p < q$ are primes and $p \nmid (q-1)$; these orders are not covered by [14, 6]. In particular, we show (Theorem 3.11)

*The author was supported by NSF Grant DMS-9704520.

that there are no non-group G-loops of order $3q$ whenever $q > 3$ is prime and $3 \nmid (q-1)$.

By E. L. Wilson [12], a loop is a G-loop iff it is both a left G-loop and a right G-loop, where a right G-loop is one in which every element is the companion of a right pseudo-automorphism. Improving on [14], we show (Theorem 2.21) that there are no non-group right or left G-loops of prime order; however (Theorem 2.22), there are such loops in all composite orders greater than 5.

In pursuing this work, we have found a number of computer tools useful: OTTER [9] is used to derive equations from other equations. SEM [15] is used for constructing models of various algebraic theories, such as the G-loop in Table 1, Section 4. MAGMA [8] is used (among other things) for computations with permutation groups, and includes a database of transitive groups and primitive groups of small degrees.

2 Isotopy

Throughout this section, $(G, \cdot)$ always denotes a loop. Since loops are rather intractable, in comparison with groups, one attaches to G a number of permutation groups, and the study of these elucidates properties of G. See Dixon and Mortimer [4] for basic facts about permutation groups. We use the following standard notation:

Definition 2.1 *If G is any set, then $\mathcal{SYM}(G)$ is the group of all permutations of G. For a subgroup $\mathcal{X} \leq \mathcal{SYM}(G)$ and $c \in G$, the* stabilizer *of c is $\mathcal{X}_c = \{\alpha \in \mathcal{X} : c\alpha = c\}$. If $\alpha \in \mathcal{SYM}(G)$, then* $\mathrm{fix}(\alpha) = \{x \in G : x\alpha = x\}$. *$S_n = \mathcal{SYM}(\{1, 2, \ldots, n\})$.*

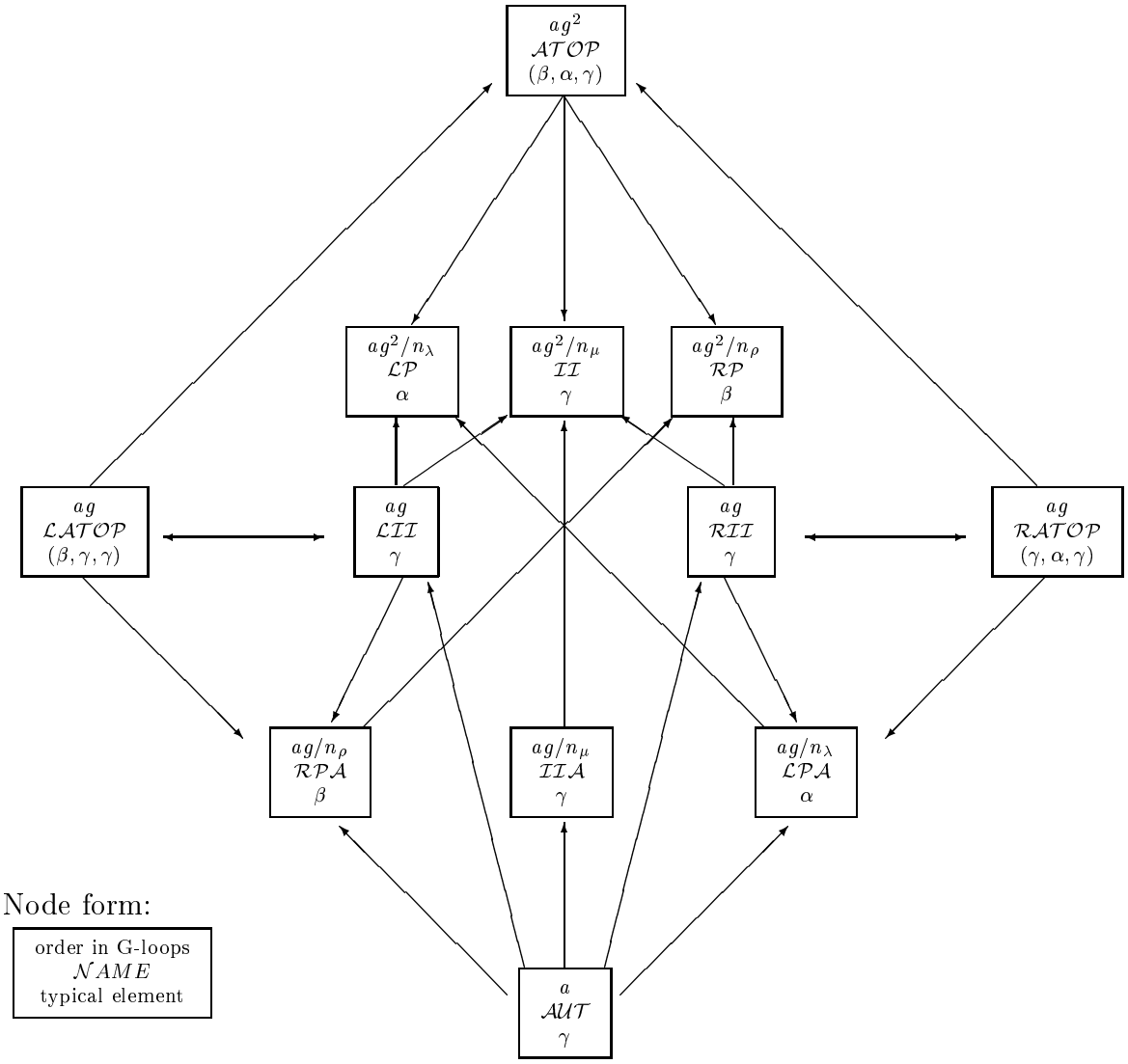
As with groups, the left and right actions of G on itself are important:

Definition 2.2 *Define, for each $a \in G$, L_a and R_a in $\mathcal{SYM}(G)$ by:*

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

In addition, the *autotopy group* (see [1, 2]), plays a much larger role in loop theory than in group theory. This, and some associated groups and the key maps between them, are displayed in Figure 1. This figure also displays the order of each group in the case that G is a G-loop. These groups all occur somewhere in the literature, although not all together in such a diagram, and not with uniform names, so we now present all the relevant definitions; see [7] for further discussion.

Figure 1: The Basic Permutation Groups



$g = |G| \quad a = |\mathcal{AUT}| \quad n_\mu = |N_\mu| \quad n_\rho = |N_\rho| \quad n_\lambda = |N_\lambda|$

Upward sloping arrows are injections.
Downward sloping arrows are surjections.
Horizontal arrows are bijections.

Definition 2.3 *The* autotopy group, $\mathcal{ATOP}(G,\cdot)$, *is the set of all triples* (β,α,γ) *in* $(\mathcal{SYM}(G))^3$ *such that*

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

Then

$$\begin{aligned}\mathcal{LATOP}(G,\cdot) &= \{(\beta,\gamma,\gamma):(\beta,\gamma,\gamma)\in\mathcal{ATOP}(G)\}\\ \mathcal{RATOP}(G,\cdot) &= \{(\gamma,\alpha,\gamma):(\gamma,\alpha,\gamma)\in\mathcal{ATOP}(G)\}\end{aligned}$$

Observe that $\mathcal{ATOP}(G)$ is a subgroup of $(\mathcal{SYM}(G))^3$, and that both $\mathcal{LATOP}(G)$ and $\mathcal{RATOP}(G)$ are subgroups of $\mathcal{ATOP}(G)$. Furthermore, the L_a and R_a are related to the autotopy group by:

Lemma 2.4 *Suppose that* $(\beta,\alpha,\gamma)\in\mathcal{ATOP}(G,\cdot)$. *Let*

$$b=1\beta^{-1}\qquad a=1\alpha^{-1}\qquad c=1\alpha\qquad d=1\beta\quad .$$

Then

$\beta=R_a\gamma$	$\alpha=L_b\gamma$	$(xa)\gamma\cdot(by)\gamma=(xy)\gamma$
$\gamma=\beta R_c$	$\alpha=L_b\beta R_c$	$x\beta\cdot((by)\beta\cdot c)=(xy)\beta\cdot c$
$\gamma=\alpha L_d$	$\beta=R_a\alpha L_d$	$(d\cdot(xa)\alpha)\cdot y\alpha=d\cdot(xy)\alpha$

for all $x,y\in G$.

Equations of this sort, for a *single* permutation, are more valuable than facts about triples, and we get important subgroups of $\mathcal{SYM}(G)$ by projecting out triples:

Definition 2.5 *Define* $\Pi_\lambda,\Pi_\rho,\Pi_\mu:(\mathcal{SYM}(G))^3\to\mathcal{SYM}(G)$ *by:*

$$\Pi_\lambda(\beta,\alpha,\gamma)=\beta\qquad\Pi_\rho(\beta,\alpha,\gamma)=\alpha\qquad\Pi_\mu(\beta,\alpha,\gamma)=\gamma$$

Definition 2.6

$\mathcal{II}(G)=\Pi_\mu(\mathcal{ATOP}(G))$
$\mathcal{RP}(G)=\Pi_\lambda(\mathcal{ATOP}(G))\qquad\mathcal{LP}(G)=\Pi_\rho(\mathcal{ATOP}(G))$
$\mathcal{RII}(G)=\Pi_\mu(\mathcal{RATOP}(G))=\Pi_\lambda(\mathcal{RATOP}(G))$
$\mathcal{LII}(G)=\Pi_\mu(\mathcal{LATOP}(G))=\Pi_\rho(\mathcal{LATOP}(G))$
$\mathcal{RPA}(G)=\Pi_\lambda(\mathcal{LATOP}(G))\qquad\mathcal{LPA}(G)=\Pi_\rho(\mathcal{RATOP}(G))$
$\mathcal{AUT}(G)=\Pi_\mu(\mathcal{RATOP}(G)\cap LATOP(G))$
$\mathcal{IIA}(G)=(\mathcal{II}(G))_1$

The groups $\mathcal{II}, \mathcal{RP}, \mathcal{LP}, \mathcal{RII}, \mathcal{LII}$ are important because, for G-loops, they act transitively on G; when G is a group, these five are the same, and are known as the holomorph of G. $\mathcal{RPA}, \mathcal{LPA}, \mathcal{AUT}, \mathcal{IIA}$ occur naturally as stabilizers of 1:

Lemma 2.7 $\mathcal{RPA}(G) = (\mathcal{RP}(G))_1$. $\mathcal{LPA}(G) = (\mathcal{LP}(G))_1$. $\mathcal{AUT}(G) = (\mathcal{LII}(G))_1 = (\mathcal{RII}(G))_1$.

In terms of equations, we have:

$$\begin{aligned}
\gamma \in \mathcal{II}(G) &\iff \exists a,b \in G\, \forall xy \in G[(xa)\gamma \cdot (by)\gamma = (xy)\gamma] && (1)\\
\gamma \in \mathcal{RII}(G) &\iff \exists b \in G\, \forall xy \in G[x\gamma \cdot (by)\gamma = (xy)\gamma] && (2)\\
\gamma \in \mathcal{LII}(G) &\iff \exists a \in G\, \forall xy \in G[(xa)\gamma \cdot y\gamma = (xy)\gamma] && (3)\\
\gamma \in \mathcal{AUT}(G) &\iff \forall xy \in G[x\gamma \cdot y\gamma = (xy)\gamma] && (4)\\
\beta \in \mathcal{RPA}(G) &\iff \exists c \in G\, \forall xy \in G[x\beta \cdot (y\beta \cdot c) = (xy)\beta \cdot c] && (5)\\
\alpha \in \mathcal{LPA}(G) &\iff \exists d \in G\, \forall xy \in G[(d \cdot x\alpha) \cdot y\alpha = d \cdot (xy)\alpha] && (6)\\
\beta \in \mathcal{RP}(G) &\iff \exists b,c \in G\, \forall xy \in G[x\beta \cdot ((by)\beta \cdot c) = (xy)\beta \cdot c] && (7)\\
\alpha \in \mathcal{LP}(G) &\iff \exists a,d \in G\, \forall xy \in G[(d \cdot (xa)\alpha) \cdot y\alpha = d \cdot (xy)\alpha] && (8)
\end{aligned}$$

$\mathcal{AUT}(G)$ is the group of automorphisms of (G). Elements of $\mathcal{RPA}$ and $\mathcal{LPA}$ are the right and left *pseudo-automorphisms* of G; the c in (5) and the d in (6) are called *companions* of β and α, respectively. In (2), $b = 1\gamma^{-1}$, and in (3), $a = 1\gamma^{-1}$. Drisko [5] calls the elements of $\mathcal{IIA}(G)$ the *middle* pseudo-automorphisms; for $\gamma \in \mathcal{IIA}(G)$, we have (1) with $ba = 1$.

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

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

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

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

Elements of $\mathcal{IIA}, \mathcal{RPA}, \mathcal{LPA}$ need not be automorphisms of G, but they define automorphisms of the various nuclei:

Lemma 2.10

1. *For* $\gamma \in \mathcal{II}\mathcal{A}(G)$*:*
   a. *If either* $x \in N_\lambda$ *or* $y \in N_\rho$*, then* $x\gamma \cdot y\gamma = (xy)\gamma$.
   b. $\gamma \restriction N_\lambda \in \mathcal{AUT}(N_\lambda)$.
   c. $\gamma \restriction N_\rho \in \mathcal{AUT}(N_\rho)$.
2. *For* $\beta \in \mathcal{RPA}(G)$*:*
   a. *If either* $x\beta \in N_\lambda$ *or* $y\beta \in N_\mu$*, then* $x\beta \cdot y\beta = (xy)\beta$.
   b. $\beta \restriction N_\lambda \in \mathcal{AUT}(N_\lambda)$.
   c. $\beta \restriction N_\mu \in \mathcal{AUT}(N_\mu)$.
3. *For* $\alpha \in \mathcal{LPA}(G)$*:*
   a. *If either* $y\alpha \in N_\rho$ *or* $x\alpha \in N_\mu$*. then* $x\alpha \cdot y\alpha = (xy)\alpha$.
   b. $\alpha \restriction N_\rho \in \mathcal{AUT}(N_\rho)$.
   c. $\alpha \restriction N_\mu \in \mathcal{AUT}(N_\mu)$.

See [7] for a proof of (1). (2) and (3) are similar.

Corollary 2.11 *If* G *is finite:*

1. *For* $\gamma \in \mathcal{II}(G)$*:*
   $N_\lambda \subseteq \mathrm{fix}(\gamma) \Rightarrow |N_\lambda| \mid |\mathrm{fix}(\gamma)|$
   $N_\rho \subseteq \mathrm{fix}(\gamma) \Rightarrow |N_\rho| \mid |\mathrm{fix}(\gamma)|$
2. *For* $\beta \in \mathcal{RP}(G)$*:*
   $N_\mu \subseteq \mathrm{fix}(\beta) \Rightarrow |N_\mu| \mid |\mathrm{fix}(\beta)|$
   $N_\lambda \subseteq \mathrm{fix}(\beta) \Rightarrow |N_\lambda| \mid |\mathrm{fix}(\beta)|$
3. *For* $\alpha \in \mathcal{LP}(G)$*:*
   $N_\mu \subseteq \mathrm{fix}(\alpha) \Rightarrow |N_\mu| \mid |\mathrm{fix}(\alpha)|$
   $N_\rho \subseteq \mathrm{fix}(\alpha) \Rightarrow |N_\rho| \mid |\mathrm{fix}(\alpha)|$

Proof. For (1): assume that $N_\lambda \subseteq \mathrm{fix}(\gamma)$. Then $1 \in \mathrm{fix}(\gamma)$, so $\gamma \in \mathcal{II}\mathcal{A}$. By Lemma 2.10, we have $u \cdot v\gamma = (uv)\gamma$ whenever $u \in N_\lambda$, so that $v \in \mathrm{fix}(\gamma) \Rightarrow N_\lambda \cdot v \subseteq \mathrm{fix}(\gamma)$. Since distinct right cosets of N_λ are disjoint, we have $|N_\lambda| \mid |\mathrm{fix}(\gamma)|$. □

We remark that the apparent symmetry among N_λ, N_ρ, N_μ in statements such as 2.10 and 2.11 is related to the existence of auxiliary loop operations. For example, if $x \circ y = y \cdot x$, then $N_\lambda(G,\circ) = N_\rho(G,\cdot)$, $N_\rho(G,\circ) = N_\lambda(G,\cdot)$, and $N_\mu(G,\circ) = N_\mu(G,\cdot)$. If $x \star y = x/(y\backslash 1)$, then $N_\lambda(G,\star) = N_\lambda(G,\cdot)$, $N_\rho(G,\star) = N_\mu(G,\cdot)$, and $N_\mu(G,\star) = N_\rho(G,\cdot)$. This part of the exposition might be more transparent if done geometrically, from the point of view of 3-nets, as in [1].

Using Lemma 2.9, we can embed the three nuclei into the autotopy group, and then identify the kernels of the surjections shown in Figure 1:

Definition 2.12 *Define* $\Phi_\lambda, \Phi_\rho, \Phi_\mu : G \to (\mathcal{SYM}(G))^3$ *by:*

$$\begin{aligned} \Phi_\lambda(a) &= (L_a^{-1}, I, L_a^{-1}) \\ \Phi_\rho(a) &= (I, R_a, R_a) \\ \Phi_\mu(a) &= (R_a, L_a^{-1}, I) \end{aligned}$$

Lemma 2.13 *The maps* $\Phi_\lambda \restriction N_\lambda$, $\Phi_\rho \restriction N_\rho$, $\Phi_\mu \restriction N_\mu$ *are isomorphic embeddings from* N_λ, N_ρ, N_μ, *respectively, into* $(\mathcal{ATOP}(G))^3$.

Lemma 2.14

$\ker(\Pi_\lambda : \mathcal{ATOP} \to \mathcal{RP}) = \Phi_\rho(N_\rho) = \ker(\Pi_\lambda : \mathcal{LATOP} \to \mathcal{RPA})$
$\ker(\Pi_\rho : \mathcal{ATOP} \to \mathcal{LP}) = \Phi_\lambda(N_\lambda) = \ker(\Pi_\rho : \mathcal{RATOP} \to \mathcal{LPA})$
$\ker(\Pi_\mu : \mathcal{ATOP} \to \mathcal{II}) = \Phi_\mu(N_\mu)$
$\ker(\Pi_\mu : \mathcal{LATOP} \to \mathcal{LII}) = \{(I, I, I)\} = \ker(\Pi_\mu : \mathcal{RATOP} \to \mathcal{RII})$

We now turn to G-loops:

Definition 2.15

G *is a* G-loop *iff* $\forall a, b \in G\, \exists \alpha\, [(R_a\alpha, L_b\alpha, \alpha) \in \mathcal{ATOP}(G)]$.
G *is a* right G-loop *iff* $\forall a \in G\, \exists \alpha\, [(R_a\alpha, \alpha, \alpha) \in \mathcal{ATOP}(G)]$.
G *is a* left G-loop *iff* $\forall b \in G\, \exists \alpha\, [(\alpha, L_b\alpha, \alpha) \in \mathcal{ATOP}(G)]$.

Lemma 2.16 *G is a right G-loop iff $\mathcal{LII}(G)$ acts transitively on G, and G is a left G-loop iff $\mathcal{RII}(G)$ acts transitively on G.*

Another equivalent to right G-loop is that every element of the loop is the companion of some right pseudo-automorphism; likewise for left G-loops.

Lemma 2.17 *A loop is a G-loop iff it is both a left G-loop and a right G-loop.*

The non-obvious direction of this lemma is due to E. L. Wilson [12]; see also [7] for a proof, and for further references to the literature. Bryant and Schneider [3] called $\mathcal{II}(G)$ the *group* of G. We use the term $\mathcal{II}(G)$ because its elements are the Isomorphisms onto principal loop Isotopes, and a G-loop is a loop which is isomorphic to all its loop isotopes. In [7], it is shown that the G-loops do not form an equational variety, so that we cannot expect in general that the α in Definition 2.15 be uniformly definable by some expression in R_a, L_a, R_b, L_b. The emphasis in [7] is on the *conjugacy closed (CC) loops*, introduced by Goodaire and Robinson [6]; these form an equational variety which is a sub-class of the G-loops.

Definition 2.18 *G is* right CC *iff $L_a \in \mathcal{LII}(G)$ for all $a \in G$. G is* left CC *iff $R_b \in \mathcal{RII}(G)$ for all $b \in G$. G is* conjugacy closed *iff G is both left CC and right CC.*

It is clear by Lemma 2.16 that right CC implies right G and left CC implies left G. It is easy to express right CC and left CC as equations. By [6], $N(G) = N_\lambda(G) = N_\mu(G) = N_\rho(G)$ for CC-loops; see [7, 10] for further discussion. Furthermore, by [6], in CC-loops, $R_a R_b R_{ab}^{-1} \in \mathcal{AUT}(G)$ and $L_a L_b L_{ba}^{-1} \in \mathcal{AUT}(G)$ (this is immediate by Lemma 2.7 and Definition 2.18); this provides some non-trivial automorphisms for G, since a loop in which $R_a R_b R_{ab}^{-1} = I$ for all a, b is a group. However, there is a G-loop of order 8 (see Table 1, Section 4) whose automorphism group is trivial. This is the smallest possible such order, since G-loops of prime order are groups (by [13]), and Bryant and Schneider [3] computed all the 109 loops of order 6, together with their isotopy classes, finding only three G-loops: the two groups, plus one CC-loop.

The next two lemmas justify the orders displayed in Figure 1.

Lemma 2.19 *Suppose that G is a finite right G-loop. Then*

$$\begin{aligned} |\mathcal{LII}(G)| &= |\mathcal{AUT}(G)| \cdot |G| && (1)\\ |\mathcal{LATOP}(G)| &= |\mathcal{AUT}(G)| \cdot |G| && (2)\\ |\mathcal{RPA}(G)| &= |\mathcal{AUT}(G)| \cdot |G| \;/\; |N\rho| && (3) \end{aligned}$$

Proof. (1) is immediate from 2.7 and the transitivity of $LII(G)$. Then, (2) and (3) follow by Lemma 2.14. □

Of course, the mirror of this argument justifies the orders for $\mathcal{RII}(G)$, $\mathcal{RATOP}(G)$, and $\mathcal{LPA}(G)$ in Figure 1 for left G-loops.

Lemma 2.20 *Suppose that G is a finite G-loop. Then all the orders shown in Figure 1 are correct.*

Proof. Let $\mathcal{L} = \mathcal{LATOP} \cap \mathcal{RATOP}$; so $\mathcal{L}$ is the set of triples (γ, γ, γ) such that $\gamma \in \mathcal{AUT}$. Then $\mathcal{L} \leq \mathcal{ATOP}$ and $|\mathcal{L}| = |\mathcal{AUT}|$. Now, as in Definition 2.15, suppose we have $\psi = (R_a\gamma, L_b\gamma, \gamma) \in \mathcal{ATOP}$ and also $\psi' = (R_a\gamma', L_b\gamma', \gamma') \in \mathcal{ATOP}$. Then $\psi'\psi^{-1} \in \mathcal{L}$, so that ψ and ψ' are in the same right coset of $\mathcal{L}$. If follows from this that $[\mathcal{ATOP} : \mathcal{L}] = |G|^2$. The rest follows by Lemma 2.14. □

The equation $|\mathcal{II}(G)| = |\mathcal{AUT}(G)| \cdot |G|^2 \;/\; |N_\mu|$ is due to Bryant and Schneider [3]. R. L. Wilson, Jr. [13] used this to conclude that if $|G| = p$, a

prime, then G must be a group: if not, then $|N_\mu| = 1$, so that $p^2 \mid |\mathcal{II}|$, which is impossible, since $\mathcal{II} \leq \mathcal{SYM}(G)$ and $p^2 \nmid p!$. In fact:

Theorem 2.21 *If G is a right G-loop or a left G-loop and $p = |G|$ is prime, then G is a group.*

Proof. Assume that G is a right G-loop. $\mathcal{RPA} \leq \mathcal{SYM}(G\backslash\{1\})$, and hence $p \nmid |\mathcal{RPA}|$. Then, by Lemma 2.19.3, $p \mid |N_\rho|$, so that $N_\rho = G$. □

This is the only restriction on the orders of non-group right and left G-loops, other than the obvious remark that every loop of order less than 5 is a group:

Theorem 2.22 *There are non-group right CC and left CC loops of all composite orders greater than* 5.

Proof. Since there are in fact non-group CC-loops of all even orders greater than 5 (see Goodaire and Robinson [6] and Wilson [14]), it is sufficient to produce a right CC-loop of order mn whenever $m, n \geq 3$. We shall produce such a loop operation on $\mathbb{Z}_m \times \mathbb{Z}_n$. In the following, r, s, t denote elements of the cyclic group $\mathbb{Z}_m$, with addition being understood to be modulo m, and i, j, k denote elements of $\mathbb{Z}_n$.

Fix a map $\epsilon : \mathbb{Z}_m \to \mathbb{Z}_n$, and define

$$(r, i) \cdot (s, j) = (r + s,\ i + \epsilon(r) \cdot j) \quad .$$

We shall show that for an appropriate choice of ϵ, this product satisfies the theorem.

First, assume $1 \leq \epsilon(r) < r$ and $\epsilon(r)$ is relatively prime to n, so that it is a unit in the ring $\mathbb{Z}_n$. This is sufficient to ensure that $\cdot$ is a quasigroup operation. Next, assume that $\epsilon(0) = 1$, so that $(0, 0)$ is the identity element.

Now, right CC is equivalent to the equation $z(yx) = ((zy)/z)(zx)$ (see [6]). This equation holds because if we set $x = (r, i)$, $y = (s, j)$, $z = (t, k)$, then we compute both sides of the equation to be $(t + s + r, k + \epsilon(t)j + \epsilon(s)\epsilon(t)i)$.

Finally, we need associativity to fail. With the same x, y, z, we see that $(xy)z \neq x(yz)$ whenever $\epsilon(r+s)k \neq \epsilon(r)\epsilon(s)k$. Since $m, n \neq 2$, let $\epsilon(1) = 1$ and $\epsilon(-1) = -1$, so that $\epsilon(1 + -1) = 1 \neq -1 = \epsilon(1)\epsilon(-1)$. Then $(xy)z \neq x(yz)$ whenever $r = 1, s = -1, k = 1$. □

The situation for G-loops of composite order is more complicated, as we see in the next section.

3 Order pq

Here, we consider non-group G-loops of order pq, where p, q are distinct primes, $p \nmid (q-1)$, and $q \nmid (p-1)$. We do not know if there are any such loops, but we can prove enough lemmas about them to prove that there are none in the case $p = 3$. For simplicity of exposition, we do not assume $p < q$, since a number of arguments are symmetric in p, q.

Lemma 3.1 *Suppose that G is any non-group loop of order pq, where p, q are distinct primes and $q \nmid (p-1)$:*

1. *If $q \mid \mathcal{III}\mathcal{A}(G)$, then $|N_\lambda|$ is 1 or q and $|N_\rho|$ is 1 or q.*
2. *If $q \mid \mathcal{RPA}(G)$, then $|N_\lambda|$ is 1 or q and $|N_\mu|$ is 1 or q.*
3. *If $q \mid \mathcal{LPA}(G)$, then $|N_\rho|$ is 1 or q and $|N_\mu|$ is 1 or q.*

Proof. For (1): choose $\gamma \in \mathcal{III}\mathcal{A}$ such that γ has order q; then $q \mid |\mathrm{fix}(\gamma)|$. Now, assume that $|N_\lambda|$ is neither 1 nor q; since G is not a group, we have $|N_\lambda| = p$, so that $N_\lambda \cong \mathbb{Z}_q$. Since γ is an automorphism of N_λ (by Lemma 2.10) and $q \nmid (p-1)$, we have $N_\lambda \subseteq \mathrm{fix}(\gamma)$, so that $p \mid |\mathrm{fix}(\gamma)|$ (by Corollary 2.11), which is impossible, since $\gamma \neq I$. □

Lemma 3.2 *Suppose that G is a non-group G-loop of order pq, where p, q are distinct primes and $q \nmid (p-1)$. Then either $|N_\mu|, |N_\rho|, |N_\lambda|$ are all in $\{1, q\}$, or one of these three numbers is p and the other two are q.*

Proof. Say $|N_\mu| \notin \{1, q\}$; then $|N_\mu| = p$, so that $q \mid \mathcal{III}\mathcal{A}(G)$ because $|\mathcal{III}\mathcal{A}| = |G| \cdot |\mathcal{AUT}|/|N_\mu|$. Then Lemma 3.1.1 implies that $|N_\rho|, |N_\lambda| \in \{1, q\}$. But if $|N_\rho|$ or $|N_\lambda|$ were 1 rather than q, a similar argument, using $|\mathcal{RPA}|$ or $|\mathcal{LPA}|$, respectively, would contradict 3.1.2 or 3.1.3. □

In the case where $N_\mu = N_\rho = N_\lambda = N$ (as we have with CC-loops), this lemma says that $|N|$ is either 1 or q. If $q < p$ and $q \nmid (p-1)$, then there are no non-group CC-loops of order pq (see [7]), whereas if $q > p$ (so the $q \nmid (p-1)$ is trivial), then there is a CC-loop of order pq whenever $p \mid (q-1)$ (see Goodaire and Robinson [6]; their loop had $|N| = q$). It is not in general true that the three nuclei of a G-loop are the same; see Section 4.

Corollary 3.3 *Suppose that G is a non-group G-loop of order pq, where p, q are distinct primes $q \nmid (p-1)$, and $p \nmid (q-1)$. Then $|N_\mu| = |N_\rho| = |N_\lambda| = 1$.*

We insert here a few simple facts about permutation groups:

Lemma 3.4 *Suppose that p, q are distinct primes and $q \nmid (p-1)$. Suppose that $\mathcal{X}$ is a transitive subgroup of S_{pq} and $p^2 \nmid |\mathcal{X}|$. Suppose also that $\mathcal{X}$ has only one Sylow p-subgroup. Then $\mathcal{X}$ contains a pq-cycle.*

Proof. Let $\mathcal{P} = \langle \alpha \rangle$ be a Sylow p-subgroup and let β have order q. Note that $\mathrm{fix}(\alpha) = \emptyset$, since $a \in \mathrm{fix}(\alpha)$ would imply that $\mathcal{P} \leq \mathcal{X}_a$, whereas $p \nmid |\mathcal{X}_a|$. Thus, α is a product of q p-cycles. Since $\mathcal{P}$ is unique, $\beta^{-1}\mathcal{P}\beta = \mathcal{P}$, and hence, by $q \nmid (p-1)$, $\beta\alpha = \alpha\beta$. It follows that $\alpha\beta$ is a pq-cycle. □

Corollary 3.5 *Suppose that p, q are distinct primes, $q \nmid (p-1)$ and $p \nmid (q-1)$. Suppose that $\mathcal{X}$ is a transitive subgroup of S_{pq}, and $|\mathcal{X}|$ is either pq or $2pq$. Then $\mathcal{X}$ contains a pq-cycle.*

Proof. A simple counting argument shows that $\mathcal{X}$ must have either a unique Sylow p-subgroup or a unique Sylow q-subgroup, so apply Lemma 3.4. □

Lemma 3.6 *Suppose that p, q are primes, $p < q$, and $p \nmid (q-1)$. Suppose that $\mathcal{X}$ is a transitive subgroup of S_{pq}, with $q^2 \mid |\mathcal{X}|$ and $q^3 \nmid |\mathcal{X}|$. Then $\mathcal{X}$ cannot contain a pq-cycle.*

Proof. Suppose that $\mathcal{X}$ does contain a pq-cycle; equivalently, there are $\alpha, \beta \in \mathcal{X}$, where α is a product of q p-cycles, β is a product of q p-cycles, and $\beta\alpha = \alpha\beta$. We may assume that β is $\sigma_0 \cdots \sigma_{p-1}$, where each σ_i is a q-cycle, and $\alpha^{-1}\sigma_i\alpha = \sigma_{(i+1) \bmod p}$.

Now, let $\mathcal{Q}$ be a Sylow q-subgroup of $\mathcal{X}$ with $\beta \in \mathcal{Q}$. Then $\mathcal{Q} \cong \mathbb{Z}_q \times \mathbb{Z}_q$. Say $\mathcal{Q} = \langle \beta, \delta \rangle$. Since $\delta^{-1}\beta\delta = \beta$, each $\delta^{-1}\sigma_i\delta$ must be σ_j for some j. But since $q > p$, there is no non-trivial permutation of $\{\sigma_0, \ldots, \sigma_{p-1}\}$ of order q, so in fact each $\delta^{-1}\sigma_i\delta = \sigma_i$. It follows that δ is of the form $\sigma_0^{\ell_0} \cdots \sigma_{p-1}^{\ell_{p-1}}$. Then, replacing δ by another generator, we may assume that $\ell_0 = 0$, so that $\delta = \sigma_1^{\ell_1}\sigma_2^{\ell_2} \cdots \sigma_{p-1}^{\ell_{p-1}}$. Let $\theta = \alpha\delta\alpha^{-1} = \sigma_0^{\ell_1}\sigma_1^{\ell_2} \cdots \sigma_{p-2}^{\ell_{p-1}}$. This is another element of order q which commutes with β, δ, so that $\langle \beta, \delta, \theta \rangle$ would have order q^3 (which is impossible) unless $\theta \in \langle \beta, \delta \rangle$

Since $\theta \in \langle \beta, \delta \rangle$, we have, over the field $\mathbb{Z}_q$, three linearly dependent vectors:

$$\begin{aligned} \vec{u} &= (1, 1, 1, \quad \cdots \quad, 1, 1) \\ \vec{v} &= (0, \ell_1, \ell_2, \quad \cdots \quad, \ell_{p-2}, \ell_{p-1}) \\ \vec{w} &= (\ell_1, \ell_2, \ell_3 \quad \cdots \quad, \ell_{p-1}, 0) \end{aligned}$$

Say (over $\mathbb{Z}_q$),we have $\vec{w} = x\vec{u} + y\vec{v}$. If $\ell_1 = 0$, we easily derive $\ell_2 = \ell_3 = \cdots = 0$, which is impossible, so, multiplying by a scalar, we might as well assume that $\ell_1 = 1$, and hence $x = 1$, so that $\vec{w} = \vec{u} + y\vec{v}$. Then $\ell_2 = 1 + y$, and then $\ell_3 = 1 + y\ell_2 = 1 + y + y^2$, and so forth. In particular, $\ell_{p-1} = 1 + y\ell_{p-2} = 1 + y + y^2 + \cdots y^{p-2}$, and then $0 = 1 + y\ell_{p-1} = 1 + y + y^2 + \cdots y^{p-1}$, and hence $y^p = 1$. Since also $y^{q-1} = 1$ (in $\mathbb{Z}_q$) and $p \nmid (q-1)$, we have $y = 1$, contradicting $1 + y + y^2 + \cdots y^{p-1} = 0$. □

Theorem 3.7 *Suppose that G is a G-loop of order pq, where p, q are primes, $p < q$, and $p \nmid (q-1)$. Then $|\mathcal{AUT}(G)| \geq 3$; equivalently, $|\mathcal{LII}| = |\mathcal{RII}| \geq 3pq$.*

Proof. Suppose that $a = |\mathcal{AUT}(G)|$ is either 1 or 2. Since $|\mathcal{LII}| = apq$, Corollary 3.5 implies that $\mathcal{LII}$ contains a pq-cycle. However, since $|N_\mu| = 1$ by Corollary 3.3, $|\mathcal{II}| = ap^2q^2$, so that by Lemma 3.6, $\mathcal{II}$ cannot contain a pq-cycle, which is a contradiction, since $\mathcal{LII} \leq \mathcal{II}$. □

It is actually not hard to improve this to $|\mathcal{AUT}(G)| \geq 6$, using the Sylow Theorems plus the fact that the case $p = 3$ will be excluded by Theorem 3.11. However, there seems to be little point in pursuing a detailed study of a class of loops which might very well be empty.

We proceed to show that $p = 3$ is impossible. First note the following fact, which is easily proved by elementary combinatorics:

Lemma 3.8 *If G is a finite loop and H is a proper subloop of G, then $|H| \leq \frac{1}{2}|G|$.*

This lemma, plus the fact that $\mathrm{fix}(\alpha)$ is a subloop whenever α is an automorphism, can be used to limit $\mathcal{AUT}(G)$:

Lemma 3.9 *Suppose that G is a non-group G-loop of order $3q$, where q is a prime, $3 < q$, and $3 \nmid (q-1)$. Then $q \nmid |\mathcal{AUT}(G)|$.*

Proof. Suppose that $q \mid |\mathcal{AUT}|$. We shall derive a contradiction. First note that $q^2 \nmid |\mathcal{AUT}|$ because $|\mathcal{II}| = 9q^2|\mathcal{AUT}|$ since $|N_\mu| = 1$ by (Corollary 3.3), and $|\mathcal{II}| \mid (3q)!$ whereas $q^4 \nmid (3q)!$. Likewise, $q^2 \mid |\mathcal{LII}|$ and $q^3 \nmid |\mathcal{LII}|$. We can now describe the Sylow q-subgroups of $\mathcal{AUT}$ and $\mathcal{LII}$.

Consider any $\gamma \in \mathcal{LII}$ of order q. γ cannot be a single q-cycle: If it were, then let $\gamma' \in (\mathcal{LII})_1 = \mathcal{AUT}$ be conjugate to γ. Then $\mathrm{fix}(\gamma')$ is a subloop of order $2q$, contradicting Lemma 3.8. Hence, γ is a product of 2 or 3 q-cycles.

Now, fix an $\alpha \in \mathcal{AUT}$ of order q. Then we can partition G into disjoint sets A, B, C, where $1 \in A = \mathrm{fix}(\alpha)$, and $\alpha = \sigma\tau^{-1}$, where σ, τ are q-cycles acting on B, C, respectively. A is a subloop of G, and $|A| = |B| = |C| = q$.

Next let $\mathcal{Q}$ a Sylow q-subgroup of $\mathcal{LII}$ containing α. Then $\mathcal{Q} \cong \mathbb{Z}_q \times \mathbb{Z}_q$ and no element of $\mathcal{Q}$ can be a single q-cycle. It follows that one can find a q-cycle λ acting on A such that $\mathcal{Q} = \{\lambda^i\sigma^j\tau^k : i + j + k \equiv 0 \bmod q\}$.

Now, $A = \mathrm{fix}(\alpha)$ is a subloop of G and $\lambda \in \mathcal{LII}(A)$, so that A is a right G-loop, and hence $A \cong \mathbb{Z}_q$ by Theorem 2.21. Furthermore, A is the *only* subloop of G isomorphic to $\mathbb{Z}_q$. To see this, let U be the union of all such subloops. Then $|U| = 1 + \ell(q-1)$ for some $\ell \leq 3$, since two such subloops must meet in $\{1\}$. However, by applying the automorphism α, we see that $U \cap (B \cup C)$ must be either B, C, $B \cup C$, or $\emptyset$, so $q \mid |U|$. Hence, $\ell = 1$ and $U \cap (B \cup C) = \emptyset$.

It follows now that every automorphism of G takes A to A, and hence every automorphism of order q is the identity on A.

Next, note that $\mathcal{Q}$ is the *only* Sylow q-subgroup of $\mathcal{LII}$. To see this, suppose we had another one, $\widehat{\mathcal{Q}} = \{\hat{\lambda}^i\hat{\sigma}^j\hat{\tau}^k : i+j+k \equiv 0 \bmod q\}$, where $\hat{\lambda}, \hat{\sigma}, \hat{\tau}$ are q-cycles acting on the disjoint sets $\hat{A}, \hat{B}, \hat{C}$ respectively, with $1 \in \hat{A}$. Since the automorphism $\hat{\sigma}\hat{\tau}^{-1}$ is the identity on A, we must have $\hat{A} = A$. We may assume (switching $\hat{B}, \hat{C}$ if necessary) that $|B \cap \hat{B}| \geq 2$, so fix distinct $b_1, b_2 \in B \cap \hat{B}$. Say $b_2 = b_1\sigma^r$ and $b_2 = b_1\hat{\sigma}^s$. Now consider the automorphism $\gamma = \sigma^r\tau^{-r}\hat{\sigma}^{-s}\hat{\tau}^s$. Then $A \cup \{b_1\} \subseteq \mathrm{fix}(\gamma) \subseteq G$, so that one of the pairs $(A, \mathrm{fix}(\gamma))$ or $(\mathrm{fix}(\gamma), G)$ will contradict Lemma 3.8 unless $\mathrm{fix}(\gamma) = G$. Hence, $\hat{\sigma}^s\hat{\tau}^{-s} = \sigma^r\tau^{-r} \in \mathcal{Q}$, so that $\hat{A} = A$, $\hat{B} = B$, $\hat{\sigma} \in \langle\sigma\rangle$, and $\hat{\tau} \in \langle\tau\rangle$. Furthermore, $\hat{\lambda} \in \mathcal{LII}(A)$, so that $\hat{\lambda} \in \langle\lambda\rangle$, since $\mathcal{LII}(\mathbb{Z}_q)$ contains just one q-subgroup (the translations). It follows that $\langle\mathcal{Q} \cup \widehat{\mathcal{Q}}\rangle$ is an abelian q-group, which is impossible.

Now, fix $\delta \in \mathcal{LII}$ of order 3, and let $\mathcal{M} = \langle\mathcal{Q}, \delta\rangle$. Then $|\mathcal{M}| = 3q^2$ (since $\mathcal{Q} \triangleleft \mathcal{LII}$). Note also that $\mathcal{M}$ is non-abelian, since no product of 3-cycles could commute with both $\sigma\tau^{-1}$ and $\lambda\tau^{-1}$.

In fact, there is an $\mathcal{M} < S_{3q}$ with this description. However, our $\mathcal{M}$ is isomorphic to an $\mathcal{N} < S_{3q-1} \cong \mathcal{SYM}(G\backslash\{1\})$, since $\mathcal{LACOP} \cong \mathcal{LII}$ (via Π_μ) and $\mathcal{LACOP} \cong \mathcal{RPA}$ (via Π_λ, since $|N_\rho| = 1$). This yields a contradiction as follows: Let $\mathcal{Q}'$ be the (unique) Sylow subgroup of $\mathcal{N}$ and let δ' be an element of $\mathcal{N}$ of order 3. Then $\mathcal{Q}' \cong \mathbb{Z}_q \times \mathbb{Z}_q$ must be generated by two disjoint q-cycles. Conjugation by δ' maps $\mathcal{Q}'$ to $\mathcal{Q}'$, and this cannot happen unless this conjugation is the identity, which is impossible because $\mathcal{N}$ is non-abelian. □

Lemma 3.10 *Suppose that G is a non-group G-loop of order pq, where $p < q$ are primes and $p \nmid (q-1)$. Then each of the groups $\mathcal{LP}(G), \mathcal{II}(G), \mathcal{RP}(G)$ is non-primitive, and leaves invariant some block system Σ consisting of p blocks of size q.*

Proof. Let $\mathcal{X}$ denote one of these groups. Then $\mathcal{X} \leq S_{pq}$ is transitive, and, by Corollary 3.3, $|\mathcal{X}| = |\mathcal{AUT}(G)|p^2q^2$. Since $q^2 \mid |\mathcal{X}|$, a theorem of Praeger [11] implies that $\mathcal{X}$ cannot be primitive unless $A_{pq} \leq \mathcal{X}$. However, if $A_{pq} \leq \mathcal{X}$, then, since $[\mathcal{X} : \mathcal{AUT}(G)]$ is odd, the Sylow 2-subgroups of $\mathcal{AUT}(G)$ are also Sylow 2-subgroups of $\mathcal{X}$, so that $\mathcal{AUT}(G)$ would contain an element of the form $\alpha = (a,b)(c,d)$. But then $\mathrm{fix}(\alpha)$ would be a subloop of G of order $pq-4$, contradicting Lemma 3.8.

Finally a block system for $\mathcal{X}$ cannot consist of q blocks of size p, since that would imply that $|\mathcal{X}| \mid (p!)^q(q!)$, whereas $q^2 \nmid (p!)^q(q!)$. □

Theorem 3.11 *Suppose that q is a prime, $3 < q$, and $3 \nmid (q-1)$. Then the only G-loop of order $3q$ is the group of order $3q$.*

Proof. Assume that G is not a group. Let $\Sigma_{lp}, \Sigma_{ii}, \Sigma_{rp}$ be block systems for $\mathcal{LP}, \mathcal{II}, \mathcal{RP}$, as in Lemma 3.10. Observe first that each of these block systems is unique for its respective group (since q is prime); then, in view of the containments of the transitive groups $\mathcal{LII}, \mathcal{RII}$ in $\mathcal{LP}, \mathcal{II}, \mathcal{RP}$ (see Figure 1), the three are actually all the same, so now denote them just by $\Sigma = \{A, B, C\}$, where $|A| = |B| = |C| = q$, and $1 \in A$. Then Σ is also a block system for the intransitive groups $\mathcal{RPA}, \mathcal{LPA}$.

Let $\Psi : \mathcal{LII} \to \mathcal{RPA}$ be the canonical surjection, which is an isomorphism here because $|N_\rho| = 1$. Note that if $\gamma \in \mathcal{LII}$, then we have the equation $(xa)\gamma \cdot y\gamma = (xy)\gamma$, where $a = 1\gamma^{-1}$, and then $\Psi(\gamma) = R_a\gamma$.

Since $q \mid |\mathcal{LII}|$ and $q^2 \nmid |\mathcal{LII}|$ (by Lemma 3.9), let $\mathcal{Q} = \langle\alpha\rangle$ be a Sylow q-subgroup of $\mathcal{LII}$. Then $\alpha = \lambda\sigma\tau$, where λ, σ, τ are q-cycles acting on A, B, C respectively. If $a\alpha = 1$, then $\Psi(\alpha) = R_a\alpha$ fixes 1 and hence is the identity on A, since it has order q and leaves Σ invariant. Thus, the permutations R_a and λ^{-1} agree on A. Say $A = \{1 = a_0, a = a_1, a_2, \ldots, a_{q-1}\}$, where $\lambda^{-1} = (a_0, a_1, a_2, \ldots, a_{q-1})$. Then $a_m \cdot a_1 = a_{m+1 \bmod q}$. But repeating this argument with every α^n, we see that $a_m \cdot a_n = a_{m+n \bmod q}$. Hence, A is a subloop of G and $A \cong \mathbb{Z}_q$.

Next, note that $\mathcal{Q}$ is the *only* Sylow q-subgroup of $\mathcal{LII}$. To see this, suppose we had a different one, $\widehat{\mathcal{Q}} = \langle\hat{\alpha}\rangle$, where $\hat{\alpha} = \hat{\lambda}\hat{\sigma}\hat{\tau}$ and $\hat{\lambda}, \hat{\sigma}, \hat{\tau}$ are q-cycles acting on A, B, C. Then $\hat{\lambda} \in \langle\lambda\rangle$, since $\mathcal{LII}(\mathbb{Z}_q) \cong AGL_1(q)$ has only

one q-subgroup. Conjugating with an element which permutes the blocks, we see also that $\hat{\sigma} \in \langle\sigma\rangle$ and $\hat{\tau} \in \langle\tau\rangle$, so that $\alpha, \hat{\alpha}$ commute, which is impossible.

But then α commutes with every element $\delta \in \mathcal{LII}$ of order 3 (since $3 \nmid (q-1)$), and then $\delta\alpha \in \mathcal{LII} \subseteq \mathcal{II}$ would be a $3q$-cycle, contradicting Lemma 3.6. □

4 An Example

The G-loop in Table 1 has a trivial automorphism group; to verify this, note that the loop is generated by elements $2, 3$, the only elements besides 1 whose square is 1, and 2 has two square roots, whereas 3 has only one. $N_\mu = \{1, 2\}$, while $N_\rho = N_\lambda = \{1\}$. Let $\alpha = (1,2)(3,6)(4,5)(7,8)$, $\beta = (1,6,5,8)(2,7,4,3)$, and $\gamma = (1,6,7,4)(2,5,8,3)$. To verify that the loop is a G-loop, check that $\alpha, \beta \in \mathcal{RII}$, and $\alpha, \gamma \in \mathcal{LII}$, which implies that $\mathcal{RII}$ and $\mathcal{LII}$ are transitive. Then, since $|\mathcal{AUT}| = 1$, we have $|\mathcal{LII}| = |\mathcal{RII}| = 8$, so that in fact $\mathcal{RII} = \langle\alpha, \beta\rangle$ and $\mathcal{LII} = \langle\alpha, \gamma\rangle$, since these are 8-element groups. $\mathcal{LII} \cap \mathcal{RII} = \{I, \alpha\}$; in general, in a G-loop, $|\mathcal{LII} \cap \mathcal{RII}| = |\mathcal{AUT}| \cdot |N_\mu|$.

Table 1: A G-Loop

•	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	8	1	6	4	7	2	5
4	4	5	7	2	1	8	6	3
5	5	4	2	7	8	1	3	6
6	6	7	5	8	2	3	1	4
7	7	6	8	5	3	2	4	1
8	8	3	6	1	7	4	5	2

References

[1] A. Barlotti and K. Strambach, The geometry of binary systems, *Advances in Mathematics* 49 (1983) 1 – 105.

[2] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, 1958; third printing, 1971.

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

[4] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics #163 , Springer, 1996.

[5] A. A. Drisko, Loops with transitive automorphisms, *J. Algebra* 184 (1996) 213 – 229.

[6] 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.

[7] K. Kunen, The structure of conjugacy closed loops, *Trans. Amer. Math. Soc.*, to appear; or see `http://www.math.wisc.edu/~kunen/` .

[8] MAGMA: see: `http://www.maths.usyd.edu.au:8000/u/magma/`

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

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

[11] C. E. Praeger, Primitive permutation groups containing an element of order p of small degree, p a prime, *J. Algebra* 34 (1975) 540 – 546.

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

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

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

[15] 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; or see: `http://www.cs.uiowa.edu/~hzhang/`