Can. J. Math., Vol. XXXIV, No. 3, 1982, pp. 662–672

A CLASS OF LOOPS WHICH ARE ISOMORPHIC TO ALL LOOP ISOTOPES

EDGAR G. GOODAIRE AND D. A. ROBINSON

1. Introduction. It is convenient and not without precedent (see [**2**], [**1**], and also [**6**]) to call a loop which is isomorphic to all of its loop isotopes a *G*-loop. Since all groups are readily seen to be *G*-loops, the only interest in such loops, from a loop-theoretic standpoint, resides with those which are not associative. Examples and ad hoc constructions of such loops have appeared sporadically in the literature (see, for instance, [**1**], [**2**], [**4**], [**6**], [**8**], [**9**], and [**13**]).

Any finite loop of order $n < 5$ is a group and, hence, must also be a *G*-loop. R. L. Wilson [**11, 12, 13**] proved that a finite *G*-loop of prime order is necessarily a group; he also exhibited for each even integer $n > 5$ a *G*-loop of order n which is not associative and then raised questions concerning the existence of finite *G*-loops which are not groups for every possible composite order $n > 5$. It is to this latter issue that our efforts are directed in this paper.

In Section 2 we call attention to a class of so-called conjugacy closed loops (see Definition 2.1 and Theorem 2.1) and establish (see Theorem 2.2) various algebraic properties for such loops. For our purposes the most relevant feature of conjugacy closed loops is that they are all *G*-loops, and so in Section 3, where constructions of such loops are presented, we do manage to obtain finite *G*-loops of most composite orders. In fact, it will become clear (see Section 4) that for each composite integer $n > 5$ with the exception of $n = p_1p_2 \ldots p_l$ where the p_i are primes such that $2 < p_1 < p_2 < \ldots < p_l$ and $p_j \not\equiv 1 \pmod{p_i}$ whenever $j > i$ there exists a *G*-loop of order n which is not a group.

2. Conjugacy closed loops. Although all of the basic facts from loop theory which are assumed in this paper (e.g., isotopes, autotopisms, nuclei, etc.) can be found in [**3**], we do deem it appropriate to include a few preliminary remarks which have direct bearing on the present discussion. Let $(G, \cdot\ )$ be a loop and for each $a \in G$ let $R(a)$ and $L(a)$ denote those bijections of the set G defined by $xR(a) = x \cdot a$ and $xL(a) = a \cdot x$

Received August 28, 1980. The first author wishes to thank the faculty and staff of the School of Mathematics at the Georgia Institute of Technology for many kindnesses during his 1979–80 visit and also the Natural Sciences and Engineering Research Council of Canada for its support, Grant No. A9087.

https://doi.org/10.4153/CJM-1982-043-2 Published online by Cambridge University Press

for all $x \in G$. Given $f, g \in G$ define $x \circ y$ by

$$x \circ y = xR(g)^{-1} \cdot yL(f)^{-1} \text{ for all } x, y \in G.$$

Then $(G, \circ)$ is a loop which is isotopic to $(G, \cdot)$. Any loop $(G, \circ)$ obtained from $(G, \cdot)$ in this manner is called a *principal* f, g*-isotope of* $(G, \cdot)$. It is well-known (see [**3**; p. 56]) that any loop isotopic to $(G, \cdot)$ is necessarily isomorphic to some principal f, g-isotope of $(G, \cdot)$. Consequently, a loop is a G-loop if and only if it is isomorphic to all of its principal f, g-isotopes. In practice, however, one never needs to examine all of the principal f, g-isotopes of a loop $(G, \cdot)$ to see whether or not $(G, \cdot)$ is a G-loop. In fact, if e denotes the identity element of a loop $(G, \cdot)$, then a necessary and sufficient condition for $(G, \cdot)$ to be a G-loop is that $(G, \cdot)$ be isomorphic merely to its principal f, e- and principal e, g-isotopes. (For justification of this last result see [**10**] and also [**5**].)

For any loop $(G, \cdot)$ let $R(G, \cdot)$ and $L(G, \cdot)$ be those non-empty subsets of the symmetric group Sym (G) on the set G defined by

$$R(G, \cdot) = \{R(a) | \text{all } a \in G\} \text{ and } L(G, \cdot) = \{L(a) | \text{all } a \in G\}.$$

We are especially interested in those loops $(G, \cdot)$ for which $R(G, \cdot)$ and $L(G, \cdot)$ are closed under conjugation in the group Sym (G). More precisely, we make the following

Definition 2.1. A loop $(G, \cdot)$ is a *conjugacy closed loop* means that $R(x)^{-1}R(y)R(x) \in R(G, \cdot)$ and $L(x)^{-1}L(y)L(x) \in L(G, \cdot)$ for all $x, y \in G$.

Some useful characterizations of such loops are provided by the following

THEOREM 2.1. *For any loop $(G, \cdot)$ the following statements are equivalent.*

(i) *The loop $(G, \cdot)$ is conjugacy closed.*

(ii) *The triples $\langle R(a), R(a)L(a)^{-1}, R(a)\rangle$ and $\langle L(a)R(a)^{-1}, L(a), L(a)\rangle$ are autotopisms of $(G, \cdot)$ for all $a \in G$.*

(iii) *The identities*

$$g \cdot (x \cdot y) = (g \cdot x)R(g)^{-1} \cdot (g \cdot y)$$
$$(x \cdot y) \cdot f = (x \cdot f) \cdot (y \cdot f)L(f)^{-1}$$

hold for all $x, y, f, g \in G$.

Proof. The equivalence of (ii) and (iii) is obvious from the definition of autotopism (see [**3**; p. 112]).

Suppose now that $R(G, \cdot)$ is closed under conjugation. Then for $a, b \in G$ there is $u \in G$ so that $R(a)^{-1}R(b)R(a) = R(u)$. Thus,

$$(x \cdot a)R(a)^{-1}R(b)R(a) = (x \cdot a)R(u) \text{ for all } x \in G.$$

https://doi.org/10.4153/CJM-1982-043-2 Published online by Cambridge University Press

Setting $x = a^\lambda$, the left inverse of a in $(G, \cdot)$, we see that $u = (a^\lambda \cdot b) \cdot a$. It follows that

$$(x \cdot b) \cdot a = (x \cdot a) \cdot ((a^\lambda \cdot b) \cdot a) \text{ for all } x, b \in G$$

and so $\langle R(a), U, R(a) \rangle$ is an autotopism of $(G, \cdot)$ where $U = L(a^\lambda)R(a)$. Setting $x = e$, the identity element of $(G, \cdot)$, in the expression $(x \cdot a) \cdot yU = (x \cdot y) \cdot a$, we deduce that $U = R(a)L(a)^{-1}$. Hence, $\langle R(a), R(a)L(a)^{-1}, R(a) \rangle$ is an autotopism of $(G, \cdot)$.

Conversely, suppose that $\langle R(a), R(a)L(a)^{-1}, R(a) \rangle$ is an autotopism of $(G, \cdot)$ for each $a \in G$. It follows that

$$(x \cdot a) \cdot (bR(a)L(a)^{-1}) = (x \cdot b)R(a) \text{ for all } x, b \in G.$$

Replacing x by $xR(a)^{-1}$, we see that

$$xR(bR(a)L(a)^{-1}) = xR(a)^{-1}R(b)R(a) \text{ for all } x \in G.$$

Thus,

$$R(a)^{-1}R(b)R(a) = R(bR(a)L(a)^{-1}) \text{ for all } a, b \in G,$$

and so $R(G, \cdot)$ is closed under conjugation.

Likewise, one can prove that $L(G, \cdot)$ is closed under conjugation if and only if $\langle L(a)R(a)^{-1}, L(a), L(a) \rangle$ is an autotopism of $(G, \cdot)$ for each $a \in G$. Hence, statements (i) and (ii) are equivalent and our proof of Theorem 2.1 is complete.

We now turn to the algebraic properties of conjugacy closed loops with the following

THEOREM 2.2. *If $(G, \cdot)$ is a conjugacy closed loop, then*

(i) *$(G, \cdot)$ is a G-loop,*

(ii) *the nuclei of $(G, \cdot)$ coincide,*

(iii) *the inner maps*

$$R(a, b) = R(a)R(b)R(a \cdot b)^{-1} \text{ and } L(a, b) = L(a)L(b)L(b \cdot a)^{-1}$$

are automorphisms of $(G, \cdot)$ for all $a, b \in G$ and the inner map $T(a) = L(a)R(a)^{-1}$ is a pseudo-automorphism of $(G, \cdot)$ with companion a for all $a \in G$,

(iv) *the nucleus N of $(G, \cdot)$ is a normal subloop of $(G, \cdot)$ (and so the quotient loop G/N exists),*

(v) *every subloop of $(G, \cdot)$ is a conjugacy closed loop,*

(vi) *every homomorphic image of $(G, \cdot)$ is a conjugacy closed loop (and so, in particular, G/N is a conjugacy closed loop in view of* (iv)).

Proof. (i) Let e denote the identity element of $(G, \cdot)$. It is clear from (iii) of Theorem 2.1 that $L(g)$ is an isomorphism of $(G, \cdot)$ onto its principal e, g-isotope and that $R(f)$ is an isomorphism of $(G, \cdot)$ onto its principal f, e-isotope for all $f, g \in G$. In view of the comments at the

https://doi.org/10.4153/CJM-1982-043-2 Published online by Cambridge University Press

beginning of this section this observation suffices to guarantee that $(G, \cdot)$ is a G-loop.

(ii) For each $a \in G$ let $A(a)$ and $B(a)$ be defined by

$$A(a) = \langle R(a), R(a)L(a)^{-1}, R(a)\rangle \text{ and}$$
$$B(a) = \langle L(a)R(a)^{-1}, L(a), L(a)\rangle.$$

In view of Theorem 2.1, $A(a)$ and $B(a)$ are autotopisms of $(G, \cdot)$ for all $a \in G$. Recall that an element $a \in G$ is in the left, middle, or right nucleus of $(G, \cdot)$ according as $\langle L(a), I, L(a)\rangle$, $\langle R(a)^{-1}, L(a), I\rangle$, or $\langle I, R(a), R(a)\rangle$, respectively, is an autotopism of $(G, \cdot)$ where I denotes the identity map on G. Since

$$\langle L(a), I, L(a)\rangle \langle R(a)^{-1}, L(a), I\rangle = B(a) \text{ and}$$
$$A(a) \langle R(a)^{-1}, L(a), I\rangle = \langle I, R(a), R(a)\rangle,$$

it is clear that a is in all three of the nuclei mentioned above whenever it is in any one of the three nuclei. Hence, the nuclei of $(G, \cdot)$ coincide.

(iii) Define $A(a)$ and $B(a)$ as in the proof of (ii) above. Then $B(a)B(b)B(ab)^{-1} = \langle R(a)R(b)R(ab)^{-1}, U, R(a)R(b)R(ab)^{-1}\rangle$ is an autotopism of $(G, \cdot)$ for some bijection U of G. Then since

$$eR(a)R(b)R(ab)^{-1} = e,$$

it is easy to see that

$$U = R(a)R(b)R(ab)^{-1}.$$

Consequently, $R(a)R(b)R(ab)^{-1}$ is an automorphism of $(G, \cdot)$. Likewise, using $A(a)A(b)A(ba)^{-1}$, one can show that $L(a)L(b)L(ba)^{-1}$ is an automorphism of $(G, \cdot)$. Thus, the inner maps $R(a, b)$ and $L(a, b)$ are automorphisms of $(G, \cdot)$. Since

$$\begin{aligned} A(a) &= \langle L(a)R(a)^{-1}, L(a), L(a)\rangle \\ &= \langle L(a)R(a)^{-1}, L(a)R(a)^{-1}R(a), L(a)R(a)^{-1}R(a)\rangle \\ &= \langle T(a), T(a)R(a), T(a)R(a)\rangle \end{aligned}$$

is an autotopism of $(G, \cdot)$, we see that $T(a)$ is a pseudo-automorphism of $(G, \cdot)$ with companion a.

(iv) Since $T(a)$ is a pseudo-automorphism of $(G, \cdot)$, one can adopt almost verbatim an argument of R. H. Bruck [**3**; p. 114] to show that the restriction of $T(a)$ to the left nucleus of $(G, \cdot)$ is, in fact, an automorphism of the left nucleus. But, in view of (ii) above, the nucleus N of $(G, \cdot)$ coincides with the left nucleus of $(G, \cdot)$, and so $NT(a) = N$ for all $a \in G$. Hence, N is a normal subloop of $(G, \cdot)$.

(v) Clearly every subloop of $(G, \cdot)$ inherits the identities displayed in (iii) of Theorem 2.1. Consequently, because of the equivalence of

https://doi.org/10.4153/CJM-1982-043-2 Published online by Cambridge University Press

statements (i) and (iii) of Theorem 2.1, every subloop of $(G, \cdot)$ must also be a conjugacy closed loop.

(vi) Let $S(G, \cdot)$ be that subsemigroup of the symmetric group Sym (G) on the set G which is generated by $R(G, \cdot) \cup L(G, \cdot)$. A sufficient condition for every homomorphic image of the loop $(G, \cdot)$ to also be a loop is that $S(G, \cdot)$ is a subgroup of Sym (G) (see [**3**; p. 110]). To show that $S(G, \cdot)$ is a subgroup of Sym (G) it suffices to prove that for each $a \in G$ there exist elements $\bar{R}(a)$ and $\bar{L}(a)$ in $S(G, \cdot)$ so that $\bar{R}(a)R(a) = \bar{L}(a)L(a) = I$, the identity map on G. Returning to the proof of Theorem 2.1, one finds that

$$L(a^\lambda)R(a) = R(a)L(a)^{-1}.$$

One can also prove that

$$R(a^\rho)L(a) = L(a)R(a)^{-1}.$$

Then, by choosing

$$\bar{R}(a) = R(a^\rho)L(a)L(a^\lambda) \text{ and } \bar{L}(a) = L(a^\lambda)R(a)R(a^\rho),$$

we see that $\bar{R}(a)$ and $\bar{L}(a)$ are in $S(G, \cdot)$ and that $\bar{R}(a)R(a) = \bar{L}(a)L(a) = I$. Thus, every homomorphic image of a conjugacy closed loop $(G, \cdot)$ is a loop. (In general, a homomorphic image of a loop need not be a loop.) Any homomorphic image of a conjugacy closed loop inherits the identities of (iii) of Theorem 2.1. Thus, every homomorphic image of a conjugacy closed loop is also a conjugacy closed loop.

We conclude the present section with a few remarks.

Remark 2.1. E. L. Wilson [**10**] considered those loops $(G, \cdot)$ which satisfy the identity

$$(\#) \quad x \cdot (x \cdot y)^\rho = (x \cdot z) \cdot (x \cdot (y \cdot z))^\rho$$

for all $x, y, z \in G$ and showed that such loops are G-loops. Using autotopism arguments and information from [**10**] and [**8**], one can show that a loop $(G, \cdot)$ satisfies E. L. Wilson's identity (#) for all $x, y, z \in G$ if and only if $(G, \cdot)$ is a conjugacy closed loop and satisfies the weak inverse property.

Remark 2.2. From Theorem 2.2 we have the following result: If $(G, \cdot)$ is a conjugacy closed loop with nucleus N, then N is a normal subloop of $(G, \cdot)$ and the quotient loop G$/N$ is also a conjugacy closed loop. In all of our examples in Section 3 the loop G/N is an Abelian group. Unfortunately, we do not know if this must be true in general.

3. Constructions of conjugacy closed loops. In this section our purpose is to present results and constructions which can be used to produce examples of conjugacy closed loops (and, hence, also G-loops) which are not associative.

https://doi.org/10.4153/CJM-1982-043-2 Published online by Cambridge University Press

THEOREM 3.1. *Let N denote the nucleus of a loop $(G, \cdot)$. If $[G:N] = 2$, then $(G, \cdot)$ is a conjugacy closed loop which is not a group.*

Proof. Since $[G:N] = 2$, we see that N coincides with the left, middle, and right nucleus of $(G, \cdot)$ and, furthermore, that $G = N \cup Na = N \cup aN$ for all $a \in G$ such that $a \notin N$. Let g be any element in G and consider two cases according as $g \in N$ or $g \notin N$.

Case 1. $g \in N$. Then

$$(g\cdot x)R(g)^{-1}\cdot(g\cdot y) = ((g\cdot x)R(g)^{-1}\cdot g)\cdot y$$
$$= (g\cdot x)\cdot y = g\cdot(x\cdot y) \text{ for all } x, y \in G.$$

Case 2. $g \notin N$. Let x be any element in G. If $x \in N$, then we must have $(g\cdot x)R(g)^{-1} \in N$ and so we see that

$$(g\cdot x)R(g)^{-1}\cdot(g\cdot y) = ((g\cdot x)R(g)^{-1}\cdot g)\cdot y$$
$$= (g\cdot x)\cdot y = g\cdot(x\cdot y) \text{ for all } y \in G.$$

Now in what follows $x \notin N$. Then we have $(g\cdot x)R(g)^{-1} \notin N$ and so $(g\cdot x)R(g)^{-1} = g\cdot n$ for some $n \in N$. But note that $(g\cdot x)R(g)^{-1} = g\cdot n$ for some $n \in N \Rightarrow g\cdot x = (g\cdot n)\cdot g \Rightarrow g\cdot x = g\cdot(n\cdot g) \Rightarrow x = n\cdot g$. Hence, we see that

$$(g\cdot x)R(g)^{-1}\cdot(g\cdot y) = (g\cdot n)\cdot(g\cdot y) = g\cdot(n\cdot(g\cdot y))$$
$$= g\cdot((n\cdot g)\cdot y) = g\cdot(x\cdot y) \text{ for all } y \in G.$$

In every case we have shown that

$$(g\cdot x)R(g)^{-1}\cdot(g\cdot y) = g\cdot(x\cdot y).$$

Similarly, we can show that

$$(x\cdot y)\cdot f = (x\cdot f)\cdot(y\cdot f)L(f)^{-1} \text{ for all } x, y, f \in G.$$

Thus, by Theorem 2.1, the loop $(G, \cdot)$ is a conjugacy closed loop. Since $N \neq G$, we see that $(G, \cdot)$ is not a group. This completes our proof.

The preceding result reinforces something already mentioned in the literature: any loop with index 2 nucleus is a G-loop. (See [**2**] and [**1**].) It is also of interest to view this in the context of cyclic loop-extensions (see [**7**]).

For each even integer $n > 5$ R. L. Wilson [**13**] has constructed a loop of order n which satisfies the hypothesis of Theorem 3.1. Thus, appealing to Wilson's construction, we have the following

COROLLARY 3.1.1. *For each even integer $n > 5$ there is a conjugacy closed loop of order n which is not a group.*

The next result describes another procedure for obtaining conjugacy closed loops.

https://doi.org/10.4153/CJM-1982-043-2 Published online by Cambridge University Press

THEOREM 3.2. *Let R and S be rings with R commutative and associative and let $\theta:R \rightarrow S$ be a homomorphism of $(R, +)$ into $(S, +)$. For (a, α) and (b, β) in G where $G = R \times S$ define*

$$(a, \alpha)\cdot(b, \beta) = (a + b, \alpha + \beta + (ab^2)\theta).$$

Then $(G, \cdot)$ is a conjugacy closed loop whose nucleus N is given by

$$N = \{(a, \alpha) \in G|\ 2abc \in \text{Kern}\,\theta \textit{ for all } b, c \in R\}.$$

Furthermore, N is normal in $(G, \cdot)$ and G/N is a commutative group.

Proof. It is easy to show that $(G, \cdot)$ is a loop. The identity element is $(0, 0)$ and for $x = (a, \alpha)$ and $y = (b, \beta)$ in G we see that

$$xR(y)^{-1} = (a - b, \alpha - \beta - ((a - b)b^2)\theta)$$

and

$$xL(y)^{-1} = (a - b, \alpha - \beta - (b(a - b)^2)\theta).$$

Now let $f = (r, \rho)$ and $g = (s, \sigma)$ be in G and note that, upon simplifying, both $g\cdot(x\cdot y)$ and $(g\cdot x)R(g)^{-1}\cdot(g\cdot y)$ are equal to the element

$$(a + b + s, \alpha + \beta + \sigma + (ab^2)\theta + (sa^2)\theta + (sb^2)\theta + 2(sab)\theta);$$

and both $(x\cdot y)\cdot f$ and $(x\cdot f)\cdot(y\cdot f)L(f)^{-1}$ are equal to

$$(a + b + r, \alpha + \beta + \rho + (ab^2)\theta + (ar^2)\theta + (br^2)\theta).$$

(Note that only the commutativity and associativity of the ring R and the homomorphism property for θ relative to the $+$ operations were needed to perform these simplifications.) Hence, by Theorem 2.1, we conclude that $(G, \cdot)$ is a conjugacy closed loop.

Now with $z = (c, \gamma)$ we see that

$$(x\cdot y)\cdot z = (a + b + c, \alpha + \beta + \gamma + (ab^2)\theta + (ac^2)\theta + (bc^2)\theta)$$

whereas

$$x\cdot(y\cdot z) = (a + b + c, \alpha + \beta + \gamma + (ab^2)\theta + (ac^2)\theta + (bc^2)\theta + 2(abc)\theta).$$

It follows that $x = (a, \alpha)$ is in N if and only if $2abc \in \text{Kern}\,\theta$ for all $b, c \in R$. Since $(G, \cdot)$ is a conjugacy closed loop, it is clear that N is normal in $(G, \cdot)$. Furthermore, with our explicit description of N, it is clear that G/N is an Abelian group and our proof is complete.

COROLLARY 3.2.1. *If m and n are positive integers with $m > 2$, then there is a conjugacy closed loop of order m^2n which is not a group.*

Proof. Let $R = \mathbf{Z}/(mn)$ and $S = \mathbf{Z}/(m)$ be the rings of integers modulo mn and m, respectively. Employing the usual additive coset

https://doi.org/10.4153/CJM-1982-043-2 Published online by Cambridge University Press

notation, we define $\{a + (mn)\}\theta = a + (m)$ for all $a + (mn) \in R$. Note that for $a, b \in \mathbf{Z}$ we have

$$a + (mn) = b + (mn) \Rightarrow mn|a - b \Rightarrow m|a - b \Rightarrow a + (m) = b + (m)$$

and so θ is well-defined. It is now easy to see that θ is a homomorphism of $(R, +)$ onto $(S, +)$ and that a $+ (mn) \in \text{Kern}\,\theta$ if and only if $m|a$. With $m > 2$ we see that $m \nmid 2 \cdot 1 \cdot 1 \cdot 1$ and so $2R^3 \not\subseteq \text{Kern}\,\theta$. It follows that the loop $(G, \cdot)$ constructed from R and S in Theorem 3.2 is a conjugacy closed loop which is not a group. Finally note that $|G| = |R|\,|S| = m^2n$.

The loop constructed in the next result was originally offered by V. D. Belousov [**2**; p. 184] as an example of a G-loop.

THEOREM 3.3. *Let F be a field, let $F^* = \{a \in F | a \neq 0\}$, and let $G = F^* \times F$. For (a, α) and (b, β) in G define*

$$(a, \alpha) \cdot (b, \beta) = (ab, (a^{-1} - 1)(b^{-1} - 1) + b^{-1}\alpha + \beta).$$

Then $(G, \cdot)$ is a conjugacy closed loop whose nucleus N is given by

$$N = \{(1, \alpha) |\ all\ \alpha \in F\}.$$

Furthermore, N is normal in $(G, \cdot)$ and G/N is a commutative group.

Proof. Although the computational details are quite different, we are able to proceed as in the proof of Theorem 3.2. Clearly $(G, \cdot)$ is a loop. Its identity element is $(1, 0)$ and for $x = (a, \alpha)$ and $y = (b, \beta)$ in G we have

$$xR(y)^{-1} = (ab^{-1}, b(\alpha - \beta) - a^{-1}(a - b)(b - 1))$$

and

$$xL(y)^{-1} = (ab^{-1}, \alpha - a^{-1}b\beta - a^{-1}b^{-1}(a - b)(b - 1)).$$

Now let $f = (r, \rho)$ and $g = (s, \sigma)$ be in G and note, following direct, but tedious, computations, that $g \cdot (x \cdot y)$ and $(g \cdot x)R(g)^{-1} \cdot (g \cdot y)$ are both equal to the element

$$(abs, a^{-1}b^{-1}s^{-1} + a^{-1}b^{-1}\sigma + b^{-1}\alpha - s^{-1} - a^{-1} - b^{-1} + \beta + 1 + 1)$$

and that $(x \cdot y) \cdot f$ and $(x \cdot f) \cdot (y \cdot f)L(f)^{-1}$ are both equal to

$$(abr, 2a^{-1}b^{-1}r^{-1} + r^{-1}b^{-1}\alpha - a^{-1}b^{-1} - r^{-1}a^{-1} - r^{-1}b^{-1} + r^{-1}\beta + \rho + 1).$$

Thus, by Theorem 2.1, the loop $(G, \cdot)$ is a conjugacy closed loop.

Now, if $z = (c, \gamma)$, we can exhibit $(x \cdot y) \cdot z$ and $x \cdot (y \cdot z)$. Upon com-

https://doi.org/10.4153/CJM-1982-043-2 Published online by Cambridge University Press

parison, we see that $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ if and only if

$$(a^{-1} - 1)(b^{-1} - 1)(c^{-1} - 1) = 0.$$

Thus, $(a, \alpha) \in N$ if and only if $a = 1$. It then follows easily that N is normal in $(G, \cdot)$ and that G/N is an Abelian group.

COROLLARY 3.3.1. *If p and q are distinct odd primes with $p|q - 1$, then there is a conjugacy closed loop of order pq which is not a group.*

Proof. Let F be the finite field of prime order q. Then the multiplicative group F^* of non-zero elements of F is cyclic of order $q - 1$. Since $p|q - 1$ the cyclic group F^* has a (unique) subgroup H of order p. Now let $L = H \times F$ and note that L is a subloop of the conjugacy closed loop $(G, \cdot)$ of Theorem 3.3. As such, $(L, \cdot)$ is also a conjugacy closed loop (see Theorem 2.2 (v)). Since $p > 2$ there exist elements $a, b, c \in H$ so that

$$(a^{-1} - 1)(b^{-1} - 1)(c^{-1} - 1) \neq 0.$$

Thus, $(L, \cdot)$ is not associative (see the proof of Theorem 3.3). Furthermore, $|L| = |H|\,|F| = pq$.

An obvious modification in our proof of the preceding corollary yields the following generalization: If q is a prime, if n and m are positive integers with $m > 1$, and if $m|q^n - 1$, then there is a conjugacy closed loop of order mq^n which is not a group. As will be seen in Section 4 we have no need to exploit this observation.

4. Conclusions. We now return to the issue raised in Section 1, namely, the existence of finite G-loops which are not groups for every composite order $n > 5$.

Recalling that conjugacy closed loops are G-loops and drawing on information from Section 3, we consider various cases. In every case n shall denote a composite integer with $n > 5$.

Case 1. n even. By Corollary 3.1.1 there is a G-loop of order n which is not a group.

Case 2. n odd and not square free. Clearly then either $n = p_1^{\alpha_1}$ or $n = p_1^{\alpha_1}p_2^{\alpha_2} \dots p_l^{\alpha_l}$ where the p_i are distinct odd primes, the α_i are positive integers with $\alpha_i \geqq 2$ for some i, and $l > 1$. There is no loss of generality if we assume $\alpha_1 \geqq 2$. If $n = p_1^{\alpha_1}$, then

$$n = p_1^2 p_1^{\alpha_1 - 2};$$

if $n = p_1^{\alpha_1}p_2^{\alpha_2} \dots p_l^{\alpha_l}$, then

$$n = p_1^2(p_1^{\alpha_1 - 2}p_2^{\alpha_2} \dots p_l^{\alpha_l}).$$

In either event, we get a loop of the type we desire by appealing to Corollary 3.2.1.

https://doi.org/10.4153/CJM-1982-043-2 Published online by Cambridge University Press

Case 3. n odd and square free. Then $n = p_1p_2 \ldots p_l$ where the p_i are primes numbered so that $2 < p_1 < p_2 < \ldots < p_l$. Since n is composite in all of our cases, we have $l > 1$. If $p_r|p_s - 1$ for some integers r and s with $r < s$, we use Corollary 3.3.1 to obtain a G-loop H of order p_rp_s which is not a group. Now let K be any group of order n/p_rp_s. Then H and K are both G-loops and so the direct product $H \times K$ is also a G-loop (see [**11**; Theorem 4.1]) of order n. The loop $H \times K$ cannot be associative because H is not a group. Finally, note that $|H \times K| = n$. If, on the other hand, $p_s \not\equiv 1 \pmod{p_r}$ for all integers r and s with $1 \leqq r < s \leqq l$, the authors have been frustrated in their attempts to produce a G-loop of order n which is not a group (see the comments below and also Theorem 4.2).

The preceding case-by-case discussion serves as a proof of the following

THEOREM 4.1. *If n is any composite integer with $n > 5$ which cannot be expressed as $n = p_1p_2 \ldots p_l$ for primes p_i such that $2 < p_1 < p_2 < \ldots < p_l$ and $p_s \not\equiv 1 \pmod{p_r}$ whenever $1 \leqq r < s \leqq l$, then there exists a G-loop of order n which is not a group.*

To prove that the conclusion of Theorem 4.1 remains valid for all composite integers $n > 5$ it would be sufficient to construct for each pair of primes p and q with $2 < p < q$ and $q \not\equiv 1 \pmod{p}$ a G-loop of order pq which is not associative, for as soon as such a loop is available one could merely form the direct product of it with a group of the obvious order (à la Case 3 above). Of course, a related question would be: Do there exist any conjugacy closed loops of these special orders which are not groups? Although this question remains unresolved, we conclude this paper with the following result which seems pertinent and somewhat provocative.

THEOREM 4.2. *Let $(G, \cdot)$ be a finite conjugacy closed loop of order pq where p and q are primes with $2 < p < q$. If $(G, \cdot)$ is not a group, then either $q \equiv 1 \pmod{p}$ or $(G, \cdot)$ has trivial nucleus.*

Proof. Let N denote the nucleus of $(G, \cdot)$. We assume now that $(G, \cdot)$ is not a group and that $|N| \neq 1$; we proceed to prove that $q \equiv 1 \pmod{p}$. Since $|N|$ divides $|G|$ (see [**3**; p. 92]), we have $|N| = p$ or $|N| = q$. Since G/N is a G-loop (see Theorem 2.2) of prime order, we know that G/N is a group (see [**12**]). Appealing to results from cyclic loop-extensions (see [**7**]), we know that there is an automorphism θ of $(N, \cdot)$ so that $\theta^{|G/N|} = I$, the identity map on N. Now let a be a generator of the cyclic group $(N, \cdot)$ and let s be an integer such that $a\theta = a^s$. If $|N| = q$, then $a\theta^p = a^{sp} = I$ and so $s^p \equiv 1 \pmod{q}$. Thus, since $|N| = p$, we conclude that either $s \equiv 1 \pmod{q}$ or $p|q - 1$. Now, if $|N| = q$, we deduce in like manner that either $s \equiv 1 \pmod{p}$ or $q|p - 1$. Since

https://doi.org/10.4153/CJM-1982-043-2 Published online by Cambridge University Press

$p < q$, it is not possible to have $q|p - 1$. Also $s \equiv 1 \pmod{|N|}$ implies that $\theta = I$ and, hence, forces $(G, \cdot)$ to be a group (see [7]). We conclude that $|N| = q$ and that $p|q - 1$. This completes our proof.

References

1. A. S. Basarab, *On a class of G-loops* (Russian), Mat. Issled., *3* vyp. 2(1968), 3–24.
2. V. D. Belousov, *Foundations of the theory of quasigroups and loops* (Russian), Izdat. "Nauka" (Moscow, 1967).
3. R. H. Bruck, *A survey of binary systems* (Springer-Verlag, Berlin and New York, 1958).
4. ——— *Some theorems on Moufang loops*, Math. Z. *73* (1960), 59–78.
5. B. F. Bryant and Hans Schneider, *Principal loop-isotopes of quasigroups*, Can. J. Math. *18* (1966), 120–125.
6. Orin Chein and H. Pflugfelder, *On maps $x \to x^m$ and the isotopy-isomorphy property of Moufang loops*, Aequationes Math. *6* (1971), 157–161.
7. Edgar G. Goodaire and D. A. Robinson, *Loops which are cyclic extensions of their nuclei*, Compositio Math. *45* (1982), 341–356.
8. J. Marshall Osborn, *Loops with the weak inverse property*, Pacific J. Math. *10* (1960), 295–304.
9. D. A. Robinson, *A Bol loop isomorphic to all loop isotopes*, Proc. Amer. Math. Soc. *19* (1968), 671–672.
10. E. L. Wilson, *A class of loops with the isotopy-isomorphy property*, Can. J. Math. *18* (1966), 589–592.
11. R. L. Wilson, Jr., *Loop isotopism and isomorphism and extensions of universal algebras*, Ph.D. Thesis, University of Wisconsin, Madison (1969).
12. ——— *Isotopy-isomorphy loops of prime order*, J. Algebra *31* (1974), 117–119.
13. ——— *Quasidirect products of quasigroups*, Comm. Algebra *3* (1975), 835–850.

Memorial University of Newfoundland,
St. John's, Newfoundland;
Georgia Institute of Technology,
Atlanta, Georgia

https://doi.org/10.4153/CJM-1982-043-2 Published online by Cambridge University Press