Constructing right conjugacy closed loops

Mark Greer

Department of Mathematics

Fourth Mile High Conference
1 August 2017

Definition

For a loop Q, we define:

left and right translations of a by x	$aL_x = xa \qquad aR_x = ax$
right section of Q	$R_Q = \{R_x \mid x \in Q\}$
right multiplication group of Q	$\mathrm{Mlt}_\rho(Q) = \langle R_Q \rangle$
multiplication group of Q	$\mathrm{Mlt}(Q) = \langle L_x, R_x \mid \forall x \in Q \rangle$
inner mapping group of Q	$\mathrm{Inn}(Q) = \{\theta \in \mathrm{Mlt}(Q) \mid 1\theta = 1\}$

Definition

A subset S of a group G is *closed under conjugation* if $x^{-1}yx \in S$ for all $x, y \in S$.

Defintion

A loop Q is a *right conjugacy closed loop* (or RCC loop) if R_Q is closed under conjugation.

Note: $R_x^{-1} R_y R_x \in R_Q$ for all $x, y \in Q$.

Proposition

For a loop Q, the following are equivalent:

(1) Q is an RCC loop,

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

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

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

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

Definition

For a loop Q, a subset S of Q is a subloop if $(S, \cdot, \backslash, /)$ is a loop. A subloop N of a loop Q is a *normal subloop*, $N \trianglelefteq Q$, if it is invariant under $\mathrm{Inn}(Q)$.

Definitions

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,	$Z(Q) = N(Q) \cap C(Q)$.

Proposition

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

Proposition

Let Q be a RCC loop. Then

(i) $N_\mu(Q) = N_\rho(Q) \trianglelefteq Q$ and

(ii) $C(Q) \leq N_\lambda(Q)$.

Setup

Let $\mathbb{F}_q$ be the finite field of order where $q = p^n$ for a prime p and some $n > 0$. Take $f(x) = x^2 - rx + s$ 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: 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 $a \neq 0$.

Theorem (Hall, Artic & Hiss, G.)

Let $f(x) = x^2 - rx + s$ be irreducible in $\mathbb{F}_p[x]$. 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

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

Then $(Q, \circ_f)$ is a loop.

Note: In $(Q, \circ_f)$, we have

(i) $[a,b] \circ_f [c,d] = [a(r-d)+bc, \frac{-af(d)}{c} + bd] \qquad c \neq 0,$

(ii) $[a,b] \circ_f [c,d] = [ad, bd] \qquad c = 0,$

Elements

Let $q = 3$ and so the elements of $(Q, \circ_f)$ are

$$\{[0,1],[0,2],[1,0],[1,1],[1,2],[2,0],[2,1],[2,2]\}.$$

Conjugacy Class

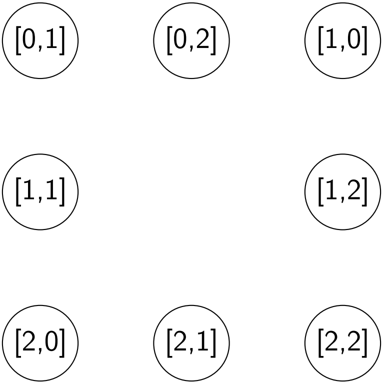
Let $f(x) = x^2 + 2x + 2$, irreducible in $\mathbb{F}_3$.

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

Full Set of Matrices

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

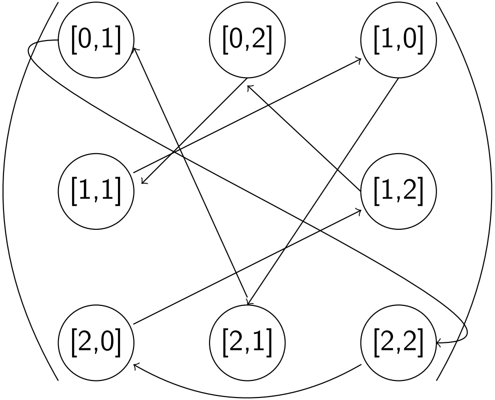
Visualizing the construction



Visualizing the construction

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

Visualizing the construction



$$\begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}$$

Right Section

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

Loop $(Q, \circ_f)$

$\circ_f$	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

Table: Multiplication Table for $(Q, \circ_f)$

Lemma (G.)

In $(Q, \circ_f)$

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

(ii) $R_{[0,b]}^{-1} = \frac{1}{b}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$,

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

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

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

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

Theorem (Artic & Hiss, G.)

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

Lemma

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

Lemma (G.)

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

Note:

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 $\forall y \in Q$, $R_y R_x R_y^{-1} = R_{(yx/y)} \in R_N$ since $yx/y \in N$. Hence, normal subloops of Q correspond to unions of conjugacy classes in R_Q.

Note

Since 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 $|Q| = q^2 - 1$.

Lemma (G.)

The only non-trivial normal subgroups of $(Q, \circ_f)$ are $C(Q, \circ_f)$ and $\{[0,1],[0,-1]\}$.

Theorem (G.)

Let $f(x) = x^2 - rx + s$ be irreducible.

(i) If $r \neq 0$, then $(Q, \circ_f)$ is simple.

(ii) If $r = 0$, then $Z(Q, \circ_f) = \{[0, \pm 1]\}$ and $(Q, \circ_f)/Z(Q, \circ_f)$ is simple.

Irreducible Polynomials

For $\mathbb{F}_q$, there are $\dfrac{q^2 - q}{2}$ irreducible polynomials (degree 2).

- $q = 3$, $\dfrac{3^2 - 3}{2} = 3$ and there are 3 nonisomorphic RCC loops constructed.
- $q = 4$, $\dfrac{4^2 - 4}{2} = 6$ and there are 3 nonisomorphic RCC loops constructed.
- $q = 8$, $\dfrac{8^2 - 8}{2} = 28$ and there are 10 nonisomorphic RCC loops constructed.

Theorem

Let $f(x) = x^2 - r_1 x + s_1$ and $g(x) = x^2 - r_2 x + s_2$ be irreducible in $\mathbb{F}_q[x]$. Then $\phi : (Q, \circ_f) \to (Q, \circ_g)$ is an isomorphism *if and only if* $[a, b]\phi = [\alpha(a), \alpha(b)]$ for some $\alpha \in \mathrm{Aut}(\mathbb{F}_q)$.

Theorem

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

Exhausted Search

- This construction gives all simple RCC loops of order ≤ 15.
- (Artic) There are 471,995 RCC loops of order 24, with 17 simple.
- This construction gives 10 RCC loops from matrices in $GL(2,5)$ and 3 RCC loops from matrices in $GL(2,7)$, with 11 simple.
- The other 6 have $\mathrm{Mlt}\rho(Q) = GL(2,3) \times S_3$.

THANKS!