Contemporary Mathematics
Volume **721**, 2019
https://doi.org/10.1090/conm/721/14503

Simple right conjugacy closed loops

Mark Greer

Abstract. We give a general construction for right conjugacy closed loops, using $GL(2, q)$ for q a prime power. Under certain conditions, the loops constructed are simple, providing a general construction for finite, simple right conjugacy closed loops. Finally, a complete description of the isomorphism classes for the construction is given, yielding an exact count of non isomorphic loops for each q.

1. Introduction

A *loop* $(Q, \cdot)$ consists of a set Q with a binary operation $\cdot : Q \times Q \to Q$ such that (i) for all $a, b \in Q$, the equations $ax = b$ and $ya = b$ have unique solutions $x, y \in Q$, and (ii) there exists $1 \in Q$ such that $1x = x1 = x$ for all $x \in Q$. We denote these unique solutions by $x = a\backslash b$ and $y = b/a$, respectively. Standard references in loop theory are [**3**, **18**].

We say a subset S of a group G is closed under conjugation if $x^{-1}yx \in S$ for all $x, y \in S$. A loop Q is a *right conjugacy closed loop* (or RCC loop) if R_Q is closed under conjugation. That is, $R_x^{-1} R_y R_x \in R_Q$ for all $x, y \in Q$. Similarly, a loop Q is *left conjugacy closed* (LCC) if $L_x^{-1} L_y L_x \in L_Q$ for all $x, y \in Q$. Most of the literature on the one-sided conjugacy closed loops deals with left conjugacy closed loops [**2**, **4**, **5**, **15**]. RCC loops are the more natural choice here since our permutations act on the right.

For (two-sided) CC-loops, the existence of nonassociative simple loops is settled in the negative by Basarab's Theorem [**2**]: *The factor of a CC-loop by its (necessarily normal) nucleus is an abelian group.* It follows that a simple CC-loop must have nucleus coinciding with the whole loop, hence is a group.

In the one-sided case, nonassociative simple RCC loops are known to exist. The first example occurring in the literature seems to be the simple Bol loop of exponent 2 and order 96 constructed by G. Nagy [**13**], because a right Bol loop of exponent 2 is necessarily an RCC loop. Other examples arose in the computer search for nonassociative, finite simple automorphic loops [**11**], since every RCC loops is a right automorphic loop.

Here we give a general construction of a large class of nonassociative, finite simple RCC loops. Our construction by no means accounts for all such loops; for example, Nagy's Bol loop of exponent 2 does not fit this construction. Thus a full

2010 *Mathematics Subject Classification.* Primary 20N05.
Key words and phrases. Conjugacy closed loops, simple loops, finite fields.

classification of finite simple RCC loops is still elusive. Nevertheless, using Mace4 [**14**] and the loops package for GAP [**8**, **16**], we have found by exhaustive computer search that our construction accounts for all finite simple RCC loops up to order 15.

It turns out that our construction is isomorphic to a construction due to Hall for projective planes, called *Hall Planes* [**10**]. For each irreducible monic quadratic over a finite field, there is a unique Hall quasifield created. Hall planes of the same order turn out to be isomorphic [**17**]. The multiplication loops in Hall's quasifields are isomorphic to the RCC loops constructed in this paper, however, we will have non-trivial isomorphism classes (Theorem 4.3). It is interesting to note another paper which relates quasifields to (one-sided) conjugacy closed loops is [**12**].

In section §2, we review basic notions from loop theory. We also give some basic results concerning with RCC loops. In section §3, we give our construction for our loops (Theorem 3.3) and prove these loops are indeed RCC (Theorem 3.7). After proving several structural results about these RCC loops, we show our construction gives simple RCC loops (Theorem 3.10).

As previously stated, our construction may give isomorphic RCC loops for certain orders. We explain this phenomenon in §4, showing that isomorphisms reduce to automorphisms of finite fields (Lemmas 4.1 & 4.2) and count the isomorphism classes (Theorem 4.3). Finally, we end with some open questions.

2. Right conjugacy closed loops

To avoid excessive parentheses, we use the following convention:

- multiplication $\cdot$ will be less binding than divisions $\backslash, /$,
- divisions are less binding than juxtaposition.

For example $xy/z \cdot y\backslash xy$ reads as $((xy)/z)(y\backslash(xy))$.

In a loop Q, the left and right translations by $x \in Q$ are defined by $yL_x = xy$ and $yR_x = yx$ respectively. We thus have $\backslash, /$ as $x\backslash y = yL_x^{-1}$ and $y/x = yR_x^{-1}$. We define the *right section* of Q, $R_Q = \{R_x \mid x \in Q\}$, *right multiplication group* of Q, $\mathrm{Mlt}_\rho(Q) = \langle R_x \mid x \in Q\rangle$ and *multiplication group* of Q, $\mathrm{Mlt}(Q) = \langle R_x, L_x \mid x \in Q\rangle$. We define the *inner mapping group* of Q, $\mathrm{Inn}(Q) = \mathrm{Mlt}(Q)_1 = \{\theta \in \mathrm{Mlt}(Q) \mid 1\theta = 1\}$.

A bijection $\theta : Q \to Q$ is an *automorphism* if $(xy)\theta = x\theta \cdot y\theta$ for all $x, y \in Q$. Under composition, we define the *automorphism group of* Q, $\mathrm{Aut}(Q)$. A triple (α, β, γ) of bijections of a loop Q is an *autotopism* if for all $x, y \in Q$, $x\alpha \cdot y\beta = (xy)\gamma$. The set $\mathrm{Atp}(Q)$ of all autotopisms of Q is a group under composition.

A subloop N of Q is normal ($N \trianglelefteq Q$) if for every $x, y \in Q$ we have $xN = Nx$, $x(yN) = (xy)N$, $(Nx)y = N(xy)$, and $x(Ny) = (xN)y$. A loop Q is simple if the only normal subloops are the trivial, $\{1\}$ and Q.

The following proposition will be useful later. It uses right translations to check whether a magma $(Q, \cdot)$ is indeed a loop.

Proposition 2.1. *([**11**]) Let $(Q, \cdot)$ be a right loop with $1 \in Q$ an identity element. Then Q is a loop* if and only if *$R_x R_y^{-1}$ is fixed point free for every x, $y \in Q$ with $x \neq y$.*

Proof. This follows from Lemmas 2.1 and 2.2 of [**11**]. □

For a loop Q, we have the following subsets of interest:

the left nucleus of Q,	$N_\lambda(Q) = \{a \in Q \mid a \cdot xy = ax \cdot y \ \forall x, y \in Q\ \}$,
the middle nucleus of Q,	$N_\mu(Q) = \{a \in Q \mid x \cdot ay = xa \cdot y \ \forall x, y \in Q\ \}$,
the right nucleus of Q,	$N_\rho(Q) = \{a \in Q \mid x \cdot ya = xy \cdot a \ \forall x, y \in Q\ \}$,
the nucleus of Q,	$N(Q) = N_\lambda(Q) \cap N_\mu(Q) \cap N_\rho(Q)$,
the commutant of Q,	$C(Q) = \{a \in Q \mid xa = ax \ \forall x \in Q\}$,
the center of Q,	$Z(Q) = N(Q) \cap C(Q)$.

For a loop Q, the nuclei $N(Q), N_\lambda(Q), N_\mu(Q)$, and $N_\rho(Q)$ are all subloops of Q and the center $Z(Q)$ is a normal subloop of Q. However, the commutant, $C(Q)$ need not be a subloop in general of Q.

PROPOSITION 2.2. *Let Q be a loop. Then $a \in C(Q) \cap N_\lambda(Q) \Leftrightarrow R_a \in Z(Mlt_\rho(Q))$.*

PROOF. Let $a \in C(Q) \cap N_\lambda(Q)$. Then $\forall x, y \in Q$,

$$yR_aR_x = ya \cdot x = ay \cdot x = a \cdot yx = yx \cdot a = yR_xR_a.$$

Hence, $R_a \in Z(\mathrm{Mlt}_\rho(Q))$. Conversely, let $R_a \in Z(\mathrm{Mlt}_\rho(Q))$. Then $ax = 1R_aR_x = 1R_xR_a = xa$. Hence $a \in C(Q)$. Moreover,

$$a \cdot yx = yx \cdot a = yR_xR_a = yR_aR_x = ya \cdot x = ay \cdot x.$$

Thus, $a \in C(Q) \cap N_\lambda(Q)$. □

PROPOSITION 2.3. *For a loop Q, the following are equivalent:*

(1) *Q is an RCC loop,*
(2) *The following holds for all $x, y, z \in Q$:*

$$R_x^{-1}R_yR_x = R_{x\backslash yx}. \tag{RCC$_1$}$$

(3) *The following holds for all $x, y, z \in Q$:*

$$(xy)z = (xz) \cdot z\backslash(yz). \tag{RCC$_2$}$$

(4) *For all $x \in Q$, $(R_a, R_aL_a^{-1}, R_a) \in \mathrm{Atp}(Q)$.*

PROOF. If Q is an RCC loop, then $\forall x, y \in Q$, we have $R_x^{-1}R_yR_x = R_z \Leftrightarrow R_yR_x = R_xR_z$. Hence, applying this to 1 gives $yx = xz$, and thus, $z = x\backslash yx$. Similarly, (RCC$_1$) holds if and only if $R_yR_z = R_zR_{z\backslash yz}$ for all $y, z \in Q$, which is clearly equivalent to (RCC$_2$). Finally, $(R_a, R_aL_a^{-1}, R_a) \in \mathrm{Atp}(Q)$ is simply (RCC$_2$). □

PROPOSITION 2.4. *Let Q be a RCC loop. Then*

(i) *$N_\mu(Q) = N_\rho(Q) \trianglelefteq Q$ and*
(ii) *$C(Q) \leq N_\lambda(Q)$.*

PROOF. For (i), note that

$$(id_Q, R_a, R_a)(R_a, L_a^{-1}, id_Q) = (R_a, R_aL_a^{-1}, R_a) \in \mathrm{Atp}(Q).$$

Therefore, if (id_Q, R_a, R_a) or (R_a, L_a^{-1}, id_Q) is in $\mathrm{Atp}(Q)$, the other one is as well. For normality, see [**4**].

For (ii), let $a \in C(Q)$. Then, using (RCC$_2$), we have

$$ax \cdot y = xa \cdot y = xy \cdot y\backslash(ay) = xy \cdot a = a \cdot xy.$$ □

3. Constructing simple RCC loops

Let $\mathbb{F}_q$ be the finite field of order $q = p^n$ for a prime p and some $n > 0$. For a matrix M, let $Det(M)$, $Tr(A)$, and $Char(M)$ denote the standard *determinant*, *trace* and *characteristic polynomial of the matrix M.* In this paper, all matrices will be of size 2×2 (*i.e.* $M \in GL(2,q)$), hence $Char(M) = x^2 - Tr(M)x + Det(M) \in \mathbb{F}_q[x]$.

Let $f(x) = x^2 - rx + s$ be irreducible in $\mathbb{F}_q[x]$. For each $b \in \mathbb{F}_q$, define

$$M_{(0,b)} = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$$

and for $a \neq 0$,

$$M_{(a,b)} = \begin{pmatrix} r-b & \frac{f(b)}{-a} \\ a & b \end{pmatrix}.$$

Note that $Det(M_{(a,b)}) = s$ and $Tr(M_{(a,b)}) = r$ and thus $Char(M_{(a,b)}) = f(x)$.

LEMMA 3.1. *Let $f(x) = x^2 - rx + s$ be irreducible in $\mathbb{F}_q[x]$. The conjugacy class of all matrices in $GL(2,q)$ with characteristic polynomial $f(x)$ is precisely the set $\{M_{(a,b)} \mid a, b \in \mathbb{F}_q\}$ for $a \neq 0$.*

PROOF. Note that if two elements of $GL(2,q)$ are conjugate then they both have the same characteristic polynomial, and hence for a 2×2 matrix, have the same determinant and trace [**19**]. Now suppose $M = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$ has $Char(M) = f(x)$. Note that $a \neq 0$ since $f(x)$ is irreducible; otherwise, M would have c and b as eigenvalues. Now $r = Tr(M) = c + b$, so that $c = r - b$. Also, $s = Det(M) = (r-b)b - da$, and so $-da = b^2 - rb + s = f(b)$. Hence $d = f(b)/(-a)$. Therefore $M = M_{(a,b)}$ as claimed. $\square$

Let $f(x) = x^2 - rx + s$ be irreducible in $\mathbb{F}_q[x]$. Let $Q = \mathbb{F}_q^2 \backslash \{[0,0]\}$, written as a set of row vectors. Define a binary operation $\circ_f$ on Q by

$$[a,b] \circ_f [c,d] = [a,b]M_{(c,d)}.$$

Note that

$$\begin{aligned} [a,b] \circ_f [c,d] &= [a(r-d) + bc, \frac{-af(d)}{c} + bd] \qquad && c \neq 0, \\ [a,b] \circ_f [0,d] &= [ad, bd] && c = 0. \end{aligned}$$

It is clear that $\circ_f$ is closed on Q. Indeed, if $[a,b] \circ_f [c,d] = [0,0]$ and $c = 0$, then either both $a = b = 0$ or $d = 0$.

For $c \neq 0$, if $d = 0$, then $ar + bc = \frac{-as}{c} = 0$. Thus, either $a = 0$ implying $b = 0$ or $s = 0$. For $d \neq 0$, we have

$$r - d = \frac{-bc}{a} = -d + r - \frac{s}{d}$$

implying $s = 0$, hence $f(x)$ irreducible, a contradiction. Therefore, $[a,b] \circ_f [c,d] = [0,0]$ *if and only if* either $[a,b] = [0,0]$ or $[c,d] = [0,0]$.

REMARK 3.2. To keep notation clear,

(1) $[x, y]$ denotes an element in Q;
(2) $R_{[x,y]}$ denotes the right translation by $[x, y]$;
(3) $M_{(x,y)}$ denotes the matrix associated with the right translation by $[x, y]$.
(4) maps on Q act on the right (*i.e.* $x\theta$) and maps on $\mathbb{F}_q$ act on the left (*i.e.* $\theta(x)$).

An isomorphic construction can be found in [**9**]. To keep this paper self-contained, we give our own proof of the following.

THEOREM 3.3. *(Hall* [**9**]*)* $(Q, \circ_f)$ *is a loop with identity element* $[0, 1]$ *with* 0 *and* 1 *being the additive and multiplicative identity in* $\mathbb{F}_q$*, respectively.*

PROOF. First note that $R_{(Q,\circ_f)} = \{M_{(a,b)} \mid a, b \in F_q\} \backslash \{M_{(0,0)}\}$ by the definition of $\circ_f$. That is, $R_{[a,b]}$ corresponds uniquely to $M_{(a,b)}$ by construction. Now, by Proposition 2.1, it is enough to show that each $R_{[y,z]}R^{-1}_{[u,v]} = M_{(y,z)}M^{-1}_{(u,v)}$ is fixed-point free.

Let $M_{(y,z)}, M_{(u,v)} \in R_{(Q,\circ_f)}$ and suppose $M_{(y,z)}M^{-1}_{(u,v)}$ has a fixed point. Then, $M_{(y,z)}M^{-1}_{(u,v)}$ has an eigenvalue of 1. Let $g(x) = Char(M_{(y,z)}M^{-1}_{(u,v)})$. Then

$$\begin{aligned} g(x) &= x^2 - Tr(M_{(y,z)}M^{-1}_{(u,v)})x + Det(M_{(y,z)}M^{-1}_{(u,v)}), \\ 0 = g(1) &= 1^2 - Tr(M_{(y,z)}M^{-1}_{(u,v)}) + Det(M_{(y,z)}M^{-1}_{(u,v)}) \\ &= 1 - Tr(M_{(y,z)}M^{-1}_{(u,v)}) + 1. \end{aligned}$$

Thus, $Tr(M_{(y,z)}M^{-1}_{(u,v)}) = 2$. Therefore, $g(x) = x^2 - 2x + 1 = (x-1)^2$. Then, either $M_{(y,z)}M^{-1}_{(u,v)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ or $M_{(y,z)}M^{-1}_{(u,v)}$ is similar to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. In the first case, we have $M_{(y,z)} = M_{(u,v)}$. For the second, suppose $M_{(y,z)} \neq M_{(u,v)}$ and let $P \in GL(2, q)$ such that $PM_{(y,z)}M^{-1}_{(u,v)}P^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then define $A = PM_{(y,z)}P^{-1}$ and $B = PM_{(u,v)}P^{-1}$, so that $AB^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Note that A and B have the same determinant and trace as $M_{(y,z)}$ and $M_{(u,v)}$, respectively and hence $Char(A) = Char(B) = f(x)$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$. Then $[1, 0]A = [1, 1]B$ and $[0, 1]A = [0, 1]B$. Hence $a = e + g, b = f + h, c = g, d = h$. Thus $A = \begin{pmatrix} e+g & f+h \\ g & h \end{pmatrix}$ and since $Tr(A) = Tr(B)$, $g = 0$. Hence, A, B are upper triangular matrices and therefore $Char(A) = f(x)$ is reducible, which is a contradiction. $\square$

LEMMA 3.4. *In* $(Q, \circ_f)$

(i) *for* $a \neq 0$, $R^{-1}_{[a,b]} = M^{-1}_{(a,b)} =$
$$\begin{pmatrix} r-b & \frac{f(b)}{-a} \\ a & b \end{pmatrix}^{-1} = \frac{1}{s}\begin{pmatrix} b & f(b)/a \\ -a & r-b \end{pmatrix} = \frac{1}{s}M_{[-a,r-b]},$$
(ii) $R^{-1}_{[0,b]} = \frac{1}{b}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$,

(iii) $R_{[a,b],[c,d]} = M_{(a,b)}M_{(c,d)}M^{-1}_{[a,b]\circ_f[c,d]} =$
$$\begin{pmatrix} s & \frac{-(a^2sf(d)-abcds-abcd+abcr+acdr-acr^2+acrs+c^2f(b))}{(ac(bc-ad+ar))} \\ 0 & 1 \end{pmatrix},$$

(iv) $R_{[a,b],[0,d]} = M_{(a,b)}M_{(0,d)}M^{-1}_{[a,b]\circ_f[0,d]} = \begin{pmatrix} d^2 & \frac{(d-1)(b-r+bd)}{a} \\ 0 & 1 \end{pmatrix}$,

(v) $R_{[0,b],[c,d]} = M_{(0,b)}M_{(c,d)}M^{-1}_{[0,b]\circ_f[c,d]} = \begin{pmatrix} b^2 & \frac{(b-1)(d-r+bd)}{c} \\ 0 & 1 \end{pmatrix}$ *and*

(vi) $R_{[0,b],[0,d]} = M_{(0,b)}M_{(0,d)}M^{-1}_{[0,b]\circ_f[0,d]} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

PROOF. For (i), simply note
$$\begin{aligned} &[x,y]\begin{pmatrix} r-b & \frac{f(b)}{-a} \\ a & b \end{pmatrix}\begin{pmatrix} r-b & \frac{f(b)}{-a} \\ a & b \end{pmatrix}^{-1} \\ &= [x(r-b)+ay, \frac{-x(f(b))}{a}+by]\begin{pmatrix} \frac{b}{s} & \frac{f(b)}{sa} \\ \frac{-a}{s} & \frac{r-b}{s} \end{pmatrix} \\ &= [x,y]. \end{aligned}$$

Similarly, for (ii). For (iii), using (i), we have
$$M^{-1}_{(a,b)\circ_f(c,d)} = \begin{pmatrix} \frac{\frac{-af(d)}{c}+bd}{s} & \frac{f(\frac{-af(d)}{c}+bd)}{sa} \\ \frac{-(a(r-d)+bc)}{s} & \frac{r-(\frac{-af(d)}{c}+bd)}{s} \end{pmatrix}.$$

Therefore, we have
$$\begin{aligned} &\begin{pmatrix} r-b & \frac{f(b)}{-a} \\ a & b \end{pmatrix}\begin{pmatrix} r-d & \frac{f(d)}{-c} \\ c & d \end{pmatrix}\begin{pmatrix} \frac{\frac{-af(d)}{c}+bd}{s} & \frac{f(\frac{-af(d)}{c}+bd)}{sa} \\ \frac{-(a(r-d)+bc)}{s} & \frac{r-(\frac{-af(d)}{c}+bd)}{s} \end{pmatrix} \\ &= \begin{pmatrix} s & \frac{-(a^2sf(d)-abcds-abcd+abcr+acdr-acr^2+acrs+c^2f(b))}{(ac(bc-ad+ar))} \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

A similar calculation gives (iv). Finally, (v) and (vi) follow from (iv) and Lemma 2.2. □

For a loop Q, x has a *two-sided inverse* if $1/x = x\backslash 1$, denoted x^{-1}. A loop is said to satisfy the *right inverse property* if $(yx)x^{-1} = y \Leftrightarrow R_{x^{-1}} = R_x^{-1}$ for all $x, y \in Q$. Note that a loop Q satisfying RIP has two-sided inverses for all $x \in Q$.

COROLLARY 3.5. $(Q, \circ_f)$ *satisfies RIP* if and only if $s = 1$.

PROOF. This follows quickly from (3.4) (i) and (ii). □

It is well known that the center of $GL(n,q)$ are scalar multiples of I [**19**]. Thus, we have the following:

LEMMA 3.6. $C(Q, \circ_f) = \{[0,b] \mid \forall b \in \mathbb{F}_q\ b \neq 0\}$. *That is, the only elements of* $C(Q, \circ_f)$ *are in the set* $\{R_{[a,b]} \mid [a,b] \in C(Q, \circ_f)\}$. *Moreover,* $C(Q, \circ_f)$ *is a subloop of* $(Q, \circ_f)$.

PROOF. Using Propositions 2.2, 2.4 and the above remark, we are done. □

Now, the loop $(Q, \circ_f)$ has been constructed such that $R_{(Q,\circ_f)}$ is a union of conjugacy classes in $GL(2,q)$, namely the center $Z(GL(2,q))$ (scalar matrices) and the conjugacy class of matrices M with $Char(M) = f(x)$.

THEOREM 3.7. *$(Q, \circ_f)$ is an RCC loop.*

PROOF. Let $[a,b] \in (Q, \circ_f)$. First, if $a \neq 0$ then, it follows from Lemma 3.1 that $R_{[c,d]}R_{[0,b]}R^{-1}_{[c,d]} \in R_{(Q,\circ)}$.

If $a = 0$ then $M_{(0,b)} = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$ and $[0,b] \in C(Q,\circ) \cap N_\lambda(Q,\circ)$ by Lemma 3.6 implying $R_{(0,b)} \in Z(Mlt_\rho(Q,\circ))$ by Proposition 2.2.

Hence, for any $[c,d] \in (Q,\circ)$, $R_{[c,d]}R_{[0,b]}R^{-1}_{[c,d]} = R_{[0,b]}$. □

LEMMA 3.8. *Let $q \neq 3$. Then $C(Q,\circ_f) = N_\lambda(Q,\circ_f)$. If $q = 3$ then $C(Q,\circ_f) =$ $N_\lambda(Q,\circ_f)$* if and only if $r \neq 0$.

PROOF. First, if $q = 2$, then $|(Q,\circ_f)| = 3$ and is an abelian group.

Let $q > 3$ and note that there exists a $d \in \mathbb{F}_q$ such that $d^2 \neq 1$. Suppose $[x,y] \in N_\lambda(Q,\circ_f)$. Then for any $a \in \mathbb{F}_q \backslash \{0\}$,

$$([x,y] \circ_f [a,0]) \circ_f [0,d] = [x,y] \circ_f ([a,0] \circ_f [0,d]),$$

or equivalently, $[x,y]R_{[a,0],[0,d]} = [x,y]$. Hence, by Proposition 3.4(iv), $d^2x = x$. But $d^2 \neq 1$, and thus we have $x = 0$. Therefore $C(Q,\circ_f) = N_\lambda(Q,\circ f)$.

Suppose $q = 3$ and $r \neq 0$ and take $d \neq 1$. Thus Proposition 3.4(iv) gives

$$y - \frac{rx(d-1)}{a} = y.$$

But $r \neq 0$ and hence, $x = 0$. Therefore $C(Q,\circ_f) = N_\lambda(Q,\circ f)$.

Finally, when $q = 3$ and $r = 0$, it can be verified that $C(Q,\circ_f) < N_\lambda(Q,\circ f)$ [**8**, **16**]. □

Our goal is to construct simple RCC loops. Therefore, it is vital to understand the structure of normal subloops of an RCC loop. Let Q be a RCC-loop with $N \trianglelefteq Q$ and consider $R_N = \{R_x \mid x \in N\}$. Fix $x \in N$ and then $\forall y \in Q$, $R_yR_xR_y^{-1} = R_{(yx/y)} \in R_N$ since $yx/y \in N$. Hence, normal subloops of Q correspond to unions of conjugacy classes in R_Q. That is, normal subloops of Q correspond to unions of conjugacy classes of matrices in GL(2,q) which are contained in $R_{(Q,\circ_f)}$. $R_{(Q,\circ_f)}$ itself is the union of conjugacy classes, namely, $\{M_{(a,b)} | a,b \in Q, a,b \neq 0\}$, which has size $q^2 - q$, and the $q-1$ one-element conjugacy classes in the center of $GL(2,q)$. Since the order of a normal subloop of Q must divide $|Q| = q^2 - 1$, we have the following.

LEMMA 3.9. *The only nontrivial normal subloops of $(Q,\circ_f)$ are subloops of $C(Q,\circ_f)$.*

PROOF. Using the above remark, any nontrivial normal subloop must be a union of conjugacy classes with order dividing $q^2 - 1$. However, the possible orders of conjugacy classes in $GL(n,q)$ are $1, q^2 - q, q^2 - 1$ and $q^2 + q$ [**7**]. Thus, the only options are the $q-1$ one-element conjugacy classes and hence, all nontrivial normal subloops are subloops of $C(Q,\circ_f)$ (and hence subgroups since $C(Q) \leq N_\lambda(Q)$ for any RCC loop). □

THEOREM 3.10. *Let $f(x) = x^2 - rx + s$ be irreducible. If $r \neq 0$, then $(Q, \circ_f)$ is simple. If $r = 0$, then $Z(Q, \circ_f) = \{[0, \pm 1]\}$ and $(Q, \circ_f)/Z(Q, \circ_f)$ is simple.*

PROOF. Let $Tr(M_{(a,b)}) \neq 0$ and suppose $(S, \circ_f) \trianglelefteq (Q, \circ_f)$. Then, by Lemma 3.8, $(S, \circ_f) \leq C(Q, \circ_f) = N_\lambda(Q, \circ_f)$. Fix $[0, z] \in (S, \circ_f)$ and let $[0, a], [0, c] \in (Q, \circ_f)$. Then

$$[c, 0] \circ_f ([a, 0] \circ_f [0, z]) = ([c, 0] \circ_f [a, 0]) \circ_f [0, z].$$

Thus, $[cr, \frac{-cs}{az}] = [crz, \frac{-csz}{a}]$. Hence $z = 1$. That is, if

$$(S, \circ_f) \trianglelefteq (Q, \circ_f) \Leftrightarrow (S, \circ_f) = \{[0, 1]\}.$$

Therefore, the only normal subloops are trivial and $(Q, \circ_f)$ is simple.

For $Tr(M_{a,b}) = 0$, let $[a, b], [c, d] \in (Q, \circ_f)$ and $[0, z] \in (S, \circ_f)$ Note that

$$M_{(a,b)} = \begin{pmatrix} -b & \frac{s+b^2}{-a} \\ a & b \end{pmatrix} \qquad M_{(c,d)} = \begin{pmatrix} -d & \frac{s+d^2}{-c} \\ c & d \end{pmatrix}.$$

Now,

$$[c, d] \circ_f ([a, b] \circ_f [0, z]) = ([c, d] \circ_f [a, b]) \circ_f [0, z].$$

implies

$$[z(ad - bc), bdz - \frac{c(b^2z^2 + s)}{az}] = [z(ad - bc), z(bd - \frac{c(b^2 + s)}{a})].$$

This is only solvable when $z = \pm 1$, so $(S, \circ_f) = \{[0, \pm 1]\}$. But

$$\begin{aligned} [a, b] \circ_f ([0, -1] \circ_f [c, d]) &= [a, b] \circ_f [-c, -d] \\ &= [ad - bc, \frac{a(d^2 + s)}{c} - bd] \\ &= [-a, -b] \circ_f [c, d] \\ &= ([a, b] \circ_f [0, -1]) \circ [c, d]. \end{aligned}$$

That is, $[0, -1] \in N_\mu(Q, \circ_f) = N_\rho(Q, \circ_f)$ and $(S, \circ_f) = N_\mu(Q, \circ_f) = N_\rho(Q, \circ_f)$.

Hence $Z(Q, \circ_f) = (S, \circ) = \{[0, \pm 1]\}$ with $(Q, \circ_f)$ not simple. $(Q, \circ_f)/Z(Q, \circ_f)$ is simple, since our computation above would give $z = \pm 1$, but $[0, 1] = [0, -1]$ in $(Q, \circ_f)/Z(Q, \circ_f)$. Thus, the only possible normal subloops are again trivial. $\square$

The following is an example for constructing a simple RCC loop of order 8, from $GL(2, 3)$.

EXAMPLE 3.11. Let $q = 3$, thus elements of $(Q, \circ_f)$ are

$$\{1 = [0, 1], 2 = [0, 2], 3 = [1, 0], 4 = [1, 1], 5 = [1, 2], 6 = [2, 0], 7 = [2, 1], 8 = [2, 2]\}.$$

Take $f(x) = x^2 + 2x + 2$, irreducible in $\mathbb{F}_3$. The conjugacy class of all matrices in $GL(2, 3)$ with characteristic polynomial $f(x)$ are

$$\left\{ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} \right\},$$

with the full set of matrices in $R_{(Q,\circ_f)}$

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} \right\}.$$

Note

$$M_{(0,1)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, M_{(0,2)} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} M_{(1,0)} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \ldots$$

Now, act on elements in $(Q, \circ_f)$ by the matrices above, giving the permutations for $R_{(Q,\circ_f)}$. For example, $M_{(2,2)} = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}$ gives the permutation $(1,8,6,5,2,4,3,7)$ since

$$[0,1]\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} = [2,2], \qquad [0,2]\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} = [1,1], \qquad [1,0]\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} = [2,1],$$
$$[1,1]\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} = [2,1], \qquad [1,2]\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} = [0,2], \qquad [2,0]\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} = [1,2],$$
$$[2,1]\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} = [0,1], \qquad [2,2]\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix} = [2,0].$$

Hence, we have

$$\begin{aligned} R_{(Q,\circ_f)} = \{&(), (1,2)(3,6)(4,8)(5,7), (1,3,4,7,2,6,8,5), (1,4,5,6,2,8,7,3), \\ &(1,5,3,8,2,7,6,4), (1,6,7,4,2,3,5,8), (1,7,8,3,2,5,4,6), \\ &(1,8,6,5,2,4,3,7)\}. \end{aligned}$$

Since $r \neq 0$, $(Q, \circ_f)$ is simple and has the following multiplication table.

TABLE 1. Multiplication table for $(Q, \circ_f)$

$\circ_f$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	6	8	7	3	5	4
3	3	6	4	1	8	5	2	7
4	4	8	7	5	1	2	6	3
5	5	7	1	6	3	8	4	2
6	6	3	8	2	4	7	1	5
7	7	5	2	3	6	4	8	1
8	8	4	5	7	2	1	3	6

4. Isomorphism classes

For $\mathbb{F}_q$, there are $\frac{q^2-q}{2}$ irreducible polynomials of degree 2 over $\mathbb{F}_q$ [**6**]. Hence, it is natural to assume we would create the same number of *nonisomorphic* RCC loops for a given q. This turns out not to be the case. For example, when $q = 4$, there are 6 irreducible polynomials over $\mathbb{F}_4$ and we create 6 RCC loops associated to each polynomial. However, only 3 are nonisomorphic, each simple. For $q = 8$, we have only 10 nonisomorphic RCC loops, instead of 28 we can construct. Recently, all RCC loops of order $n \leq 31$ have been classified [**1**], and included in the GAP library up to $n \leq 27$. Our construction is exhaustive for simple RCC loops for $n \leq 15$ [**1, 8, 14, 16**]. However, there are 6 simple RCC loops of order 24 whose right multiplication group is $GL(2,3) \times S_3$ and one of order 27, whose right multiplication group is $S_3 \times S_3 \times S_3$, all differing from this construction.

The following table gives a count of RCC loops constructed from $GL(2,q)$, including the simple loops of the form $(Q, \circ_f)/Z(Q, \circ_f)$ when $r = 0$. Note that RCC loops of order p a prime are groups [**4**].

TABLE 2. RCC loops constructed

Order	q	RCC loops constructed	Nonisomorphic	Nonisom. and simple	Exhaustive
8	3	3	3	2	✓
12	5	2	2	2	✓
15	4	6	3	3	✓
24	5,7	10,3	13	11	×
40	9	2	2	2	
48	7	21	21	18	
60	11	5	5	5	
63	8	28	10	10	
80	9	36	18	16	
84	13	6	6	6	
120	11	55	55	50	
168	13	78	78	72	
255	16	120	30	30	

We now describe the isomorphism classes for this construction. It is well-known that $\alpha \in \mathrm{Aut}(\mathbb{F}_q) \Leftrightarrow \alpha(x) = x^{p^i}$ for $0 \leq i \leq n$, the Frobenius automorphisms. Note that if $f(x) = x^2 - rx + s$ is irreducible, then $g(x) = x^2 - r^{p^i}x + s^{p^i}$ is irreducible as well.

LEMMA 4.1. *Let $f(x) = x^2 - rx + s$ be irreducible, $\beta(x)$ be an automorphism of $\mathbb{F}_q$ and $T \in \mathbb{F}_q^*$. If $g(x) = x^2 - \beta(r) + \beta(s)$, then $\phi : (Q, \circ_f) \to (Q, \circ_g)$ is an isomorphism with $[a,b]\phi = [T\beta(a), \beta(b)]$.*

PROOF. Clearly, ϕ is a bijection. Now,

$$\begin{aligned}([a,b] \circ_f [0,d])\phi &= [ad, bd]\phi = [T\beta(ad), \beta(bd)] \\ &= [T\beta(a)\beta(d), \beta(b)\beta(d)] = [T\beta(a), \beta(b)] \circ_g [0, \beta(d)] \\ &= [a,b]\phi \circ_g [0,d]\phi.\end{aligned}$$

Else,

$$\begin{aligned}&([a,b] \circ_f [c,d])\phi \\ &= [a(r-d) + bc, \frac{-af(d)}{c} + bd]\phi \\ &= [T\beta(a(r-d)+bc), \beta(\frac{-af(d)}{c} + bd)] \\ &= [T\left(\beta(a)(\beta(r) - \beta(d)) + \beta(bc)\right), \frac{-\beta(a)\beta(f(d))}{\beta(c)} + \beta(bd)] \\ &= [T\left(\beta(a)(\beta(r) - \beta(d)) + \beta(bc)\right), \frac{-\beta(a)\beta(d^2 - rd + s)}{\beta(c)} + \beta(bd)] \\ &= [T\left(\beta(a)(\beta(r) - \beta(d)) + \beta(bc)\right), \frac{-\beta(a)(\beta(d^2) - \beta(r)\beta(d) + \beta(s))}{\beta(c)} + \beta(bd)] \\ &= [T\beta(a)(\beta(r) - \beta(d)) + \beta(b)\beta(c), \frac{-T\beta(a)g(\beta(d))}{T\beta(c)} + \beta(b)\beta(d)] \\ &= [T\beta(a), \beta(b)] \circ_g [T\beta(c), \beta(d)] \\ &= [a,b]\phi \circ_g [c,d]\phi.\end{aligned}$$

□

LEMMA 4.2. *Let* $f(x) = x^2 - r_1x + s_1$ *and* $g(x) = x^2 - r_2x + s_2$ *be irreducible in* $\mathbb{F}_q[x]$. *If* $\phi : (Q, \circ_f) \to (Q, \circ_g)$ *is an isomorphism then* $[a, b]\phi = [T\beta(a), \beta(b)]$ *for some* $\beta \in \mathrm{Aut}(\mathbb{F}_q)$ *and* $T \in \mathbb{F}_q^*$, *and* $\beta(r_1) = r_2$ *and* $\beta(s_1) = s_2$.

PROOF. Since ϕ is an isomorphism, ϕ maps $C(Q, \circ_f)$ to $C(Q, \circ_g)$, *i.e.* for all $b \in \mathbb{F}_q^*, [0, b]\phi = [0, y]$ for some $, y \in \mathbb{F}_q^*$. Moreover, $[0, ab]\phi = ([0, a] \circ_f [0, b])\phi = [0, a]\phi \circ_g [0, b]\phi$. So, ϕ is a automorphism of $\mathbb{F}_q^*$ on the second slot, say β, with β of the form $\beta(x) = x^k$ for some k ($\mathbb{F}_q^*$ cyclic).

Now suppose $[a, b]\phi = [x, y]$, $[a, c]\phi = [x', z]$, and $[1, 0]\phi = [u, 0]$ for some $a, b, c, x, x', y, z, u \in \mathbb{F}_q$. Then

$$\begin{aligned}([a, b] \circ_f [1, 0])\phi &= [ar_1 + b, -as_1]\phi = [w, (-as_1)^k] \\ &= [xr_2 + yu, \frac{-xs_2}{u}] = [x, y] \circ_g [u, 0] = [a, b]\phi \circ_g [1, 0]\phi, \\ ([a, c] \circ_f [1, 0])\phi &= [ar_1 + c, -as_1]\phi = [w', (-as_1)^k] \\ &= [x'r_2 + zu, \frac{-x's_2}{u}] = [x', z] \circ_g [u, 0] = [a, c]\phi \circ_g [1, 0]\phi.\end{aligned}$$

Hence, $\dfrac{-xs_2}{u} = (-as_1)^k = \dfrac{-x's_2}{u}$, thus $x = x'$. That is, $[a, b]\phi = [\alpha(x), \beta(b)]$ for some bijection α with $\alpha(0) = 0$.

Now,

$$\begin{aligned}[\alpha(ab), 0] = [ab, 0]\phi &= ([a, 0] \circ_f [0, b])\phi = [a, 0]\phi \circ_g [0, b]\phi \\ &= [\alpha(a), 0] \circ_g [0, \beta(b)] = [\alpha(a)\beta(b), 0].\end{aligned}$$

Hence $\alpha(a)\beta(b) = \alpha(ab)$. Setting $a = 1$ with $\alpha(1) = T$ for some $T \in \mathbb{F}_q^*$, we have $\alpha(b) = \alpha(1)\beta(b) = T\beta(b)$ for all $b \in \mathbb{F}_q$.

Moreover,

$$\begin{aligned}([1, 0] \circ_f [1, 0])\phi = [r_1, s_1]\phi &= [Tr_1^k, s_1^k], \\ [1, 0]\phi \circ_g [1, 0]\phi = [T, 0] \circ_g [\alpha(1), 0] &= [Tr_2, s_2].\end{aligned}$$

Thus, $r_1^k = r_2$ and $s_1^k = s_2$. Considering the second slot for

$$([a, b] \circ_f [a, b])\phi = [a, b]\phi \circ_g [a, b]\phi,$$

we have $(r_1b - s_1)^k = r_2b^k - s_2 = r_1^kb^k - s_1^k$. Setting $b = \frac{c+d+s_1}{r_1}$ for any c, d, we have $(c + d)^k = (c + d + s_1)^k - s_1^k$. Hence, $\beta(x) = x^{p^i}$ is a Frobenius map, that is, $\beta \in \mathrm{Aut}(\mathbb{F}_q)$.

□

Hence, isomorphism of $(Q, \circ_f)$ correspond exactly to automorphisms of $\mathbb{F}_q$. Note that $|\mathrm{Aut}(\mathbb{F}_q)| = n$ for $q = p^n$, and hence one would expect the number of nonisomorphic RCC loops constructed to be $\frac{q^2-q}{2n}$. However, it is sometimes the case that $\frac{q^2-q}{2n} \notin \mathbb{N}$. Therefore, we have the following.

THEOREM 4.3. *Let* p *be a prime number and* $q = p^n$. *The number of nonisomorphic RCC loops constructed from* $GL(2, q)$ *is* $\left\lfloor \frac{q^2-q}{2n} \right\rfloor + \left(\frac{q^2-q}{2} \mod n \right)$.

PROOF. This follows quickly from Lemmas 4.1 and 4.2, along the above note.

□

Hence, we construct $\frac{p^2-p}{2}$ distinct RCC loops from $\mathbb{F}_p$, $\frac{p^4-p^2}{4}$ distinct RCC loops from $\mathbb{F}_{p^2}$, etc. For $\mathbb{F}_8$, $\frac{8^2-8}{6} \notin \mathbb{N}$, so we have $\left\lfloor \frac{8^2-8}{6} \right\rfloor = 9$ and $\left(\frac{8^2-8}{2} \mod 3\right) = 1$, and thus we have $9+1=10$ nonisomorphic RCC loops.

Lastly, we consider

QUESTION 4.4. *What group is $Mlt_\rho(Q, \circ_f)$?*

We have $Mlt_\rho(Q) = \mathrm{Inn}_\rho(Q) \cdot R_Q$. Indeed, for $\theta \in \mathrm{Mlt}_\rho(Q)$ set $a = 1\theta$. Then $\psi = \theta R_a^{-1}$ fixes 1, hence is an element of $\mathrm{Inn}_\rho(Q)$. Therefore, $\theta = \psi R_a$ and since $\mathrm{Inn}_\rho(Q) \cap R_Q = \iota$, we have the factorization.

CONJECTURE 4.5. $\mathrm{Inn}_\rho(Q, \circ_f) = \{\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \mid x = a^2 s^m \quad a, y \in \mathbb{F}_q \quad m \in \mathbb{Z}\}$.

We know x must have this form from Lemma 3.4. The question is whether we can have any value for $y \in \mathbb{F}_q$. We do have the following.

LEMMA 4.6. *Let $H = \{\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \mid x, y \in \mathbb{F}_q\}$. Then $GL(2,q) = R_{(Q,\circ_f)} \cdot H$.*

PROOF. Note that $|R_{(Q,\circ_f)}| = q^2 - 1$ and $|H| = q(q-1)$. We have $|GL(2,q)| = (q^2-1)(q^2-q) = q(q+1)(q-1)^2 = |R_Q||H|$. Since $R_{(Q,\circ_f)} \cap H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, we have the desired result. □

Hence, Question 4.4 reduces to what subgroups of H can occur as $\mathrm{Inn}_\rho(Q, \circ_f)$? Note that in some cases $H = \mathrm{Inn}_\rho(Q, \circ_f)$.

Acknowledgments

Some investigations in this paper were assisted by the finite model builder MACE4 developed by McCune [**14**]. Similarly, all presented examples were verified using the GAP system [**8**] together with the LOOPS package [**16**]. We also thank the anonymous referee for several comments that improved the manuscript.

References

[1] K. Artic, *On conjugacy closed loops and conjugacy closed loop folders,* PhD thesis, RWTH Aachen University, 2015.

[2] A. S. Basarab, *A class of* LK*-loops* (Russian), Mat. Issled. **120** (1991), 3–7, 118. MR1121425

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

[4] Aleš Drápal, *On multiplication groups of left conjugacy closed loops*, Comment. Math. Univ. Carolin. **45** (2004), no. 2, 223–236. MR2075271

[5] A. Drápal, *On left conjugacy closed loops with a nucleus of index two*, Abh. Math. Sem. Univ. Hamburg **74** (2004), 205–221, DOI 10.1007/BF02941536. MR2112832

[6] David S. Dummit and Richard M. Foote, *Abstract algebra*, 3rd ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR2286236

[7] W. Fulton and J. Harris, *Representation Theory. A First Course*, **129**, Springer Verlag Graduate Texts in Mathematics, 1996.

[8] The GAP Group, *Groups, Algorithms, and Programming*, http://www.gap-system.org (2008).

[9] Marshall Hall Jr., *Finite projective planes*, Amer. Math. Monthly **62** (1955), no. 7, 18–24, DOI 10.2307/2308176. MR0073214

[10] Marshall Hall Jr., *The theory of groups*, The Macmillan Co., New York, N.Y., 1959. MR0103215

[11] Kenneth W. Johnson, Michael K. Kinyon, Gábor P. Nagy, and Petr Vojtěchovský, *Searching for small simple automorphic loops*, LMS J. Comput. Math. **14** (2011), 200–213, DOI 10.1112/S1461157010000173. MR2831230

[12] István Matievics, *Geometries over universal left conjugacy closed quasifields*, Geom. Dedicata **65** (1997), no. 2, 127–133, DOI 10.1023/A:1017992531922. MR1451967

[13] Gábor P. Nagy, *A class of finite simple Bol loops of exponent 2*, Trans. Amer. Math. Soc. **361** (2009), no. 10, 5331–5343, DOI 10.1090/S0002-9947-09-04646-7. MR2515813

[14] W.W. McCune, *Prover9, Mace4*, http://www.cs.unm.edu/˜mccune/prover9/ (2009).

[15] Péter T. Nagy and Karl Strambach, *Loops as invariant sections in groups, and their geometry*, Canad. J. Math. **46** (1994), no. 5, 1027–1056, DOI 10.4153/CJM-1994-059-8. MR1295130

[16] G.P. Nagy and P. Vojtěchovský, *Loops: Computing withquasigroups and loops*, http://www.math.du.edu/loops (2008).

[17] S. B. Nesbitt-Stobert and C. W. L. Garner, *A direct proof that all Hall planes of the same finite order are isomorphic* (English, with German summary), Riv. Mat. Univ. Parma (4) **12** (1986), 241–247 (1987). MR913046

[18] Hala O. Pflugfelder, *Quasigroups and loops: introduction*, Sigma Series in Pure Mathematics, vol. 7, Heldermann Verlag, Berlin, 1990. MR1125767

[19] Joseph J. Rotman, *An introduction to the theory of groups*, 4th ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995. MR1307623

Department of Mathematics, One Harrison Plaza, University of North Alabama, Florence, Alabama 35632

Email address: mgreer@una.edu