Powers of elements in Jordan loops

Kyle Pula

Abstract. A Jordan loop is a commutative loop satisfying the Jordan identity $(x^2y)x = x^2(yx)$. We establish several identities involving powers in Jordan loops and show that there is no nonassociative Jordan loop of order 9.

Keywords: Jordan loop, Jordan quasigroup, well-defined powers, nonassociative loop, order of a loop

Classification: 20N05

1. Introduction

A magma $(Q, \cdot)$ is a *quasigroup* if, for each $a, b \in Q$, the equations $ax = b$ and $ya = b$ have unique solutions $x, y \in Q$. A *loop* is a quasigroup with a neutral element, which we denote e. Standard references on quasigroup and loop theory are [1], [6]. A commutative loop is said to be *Jordan* if it satisfies the *Jordan identity*

$$x^2(yx) = (x^2y)x. \tag{J}$$

Kinyon, Pula, and Vojtěchovský [3] showed that there exists a nonassociative (that is, not associative) Jordan loop of order n if and only if $n \geq 6$ and $n \neq 9$.

For the order 9 case, their work relied upon an exhaustive computer search. In this paper, we establish several identities involving powers in Jordan loops and present a more "human-sized" proof that there are no nonassociative Jordan loops of order 9.

2. Powers of elements

We write x^k for the right associated term $L_x^k(e) = x(x(\cdots(xe)\cdots))$. We say that x^k *is well-defined* if the value of this term does not depend on how it is associated.

Lemma 2.1. *If Q is a Jordan loop and $x \in Q$, then x^3, x^4, and x^5 are well-defined.*

Proof: Third powers are well-defined in any commutative loop. For the fourth power, $x^3x = x^2x \cdot x = x^2 \cdot xx = x^2x^2$. For the fifth power, $x^4x = x^2x^2 \cdot x = x^2 \cdot x^2x = x^2x^3$. □

Lemma 2.2. *The following identities hold in any Jordan loop:*

(i) $x^n x^2 = x^{n+2}$,

(ii) $x^n x^4 = x^{n+4}$,

(iii) $x^n x^8 = x^{n+8}$ *if* $n \not\equiv 3 \mod 4$ *or* $x^3 x^8 = x^{11}$,

(iv) $x^n x^{2^k} = x^{n+2^k}$ *if* $n \equiv 2^m \mod 2^{k-1}$ *for* $0 \leq m \leq (k-1)$,

(v) $x^{2^n} = (x^{2^{n-1}})^2$.

Proof: (i) This is trivial for $n = 0$. Assuming the identity holds for $n-1$ and using (J), $x^n x^2 = xx^{n-1} \cdot x^2 = x^2 x^{n-1} \cdot x = x^{n+1}x = x^{n+2}$.

(ii) This is trivial for $n = 0$ and $n = 1$. Assuming the identity holds for $n-2$ and using (i) and (J), $x^n x^4 = x^{n-2}x^2 \cdot x^4 = x^{n-2}x^4 \cdot x^2 = x^{n+2}x^2 = x^{n+4}$.

(iii) This is trivial for $n = 0$ and $n = 1$ while $n = 2$ follows from (i) and $n = 3$ holds by assumption. Assuming the identity holds for $n-4$, $x^n x^8 = x^{n-4}x^4 \cdot x^8 = x^{n-4}x^8 \cdot x^4 = x^{n+4}x^4 = x^{n+8}$, using (ii) and (J). By induction, the identity holds for all $n \not\equiv 3 \mod 4$ and if the identity holds for $n = 3$, then it holds for all n.

(iv) We say $\mathrm{J}(n,k)$ holds if (iv) holds for n and k. Note that for $k = 1, 2$, and 3, $\mathrm{J}(n,k)$ is a special case of (i), (ii), and (iii). Assume that $\mathrm{J}(m,i)$ holds for all m and for all $i < k$ and consider $\mathrm{J}(n,k)$. For $n = 2^m$ where $0 \leq m \leq (k-1)$, the identity $\mathrm{J}(n,k)$ is $x^{2^m}x^{2^k} = x^{2^m+2^k}$ but, in the presence of commutativity, this identity is also $\mathrm{J}(2^k,m)$. Since $m < k$, $\mathrm{J}(2^k,m)$ holds by our induction assumption.

We now keep k fixed and induct on n. Assume that $n \equiv 2^m \mod 2^{k-1}$ for $0 \leq m \leq (k-1)$ and that $\mathrm{J}(n-2^{k-1},k)$ holds. Note that if $n \equiv 2^m \mod 2^{k-1}$, then $n - 2^{k-1} \equiv 2^m \mod 2^{k-2}$ and thus it follows from $\mathrm{J}(n-2^{k-1},k-1)$ that $x^n = x^{n-2^{k-1}}x^{2^{k-1}}$ and by $\mathrm{J}(2^{k-1},k-1)$, we have $x^{2^k} = x^{2^{k-1}}x^{2^{k-1}} = (x^{2^{k-1}})^2$.

Therefore, we have:

$$\begin{aligned}
x^n x^{2^k} &= x^{n-2^{k-1}}x^{2^{k-1}} \cdot (x^{2^{k-1}})^2 && \mathrm{J}(n-2^{k-1},k-1) \text{ and } \mathrm{J}(2^{k-1},k-1)\\
&= x^{n-2^{k-1}}(x^{2^{k-1}})^2 \cdot x^{2^{k-1}} && (\mathrm{J})\\
&= x^{n-2^{k-1}}x^{2^k} \cdot x^{2^{k-1}} && \mathrm{J}(2^{k-1},k-1)\\
&= x^{n+2^{k-1}}x^{2^{k-1}} && \mathrm{J}(n-2^{k-1},k) \text{ and } n-2^{k-1} \equiv 2^m \mod 2^{k-1}\\
&= x^{n+2^k}.
\end{aligned}$$

The final line follows since $\mathrm{J}(n+2^{k-1},k-1)$ holds and $n+2^{k-1} \equiv 2^m \mod 2^{k-2}$.

(v) This is just the identity $\mathrm{J}(2^{n-1},n-1)$, which applies since $2^{n-1} \equiv 0 \mod 2^{n-2}$. □

Corollary 2.3. *If Q is a Jordan loop and $x \in Q$, then*

$$x^n = x^{1\cdot a_0}(x^{2\cdot a_1}(\cdots(x^{2^k\cdot a_k})))$$

where $a_k \ldots a_0$ is the binary expansion of n.

Example 2.4. *The following identity holds in any Jordan loop:*

$$x^{317} = x^{(100111101)_2} = x(x^4(x^8(x^{16}(x^{32}(x^{256}))))).$$

Lemma 2.5. *The following identities hold in any Jordan loop:*

(i) $x^2x^{-1} = x$,
(ii) $x^4x^{-1} = x^3$,
(iii) $x^8x^{-1} = x^7$ *if* $x^3x^8 = x^{11}$.

Proof: (i) By (J), $x^2 = x^2 \cdot xx^{-1} = x \cdot x^2x^{-1}$ and we may now cancel x from both sides to get $x = x^2x^{-1}$.

(ii) Recall that $x^4 = (x^2)^2$. By (J) and (i), $x^2 \cdot x^4x^{-1} = x^4 \cdot x^2x^{-1} = x^4x = x^2x^3$ and we may now cancel x^2 from both sides to get $x^4x^{-1} = x^3$.

(iii) Recall that $x^8 = (x^4)^2$. By (J) and (ii), $x^4 \cdot x^8x^{-1} = x^8 \cdot x^4x^{-1} = x^8x^3 = x^{11} = x^4x^7$ and we may cancel x^4 from both sides to get $x^8x^{-1} = x^7$. □

Lemma 2.6. *If Q is a Jordan loop and $x \in Q$, then $(x^{2^n})^{-1} = (x^{-1})^{2^n}$.*

Proof: The identity is trivial for $n = 0$. For $n = 1$, we have

$$\begin{aligned}
(x^{-1})^2 &= (x^{-1})^2 \cdot xx^{-1} \\
&= (x^{-1})^2x \cdot x^{-1} && \text{(J)} \\
&= (x^{-1})^2(x^2x^{-1}) \cdot x^{-1} && \text{(i) of Lemma 2.5} \\
&= ((x^{-1})^2x^2)x^{-1} \cdot x^{-1}. && \text{(J)}
\end{aligned}$$

Cancel x^{-1} from both sides twice to get $e = (x^{-1})^2x^2$. Thus $(x^{-1})^2 = (x^2)^{-1}$. Now assuming the identity holds for $n-1$, we have

$$\begin{aligned}
(x^{2^n})^{-1} &= ((x^{2^{n-1}})^2)^{-1} && \text{(v) of Lemma 2.2} \\
&= ((x^{2^{n-1}})^{-1})^2 && \text{Previous Case} \\
&= ((x^{-1})^{2^{n-1}})^2 && \text{Induction Assumption} \\
&= (x^{-1})^{2^n}. && \text{(v) of Lemma 2.2}
\end{aligned}$$

□

Lemma 2.7. *The following identities hold in any Jordan loop:*

(i) $(x^2)^{-1}x = x^{-1}$,
(ii) $x^3x^{-2} = x$,
(iii) $x^3x^{-1} = x^2$,
(iv) $x^4(x^{-1})^3 = x$,
(v) $x^6x^{-2} = x^4$,
(vi) $x^6x^{-4} = x^2$.

Proof: (i) Let $y = x^{-1}$. Then $(x^2)^{-1}x = (x^{-1})^2x = y^2y^{-1} = y = x^{-1}$, using Lemma 2.6 and (i) of Lemma 2.5.

(ii) First, $x^3x^{-2} = x^4x^{-1} \cdot x^{-2} = x^4x^{-1} \cdot (x^{-1})^2 = x^4(x^{-1})^2 \cdot x^{-1}$, using (ii) of Lemma 2.5. Let $y = x^2$ then $x^4(x^{-1})^2 \cdot x^{-1} = y^2y^{-1} \cdot x^{-1} = yx^{-1} = x^2x^{-1} = x$, using (i) of Lemma 2.5 twice.

(iii) Using (J) and (ii), $x^{-2} \cdot x^{-1}x^3 = x^{-1} \cdot x^{-2}x^3 = x^{-1}x = e$. Thus $x^3x^{-1} = (x^{-2})^{-1} = x^2$.

(iv) Let $y = x^{-1}$. Then $x^2 \cdot x^4(x^{-1})^3 = x^4 \cdot x^2(x^{-1})^3 = x^4 \cdot y^{-2}y^3 = x^4y = x^3$, using (J), (ii), and (i) of Lemma 2.5. Now cancel x^2 from both sides to get $x^4(x^{-1})^3 = x$.

(v) Using (i) of Lemma 2.2, Lemma 2.6, and (iii), $x^6x^{-2} = (x^2)^3(x^2)^{-1} = (x^2)^2 = x^4$.

(vi) Using (i) of Lemma 2.2, Lemma 2.6, and (ii), $x^6x^{-4} = (x^2)^3(x^2)^{-2} = x^2$. □

Theorem 2.8. *If Q is a Jordan loop and $x \in Q$ such that $x^3x^3 = x^6$, then*

(i) *x^6 is well-defined,*
(i) *x^7 is well-defined,*
(i) *$x^6x^{-1} = x^5$,*
(i) *x^8 is well-defined.*

Proof: (i) $x^3x^3 = x^6 = xx^5 = x \cdot x^2x^3 = x^2 \cdot xx^3 = x^2x^4$.

(ii) $x^6x = x^2x^4 \cdot x = x^2x^5 = x^4x \cdot x^2 = x^4x^3$.

(iii) $x^6x^{-1} = (x^3)^2 \cdot x^3x^{-4} = x^3 \cdot (x^3)^2x^{-4} = x^3 \cdot x^6x^{-4} = x^3x^2 = x^5$.

(iv) $x^8 = x^6x^2 = (x^3)^2 \cdot x^3x^{-1} = x^3 \cdot (x^3)^2x^{-1} = x^3x^5$. □

Theorem 2.9 shows that Theorem 2.8 cannot be improved.

Theorem 2.9. *If $n > 5$ is neither a power of two nor prime, then there is a Jordan loop Q and a generating element $x \in Q$ such that x^k is well-defined for $0 \leq k < n$ but x^n is not well-defined.*

Proof: See Theorem 5.5 of [3]. □

3. Jordan loops of order 9

The following is a well-known and simple result. We reproduce it here for completeness.

Lemma 3.1. *A commutative loop Q of order n has a nontrivial involution if and only if n is even.*

Proof: Fix a multiplication table for Q. Note that every element of Q appears in the multiplication table n times. Since Q is commutative, every element appears the same number of times above the main diagonal as it does below. Thus every element appears an even number of times off the main diagonal. If n is even, then every element must appear an even number of times on the main diagonal while if n is odd, every element must appear an odd number of times on the main diagonal.

Thus, if n is odd, then every element must appear exactly once on the main diagonal. In particular, since e must appear in the cell corresponding to $e \cdot e$, it cannot appear anywhere else. If n is even, since e must appear in the $e \cdot e$ cell, it must also appear somewhere else along the main diagonal. □

Corollary 3.2. *A commutative loop Q of order n has an even-ordered subloop if and only if n is even.*

Corollary 3.3. *A commutative loop Q of order n has a well-defined square root operation if and only if n is odd.*

Lemma 3.4. *If H is a proper subquasigroup of a finite quasigroup Q, then $|H| \leq \lfloor \frac{|Q|}{2} \rfloor$.*

Proof: Let $k = |H|$ and $n + k = |Q|$. Fix a multiplication table of Q with both the rows and columns indexed first by elements of $H = \{h_i\}$ and then of $Q \setminus H = \{q_i\}$. Since H is a subquasigroup of Q, the cells corresponding to $H \times H$ contain only elements of H. Then the k cells corresponding to $q_1 \times H$ must be filled entirely with elements from $Q \setminus H$ and thus $|Q \setminus H| = n \geq k$. That is, $n + k = |Q| \geq 2|H|$ and thus $|H| \leq \lfloor \frac{|Q|}{2} \rfloor$. □

Lemma 3.5. *Let Q be a loop of order n and let $x \in Q$. If x^m is well-defined for every $1 \leq m \leq n-1$ then $\langle x \rangle$ is a cyclic group of order k, and $k = n$ whenever $k > \lfloor n/2 \rfloor$.*

Proof: See Lemma 5.3 in [3]. □

Lemma 3.6. *If Q is a Jordan loop of order 9, then Q is either of exponent 3 or cyclic.*

Proof: Suppose $e \neq x \in Q$ does not generate Q and let $k = |\langle x \rangle|$. Lemma 3.4 shows that $k \leq \lfloor \frac{9}{2} \rfloor = 4$ and Corollary 3.2 shows that $k = 3$. □

Lemma 3.7. *If $Q = \langle x \rangle$ is a Jordan loop of order 9, then $Q = \{x^k : 1 \leq k \leq 9\}$ and $x^n = x^{(n \mod 9)}$ for all $n \geq 0$.*

Proof: Suppose $x^n = x^{n+k}$ for $1 \leq n < n+k \leq 9$. Cancel terms on the left to get $e = x^k$ and consider the smallest possible value of k. It is easy to see that if $k = 1, 2,$ or 3, then $|\langle x \rangle| = k$, a contradiction. If $k = 4$, then $x^3 x^3 = x^3 x^{-1} = x^2 = x^6$ and thus x^6 is well-defined. It then follows that $|\langle x \rangle| = 4$, a contradiction. If $k = 5$, then $x^3 x^3 = x^3 (x^2)^{-1} = x^3 x^{-2} = x = x^6$ and thus x^6 is well-defined. Again it follows that $|\langle x \rangle| = 5$, a contradiction.

Suppose $k = 6$. Multiplying x^2 on both sides of $x^6 = e$ gives $x^8 = x^2$. Taking the square root of both sides gives $x^4 = x$ and thus $x^3 = e$, a contradiction.

Suppose $k = 7$. We show that x^n is well-defined for all n and by Lemma 3.5, $\langle x \rangle$ is a cyclic group of order 7, a contradiction. Since $x^7 = x^3x^4 = e$, $x^3 = (x^4)^{-1}$. Squaring both sides and applying Lemma 2.6, $x^3x^3 = (x^4x^4)^{-1} = (x^8)^{-1} = x^{-1} = x^6$. We now have that x^6 is well-defined and by Theorem 2.8 we are done.

Suppose $k = 8$. Then $x^8 = x^4x^4 = e$ and by Lemma 3.1 $x = e$.

We thus have that $x^9 = e$. Fix $n \geq 9$ and note that $x^n = x \cdot x^{n-1}$. By induction $x^{n-1} = x^{(n-1 \mod n)}$. Thus $x^n = x^{(n \mod 9)}$. □

Lemma 3.8. *If Q is a cyclic Jordan loop of order 9, then Q is a group.*

Proof: Let $\langle x \rangle = Q$. By Lemma 3.5, we will be done if we show that x^k is well-defined for $1 \leq k \leq 8$. By Lemma 2.1 and Theorem 2.8, we only need to consider $k = 6$. By Lemma 3.7, we may write every element of Q as x^k for $0 \leq k \leq 8$. We now use Lemma 2.2 to fill in a partial multiplication table for Q as in Table 1.

e	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	e
x^2	x^3	x^4	x^5	x^6	x^7	x^8	e	x
x^3	x^4	x^5		x^7				
x^4	x^5	x^6	x^7	x^8	e	x	x^2	x^3
x^5	x^6	x^7		e				x^4
x^6	x^7	x^8		x				x^5
x^7	x^8	e		x^2				
x^8	e	x		x^3	x^4	x^5		x^7

Table 1. Partial multiplication table for Q

Since values cannot repeat in columns, rows, or the main diagonal, $x^3x^3 = x$ or $x^3x^3 = x^6$. In the latter case, x^6 is well-defined and we are done. Suppose $x^3x^3 = x$ and note that $(x^3x^3)x^3 \cdot x^3 = xx^3 \cdot x^3 = x^7$, but by (J), $(x^3x^3)x^3 \cdot x^3 = x^3x^3 \cdot x^3x^3 = x \cdot x = x^2$. Thus $x^7 = x^5$ and $x^2 = e$, a contradiction. □

Theorem 3.9. *If Q is a Jordan loop of order 9, then Q is a group.*

Proof: By Lemmas 3.6 and 3.8, we only need to consider the case where Q is of exponent 3. Let $e \neq a, b, c, d \in Q$ such that $\langle a \rangle, \langle b \rangle, \langle c \rangle$, and $\langle d \rangle$ are distinct. A partial multiplication table for Q must be of the form presented in Table (A).

e	a	a^2	b	b^2	c	c^2	d	d^2
a	a^2	e						
a^2	e	a						
b			b^2	e				
b^2			e	b				
c					c^2	e		
c^2					e	c		
d							d^2	e
d^2							e	d

Table (A)

e	a	a^2	b	b^2	c	c^2	d	d^2
a	a^2	e	c					
a^2	e	a		c				
b	c		b^2	e				
b^2		c	e	b				
c					c^2	e		
c^2					e	c		
d							d^2	e
d^2							e	d

Table (B)

e	a	a^2	b	b^2	c	c^2	d	d^2
a	a^2	e	c	c^2				
a^2	e	a	d	d^2				
b	c	d	b^2	e		a		
b^2	c^2	d^2	e	b	a			
c				a	c^2	e		
c^2			a		e	c		
d							d^2	e
d^2							e	d

Table (C)

e	a	a^2	b	b^2	c	c^2	d	d^2
a	a^2	e	c	d^2		x^2	x	
a^2	e	a	d	c^2	x			x^2
b	c	d	b^2	e		y^2		y
b^2	d^2	c^2	e	b	y		y^2	
c		x		y	c^2	e		
c^2	x^2		y^2		e	c		
d	x			y^2			d^2	e
d^2		x^2	y				e	d

Table (D)

e	a	a^2	b	b^2	c	c^2	d	d^2
a	a^2	e	c	d^2	d	x^2	x	c^2
a^2	e	a	d	c^2	x	d^2	c	x^2
b	c	d	b^2	e	d^2	y^2	c^2	y
b^2	d^2	c^2	e	b	y	d	y^2	c
c	d	x	d^2	y	c^2	e	x^2	y^2
c^2	x^2	d^2	y^2	d	e	c	y	x
d	x	c	c^2	y^2	x^2	y	d^2	e
d^2	c^2	x^2	y	c	y^2	x	e	d

Table (E)

e	a	a^2	b	b^2	c	c^2	d	d^2
a	a^2	e	c	d^2	d	b^2	b	c^2
a^2	e	a	d	c^2	b	d^2	c	b^2
b	c	d	b^2	e	d^2	a^2	c^2	a
b^2	d^2	c^2	e	b	a	d	a^2	c
c	d	b	d^2	a	c^2	e	b^2	a^2
c^2	b^2	d^2	a^2	d	e	c	a	b
d	b	c	c^2	a^2	b^2	a	d^2	e
d^2	c^2	b^2	a	c	a^2	b	e	d

Table (F)

Suppose an off-diagonal 2×2 square of Table (A) contains a repeated element. Without loss of generality, we are in the case presented in Table (B). While the column indexed by d must contain the element c, there is no available row that can contain this occurrence of c. Thus, every off-diagonal 2x2 square in Table (A) must contain four distinct elements.

Suppose an off-diagonal 2×2 square of Table (A) contains both an element and its square in the same row or column. Without loss of generality, we are in the case presented in Table (C). Let $y := c \cdot b^2 = ab \cdot b^2 = ab^2 \cdot b = c^2 b$. Notice that either $y = a$ or $y = a^2$. If $y = a$, then the column indexed by d must contain the element a but there are no available rows to contain this occurrence of a. Likewise for $y = a^2$.

Thus every off-diagonal 2×2 square in Table (A) is of the form

x	y^2
y	x^2

for $\langle x \rangle \neq \langle y \rangle$.

Without loss of generality, we can assume that the $(a, a^2) \times (b, b^2)$ square is arranged as in Table (D). Set $x := da = a^2 b \cdot a = a^2 \cdot ab = a^2 c$ and $y := d^2 b = ab^2 \cdot b = ab \cdot b^2 = cb^2$ as has been done in Table (D). It is easy to see that Table (E) is the unique quasigroup completion of Table (D).

Note that $\{x, x^2\} = \{b, b^2\}$ and $\{y, y^2\} = \{a, a^2\}$. Suppose $x = b^2$. Then $d^2 = b^2 a = a^2 c \cdot a = a^2 \cdot ac = a^2 d = c$, a contradiction, and thus $x = b$. Suppose $y = a^2$. Then $c = b^2 d^2 = b^2 \cdot cb = b^2 c \cdot b = a^2 b = d$, a contradiction, and thus $y = a$.

Therefore, Table (F) must be a multiplication table for Q. Furthermore, since we only made labeling choices when completing the table, up to isomorphism, this is the only possible multiplication table for a Jordan loop of order 9 and exponent 3. Therefore, it must be the multiplication table for the unique group of order 9 and exponent 3, $Z_3 \times Z_3$. □

Acknowledgment. I would like to thank the referee for her comments and for drawing my attention to a number of notational typos.

References

[1] Bruck R.H., *A Survey of Binary Systems*, Ergebnisse der Mathematik und Ihrer Grenzgebiete, New Series, Vol. 20, Springer, Berlin, 1958.

[2] Goodaire E.G., Keeping R.G., *Jordan loops and loop rings*, preprint.

[3] Kinyon M.K., Pula J.K., Vojtěchovský P., *Admissible Orders of Jordan Loops*, J. Combinatorial Designs, to appear.

[4] McCrimmon K., *A Taste of Jordan Algebras*, Universitext, Springer, New York, 2004.

[5] McCune W.W., *Mace4 Reference Manual and Guide*, Tech. Memo ANL/MCS-TM-264, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL, August 2003; `http://www.cs.unm.edu/~mccune/mace4/`.

[6] Pflugfelder H.O., *Quasigroups and Loops: Introduction*, Sigma Series in Pure Mathematics **7**, Heldermann Verlag, Berlin, 1990.

Department of Mathematics, University of Denver, 2360 S Gaylord St., Denver, CO 80208, U.S.A.

E-mail: jpula@math.du.edu

(*Received* October 22, 2007, *revised* November 24, 2007)