On the algebraic structure of Dyson's Circular Ensembles

Jonathan D.H. SMITH

January 29, 2012

Abstract. Dyson's Circular Orthogonal, Unitary, and Symplectic Ensembles are measure spaces modeling families of physical systems with specific spin and time-reversal properties. In this paper, it is shown that each of the three ensembles carries a transitive right quasigroup structure, such that automorphisms of the measure space are automorphisms of the quasigroup structure.

1 Introduction. In a classical paper [3], the physicist Freeman Dyson studied three statistical-mechanical ensembles designed to model whole families of physical systems, under three different assumptions about the nature of systems from the family and their behavior under time-reversal:

- The Circular Orthogonal Ensemble $T_1(n)$, for even-spin systems invariant under time-reversal;
- The Circular Unitary Ensemble $T_2(n)$, for systems that are not invariant under time-reversal;
- The Circular Symplectic Ensemble $T_4(n)$, for odd-spin systems invariant under time-reversal;

each for a positive integer n. Dyson exhibited the Circular Ensembles as compact measure spaces, normalizable to probability spaces giving the statistics of the ensemble. In particular, the Circular Unitary Ensemble $T_2(n)$ is just the unitary group $U(n)$ equipped with Haar measure [4, 6]. Dyson remarked that although the Circular Orthogonal and Symplectic Ensembles are subsets of unitary groups, they themselves are not generally closed under any natural group structure [3, pp. 142, 146]. Thus the aim of the current paper is to indicate the algebra structure which is common to all three ensembles: the structure of a transitive right quasigroup (Definition 2.2). The essential features of the main results of the paper (Theorems 5.9, 6.2, and 7.10) may be collated as follows:

Theorem 1.1. *Let n be a positive integer, and let $T_d(n)$ (for $d = 1, 2, 4$) be one of Dyson's Circular Ensembles.*

(a) *$T_d(n)$ forms a transitive right quasigroup under the core operation $x \circ y = yx^{-1}y$.*

(b) *The automorphism group of the measure space $T_d(n)$ is an automorphism group of the right quasigroup $\big(T_d(n), \circ\big)$.*

2000 *Mathematics Subject Classification.* 20N05.

Key words and phrases. circular orthogonal ensemble, circular unitary ensemble, circular symplectic ensemble, Haar measure, Moufang loop, right quasigroup, symmetric space, core, twisted subset, twisted subgroup.

Note that even in the unitary case $T_2(n)$, the right quasigroup is more closely related to the measure space than is the group, since measure space automorphisms are not group automorphisms in general.

The basic definitions from quasigroup theory are listed in Section 2, while properties of the core are presented in Section 3. Section 4 recalls the definitions of the unitary and symplectic groups. The Circular Orthogonal, Unitary, and Symplectic Ensembles are then studied in Sections 5–7 respectively. It is worth remarking that although in this paper the Circular Symplectic Ensemble is treated with elementary methods, Dyson described that ensemble in terms of matrix algebra over the quaternions, including use of the conjugate mapping studied by Iseki [5].

2 Basic definitions. This section records some basic definitions. Readers may consult [8, 9] for further explanation, or for other basic notation or algebraic conventions used here without explicit clarification.

A *magma*[1] $(M, *)$ is a set M that is equipped with a binary operation

$$M^2 \to M; (x, y) \mapsto x * y\,,$$

often called *multiplication*, and occasionally denoted merely by the juxtaposition xy of its arguments. If m is an element of a magma $(M, *)$, the *right multiplication* $R_*(m)$ is the map $M \to M; x \mapsto x * m$, while the *left multiplication* $L_*(m)$ is the map $M \to M; x \mapsto m * x$. If the multiplication is denoted by juxtaposition, then no suffix is placed on the R or L.

Definition 2.1. Let $(M, \cdot)$ be a magma.

1. The magma is a (*combinatorial*) *right quasigroup* if, for all y and z in M, there is a unique element x of M such that $x \cdot y = z$.

2. The magma is a(n *equational*) *right quasigroup* $(M, \cdot, /)$ if there is a binary operation $(x, y) \mapsto x/y$ of *right division* such that the identities $(x \cdot y)/y = x = (x/y) \cdot y$ hold in M.

3. The magma is a(n *equational*) *left quasigroup* $(M, \cdot, \backslash)$ if there is a binary operation $(x, y) \mapsto x\backslash y$ of *left division* such that the identities $y\backslash(y \cdot x) = x = y \cdot (y\backslash x)$ hold in M.

4. The magma is a (*two-sided*) *quasigroup* $(M, \cdot, /, \backslash)$ if it forms both a right quasigroup $(M, \cdot, /)$ and a left quasigroup $(M, \cdot, \backslash)$. In this case one often says that $(M, \cdot)$ is a quasigroup.

5. A quasigroup $(M, \cdot)$ is a *loop* $(M, \cdot, 1)$ if there is an element 1 of M, the so-called *identity element*, such that the identities $1 \cdot x = x = x \cdot 1$ hold in M.

6. An element x of a loop $(M, \cdot, 1)$ is said to be *invertible* if there is an element x^{-1} of M (the *inverse* of x), such that $x \cdot x^{-1} = 1 = x^{-1} \cdot x$.

7. A loop $(M, \cdot, /, \backslash, 1)$ is *diassociative* if for each at most 2-element subset S of M, the subloop generated by the elements of the subset S (under all the operations $\cdot, /, \backslash, 1$) is associative, and thus forms a group. In particular, each element of a diassociative loop is invertible.

[1] Øystein Ore's earlier term "groupoid" is now often applied to denote categories in which all the arrows are invertible.

8. A loop $(M, \cdot)$ is said to be a *Moufang loop* if it satisfies any of the following equivalent identities:

   (a) The *first* or *left Moufang identity* $((z \cdot y) \cdot z) \cdot x = z \cdot (y \cdot (z \cdot x))$;

   (b) The *second* or *right Moufang identity* $((x \cdot y) \cdot z) \cdot y = x \cdot (y \cdot (z \cdot y))$;

   (c) The *third* or *middle Moufang identity* $(z \cdot x) \cdot (y \cdot z) = (z \cdot (x \cdot y)) \cdot z$;

   (compare [9, I, Prop.4.1.5]).

If a magma $(M, \cdot)$ is a combinatorial right quasigroup, then the unique solution x to the equation $x \cdot y = z$ may be taken as z/y. Conversely, if $(M, \cdot, /)$ is an equational right quasigroup, then the unique solution x to the equation $x \cdot y = z$ may be given as z/y. Thus the concepts of Definition 2.1(1) and (2) are equivalent: one simply uses the term *right quasigroup*. Similar equivalences exist for left and two-sided quasigroups, justifying the unqualified terms *left quasigroup* and *quasigroup*.

If a magma $(M, \cdot)$ is a right quasigroup, each right multiplication $R_\cdot(y)$ by an element y of M is invertible, with $z/y = zR_\cdot(y)^{-1}$ for $z \in M$. Similarly, left multiplications of left quasigroups are invertible. For a right quasigroup $(M, \cdot)$, the set $\{R_\cdot(m) \mid m \in M\}$ of all right multiplications is a subset of $M!$, the group of all permutations of M. The *right multiplication group* of $(M, \cdot)$ is the subgroup $\mathrm{RMlt}\, M$ of $M!$ generated by $\{R_\cdot(m) \mid m \in M\}$. If $(M, \cdot)$ is a quasigroup, the *multiplication group* of $(M, \cdot)$ is the subgroup $\mathrm{Mlt}\, M$ of $M!$ generated by $\{R_\cdot(m), L_\cdot(m) \mid m \in M\}$.

For the purposes of the current paper, a further definition is required. Rather surprisingly, this concept does not seem to be well-known in the literature.

Definition 2.2. A right quasigroup is said to be *transitive* if its right multiplication group acts transitively.

Example 2.3. Each quasigroup is a transitive right quasigroup. On the other hand, let M be a set with at least two elements. Then the multiplication $x \cdot y = x$ and right division $x/y = x$ on M yield a right quasigroup $(M, \cdot, /)$ which is not transitive.

3 The core of a diassociative loop. Let M be a diassociative loop, in which the multiplication is denoted by juxtaposition. For example, one may consider the case of a Moufang loop, since by Moufang's Theorem, Moufang loops are diassociative [2, §VII.4]. The *core* of M is defined as the magma $(M, \circ)$ with $x \circ y = yx^{-1}y$. (Note that this is the opposite of Bruck's original definition for Moufang loops [2, VII(5.1)]. The current choice gives a better match to other notational conventions.)

If M is a diassociative loop, then one may extend a group-theoretical definition [7] by calling substructures of the pointed magma $(M, \circ, 1)$ *twisted subsets* of M. Similarly, one may define a *twisted subloop* of a general loop M to be a substructure of the pointed magma $(M, \triangle, 1)$ with $x \triangle y = y(xy)$, extending the *twisted subgroup* terminology of [1]. Note that the set $\mathbb{N}$ of natural numbers (0 included!) is a twisted subgroup of the additive group $\mathbb{Z}$, but not a twisted subset. For Part (a) of the following, recall that an algebraic structure (A, Ω') on a set A is said to be *derived* from a structure (A, Ω) on A if each operation ω of Ω' may be expressed (as a derived operation — compare [9, IV§1.3]) in terms of the operations from Ω.

Proposition 3.1. *Let M be a diassociative loop.*

(a) *The structure $(M, \triangle, 1)$ is derived from $(M, \circ, 1)$.*

(b) *Each twisted subset of M is a twisted subloop of M.*

(c) *If M is finite, then each twisted subloop of M is a twisted subset of M.*

Proof. For (a), consider elements x, y of M. Then $x \triangle y = y(xy) = x^{-1} \circ y = (x \circ 1) \circ y$. The statement (b) is an immediate consequence of (a). Now for (c), suppose that N is a twisted subloop of M, with M finite. Let x and y be elements of N. If x has even order $2r$ with a positive integer r, then $xR_\triangle(x)^{r-1} = x^{2r-1} = x^{-1}$, so $x \circ y = yx^{-1}y = \big(xR_\triangle(x)^{r-1}\big) \triangle y \in N$. On the other hand, if x has odd order $2s+1$ with a positive integer s, then $x^{-1} = x^{2s} = xL_\triangle(1)^s$, so again $x \circ y = yx^{-1}y = \big(xL_\triangle(1)^s\big) \triangle y \in N$. □

For the following, compare [2, §VII.5].

Proposition 3.2. *Let M be a diassociative loop.*

(a) *The core $(M, \circ)$ of M is a right quasigroup.*

(b) *Inversion in M is an automorphism of $(M, \circ)$.*

(c) *If M is a Moufang loop, then the multiplication group $\operatorname{Mlt} M$ of M is a transitive group of automorphisms of $(M, \circ)$.*

Proof. Consider x, y in M. For (a), note that $xR_\circ(y)^2 = y(yx^{-1}y)^{-1}y = yy^{-1}xy^{-1}y = x$, so the right multiplication $R_\circ(y)$ is an involution. For (b), one has $(x \circ y)^{-1} = \big(yx^{-1}y\big)^{-1} = x^{-1} \circ y^{-1}$. For (c), first note that the multiplication group of any quasigroup acts transitively. Now suppose that z is an element of M. Then

$$\begin{aligned}(xy) \circ (xz) &= (xz)(xy)^{-1}(xz) = (xz)\left(y^{-1}x^{-1}\right)(xz) \\ &= \big((xz)y^{-1}\big)\big(x^{-1}(xz)\big) \text{ by the middle Moufang identity} \\ &= \big((xz)y^{-1}\big)z \\ &= x\big(z\left(y^{-1}z\right)\big) \text{ by the right Moufang identity} \\ &= x(y \circ z)\,,\end{aligned}$$

so each left multiplication in M is an automorphism of $(M, \circ)$. Dually, each right multiplication in M is an automorphism of $(M, \circ)$. □

4 Unitary and symplectic groups. Let n be a positive integer. Recall that an $n \times n$ matrix u over the complex numbers is *unitary* if $uu^* = 1 = u^*u$, with u^* as the conjugate transpose of u. (Thus if the ij-entry of u is z, then the ji-entry of u^* is $\overline{z}$.) The group of all such matrices is the *unitary group* $U(n)$. A real matrix r is unitary if and only if it is *orthogonal*: $rr^T = 1 = r^Tr$.

Now consider the $2n \times 2n$ matrix

$$j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \tag{1}$$

with n summands (the block matrix with diagonal blocks $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and all other entries zero). Note that $j^2 = -1$. Then $\{b \in U(2n) \mid j = bjb^T\}$ is the *symplectic group* $Sp(n)$.[2]

Lemma 4.1. *Let b be an element of $Sp(n)$. Then the following hold:*

(a) $jb^Tj^{-1} = b^{-1}$;

[2] This group is sometimes written as $Sp(2n)$, but the current convention better matches Dyson's notation for the circular ensembles.

(b) $j\left(b^{-1}\right)^T j^{-1} = b$.

Proof. (a): The defining relation for the symplectic group is $j = bjb^T$. Then $b^{-1}j = jb^T$, so $b^{-1} = jb^T j^{-1}$.

(b): From (a), one has $j\left(b^{-1}\right)^T j^{-1} = \left(b^{-1}\right)^{-1} = b$. □

5 The Circular Orthogonal Ensemble. Let n be a positive integer. Define

$$T_1(n) = \{s \in U(n) \mid s^T = s\}\,,$$

the set of symmetric unitary $n \times n$ matrices. This set (with an appropriate measure) is Dyson's *Circular Orthogonal Ensemble* [3]. As he observed [*op. cit.*, p.142], it does not form a subgroup of $U(n)$ for $n > 1$, although $T_1(1) = U(1)$, the unit circle $\{\exp(2\pi i\theta) \mid \theta \in \mathbb{R}\}$.

Proposition 5.1. *The Circular Orthogonal Ensemble $T_1(n)$ is a twisted subset of $U(n)$.*

Proof. Suppose $x, y \in T_1(n)$, so x and y are symmetric and unitary. Set $u = x^{-1} \in U(n)$, and note $x \circ y = yx^{-1}y \in U(n)$. Furthermore, $xu = 1$ implies $1 = u^T x^T = u^T x$, so $u^T = x^{-1} = u$, and $u \in T_1(n)$. Then

$$(yx^{-1}y)^T = (yuy)^T = y^T u^T y^T = yuy = yx^{-1}y\,,$$

so $yx^{-1}y \in T_1(n)$. □

Corollary 5.2. *The Circular Orthogonal Ensemble $T_1(n)$ is a twisted subgroup of $U(n)$.*

For the following, see [3, Th. 4].

Proposition 5.3. *For an element s of $T_1(n)$, there is a real orthogonal matrix r and a complex diagonal matrix e such that $s = r^{-1}er$, and the diagonal elements of e lie on the unit circle $\{\exp(2\pi i\theta) \mid \theta \in \mathbb{R}\}$.*

Proposition 5.4. *The right multiplication group $\mathrm{RMlt}\big(T_1(n), \circ\big)$ of the right quasigroup $\big(T_1(n), \circ\big)$ acts transitively on $\big(T_1(n), \circ\big)$.*

Proof. Given an element s of $T_1(n)$, it will be shown that there is an element x of $T_1(n)$ such that $1R_\circ(x) = s$. The desired result then follows.

By Proposition 5.3, there is a real orthogonal matrix r and diagonal matrix

$$e = \mathrm{diag}\big(\exp(2\pi i\theta_1), \ldots, \exp(2\pi i\theta_n)\big)$$

with $\theta_j \in \mathbb{R}$ for $1 \le j \le n$ such that $s = r^{-1}er$. Define

$$d = \mathrm{diag}\big(\exp(\pi i\theta_1), \ldots, \exp(\pi i\theta_n)\big) \tag{2}$$

and $x = r^{-1}dr$. Note that d and x are both unitary, while $d^2 = e$. Now

$$x^T = (r^{-1}dr)^T = (r^T dr)^T = r^T d^T r = r^{-1}dr = x\,,$$

so $x \in T_1(n)$. Finally

$$1 \circ x = x1x = x^2 = r^{-1}drr^{-1}dr = r^{-1}d^2r = r^{-1}er = s\,,$$

as required. □

Remark 5.5. The matrix d of (2) may be replaced by

$$\operatorname{diag}\Big(\exp\big(\pi i(\theta_1+\lambda_1)\big),\dots,\exp\big(\pi i(\theta_n+\lambda_n)\big)\Big)$$

for any vector $(\lambda_1,\dots,\lambda_n)$ in the unit cube $\{0,1\}^n$. This means that the solution x to $1\circ x=s$ is not unique, so $\big(T_1(n),\circ\big)$ is not a quasigroup.

For the following, compare [3, Th. 1]. Dyson's theorem states that the measure of the Circular Orthogonal Ensemble is the unique measure on the set $T_1(n)$ that is invariant under the $U(n)$-action (3).

Proposition 5.6. *Let n be a positive integer. Then $T_1(n)$ is a transitive right $U(n)$-set under the action*

$$A_1(u)\colon T_1(n)\to T_1(n); s\mapsto u^T s u \tag{3}$$

for each element u of $U(n)$.

Corollary 5.7. *The Canonical Orthogonal Ensemble may be written as*

$$T_1(n)=\{u^T u \mid u\in U(n)\}$$

for each positive integer n.

Proof. Note that $\{u^T u \mid u\in U(n)\}$ is the orbit of 1 under the transitive $U(n)$-action of Proposition 5.6. □

Proposition 5.8. *Under the action* (3)*, the unitary group $U(n)$ acts as a transitive group of automorphisms of the right quasigroup $\big(T_1(n),\circ\big)$.*

Proof. Consider $x,y\in T_1(n)$ and $u\in U(n)$. Then

$$\begin{aligned} xA_1(u)\circ yA_1(u) &= \big(u^T x u\big)\circ\big(u^T y u\big) = \big(u^T y u\big)\big(u^T x u\big)^{-1}\big(u^T y u\big)\\ &= u^T y x^{-1} y u = \big(yx^{-1}y\big)A_1(u) = (x\circ y)A_1(u)\end{aligned}$$

as required. □

The results of this section may be summarized as follows.

Theorem 5.9. *Let n be a positive integer, and let $T_1(n)$ be Dyson's Canonical Orthogonal Ensemble.*

(a) *$T_1(n)$ is a twisted subset of the unitary group $U(n)$.*

(b) *$T_1(n)$ forms a transitive right quasigroup under the core operation $x\circ y=yx^{-1}y$.*

(c) *The automorphism group $U(n)$ of the measure space $T_1(n)$ is an automorphism group of the right quasigroup $\big(T_1(n),\circ\big)$.*

6 The Circular Unitary Ensemble. Let n be a positive integer. Dyson designated the unitary group $U(n)$ (with Haar measure [4, 6]) as the *Circular Unitary Ensemble* $T_2(n)$ [3]. For current purposes, the Circular Unitary Ensemble will be taken as the magma $\big(T_2(n), \circ\big)$. By Proposition 3.2(a), $\big(T_2(n), \circ\big)$ is a right quasigroup. Proposition 5.1 shows that $\big(T_1(n), \circ\big)$ is a right subquasigroup of $\big(T_2(n), \circ\big)$, so Remark 5.5 already implies that $\big(T_2(n), \circ\big)$ is not a quasigroup. However, in parallel with Propositions 5.4 and 7.5, one may observe the following.

Proposition 6.1. *The right multiplication group* $\mathrm{RMlt}\big(T_2(n), \circ\big)$ *of the right quasigroup* $\big(T_2(n), \circ\big)$ *acts transitively on* $\big(T_2(n), \circ\big)$.

Proof. Given an element s of $T_2(n)$, it will be shown that there is an element x of $T_2(n)$ such that $1R_\circ(x) = s$. The desired result then follows.

There is a unitary matrix u and diagonal matrix

$$e = \mathrm{diag}\big(\exp(2\pi i\theta_1), \ldots, \exp(2\pi i\theta_n)\big)$$

with $\theta_j \in \mathbb{R}$ for $1 \leq j \leq n$ such that $s = u^{-1}eu$. Define

$$d = \mathrm{diag}\big(\exp(\pi i\theta_1), \ldots, \exp(\pi i\theta_n)\big)$$

and $x = u^{-1}du$. Note that d and x are both unitary, while $d^2 = e$. Then

$$1 \circ x = x1x = x^2 = u^{-1}duu^{-1}du = u^{-1}d^2u = u^{-1}eu = s\,,$$

as required. □

Since the unitary group $U(n)$ is compact, its Haar measure is both left- and right-invariant. As a consequence, the multiplication group $\mathrm{Mlt}\,U(n)$ of the unitary group $U(n)$ is a group of automorphisms of the measure space $U(n)$, the Circular Unitary Ensemble $T_2(n)$. Proposition 3.2(c) may then be invoked to yield the second statement of the following theorem, which summarizes those algebraic properties of the Circular Unitary Ensemble that have analogues for the Orthogonal and Symplectic Ensembles.

Theorem 6.2. *Let n be a positive integer, and let $T_2(n)$ be Dyson's Canonical Unitary Ensemble.*

(a) *$T_2(n)$ forms a transitive right quasigroup under the core operation $x \circ y = yx^{-1}y$.*

(b) *The automorphism group* $\mathrm{Mlt}\,U(n)$ *of the measure space $T_2(n)$ is an automorphism group of the right quasigroup* $\big(T_2(n), \circ\big)$.

7 The Circular Symplectic Ensemble. Let n be a positive integer. With the matrix j of (1), an element u of $U(2n)$ is described as *self-dual* if $ju^Tj^{-1} = u$. (Self-duality in this sense is the mathematical equivalent of the time-reversal behavior appropriate for odd-spin systems in the Circular Symplectic Ensemble.) Define

$$T_4(n) = \{u \in U(2n) \mid ju^Tj^{-1} = u\}$$

to be the set of self-dual unitary $2n \times 2n$ matrices. This set (with an appropriate measure) is Dyson's *Circular Symplectic Ensemble* [3]. As he observed [*op. cit.,* p.146], it does not form a subgroup of $U(2n)$ in general, although the case $n = 1$ is again exceptional.

Proposition 7.1. *The set $T_4(1)$ is the scalar unit circle subgroup* $\{\exp(2\pi i\theta)I_2 \mid \theta \in \mathbb{R}\}$ *of $U(2)$. In particular, $U(1) = T_1(1) = T_2(1) \cong T_4(1)$.*

Proof. Consider a complex (2×2)-matrix

$$u = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}.$$

Then the self-duality criterion $ju^T j^{-1} = u$ for $T_4(1)$,

$$ju^T j^{-1} = -ju^T j = \begin{bmatrix} u_{22} & -u_{12} \\ -u_{21} & u_{11} \end{bmatrix} = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}, \tag{4}$$

is equivalent to $u_{12} = u_{21} = 0$ and $u_{11} = u_{22}$. For $u \in U(2)$, this means $u_{11} = u_{22} = \exp(2\pi i\theta)$ for $\theta \in \mathbb{R}$. □

Proposition 7.2. *For each positive integer n, the Circular Symplectic Ensemble $T_4(n)$ is a twisted subset of $U(2n)$.*

Proof. Suppose $x, y \in T_4(n)$, so x and y are self-dual and unitary. Set $u = x^{-1} \in U(2n)$, and note $x \circ y = yx^{-1}y \in U(2n)$. Furthermore, $xu = 1$ implies $1 = (xu)^T$, so

$$1 = j(xu)^T j^{-1} = ju^t x^T j^{-1} = ju^T j^{-1} \cdot jx^T j^{-1} = (ju^T j^{-1})x\,.$$

Thus $ju^T j^{-1} = u$, and $u \in T_4(n)$. Then

$$\begin{aligned} j(yx^{-1}y)^T j^{-1} &= j(yuy)^T j^{-1} = jy^T u^T y^T j^{-1} \\ &= jy^T j^{-1} \cdot ju^T j^{-1} \cdot jy^T j^{-1} = yuy = yx^{-1}y\,, \end{aligned}$$

so $yx^{-1}y \in T_4(n)$. □

Corollary 7.3. *The Circular Symplectic Ensemble $T_4(n)$ is a twisted subgroup of $U(2n)$.*

For the following generalization of Proposition 7.1, see [3, Th. 3].

Proposition 7.4. *For each element s of $T_4(n)$, there is a symplectic matrix b and a complex diagonal matrix*

$$e = \operatorname{diag}\big(\exp(2\pi i\theta_1), \exp(2\pi i\theta_1), \ldots, \exp(2\pi i\theta_n), \exp(2\pi i\theta_n)\big)$$

with $\theta_j \in \mathbb{R}$ for $1 \leq j \leq n$ such that $s = b^{-1}eb$, and the diagonal elements of e appear doubly.

Proposition 7.5. *The right multiplication group $\mathrm{RMlt}\big(T_4(n), \circ\big)$ of the right quasigroup $\big(T_4(n), \circ\big)$ acts transitively on $\big(T_4(n), \circ\big)$.*

Proof. Given an element s of $T_4(n)$, it will be shown that there is an element x of $T_4(n)$ such that $1R_\circ(x) = s$. The desired result then follows.

By Proposition 7.4, there is a symplectic matrix b and a diagonal matrix

$$e = \operatorname{diag}\big(\exp(2\pi i\theta_1), \exp(2\pi i\theta_1), \ldots, \exp(2\pi i\theta_n), \exp(2\pi i\theta_n)\big)$$

such that $s = b^{-1}eb$. Define

$$d = \operatorname{diag}\big(\exp(\pi i\theta_1), \exp(\pi i\theta_1), \ldots, \exp(\pi i\theta_n), \exp(\pi i\theta_n)\big) \tag{5}$$

and $x = b^{-1}db$. Note that d and x are both unitary, while $d^2 = e$. Furthermore $jd^Tj^{-1} = d$, by the chosen ordering of the eigenvalues — compare (4). Then

$$\begin{aligned} jx^Tj^{-1} &= j(b^{-1}db)^Tj^{-1} = jb^Td^T(b^{-1})^Tj^{-1} \\ &= jb^Tj^{-1} \cdot jd^Tj^{-1} \cdot j(b^{-1})^Tj^{-1} = b^{-1}db \end{aligned}$$

by Lemma 4.1, so $x \in T_4(n)$. Finally

$$1 \circ x = x1x = x^2 = b^{-1}dbb^{-1}db = b^{-1}d^2b = b^{-1}eb = s\,,$$

as required. □

Remark 7.6. As in the case of the Circular Orthogonal Ensemble (Remark 5.5), the matrix d of (5) may be replaced by

$$\begin{aligned} \operatorname{diag}\Big(&\exp\big(\pi i(\theta_1 + \lambda_1)\big), \exp\big(\pi i(\theta_1 + \lambda_1)\big), \dots \\ &\dots, \exp\big(\pi i(\theta_n + \lambda_n)\big), \exp\big(\pi i(\theta_n + \lambda_n)\big)\Big) \end{aligned}$$

for any vector $(\lambda_1, \dots, \lambda_n)$ in the unit cube $\{0,1\}^n$. This means that the solution x to $1 \circ x = s$ is not unique, so $\big(T_4(n), \circ\big)$ is not a quasigroup.

For the following, compare [3, Th. 5]. Dyson's theorem states that the measure of the Circular Symplectic Ensemble is the unique measure on the set $T_4(n)$ that is invariant under the $U(2n)$-action (6).

Proposition 7.7. *Let n be a positive integer. Then $T_4(n)$ is a transitive right $U(2n)$-set under the action*

$$A_4(u)\colon T_4(n) \to T_4(n); s \mapsto ju^Tj^{-1}su \tag{6}$$

for each element u of $U(2n)$.

Corollary 7.8. *The Canonical Symplectic Ensemble may be written as*

$$T_4(n) = \{ju^Tj^{-1}u \mid u \in U(2n)\}$$

for each positive integer n.

Proof. Note that $\{ju^Tj^{-1}u \mid u \in U(2n)\}$ is the orbit of 1 under the transitive $U(2n)$-action of Proposition 7.7. □

Proposition 7.9. *Under the action (6), the unitary group $U(2n)$ acts as a transitive group of automorphisms of the right quasigroup $\big(T_4(n), \circ\big)$.*

Proof. Consider $x, y \in T_4(n)$ and $u \in U(2n)$. Then

$$\begin{aligned} xA_4(u) \circ yA_4(u) &= \big(ju^Tj^{-1}xu\big) \circ \big(ju^Tj^{-1}yu\big) = \big(ju^Tj^{-1}yu\big)\big(ju^Tj^{-1}xu\big)^{-1}\big(ju^Tj^{-1}yu\big) \\ &= ju^Tj^{-1}yu \cdot u^{-1}x^{-1}j\left(u^T\right)^{-1}j^{-1} \cdot ju^Tj^{-1}yu \\ &= ju^Tj^{-1}yx^{-1}yu = \big(yx^{-1}y\big)\,A_4(u) = (x \circ y)A_4(u) \end{aligned}$$

as required. □

The results of this section may be summarized as follows.

Theorem 7.10. *Let n be a positive integer, and let $T_4(n)$ be Dyson's Canonical Symplectic Ensemble.*

(a) *$T_4(n)$ is a twisted subset of the unitary group $U(2n)$.*

(b) *$T_4(n)$ forms a transitive right quasigroup under the core operation $x \circ y = yx^{-1}y$.*

(c) *The automorphism group $U(2n)$ of the measure space $T_4(n)$ is an automorphism group of the right quasigroup $\big(T_4(n), \circ\big)$.*

References

[1] M. Aschbacher, "Near subgroups of finite groups," *J. Group Theory* **1** (1998), 113–129.

[2] R.H. Bruck, *A Survey of Binary Systems*, Springer, Berlin, 1958.

[3] F.J. Dyson, "Statistical Theory of the Energy Levels of Complex Systems. I," *J. Math. Phys.* **3** (1962), 140–156 (doi:10.1063/1.1703773).

[4] G.B. Folland, *A Course in Abstract Harmonic Analysis*, CRC Press, Boca Raton, FL, 1995.

[5] K. Iseki, "On the conjugate mapping for quaternions," *Publ. Math. Debrecen* **2** (1952), 204–205.

[6] L.H. Loomis, *An Introduction to Abstract Harmonic Analysis*, Van Nostrand, New York, NY, 1953.

[7] A.L. Myl'nikov, "Finite tangled groups," *Siberian Math. J.* **48** (2007), 369–375.

[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, New York, NY, 1999.

J.D.H. Smith,
Department of Mathematics, Iowa State University, Ames, Iowa 50011, U.S.A.
jdhsmith@iastate.edu
http://www.orion.math.iastate.edu/jdhsmith/