European Journal of Combinatorics 31 (2010) 18–24

Contents lists available at ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

On the multiplication groups of semifields

Gábor P. Nagy

Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H-6720 Szeged, Hungary

ARTICLE INFO

Article history:
Received 26 February 2009
Accepted 26 May 2009
Available online 16 June 2009

ABSTRACT

We investigate the multiplicative loops of finite semifields. We show that the group generated by the left and right multiplication maps contains the special linear group. This result solves a BCC18 problem of A. Drápal. Moreover, we study the question of whether the big Mathieu groups can occur as multiplication groups of loops.

1. Introduction

A quasigroup is a set Q endowed with a binary operation $x{\cdot}y$ such that two of the unknowns $x, y, z \in Q$ determine uniquely the third in the equation $x{\cdot}y = z$. Loops are quasigroups with a unit element. The multiplication tables of finite quasigroups are Latin squares. The multiplication tables of finite loops are normalized Latin squares, that is, in which the first row and column contain the symbols $\{1, \ldots, n\}$ in increasing order. The left and right multiplication maps of a loop $(Q, \cdot)$ are the bijections $L_a : x \mapsto a \cdot x$ and $R_a : x \mapsto x \cdot a$, respectively. These are precisely the permutations which are given by the rows and columns of the corresponding Latin square. The group generated by the left and right multiplication maps of a loop Q is the multiplication group $\mathrm{Mlt}(Q)$.

Loops arise naturally in geometry when coordinatizing point–line incidence structures. Most importantly, any projective plane can be coordinatized by a planar ternary ring (PTR), having an additive and a multiplicative loop; cf. [6]. A special case of PTRs is the class of (pre-)semifields, where the addition is associative and both distributivities hold. More precisely, a pre-semifield is a set $\mathbb{S}$ endowed with two binary operations $x + y$ and $x \circ y$ such that the addition is an elementary Abelian group with neutral element 0, $\mathbb{S}^* = \mathbb{S} \setminus \{0\}$ is a multiplicative quasifield and the two operations satisfy both distributive laws. A semifield is a pre-semifield with multiplicative unit element, that is, where $(\mathbb{S}^*, \circ)$ is a loop. Semifields are sometimes called non-associative division rings, as well.

The most known proper semifield is the division ring of the real octonions $\mathbb{O}$ and its complex counterpart $\mathbb{O}(\mathbb{C})$. Both are alternating algebras of dimension 8 over the ground field. On the one hand, a disadvantage of the complex octonions is that they contain zero divisors. On the other hand, it can be constructed over an arbitrary field F, and the set of invertible elements form a loop in all cases.

E-mail address: nagyg@math.u-szeged.hu.

0195-6698/$ – see front matter
doi:10.1016/j.ejc.2009.05.001

It is well known that these structures play an important role in the understanding of the orthogonal group $O^+(8, F)$ and its triality automorphism. In fact, $O^+(8, F)$ is the multiplication group of the loop of the invertible elements of $\mathbb{O}(F)$. Moreover, the automorphism group of $\mathbb{O}(F)$ is the exceptional Lie group $G_2(F)$. This fact explains the natural seven-dimensional orthogonal representation of $G_2(F)$. As regards these and other basic properties of octonions, we refer the reader to [5].

Any finite semifield $\mathbb{S}$ defines a loop whose multiplication group is contained in $GL(n, q)$ where $\mathbb{F}_q$ is the center of $\mathbb{S}$. The center $Z(\mathbb{S}^*)$ of $\mathbb{S}^*$ is isomorphic to $\mathbb{F}_q^*$; hence for the multiplication group of the factor loop $Q = \mathbb{S}^*/Z(\mathbb{S}^*)$, we have $\mathrm{Mlt}(Q) \le PGL(n, q)$. Conversely, let $(Q, \cdot)$ be a loop and assume that for some n, q, its multiplication group is contained in the group $\Gamma L(n, q)$, where the latter is considered as a permutation group acting on the nonzero vectors of $V = \mathbb{F}_q^n$. Then, we can identify Q with $V^* = V \setminus \{0\}$ and consider $V = (V, +, \cdot)$ as endowed with two binary operations, where $0 \cdot x = x \cdot 0 = 0$. The fact that the left and right multiplication maps are additive is equivalent to V being a semifield.

In this paper, we investigate the following problem: Let G be a finite permutation group on the set Q. Is there a loop operation $x{\cdot}y$ on Q such that $\mathrm{Mlt}(Q) \le G$? In particular, we are interested in the cases where G is a projective linear group or a big Mathieu group. As regards this question, the most general results are due to Vesanen [14] and Drápal [7], who showed that (a) if $\mathrm{Mlt}(Q) \le P\Gamma L(2, q)$ ($q \ge 5$), then Q is a cyclic group, and (b) the answer is negative for the groups $PSp(2n, q)$ ($n \ge 2$), $PU(n, q^2)$ ($n \ge 6$), $PO(n, q)$ ($n \ge 7$odd), and $PO^{\varepsilon}(n, q)$ ($n \ge 7 - \varepsilon$ even). Recall that for the loop Q of units of $\mathbb{O}(\mathbb{F}_q)$ modulo the center, $\mathrm{Mlt}(Q) = P\Omega^+(8, q)$.

In [3, Problem 398], A. Drápal asked the above question in the following formulation: Given $n \ge 3$ and a prime power q, does there exist a normalized Latin square such that for the group G generated by the rows and the columns, $PSL(n, q) \le G \le P\Gamma L(n, q)$ holds? We answer this question affirmatively when $q^n > 8$. Our construction uses multiplicative loops of semifields and it is unique in the following sense. Let Q be a finite loop such that $PSL(n, q) \le M(Q) \le PGL(n, q)$. Then there is a semifield $\mathbb{S}$ with center $\mathbb{F}_q$ and dimension n over $\mathbb{F}_q$ such that $Q \cong \mathbb{S}^*/Z(\mathbb{S}^*)$.

2. On transitive linear groups

Let p be a prime, $V = \mathbb{F}_p^d$, and $\Gamma = GL(d, p)$. Let $G \le \Gamma$ be a subgroup acting transitively on $V^* = V \setminus \{0\}$. Then $G_0 \trianglelefteq G \le N_\Gamma(G_0)$, where we have one of the following possibilities for G_0 (cf. [2, Section 7.3]):

Case	Cond. on p	Cond. on d	G_0
(I)	p arbitrary	$e\|d$	$SL(d/e, p^e)$
(II)	p arbitrary	$e\|d$, d/e even	$Sp(d/e, p^e)$
(III)	$p = 2$	$d = 6e$	$G_2(p^e)$
(IV)	$p \in \{2, 3, 5, 7, 11, 23, 19, 29, 59\}$	$d \in \{2, 4, 6\}$	Sporadics

(I)–(III) are three infinite classes of transitive linear groups; the others are sporadic constructions. There are 25 sporadic cases; the largest group in this class has order 12 096. Using the computer algebra software GAP4 [8], the following result can easily be checked:

Lemma 2.1. *No sporadic finite transitive linear groups can be the group of multiplications of a finite loop.* □

Proposition 2.2. *Let $\mathbb{S}$ be a finite semifield of dimension n over its center $\mathbb{F}_q$. Let G be the group of multiplications of the multiplicative loop $\mathbb{S}^*$. Then $SL(n, q) \le G \le GL(n, q)$.*

Proof. Let the socle G_0 of G be $SL(n_0, r)$, $Sp(n_0, r)$ or $G_2(r)$. Then $G \le \Gamma L(n_0, r)$ and $\mathbb{F}_r$ is a normal subfield of $\mathbb{S}$. The generalized Cartan–Brauer–Hua theorem [9, Lemma 1.1] implies that $\mathbb{F}_r$ is central in $\mathbb{S}$; hence $r = q$, $n_0 = n$ and $G \le GL(n, q)$. Let us assume that $G_0 = Sp(n, q)$ or $G_0 = G_2(q)$. In the latter case $n = 6$ and q is even; hence $G_2(q) < Sp(6, q)$. Indeed, for q even, the six-dimensional representation of the exceptional Lie group $G_2(q)$ is constructed from its natural seven-dimensional orthogonal representation by using the isomorphism $O(7,q) \cong Sp(6,q)$; cf [13, Theorem 11.9]. Thus, in both cases, the multiplication group of the central factor loop $Q = \mathbb{S}^*/Z(\mathbb{S}^*)$ is contained in $PSp(n,q)$. This contradicts [14, Theorem S]. □

Proposition 2.3. *Let $n \geq 3$ be an integer and q a prime power such that $q^n > 8$. Then, there is a semifield $\mathbb{S}$ such that the multiplication group G of $\mathbb{S}^*$ satisfies $SL(n,q) \leq G \leq GL(n,q)$.*

Proof. By Proposition 2.2, we only have to present a semifield which has dimension n over its center $\mathbb{F}_q$. We distinguish between three cases: (1) $q \geq 3$, (2) $q = 2$ and n is odd, and (3) $q = 2$ and n is even.

In case (1), we can use Albert's twisted fields [1]. Let F be the finite field $\mathbb{F}_{q^n}$. Let $\theta : x \mapsto x^q$ and $\sigma : x \mapsto x^{q^{n-1}}$ be automorphisms of F and $c \in F$ such that $c = x^{q-1}$ has no solution in F. As in [1], the semifield $\mathbb{S} = (F, +, *)$ is defined using the quadruple (F, θ, σ, c). As $n \geq 3$, $\theta \neq \sigma$ and we can use [1, Theorem 1] to deduce that the center of $\mathbb{S}$ is $\mathbb{F}_q$.

In case (2), we construct a proper binary semifield $\mathbb{S} = (F, +, *)$ of Knuth's type from the fields $F = \mathbb{F}_{2^n}$, $F_0 = \mathbb{F}_2$ and the F_0-linear map $f : F \to F_0$. As in [11, Section 2], we first define $x \circ y = xy + (f(x)y + f(y)x)^2$ and put $x * y = (x/1) \circ (y/1)$ where $x/1$ is given by $(x/1) \circ 1 = x$. Let z be a nonzero element of $Z(\mathbb{S}, +, *)$. Then $(x \circ 1) * ((y \circ 1) * z) = ((x \circ 1) * (y \circ 1)) * z$ implies

$$x \circ (y \circ z/1)/1 = (x \circ y)/1 \circ z/1.$$

We define the maps $\alpha, \beta : \mathbb{S} \to \mathbb{S}$ by

$$\alpha(u) = (u \circ z/1)/1, \qquad \beta(u) = u/1 \circ z/1.$$

Then the above equation has the form

$$x \circ \alpha(y) = \beta(x \circ y),$$

and the triple $(\mathrm{id}, \alpha, \beta)$ defines an autotopism of the pre-semifield $(F, +, \circ)$. By [11, Theorem 6], $\alpha(u) = z'u$ for some $z' \in F_0$. As $\alpha \neq 0$, this implies $z' = 1$ and $\alpha = \mathrm{id}$. Thus,

$$\begin{aligned} u \circ 1 = \quad & \alpha(u) \circ 1 = u \circ z/1 \Longrightarrow 1 = z/1 \\ & \Longrightarrow z = 1 \circ 1 = 1 + (2f(1))^2 = 1. \end{aligned}$$

Hence, $Z(\mathbb{S})$ consists of 0 and 1.

In case (3), put $F = \mathbb{F}_{2^{n/2}}$ and pick elements $f, g \in F$ such that $y^3 + gy + f \neq 0$ for all $y \in F$. Define the multiplication on $\mathbb{S} = F + \lambda F$ by

$$(a + \lambda b)(c + \lambda d) = (ac + b^\sigma d^{\tau^2} f) + \lambda(bc + a^\sigma d + b^\sigma d^\tau g),$$

where $x^\sigma = x^2$ and $\tau = \sigma^{-1}$. As $n \geq 4$, $\sigma \neq \mathrm{id}$ and by [10, Section 7.4], $\mathbb{S}$ is a semifield with unit element $1 = 1 + \lambda \cdot 0$. Assume that $a + \lambda b \in Z(\mathbb{S})$. If $c \in F$ is such that $c^\sigma \neq c$ then

$$ac + \lambda(bc) = (a + \lambda b)c = c(a + \lambda b) = ac + \lambda(c^\sigma b) \Longleftrightarrow b = 0.$$

Furthermore,

$$\lambda a = a\lambda = \lambda a^\sigma \Longleftrightarrow a = a^\sigma \Longleftrightarrow a \in \mathbb{F}_2.$$

This shows $Z(\mathbb{S}) = \mathbb{F}_2$. □

Remarks. It is an easy exercise to show that a semifield cannot have dimension 2 over its center. Moreover, it is also easy to see that no proper semifield of order 8 exists.

3. The main results on multiplication groups of semifields

The first part of the following theorem gives a general affirmative answer to Drápal's problem. The second part of the theorem is a partial converse of our construction based on semifields. The proof of this part is basically contained in the proof of [14, Theorem S]. However, as it is not formulated in this way, we present a self-contained proof, using slightly different notation.

Theorem 3.1. (a) *For any integer $n \geq 3$ and prime power q with $q^n > 8$, there is a loop Q such that $PSL(n,q) \leq \mathrm{Mlt}(Q) \leq PGL(n,q)$.*

(b) *Let Q be a loop such that $\mathrm{Mlt}(Q) \leq PGL(n,q)$ with $n \geq 3$. Then there is a semifield $\mathbb{S}$ of dimension n over its center $\mathbb{F}_q$ such that $Q \cong \mathbb{S}^*/Z(\mathbb{S}^*)$.*

Proof. Part (a) follows immediately from Propositions 2.2 and 2.3. Let Q be a loop with multiplication group $G = \mathrm{Mlt}(Q) \leq PGL(n,q)$. We simply put $F = \mathbb{F}_q$ and write the elements of $Q = PG(n-1,q)$ in the form xF with $x \in F^n \setminus \{0\}$. Let us denote the unit element of Q by eF. For any element xF, the left and right translations L_{xF}, R_{xF} are represented by $n \times n$ matrices over F and we assume $L_{eF} = R_{eF} = I$. We have

$$(xF) \cdot (yF) = (xR_{yF})F = (yL_{xF})F,$$

and for all vectors x, y there is a unique nonzero scalar $c_{x,y}$ with

$$xR_{yF} = yL_{xF} \cdot c_{x,y}. \tag{1}$$

Clearly, $c_{\lambda x,y} = \lambda c_{x,y}$ holds. For any x, y, z with $x + y \neq 0$, the following is yielded:

$$zL_{(x+y)F} \cdot c_{x+y,z} = (x+y)R_{zF} = xR_{zF} + yR_{zF} = zL_{xF} \cdot c_{x,z} + zL_{yF} \cdot c_{y,z}.$$

Let us now fix the elements x, y with $x + y \neq 0$ and define the matrices

$$U = L_{(x+y)F}L_{xF}^{-1}, V = L_{yF}L_{xF}^{-1}$$

and the scalars

$$\alpha(z) = \frac{c_{x,z}}{c_{x+y,z}}, \qquad \beta(z) = \frac{c_{y,z}}{c_{x+y,z}}.$$

By [14, Lemma A], $\alpha(z)$ and $\beta(z)$ are nonzero constants; in particular, $\alpha(z) = \alpha(e)$ and $\beta(z) = \beta(e)$. Thus, for any $x, y \in F^n \setminus \{0\}$ with $x + y \neq 0$, we have

$$L_{(x+y)F} \cdot c_{x+y,e} = L_{xF} \cdot c_{x,e} + L_{yF} \cdot c_{x,e}. \tag{2}$$

Let us now consider the set

$$\mathfrak{L} = \{0\} \cup \{\alpha L_{xF} \mid \alpha \in F^*, x \in F^n \setminus \{0\}\}$$

of matrices. $\mathfrak{L}$ is closed under addition. Indeed, for fixed nonzero scalars α, β and vectors x, y, there are unique scalars λ, μ in F such that $c_{\lambda x,e} = \alpha$, $c_{\mu y,e} = \beta$. Then either $\alpha L_{xF} + \beta L_{yF} = 0 \in \mathfrak{L}$ or by (2),

$$\alpha L_{xF} + \beta L_{yF} = c_{\lambda x,e}L_{xF} + c_{\mu y,e}L_{yF} = c_{\lambda x+\mu y,e}L_{(\lambda x+\mu y)F} \in \mathfrak{L}.$$

We make the vector space $V = F^n$ into a semifield in the following way. Denote by T_x the element $c_{x,e}L_{xF}$ of $\mathfrak{L}$. Then by (1),

$$eT_x = eL_{xF} \cdot c_{x,e} = xR_{eF} = x.$$

For $x, y \in V$, define $x \circ y = yT_x$.

Claim 1. $(V \setminus \{0\}, \circ)$ *is a loop with unit element e.*

Clearly, T_e is the identity matrix; hence $e \circ x = xT_e = x$. $x \circ e = eT_x = x$ by definition. The equation $x \circ y = z$ has a unique solution $y = zT_x^{-1}$ in y. Let us fix nonzero vectors y, z and take an element $x_0 \in V$ such that $(x_0F)(yF) = zF$, that is, $yL_{x_0F} = \alpha z$ for some $\alpha \in F$. Then $\alpha^{-1} = c_{\lambda x_0,e}$ for some nonzero scalar λ. With $x = \lambda x_0$, we have $T_x = \alpha^{-1}L_{x_0F}$ and $z = yT_x = x \circ y$.

Claim 2. $(V, +, \circ)$ *is a semifield.*

Since the left multiplication maps of V are the T_x's, we have left distributivity. Moreover, as $\mathfrak{L}$ is closed under addition, for any $x, y \in V$ there is a unique z such that $T_x + T_y = T_z$. Applying both sides to e, we obtain $z = x + y$. Therefore,

$$(x + y) \circ z = zT_{x+y} = z(T_x + T_y) = zT_x + zT_y = x \circ z + y \circ z.$$

Claim 3. *The loop Q is the central factor of V.*

Let I denote the identity matrix on V. Then for all $\alpha \in F$, $\alpha I = T_{\alpha e} \in \mathfrak{L}$. Using a trick as above, one can show that $T_{\lambda x} = \lambda T_x$, which implies that $(\lambda x) \circ y = \lambda(x \circ y)$. This means that the right multiplication maps are in $GL(V)$, as well. In particular, the multiplication maps corresponding to the elements λe are centralized by all left and right multiplication maps; thus, $\lambda e \in Z(V)$ for all $\lambda \in F$. By

$$(x \circ y)F = (yT_x)F = (yL_{xF})F = (xF)(yF),$$

the map $\varphi : x \to xF$ is a surjective loop homomorphism. The kernel of φ consists of the elements λe; thus, $\ker \varphi$ is central in V. Since $PSL(n, q) \leq \mathrm{Mlt}(Q)$ acts primitively, Q is a simple loop and the kernel K of the homomorphism is a maximal normal subloop. This proves that $\ker \varphi = Z(V^*)$. □

4. Mathieu groups as multiplication groups of loops

In [7], A. Drápal made some remarks on the question of whether the Mathieu group can occur as multiplication groups of loops. As noted, there it is rather straightforward to show that the small Mathieu groups M_{10}, M_{11} are not the multiplication groups of loops. Moreover, extensive computer calculation showed that the same holds for the big Mathieu groups M_{22} and M_{23}. For M_{22}, the computation was independently repeated in [12]. The author of this paper performed an independent verification on M_{23} which gave the same result as Drápal had.

The computation was implemented in the computer algebra GAP4 [8]. In order to reduce the CPU time we used some tricks. First of all, let L be an $n \times n$ normalized Latin square and let $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_n\}$ be the permutations defined by the rows and columns of L, in order. Then $a_1 = b_1 = \mathrm{id}$, $1^{a_i} = 1^{b_i} = i$ and $a_i b_j a_i^{-1} b_j^{-1}$ leaves 1 fixed. Conversely, assume that A, B are sets of permutations of degree n such that

(T1) $\mathrm{id} \in A, B$,
(T2) for all $i \in \{1, \ldots, n\}$ there are unique elements $a \in A$, $b \in B$ such that $i = 1^a = 1^b$, and
(T3) for all $a \in A$, $b \in B$, $aba^{-1}b^{-1}$ leaves 1 fixed;

then a normalized Latin square can be constructed such that the rows and columns of L determine the elements of A and B. Indeed, for any $i, j \in \{1, \ldots, n\}$, the jth element of the ith row will be j^a, where a is the unique element of A with $1^a = i$.

Let A, B be sets of permutations of degree n satisfying (T1)–(T3) and put $G = \langle A, B\rangle$. Then, the following pairs of sets satisfy (T1)–(T3) as well:

(a) B, A;
(b) A^h, B^h, where $h \in G_1$;
(c) Au^{-1}, uBu^{-1}, where $u \in A$;
(d) vAv^{-1}, Bv^{-1}, where $v \in B$.

This implies the following:

Lemma 4.1. *Let L be a Latin square of order n and assume that the rows and columns generate the group G. Let a be an arbitrary row of L. Then for any $a^* \in a^G \cup (a^{-1})^G$ there is a Latin square L^* such that a^* is a row of L^* and the rows and columns of L^* generate G.*

Proof. Let A, B denote the sets of permutations given by the rows and columns of L. If $a^* = a^{-1}$ then define L^* from the sets $A^* = Aa^{-1}$, $B^* = aBa^{-1}$. Thus, it suffices to deal with the case $a^* = a^g$. We can write $g = hv^{-1}$ where $h \in G_1, v \in B$. The sets A^h, B^h determine a Latin square L^h such that a^h is a row of L^h. This means that we can assume that $a^* = vav^{-1}$ where $u \in A$. It follows from (d) that vAv^{-1}, Bv^{-1} determines a Latin square L^* with row a^*. In all cases, the rows and columns generate G. $\square$

Put $G = M_{23} \leq S_{23}$ such that $\{1, \dots, 7\}$ is a block of the corresponding Witt design D. Let us assume that L is a Latin square such that the rows A and columns B generate G. Let a_{14}, a_{15}, a_{23} be elements of orders 14, 15 and 23 of G, respectively, mapping 1 to 2. Any fixed point free permutation $x \in G$ is conjugate to one of the following elements: $a_{14}, a_{15}, a_{23}, a_{14}^{-1}, a_{15}^{-1}, a_{23}^{-1}$. By Lemma 4.1, we can assume that the second row of L is a_{14}, a_{15} or a_{23}. Define $X = \{(1^g, \dots, 7^g) \mid g \in G\}, |X| = 637\,560$.

On an office PC running GAP4 [8], it takes about 72 h to list all 7×7 submatrices K which have the property that all rows and columns are in X, with given first column and first and second rows. If the second row is determined by a_{14} of a_{15} then the number of such submatrices is about 4000 and it takes 1 h more to show that none of these submatrices can be extended to a Latin square of order 23 such that the rows and columns are in G. That is, about 150 h of CPU time suffices to show that no column or row of L can be of order 14 or 15. Thus, we can assume that all rows and columns of L have order 23. Moreover, for any two rows x, y of L, xy^{-1} has order 23, as well. About 3 h of computation shows that any Latin square with these properties must correspond to a cyclic group of order 23.

We have therefore the following:

Proposition 4.2. (a) *There is no loop Q of order* 10 *or* 22 *such that* $\mathrm{Mlt}(Q) \leq M_{10}$ *or* $\mathrm{Mlt}(Q) \leq M_{22}$.
(b) *Let Q be a loop of order* 11 *or* 23 *such that* $\mathrm{Mlt}(Q) \leq M_{11}$ *or* $\mathrm{Mlt}(Q) \leq M_{23}$. *Then Q is a cyclic group.*
(c) *There are loops Q_1 and Q_2 of order* 12 *and* 24 *such that* $\mathrm{Mlt}(Q_1) = M_{12}$ *and* $\mathrm{Mlt}(Q_2) = M_{24}$.

Proof. The loop Q_1 is Conway's arithmetic progression loop given in [4, Section 18]. Q_1 is commutative and its automorphism group is transitive. The multiplication table of the loop Q_2 is given by the following:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	1	4	3	15	18	11	24	8	17	21	20	9	10	22	7	5	19	23	6	12	13	16	14
3	4	1	2	20	17	9	16	23	21	8	14	19	11	6	13	12	5	15	10	24	18	22	7
4	3	2	1	19	22	14	21	11	6	10	5	7	20	23	24	18	13	9	15	17	16	8	12
5	8	7	6	12	10	13	23	15	3	19	2	4	17	14	18	24	21	16	11	20	9	1	22
6	7	8	5	16	9	17	20	1	15	14	18	24	23	19	4	2	22	10	3	13	12	11	21
7	6	5	8	2	3	4	1	18	12	16	10	23	19	17	15	11	20	14	24	22	21	13	9
8	5	6	7	9	16	20	17	21	13	1	23	10	24	3	14	19	2	18	22	11	15	12	4
9	17	20	16	24	11	18	15	19	8	12	7	5	4	13	22	21	23	2	14	1	3	6	10
10	13	23	12	22	19	21	14	5	11	2	24	18	9	4	6	8	1	20	7	16	17	15	3
11	18	15	24	1	4	3	2	14	16	5	9	20	12	7	21	22	8	13	19	10	23	17	6
12	23	13	10	11	24	15	18	7	19	20	22	21	2	9	8	6	16	4	5	3	1	14	17
13	10	12	23	17	20	16	9	4	22	18	19	14	6	24	1	3	11	8	2	5	7	21	15
14	22	19	21	8	7	6	5	13	4	17	1	3	15	16	23	10	9	11	12	18	24	2	20
15	24	11	18	23	13	10	12	17	14	6	21	22	3	8	20	9	7	1	16	2	4	19	5
16	20	17	9	18	15	24	11	12	1	22	4	2	5	21	10	23	14	7	13	6	8	3	19
17	9	16	20	4	1	2	3	10	18	7	15	11	22	5	12	13	6	21	23	19	14	24	8
18	11	24	15	21	14	22	19	16	23	3	13	12	8	1	9	20	4	6	17	7	5	10	2
19	21	14	22	13	23	12	10	6	20	4	17	16	18	2	5	7	3	24	8	15	11	9	1
20	16	9	17	10	12	23	13	2	7	15	8	6	21	11	3	1	24	22	4	14	19	5	18
21	19	22	14	6	5	8	7	20	24	13	11	15	1	12	17	16	10	3	9	4	2	18	23
22	14	21	19	3	2	1	4	24	9	23	16	17	7	10	11	15	12	5	18	8	6	20	13
23	12	10	13	7	8	5	6	22	2	24	3	1	16	18	19	14	15	17	21	9	20	4	11
24	15	18	11	14	21	19	22	3	5	9	6	8	13	20	2	4	17	12	1	23	10	7	16

Q_2 is noncommutative and $|\mathrm{Aut}(Q_2)| = 5$.

References

[1] A.A. Albert, Generalized twisted fields, Pacific J. Math. 11 (1961) 1–8.
[2] P.J. Cameron, Permutation Groups, in: London Mathematical Society Student Texts, vol. 45, Cambridge University Press, Cambridge, 1999.

[3] P.J. Cameron, Research problems from the 18th British Combinatorial Conference. The 18th British Combinatorial Conference (Brighton, 2001), Discrete Math. 266 (1–3) (2003) 441–451.
[4] J.H. Conway, The Golay codes and Mathieu groups, in: J.H. Conway, N.J.A. Sloane (Eds.), Sphere Packings, Lattices and Groups, Springer-Verlag, Berlin/New York, 1988, (Chapter 11).
[5] J.H. Conway, D.A. Smith, On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry, A K Peters, Ltd, Natick, MA, 2003.
[6] P. Dembowski, Finite Geometries, Springer-Verlag, Berlin, 1968.
[7] A. Drápal, Multiplication groups of loops and projective semilinear transformations in dimension two, J. Algebra 251 (1) (2002) 256–278.
[8] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4.12; 2008. http://www.gap-system.org.
[9] T. Grundhöfer, Projektivitätengruppen von Translationsebenen, Result. Math. 6 (1983).
[10] D.E. Knuth, Finite semifields and projective planes, J. Algebra 2 (1965) 182–217.
[11] D.E. Knuth, A class of projective planes, TAMS 115 (1965) 541–549.
[12] P. Müller, G.P. Nagy, A note on the group of projectivities of finite projective planes, Innov. Incidence Geom. 6–7 (2009) 291–294.
[13] D.E. Taylor, The Geometry of the Classical Groups, in: Sigma Series in Pure Mathematics, vol. 9, Heldermann Verlag, Berlin, 1992.
[14] A. Vesanen, Finite classical groups and multiplication groups of loops, Math. Soc. Camb. Phil. Soc. 117 (1995) 425–429.