Math. Proc. Camb. Phil. Soc. (2010), **149**, 445
doi:10.1017/S0305004110000393
First published online 19 July 2010

Catalan loops

BY LING LONG AND JONATHAN D. H. SMITH
Department of Mathematics, Iowa State University, Ames, Iowa 50011, *U.S.A.*
e-mail: linglong@iastate.edu, jdhsmith@iastate.edu

(*Received* 11 *November* 2009; *revised* 4 *May* 2010)

Abstract

Motivated by a problem from number theory about the relationship between Fermat curves and modular curves, a new class of loops is introduced, the Catalan loops. In the number-theoretic context, these loops turn out to be abelian precisely when the Fermat curves and modular curves coincide. General Catalan loops arise on certain transversals to diagonal subgroups in special linear groups over rings with a topologically nilpotent element. The transversals consist of products of certain affine shears. In a Catalan loop, the multiplication and right division are given by rational functions. The left division is algebraic, corresponding to a quadratic irrationality. The left division embodies generating functions for the Catalan numbers. Structurally, Catalan loops are shown to be residually nilpotent.

1. *Introduction*

Let R be a commutative, unital ring with a topologically nilpotent element e. Define

$$Q = \left\{ \begin{bmatrix} 1 & ex \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ ex' & 1 \end{bmatrix} \;\middle|\; x, x' \in R \right\}.$$

Then Q is a right transversal to the diagonal subgroup

$$H = \{\mathrm{diag}(d, d^{-1}) \mid d \in R^*\}$$

of SL(2, R). The topic of this paper is the loop structure defined on Q, a so-called *Catalan loop*. These structures arose initially from an issue in number theory, concerning the relationship between certain Fermat curves and modular curves. In that context, the ring R is $\mathbb{Z}/2^{n+1}\mathbb{Z}$ for $n > 0$, with $e = 2$. The motivating number-theoretic problem is described in Section 2 (which may be skipped by readers interested mainly in the actual loops). Section 3 recalls the way that right loops, and possibly two-sided loops, arise when one takes a quotient of a group by a subgroup which is not necessarily normal. Section 4 shows that with Q and H as above, the product $G = QH$ is a group in which Q is a right transversal to H. The Catalan loop structure on Q is then exhibited in Section 5. In particular, Proposition 5·4 shows how the generating function for the Catalan numbers arises within these loops. The final section examines the structure of Catalan loops, including a factorization (Proposition 6·1) and a proof of their residual nilpotence (Theorem 6·2).

2. *Number-theoretic motivation*

For an element e of a commutative, unital ring R, consider the exact sequence

$$1 \longrightarrow \Gamma(e) \hookrightarrow \mathrm{SL}(2, R) \longrightarrow \mathrm{SL}(2, R/eR) \longrightarrow 1 \tag{2·1}$$

of groups that is induced by the ring homomorphism

$$R \longrightarrow R/eR; x \longmapsto x + eR\,.$$

In particular, $\Gamma(2)$ is the subgroup

$$\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Z}) \;\middle|\; 2 \big| b, c \right\}$$

of $\mathrm{SL}(2, \mathbb{Z})$. Via the action of $\mathrm{SL}(2, \mathbb{Z})$ by linear fractional transformations on the upper half plane $\{\tau \in \mathbb{C} \mid \Im(\tau) > 0\}$, the field of meromorphic functions for $\Gamma(2)$ is generated by the classical modular lambda function

$$\begin{aligned} \lambda(\tau) &= 16q \prod_{n \geqslant 1} [(1 + q^{2n})^2 (1 - q^{2n-1})]^8 \\ &= 16q \left(1 - 8q + 44q^2 - 192q^3 + 718q^4 + \cdots\right) \end{aligned}$$

with $q = \exp(2\pi i \tau)$. The group $\Gamma(2)$ is free on the generators

$$\gamma_\infty = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \gamma_0 = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$$

[**4**, section 6·5]. For a fixed integer $r > 1$, define subgroups $G_1(r)$ and $G_2(r)$ as the respective kernels of the homomorphisms to the circle group S^1 given by

$$\chi_\infty : \Gamma(2) \longrightarrow S^1; \gamma_\infty \longmapsto 1\,,\ \gamma_0 \longmapsto \exp(2\pi i/r) \tag{2·2}$$

and

$$\chi_0 : \Gamma(2) \longrightarrow S^1; \gamma_\infty \longmapsto \exp(2\pi i/r)\,,\ \gamma_0 \longmapsto 1\,. \tag{2·3}$$

Define the *Fermat group* $\Phi(r) = G_1(r) \bigcap G_2(r)$. Set $x = \sqrt[r]{\lambda}$ and $y = \sqrt[r]{1 - \lambda}$. The field of meromorphic functions for $G_1(r)$ is generated by x over $\mathbb{C}(\lambda)$, while that for $G_2(r)$ is correspondingly generated by y. It follows that the Fermat curve

$$x^r + y^r = 1 \tag{2·4}$$

is biholomorphic to the modular curve for the Fermat group $\Phi(r)$.

For each positive integer n, the Fermat group $\Phi(2^n)$ is closely related to the subgroup

$$\Gamma_0(2^{2n+2}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Z}) \;\middle|\; 2^{2n+2} \big| c \right\}$$

of $\mathrm{SL}(2, \mathbb{Z})$. As recalled by Tu and Yang [**6**], Hashimoto observed that the Fermat curve (2·4) with $r = 2^n$ and the modular curve $X_0(2^{2n+2})$ for $\Gamma_0(2^{2n+2})$ have the same genus. When $n = 1$, both $\Phi(2)$ and $\Gamma_0(16)$ are isomorphic to the level 4 principal congruence subgroup $\Gamma(4)$. When $n = 2$, the modular curve $X_0(2^{2n+2})$ has the defining equation

$$x^4 + y^4 = z^4$$

with homogeneous coordinates in the complex projective plane [**6**]. For $n > 2$, Tu and Yang show that the Fermat curve and the modular curve $X_0(2^{2n+2})$ have distinct automorphism

groups. Thus they identify the investigation of the relationship between the two families of curves as an "interesting problem."

It turns out to be more convenient to work with the conjugate

$$\Gamma_0^0(2^{n+1}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \;\middle|\; 2^{n+1} | b, c \right\}$$

of $\Gamma_0(2^{2n+2})$. Note that $\Gamma_0^0(2^{n+1})$ is a subgroup of $\Gamma(2)$. Unlike $\Phi(2^n)$, however, $\Gamma_0^0(2^{n+1})$ is not a normal subgroup of $\Gamma(2)$ for $n > 1$. Defining

$$\Gamma_2(n) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(2) \;\middle|\; 2^{n+1} | c \right\}$$

and

$$\Gamma_1(n) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(2) \;\middle|\; 2^{n+1} | b \right\},$$

we have

$$\Gamma_0^0(2^{n+1}) = \Gamma_1(n) \cap \Gamma_2(n).$$

The set

$$Q = \{\gamma_\infty^k \gamma_0^l \mid 0 \leqslant k, l < 2^n\}$$

is a transversal to $\Gamma_0^0(2^{n+1})$ in $\Gamma(2)$. By the First Isomorphism Theorem applied to the product

$$\chi_\infty \times \chi_0 : \Gamma(2) \longrightarrow S^1 \times S^1$$

of the characters χ_∞ and χ_0 of (2·2)–(2·3), Q inherits the quotient abelian group structure $\Gamma(2)/\Phi(2^n) \cong (\mathbb{Z}/2^n\mathbb{Z})^2$. Interpreted as the homogeneous space $\Gamma_0^0(2^{n+1})\backslash\Gamma(2)$, however, Q has the structure of a Catalan loop. In particular, this loop is not abelian whenever $n > 2$ (Corollary 6·3), precisely in the cases where the Fermat curve and the modular curve are distinct.

3. *Right loops*

A *right quasigroup* $(Q, \cdot, /)$ is a set Q equipped with binary operations of *multiplication* (denoted by $x \cdot y$ or simple juxtaposition xy) and *right division* x/y such that

$$(x \cdot y)/y = x = (x/y) \cdot y$$

for x, y in Q. A *right loop* $(Q, \cdot, /, 1)$ is a right quasigroup $(Q, \cdot, /)$ with an *identity element* 1 such that $1 \cdot x = x = x \cdot 1$ for x in Q. In a right loop $(Q, \cdot, /, 1)$, the ternary derived operation

$$(x, y, z)P = (x/y) \cdot z \tag{3·1}$$

satisfies

$$(x, x, y)P = y = (y, x, x)P$$

for x, y in Q [**9**, p. 101]. It thus forms a *Mal'tsev parallelogram* in the sense of [**7**]. Note that the multiplication and right division may be recovered from the Mal'tsev parallelogram by

$$x \cdot y = (x, 1, y)P \quad \text{and} \quad x/y = (x, y, 1)P \tag{3·2}$$

for x, y in Q. A right loop $(Q, \cdot, /, 1)$ is a (*two-sided*) *loop* if the equation

$$x \cdot y = z \tag{3·3}$$

has a unique solution y in Q for each choice of x and z in Q.

Groups are right loops, with $x/y = xy^{-1}$ and $(x, y, z)P = xy^{-1}z$. Now suppose that Q is a right transversal to a subgroup H of a group G. Then a right quasigroup structure $(Q, *, ||)$ is defined by

$$tu \in H \cdot (t * u) \quad \text{and} \quad tu^{-1} \in H \cdot (t||u) \tag{3·4}$$

for t, u in Q. The transversal Q is said to be *normalized* if the subgroup H itself is represented in Q by the identity element 1 of the group G. In this case, the transversal forms a right loop $(Q, *, ||, 1)$ [**8**, proposition 2·2], [**9**, proposition I·4·3·3]. The Mal'tsev parallelogram (3·1) is defined directly by

$$tu^{-1}v \in H \cdot (t, u, v)P \tag{3·5}$$

for t, u, v in Q.

4. *Right transversals*

Let R be a commutative, unital ring, with group R^* of invertible elements. Let e be an element of R such that R is complete in the (eR)-adic topology. Thus $\bigcap_{n=1}^{\infty}(eR)^n = \{0\}$, and $1 + eR \subseteq R^*$ [**1**, section II·6], [**2**, section 2·6]. One might choose e as a nilpotent element of R, or as X in the formal power series ring $R = S[[X]]$ over a ring S. Let E be the annihilator of e in R. Let H be the subgroup of diagonal matrices in $\mathrm{SL}(2, R)$. Consider the set

$$Q = \left\{ \begin{bmatrix} 1 & ex \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ ex' & 1 \end{bmatrix} \;\middle|\; x, x' \in R \right\}.$$

Define $G = HQ$. Note that G contains H, and reduces to H if $e = 0$. It will be shown that G is a subgroup of $\mathrm{SL}(2, R)$. To that end, it is helpful to record the following elementary observation.

LEMMA 4·1. *Consider matrices*

$$A_i = \begin{bmatrix} a_i & b_i \\ c_i & d_i \end{bmatrix}$$

in $\mathrm{SL}(2, R)$*, with* d_i *invertible for* $i = 1, 2$*. If* $b_1 = b_2$*,* $c_1 = c_2$*, and* $d_1 = d_2$*, then* $A_1 = A_2$*.*

Proof. Since $\det A_i = a_i d_i - b_i c_i = 1$, we have

$$a_1 = d_1^{-1}(1 + b_1 c_1) = d_2^{-1}(1 + b_2 c_2) = a_2,$$

completing the desired equality $A_1 = A_2$.

PROPOSITION 4·2. *The set* $G = HQ$ *forms a subgroup of* $\mathrm{SL}(2, R)$.

Proof. Since the group $\Gamma(e) =$

$$\left\{ \begin{bmatrix} 1 + er_{11} & er_{12} \\ er_{21} & 1 + er_{22} \end{bmatrix} \;\middle|\; r_{ij} \in R \right\}$$

of (2·1) is normal, the subset $H\Gamma(e)$ of $\mathrm{SL}(2, R)$ is a subgroup. It will be shown that $G = H\Gamma(e)$. Certainly Q is a subset of $\Gamma(e)$, so $G = HQ \subseteq H\Gamma(e)$. For the converse direction,

note that elements of G take the form

$$\begin{bmatrix} d & 0 \\ 0 & d^{-1} \end{bmatrix} \begin{bmatrix} 1 & ex \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ ex' & 1 \end{bmatrix} = \begin{bmatrix} d(1+e^2xx') & dex \\ d^{-1}ex' & d^{-1} \end{bmatrix} \tag{4·1}$$

with $d \in R^*$ and $x, x' \in R$. To express the typical element of $\Gamma(e)$ in such a form, namely

$$\begin{bmatrix} 1+er_{11} & er_{12} \\ er_{21} & 1+er_{22} \end{bmatrix} = \begin{bmatrix} d(1+e^2xx') & dex \\ d^{-1}ex' & d^{-1} \end{bmatrix}, \tag{4·2}$$

it suffices to take

$$d = (1+er_{22})^{-1}, \tag{4·3}$$

$$x = d^{-1}r_{12} = r_{12}(1+er_{22}) \quad \text{and} \tag{4·4}$$

$$x' = dr_{21} = r_{21}(1+er_{22})^{-1}. \tag{4·5}$$

This ensures the agreement of all but the top left entries of (4·2). The full equality then follows by Lemma 4·1.

We will write

$$\mathbf{x} = \langle x, x' \rangle = \begin{bmatrix} 1 & ex \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ ex' & 1 \end{bmatrix} = \begin{bmatrix} 1+e^2xx' & ex \\ ex' & 1 \end{bmatrix}$$

for elements of Q. Observe that in this notation, $\langle x, x' \rangle = \langle y, y' \rangle$ if and only if $x - y$ and $x' - y'$ annihilate e.

PROPOSITION 4·3. *The set Q forms a normalized right transversal to the subgroup H in G.*

Proof. First note $(0, 0) = I_2$. Now suppose that $\langle x, x' \rangle \langle y, y' \rangle^{-1}$ lies in H. Computing

$$\begin{bmatrix} 1 & ex \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ ex' & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -ey' & 1 \end{bmatrix} \begin{bmatrix} 1 & -ey \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} \dots & e(x-y) - e^2xy \cdot e(x'-y') \\ e(x'-y') & \dots \end{bmatrix} = \begin{bmatrix} d & 0 \\ 0 & d^{-1} \end{bmatrix}$$

(for some d in R^*), comparison of the final two bottom left entries shows that $ex' = ey'$. Given this, comparison of the final top right entries shows that $ex = ey$. Thus $\langle x, x' \rangle = \langle y, y' \rangle$.

5. *Catalan loops*

Consider the right loop $(Q, \cdot, /, 1)$ that is defined by (3·4) on the normalized transversal Q of Proposition 4·3. It is known as the *Catalan loop*, the name being motivated by Proposition 5·4.

PROPOSITION 5·1. *Let $\mathbf{x} = \langle x, x' \rangle$, $\mathbf{y} = \langle y, y' \rangle$, and $\mathbf{z} = \langle z, z' \rangle$ be elements of Q. Suppose that $\mathbf{p} = \langle p, p' \rangle$ is the Mal'cev parallelogram $(\mathbf{x}, \mathbf{y}, \mathbf{z})P$ in the Catalan loop. Then*

$$p = x\lambda^2 - (y-z)\lambda \quad \textit{and} \tag{5·1}$$

$$p' = (x'-y')\lambda^{-1} + z' \tag{5·2}$$

with $\lambda = 1 - e^2(y-z)(x'-y')$.

Proof. By (3·5), the Mal'tsev parallelogram is given by $\mathbf{x}\mathbf{y}^{-1}\mathbf{z}\mathbf{p}^{-1} \in H$. In other words, the matrix $D =$

$$\begin{bmatrix} 1+e^2xx' & ex \\ ex' & 1 \end{bmatrix}\begin{bmatrix} 1 & -ey \\ -ey' & 1+e^2yy' \end{bmatrix}\begin{bmatrix} 1+e^2zz' & ez \\ ez' & 1 \end{bmatrix}\begin{bmatrix} 1 & -ep \\ -ep' & 1+e^2pp' \end{bmatrix}$$

is diagonal. The equation $D_{21} = 0$ becomes

$$[1+e^2z(z'-p')](x'-y') + [1-e^2y(x'-y')](z'-p') \equiv 0 \tag{5·3}$$

modulo E, while the equation $D_{12} = 0$ becomes

$$\begin{aligned}[1+e^2x(x'-y')][(z-p)-e^2zp(z'-p')] \\ + [1-e^2p(z'-p')][(x-y)-e^2xy(x'-y')] \equiv 0\end{aligned} \tag{5·4}$$

modulo E. The congruence (5·3) reduces to

$$(x'-y') + (z'-p')\lambda \equiv 0$$

modulo E. In particular, (5·2) holds in R/E. Substituting $z'-p' \equiv (y'-x')\lambda^{-1}$ into (5·4) and simplifying then yields $x\lambda - y + z - p\lambda^{-1} \equiv 0$ modulo E, so (5·1) holds in R/E.

Since the identity of Q is $\mathbf{0} = \langle 0, 0\rangle$, the multiplication and right division in Q are obtained from (5·1) and (5·2) as follows using (3·2).

COROLLARY 5·2. *In the Catalan loop* $(Q, \cdot, /, 1)$*, the multiplication and right division are given respectively by*

$$\langle x, x'\rangle \cdot \langle y, y'\rangle = \langle x\lambda_m^2 + y\lambda_m, x'\lambda_m^{-1} + y'\rangle, \tag{5·5}$$

with $\lambda_m = \lambda_m(\mathbf{x}, \mathbf{y}) = 1 + e^2yx'$*, and*

$$\langle x, x'\rangle/\langle y, y'\rangle = \langle x\lambda_r^2 - y\lambda_r, x'\lambda_r^{-1} - y'\lambda_r^{-1}\rangle \tag{5·6}$$

with $\lambda_r = 1 - e^2y(x'-y')$.

THEOREM 5·3. *The Catalan loop is two-sided.*

Proof. By construction, the Catalan loop forms a right loop. Given $\mathbf{x}$ and $\mathbf{z}$ in Q, (3·3) requires a unique solution $\mathbf{y}$ in Q to $\mathbf{x}\cdot\mathbf{y} = \mathbf{z}$, a unique element $\mathbf{y}$ of $\mathbf{x}^{-1}H\mathbf{z} \cap Q$. Let d be the unique recursive solution

$$d = 1 + e^2 \cdot x'(x-z) - e^4 \cdot 2x'^2(x-z) + \cdots \tag{5·7}$$

to the equation

$$d = (1+e^2xx') - e^2d^2x'z\,. \tag{5·8}$$

(Thus one first solves with $d = 1$ modulo e^2R. Inductively, a solution modulo $e^{2n}R$ is then refined to a solution modulo $e^{2(n+1)}R$, for each positive integer n. For an alternative approach, see the remarks following the proof of the theorem.) With

$$y = dz - d^{-1}x \tag{5·9}$$

and

$$y' = (d^{-1}z' - dx') - e^2x'z'y\,, \tag{5·10}$$

one has

$$\begin{bmatrix} 1 & -ex \\ -ex' & 1+e^2xx' \end{bmatrix}\begin{bmatrix} d & 0 \\ 0 & d^{-1} \end{bmatrix}\begin{bmatrix} 1+e^2zz' & ez \\ ez' & 1 \end{bmatrix} = \begin{bmatrix} 1+e^2yy' & ey \\ ey' & 1 \end{bmatrix}$$

as an element of the transversal Q.

In the proof of Theorem 5·3, the recursive solution (5·7) may be written in the symbolic form

$$\begin{aligned} d &= \frac{-1+\sqrt{1+4(1+e^2x'x)(e^2x'z)}}{2e^2x'z} \\ &= (1+e^2x'x)-(1+e^2x'x)^2(e^2x'z) \\ &\quad +2(1+e^2x'x)^3(e^2x'z)^2-5(1+e^2x'x)^4(e^2x'z)^3+\cdots \end{aligned}$$

of a solution to (5·8) as a quadratic equation, expanding the square root as a binomial series. The integral coefficients that appear are the Catalan numbers [**8**, p. 292], [**10**, (2·3·9)]. Appropriate substitutions in (5·9) and (5·10) yield the generating function for the Catalan numbers directly within the Catalan loop.

PROPOSITION 5·4. *In the Catalan loop* $(Q, \cdot, /, 1)$*, one has*

$$\langle 0,-1\rangle \cdot \langle d, d\rangle = \langle 1, 0\rangle$$

with

$$d = 1+e^2+2e^4+5e^6+14e^8+\cdots \tag{5·11}$$

as a generating function for the Catalan numbers.

Remark 5·5. The nth Catalan number c_n counts rooted binary trees with n leaves. In the corresponding term $c_n e^{2n-2}$ of (5·11), the power $2n-2$ of e is the number of edges in such a tree.

6. *Structure of the Catalan loop*

This section deals with the algebraic structure of a Catalan loop. Here, it is best to consider the underlying set of Q as the square $(R/E)^2$ of the quotient of R by the annihilator E of e. The first result is a straightforward consequence of Corollary 5·2.

PROPOSITION 6·1. *Let Q be the Catalan loop.*

(a) *The maps*

$$\iota_1 : (R/E, +, -, E) \longrightarrow (Q, \cdot, /, 1); x+E \longmapsto \langle x, 0\rangle$$

and

$$\iota_2 : (R/E, +, -, E) \longrightarrow (Q, \cdot, /, 1); x+E \longmapsto \langle 0, x\rangle$$

are injective homomorphisms.

(b) *Consider the respective images $Q_i = (R/E)\iota_i$ for $i = 1, 2$. Then $Q_1 \bigcap Q_2 = \{1\}$ and $Q = Q_1 \cdot Q_2$.*

Proof. For (a), note

$$\langle x, 0\rangle \cdot \langle y, 0\rangle = \langle x+y, 0\rangle \quad \text{and} \quad \langle 0, x'\rangle \cdot \langle 0, y'\rangle = \langle 0, x'+y'\rangle$$

by (5·5). In similar fashion,

$$\langle x, 0\rangle \cdot \langle 0, x'\rangle = \langle x, x'\rangle$$

establishes (b).

Proposition 6·1(b) constitutes a factorization of the Catalan loop. For what follows, recall that the *descending central series*

$$L_0 \geqslant L_1 \geqslant \cdots \geqslant L_i \geqslant \cdots$$

of a loop L is the series of normal subloops of L defined recursively by $L_0 = L$ and $L_{n+1} = [L, L_n]$ for $n \geqslant 0$. Here, the commutator $[L, N]$ of L with a normal subloop N is the normal subloop $1^{[L^2,\nu]}$ of L in the sense of [**7**, p. 42], ν being the congruence determined by N. The loop L is *residually nilpotent* [**4**, section 5·8] – *centrally ω-nilpotent* in Bruck's terminology [**3**, section VI·1] – if $\bigcap_{n=0}^{\infty} L_n = \{1\}$. It is *nilpotent* (of *class n*) if $L_n = \{1\}$.

THEOREM 6·2. *The Catalan loop is residually nilpotent.*

Proof. For a natural number n, define the quotient

$$Q^n = (R/(e^{2n}R + E))^2$$

of Q. Consider z, z' in $e^{2n-2}R$, with the corresponding element $\mathbf{z}$ of Q^n. Then for elements $\mathbf{x}, \mathbf{y}$ of Q^n, one has $z\lambda_m(\mathbf{x}, \mathbf{y}) = z$, $z'\lambda_m(\mathbf{x}, \mathbf{y}) = z'$,

$$\lambda_m(\mathbf{z}, \mathbf{x}) = 1 = \lambda_m(\mathbf{x}, \mathbf{z}) \quad \text{and}$$
$$\lambda_m(\mathbf{x} + \mathbf{z}, \mathbf{y}) = \lambda_m(\mathbf{x}, \mathbf{y}) = \lambda_m(\mathbf{x}, \mathbf{y} + \mathbf{z})$$

in the notation of Corollary 5·2. Thus (5·5) implies

$$\begin{aligned}\mathbf{z} \cdot \mathbf{x} &= \left\langle z\lambda_m(\mathbf{z}, \mathbf{x})^2 + x\lambda_m(\mathbf{z}, \mathbf{x}), z'\lambda_m(\mathbf{z}, \mathbf{x})^{-1} + x'\right\rangle \\ &= \langle z + x, x' + z'\rangle = \mathbf{z} + \mathbf{x} \\ &= \left\langle x\lambda_m(\mathbf{x}, \mathbf{z})^2 + z\lambda_m(\mathbf{x}, \mathbf{z}), x'\lambda_m(\mathbf{x}, \mathbf{z})^{-1} + z'\right\rangle = \mathbf{x} \cdot \mathbf{z}\end{aligned}$$

and

$$\begin{aligned}(\mathbf{z} \cdot \mathbf{x}) \cdot \mathbf{y} &= (\mathbf{z} + \mathbf{x}) \cdot \mathbf{y} \\ &= \langle (z + x)\lambda_m(\mathbf{z} + \mathbf{x}, \mathbf{y})^2 + y\lambda_m(\mathbf{z} + \mathbf{x}, \mathbf{y}), (z' + x')\lambda_m(\mathbf{z} + \mathbf{x}, \mathbf{y})^{-1} + y'\rangle \\ &= \langle z + x\lambda_m(\mathbf{x}, \mathbf{y})^2 + y\lambda_m(\mathbf{x}, \mathbf{y}), z' + x'\lambda_m(\mathbf{x}, \mathbf{y})^{-1} + y'\rangle \\ &= \mathbf{z} + (\mathbf{x} \cdot \mathbf{y}) = \mathbf{z} \cdot (\mathbf{x} \cdot \mathbf{y})\,.\end{aligned}$$

Similarly,

$$\begin{aligned}\mathbf{x} \cdot (\mathbf{y} \cdot \mathbf{z}) &= \mathbf{x} \cdot (\mathbf{y} + \mathbf{z}) \\ &= \langle x\lambda_m(\mathbf{x}, \mathbf{y} + \mathbf{z})^2 + (y + z)\lambda_m(\mathbf{x}, \mathbf{y} + \mathbf{z}), x'\lambda_m(\mathbf{x}, \mathbf{y} + \mathbf{z})^{-1} + (y' + z')\rangle \\ &= \langle x\lambda_m(\mathbf{x}, \mathbf{y})^2 + y\lambda_m(\mathbf{x}, \mathbf{y}) + z, x'\lambda_m(\mathbf{x}, \mathbf{y})^{-1} + y' + z'\rangle \\ &= (\mathbf{x} \cdot \mathbf{y}) + \mathbf{z} = (\mathbf{x} \cdot \mathbf{y}) \cdot \mathbf{z}\,.\end{aligned}$$

Thus $(e^{2n-2}R/(e^{2n}R + E))^2$ is contained in the center $Z(Q^n)$ of the loop Q^n. Recall that for a loop L, the set

$$\{z \in L \mid \forall\, x, y \in L,\ zx = xz,\ (zx)y = z(xy),\ x(yz) = (xy)z\}$$

is defined as the *center* $Z(L)$ of L [**8**, (3·31)].

Induction on r yields

$$(e^{2n-2r}R/(e^{2n}R+E))^2 \leqslant Z_r(Q^n)\,,$$

recalling the recursive definition $Z_0(L) = \{1\}$ and $Z_{r+1}(L)/Z_r(L) = Z(L/Z_r(L))$ for the *ascending central series*

$$Z_0(L) \leqslant Z_1(L) \leqslant \cdots Z_r(L) \leqslant \cdots$$

of a loop L. In particular, $Q^n = Z_n(Q^n)$: The loop Q^n is nilpotent of class n, and $Q^n_n = \{1\}$ [**3**, theorem VI·1·2], [**7**, p. 43]. Returning to the full Catalan loop, this translates to $Q_n \leqslant \left(e^{2n}R/E\right)^2$. Since $\bigcap_{n=1}^{\infty} e^{2n}R = \{0\}$, it follows that Q is residually nilpotent, as required.

COROLLARY 6·3. *If $e^r \in E$, then Q is nilpotent of class $\lceil r/2 \rceil$.*

The loops of a given nilpotency class form a variety, so Corollary 6·3 specifies identities that will be satisfied by Q when $e^r \in E$.

COROLLARY 6·4. *A finite Catalan loop is nilpotent.*

Remark 6·5. Going beyond the considerations of this section, many further structural questions about Catalan loops remain, such as a general specification of the *nucleus*

$$\{z \in Q \mid \forall\, x, y \in L,\ (zx)y = z(xy),\ (xz)y = x(zy),\ x(yz) = (xy)z\}$$

of a Catalan loop Q. For $n = 3$, Raasch [**5**] found the surprising result that the nonabelian loop $\Gamma_0^0(2^{n+1})\backslash\Gamma(2)$ (defined at the end of Section 2) is actually associative.

Acknowledgement. We are grateful to an anonymous referee for helpful comments on an earlier version of this paper.

REFERENCES

[**1**] S. BALCERZYK and T. JÓZEFIAK. *Commutative Rings* (Polish) (Państwowe Wydawnictwo Naukowe, Warsaw, 1985).
[**2**] S. BALCERZYK and T. JÓZEFIAK. *Commutative Noetherian and Krull Rings* (Państwowe Wydawnictwo Naukowe, Warsaw, 1989).
[**3**] R. H. BRUCK. *A Survey of Binary Systems* (Springer, 1958).
[**4**] W. MAGNUS, A. KARRASS and D. SOLITAR. *Combinatorial Group Theory* (Dover, 1976).
[**5**] J. M. RAASCH. Commutators and associators in Catalan loops. *Comm. Math. Univ. Carol.*, to appear.
[**6**] F.-T. TU and Y. YANG. Defining equations of $X_0(2^{2n})$. *Osaka J. Math.* **46** (2009), 105–113.
[**7**] J. D. H. SMITH. *Mal'cev Varieties* (Springer, 1976).
[**8**] J. D. H. SMITH. *An Introduction to Quasigroups and Their Representations* (Chapman and Hall/CRC, Boca Raton, FL, 2007).
[**9**] J. D. H. SMITH and A. B. ROMANOWSKA. *Post-Modern Algebra* (Wiley, 1999).
[**10**] H. S. WILF. *Generatingfunctionology* (Academic Press, 1990).