Inverse Conjugacies and Reversing Symmetry Groups

Geoffrey R. Goodson

INTRODUCTION. We present some elementary group theory that arises in the theory of time-reversing dynamical systems. Let G be a (usually non-abelian) group and let $a \in G$ be a fixed element. The set

$$C(a) = \{x \in G : xa = ax\},$$

the *centralizer* of a, is a subgroup of G that contains $\langle a \rangle$, the cyclic subgroup generated by a. Our aim is to study the *skew centralizer*

$$B(a) = \{x \in G : xa = a^{-1}x\}.$$

This paper arose from a course I gave on algebraic structures, where some of the results of Sections 1 and 2 and some examples from Section 4 were presented as exercises and then discussed in the classroom. In addition, the students were asked to calculate $B(a)$ and $C(a)$ for certain specific examples, sometimes with the aid of a software package.

Generally $B(a)$ is not a subgroup of G, and it may be empty. However, $E(a) = B(a) \cup C(a)$ is a group, which is called the *reversing symmetry group* of a. In dynamical systems theory, the group element a represents the time evolution operator of a dynamical system. We present some results familiar to people working in time reversing dynamical systems, but our presentation is given in an abstract setting, entirely from an elementary group theoretic point of view, in the hope that it will be of interest to teachers of a first course in group theory.

Section 1 gives some of the elementary properties of $B(a)$. We see that $B(a)$ is a group if and only if a is an involution, i.e., $a^2 = e$, the identity of G. In Section 2, we prove (following Lamb [**8**]) that $E(a)$ is a group having $C(a)$ as a normal subgroup. In dynamical systems, the case where a has infinite order is of most interest, but we show that there are interesting finite groups, such as the dihedral and dicyclic groups, that arise in a natural way from the study of $E(a)$. In Section 3 we study the inner automorphisms of $E(a)$ and apply them when G is a topological group. We give particular emphasis to the situation when $\{s^2 : s \in B(a)\}$ is a singleton set. Inverse conjugacies involving the permutation groups and some infinite groups originating in dynamical systems theory are our focus in Section 4.

In Section 5 we mention briefly the dynamical origins of the ideas discussed here, restricting our attention to the ergodic theory of measure-preserving transformations.

1. ELEMENTARY PROPERTIES OF $B(a)$. Elements $a, b \in G$ are said to lie in the same *conjugacy class* (that is, a and b are *conjugate*) if there exists some $x \in G$ satisfying $a = x^{-1}bx$. Thus $a \in G$ is conjugate to its inverse if $B(a) \neq \varnothing$.

The set $B(a)$ is a group only in special circumstances. If it is a group, then $B(a)$ contains the identity of G, which we denote by e, so $ea = a^{-1}e$, $a = a^{-1}$ or $a^2 = e$.

This in turn implies that $B(a) = \{x \in G : xa = a^{-1}x\} = C(a)$. On the other hand, if $B(a) = C(a)$, then $B(a)$ is a group. Let us also mention that if $B(a) \cap C(a)$ is non-empty, then we must have $a^2 = e$. We have proved:

Proposition 1. *For a group G and a given $a \in G$ with $B(a) \neq \varnothing$, the following are equivalent*:

(*i*) *$B(a)$ is a subgroup of G.*
(*ii*) *a is an involution, i.e., $a^2 = e$.*
(*iii*) *$B(a) = C(a)$.*
(*iv*) *$B(a) \cap C(a) \neq \varnothing$.*

If G is an abelian group, then $C(a) = G$, so from Proposition 1, either $B(a) = C(a)$ (when $a^2 = e$), or $B(a) = \varnothing$. If any of the conditions of Proposition 1 hold, we say that we have the *trivial case*.

In general, $B(a)$ may have elements of all even orders, and also of infinite order. However, if there exists an $x \in B(a)$ with $x^n = e$ for some odd $n \in \mathbb{Z}$, then

$$xa = a^{-1}x \Rightarrow x^n a = a^{-1}x^n \Rightarrow a = a^{-1} \Rightarrow a^2 = e,$$

so we again have the trivial case.

On the other hand, suppose $x \in B(a)$ is of order $2n$ and 2^m is the highest power of 2 dividing $2n$, i.e., $2n = 2^m k$ for some odd $k \in \mathbb{Z}$. Then $y = x^k \in B(a)$ and $y^{2^m} = x^{k \cdot 2^m} = x^{2n} = e$, so $B(a)$ also contains elements of order 2^m (see [**9**, p. 14]).

Notice that $a \in G$ is conjugate to a^{-1} if and only if there are $u, v \in G$ such that

$$a = vu^{-1} \quad \text{and} \quad u^2 = v^2.$$

To prove this, take any w such that $aw = wa^{-1}$. Then $(aw)^2 = awaw = wa^{-1}aw = w^2$. Set $v = aw \in B(a)$ and $u = w$. Then $a = vu^{-1}$ and $v^2 = (aw)^2 = w^2 = u^2$. Conversely, suppose $a = vu^{-1}$ and $u^2 = v^2$. Then $au = vu^{-1}u = v$ and $ua^{-1} = u(vu^{-1})^{-1} = u^2v^{-1} = v^2v^{-1} = v$, i.e., $au = ua^{-1}$.

The case where there exists an involution in $B(a)$ is important in the dynamical systems literature. We now see that a is conjugate to a^{-1} via an involution if and only if there are $u, v \in G$ such that $a = uv^{-1}$ and $u^2 = v^2 = e$ (see [**9**, p. 13] and [**4**]).

2. THE REVERSING SYMMETRY GROUP $E(a) = B(a) \cup C(a)$. We claim that the set $E(a) = B(a) \cup C(a)$, is a subgroup of G. This is clear if $B(a)$ is empty, so assume it is non-empty. Taking inverses of both sides of $xa = a^{-1}x$ gives $a^{-1}x^{-1} = x^{-1}a$, so

$$x \in B(a) \Leftrightarrow x^{-1} \in B(a) \quad \text{and} \quad xa = a^{-1}x \Leftrightarrow ax = xa^{-1}.$$

Since $B(a)$ and $C(a)$ are closed under the taking of inverses, so is $E(a)$.

Let $x, y \in E(a)$. If $x, y \in C(a)$, then $axy = xay = xya$. Therefore $xy \in C(a)$ and so $xy \in E(a)$.

If $x, y \in B(a)$, then $axy = xa^{-1}y = xya$. Therefore $xy \in C(a)$ and again $xy \in E(a)$.

The third possibility is $x \in B(a), y \in C(a)$. In this case $axy = xa^{-1}y = xya^{-1}$, so $xy \in B(a)$, and $xy \in E(a)$.

The proof that $E(a)$ is a group is completed on noting that $e \in C(a) \subseteq E(a)$.

The preceding argument shows that $C(a)$ is a subgroup of $E(a)$. Suppose $a^2 \neq e$ and $B(a) \neq \emptyset$, and let $x, y \in B(a)$. Then $x^{-1}y \in C(a)$ and $y \in x \cdot C(a)$. It follows that $B(a) \subseteq x \cdot C(a)$ and in a similar way that $x \cdot C(a) \subseteq B(a)$. In particular, the cosets of $C(a)$ in $E(a)$ are $C(a)$ and $x \cdot C(a) = B(a)$.

Clearly $x \cdot C(a) \cdot x^{-1} = C(a)$ for all $x \in E(a)$, so $C(a)$ is a normal subgroup of $E(a)$, and we see that $E(a)/C(a) \cong \mathbb{Z}_2$. If $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ is the cyclic subgroup generated by a, then $\langle a \rangle$ is a normal subgroup of both $C(a)$ and $E(a)$.

If G is a finite group having even order, then it is an easy exercise to show that there exists some $a \in G$, $a \neq e$, with $a^2 = e$; the conditions of Proposition 1 are satisfied for a, so $B(a) = C(a) \neq \emptyset$. Consequently, finite groups of even order always contain nontrivial elements that are conjugate to their inverse.

On the other hand, finite groups of *odd* order never contain a nontrivial element that is conjugate to its inverse. Suppose the order of G is odd and there is an $a \in G$, $a \neq e$, that is conjugate to its inverse. Lagrange's theorem implies that a cannot be of even order, so $a^2 \neq e$. By assumption, $B(a) \neq \emptyset$, so Proposition 1 implies that $E(a) = B(a) \cup C(a)$ is a disjoint union. Since the cosets of $C(a)$ in $E(a)$ are $C(a)$ and $B(a)$, $E(a)$ is a subgroup of G of even order. Lagrange's Theorem again tells us that this is impossible.

The fact that $E(a)$ is a group with $E(a)/C(a) \cong \mathbb{Z}_2$ appears in **[8]** and **[9**, p. 9–12]. However, the following may not be well known:

Proposition 2. *Let $a \in G$ with $B(a) \neq \emptyset$.*

- (*i*) *If $x \in B(a)$ and $x^2 \in \langle a \rangle$, then $x^4 = e$. In particular, if the order of $\langle a \rangle$ is infinite or odd, then $x^2 = e$.*
- (*ii*) *If $C(a) = \langle a \rangle$, then $\{x^2 : x \in B(a)\}$ is a singleton subset of $C(a)$.*
- (*iii*) *If $\{x^2 : x \in B(a)\}$ is a singleton set, then the order of x divides 4 for all $x \in B(a)$.*
- (*iv*) *The center of $E(a)$ is a subgroup of $C(a)$.*

Proof: (i) If $x \in B(a)$ and $x^2 \in \langle a \rangle$, then $x^2 = a^n$ for some $n \in \mathbb{Z}$. Since

$$xa = a^{-1}x \Rightarrow xa^n = a^{-n}x \Rightarrow x \cdot x^2 = x^{-2} \cdot x \Rightarrow x^4 = e,$$

we see that the order of x divides 4 and hence the order of x^2 divides 2. If $x^2 \in \langle a \rangle$, a cyclic group having infinite (or odd) order, then $\langle a \rangle$ cannot have any elements of order 2. Therefore $x^2 = e$.

(ii) In a similar way, if $x_1, x_2 \in B(a)$, then $x_1x_2 \in C(a) = \langle a \rangle$, so $x_1x_2 = a^n$ for some $n \in \mathbb{Z}$. Also $x_1a^n = a^{-n}x_1$, so $x_1x_1x_2 = (x_1x_2)^{-1}x_1$, or $x_1^2 = x_2^{-2} = x_2^2$, so $\{x^2 \colon x \in B(a)\}$ is a singleton set.

(iii) If $x \in B(a)$, then $x^3 \in B(a)$ so $x^2 = (x^3)^2 = x^6$, and this implies $x^4 = e$.

(iv) If x is in the center of $E(a)$, then $xg = gx$ for all $g \in E(a)$. In particular, $xa = ax$, so $x \in C(a)$. ■

Since $\langle a \rangle$ is a normal subgroup of $C(a)$, the quotient group $C(a)/\langle a \rangle$ is well defined. This group is sometimes called the *essential centralizer* of a. Proposition 2(ii) can be generalized to:

If $a \in G$ has infinite order and $C(a)/\langle a \rangle$ has order m for some $m \in \mathbb{Z}^+$, then every $x \in B(a)$ has order $2k$ for some k that divides m.

3. THE INNER AUTOMORPHISMS OF $E(a)$. The inner automorphisms of $E(a)$ have the form $\phi_s(x) = sxs^{-1}$ for some $s \in E(a)$. Since $C(a)$ and $\langle a \rangle$ are normal subgroups of $E(a)$, they are preserved by ϕ_s for all $s \in E(a)$. Furthermore, if $s \in B(a)$ and $x \in \langle a \rangle$, then $\phi_s(x) = x^{-1}$. This is because $x = a^n$ for some $n \in \mathbb{Z}$, and so $\phi_s(x) = sa^n s^{-1} = a^{-n} ss^{-1} = a^{-n} = x^{-1}$.

When is it true that $\phi_s(x) = x^{-1}$ for all $x \in C(a)$? Let us say that $s \in B(a)$ *conjugates* $C(a)$ *to* $C(a)^{-1}$ if $sx = x^{-1}s$ for all $x \in C(a)$, or, equivalently, if $\phi_s(x) = x^{-1}$ for all $x \in C(a)$.

We can now show that every $s \in B(a)$ conjugates $C(a)$ to $C(a)^{-1}$ if and only if $\{s^2 : s \in B(a)\}$ is a singleton set.

To see this we use the fact that $B(a) = sC(a)$ for each $s \in B(a)$. If $s \in B(a)$ conjugates $C(a)$ to $C(a)^{-1}$ then $sx = x^{-1}s$ for all $x \in C(a)$. This implies that $(sx)^2 = s^2$, and the result follows.

Conversely, suppose that $\{s^2 : s \in B(a)\}$ is a singleton set. Then $(sx)^2 = s^2$ for any $s \in B(a)$ and $x \in C(a)$. This immediately gives $sx = x^{-1}s$, so s conjugates $C(a)$ to $C(a)^{-1}$.

We leave it to the reader to show that if $\{s^2 : s \in B(a)\}$ is a singleton set, then $C(a)$ is abelian.

Our aim now is to apply the preceding results to the case where G is a metrizable topological group. Note that if $\langle a \rangle$ is dense in $C(a)$, then $C(a)$ must be abelian, and either $C(a) = \langle a \rangle$ or $C(a)$ is uncountable. An immediate consequence of the next theorem is that if $\langle a \rangle$ is dense in $C(a)$ and $B(a) \neq \varnothing$, then every $s \in B(a)$ conjugates $C(a)$ to $C(a)^{-1}$.

Theorem 1. *If* $\langle a \rangle$ *is dense in* $C(a)$ *and* $B(a) \neq \varnothing$, *then* $\{s^2 : s \in B(a)\}$ *is a singleton set.*

Proof: We are given that $\overline{\{a^n : n \in \mathbb{Z}\}} = C(a)$. Let $x_1, x_2 \in B(a)$, so $x_1 x_2 \in C(a)$. We use an argument similar to that in Proposition 2(ii).

There is a subsequence $\{n_i\}$ of integers for which $x_1 x_2 = \lim_{i \to \infty} a^{n_i}$. Furthermore, $ax_1 = x_1 a^{-1}$ implies that $a^{n_i} x_1 = x_1 a^{-n_i}$ for all i.

Letting $i \to \infty$ and using the continuity of multiplication and inversion in G, we obtain

$$x_1 x_2 x_1 = x_1 (x_1 x_2)^{-1} = x_1 x_2^{-1} x_1^{-1} \Rightarrow x_2 x_1 = x_2^{-1} x_1^{-1} \Rightarrow x_2^2 = x_1^{-2}.$$

The fact that $B(a)$ is closed under the taking of inverses now gives $x_1^2 = x_2^2$, so $\{x^2 : x \in B(a)\}$ is a singleton set. ∎

If $x \in B(a)$, then we cannot have $a \in \{x^{2n} : n \in \mathbb{Z}\}$ as this would imply $a^2 = e$, the trivial case. Whenever G is a topological group, the set $\{x^{2n} : n \in \mathbb{Z}\} \subseteq C(a)$ is never dense in $C(a)$ for any $x \in B(a)$.

This section is based on **[3]** and **[4]**; see also **[10]**, where inner automorphisms on $E'(a)$, the *reversing k–symmetry group* are discussed.

4. EXAMPLES.

(i) Dihedral and Dicyclic Groups. The *dihedral group* D_n of order $2n$ arising from the symmetries of a regular plane n-gon is

$$\langle a, x : a^n = e,\ x^2 = e,\ x^{-1}ax = a^{-1} \rangle.$$

The *dicyclic groups* of order $4m$ are

$$\langle a, x : a^{2m} = e, x^2 = a^m, x^{-1}ax = a^{-1} \rangle.$$

See [**1**, p. 6–8] or [**12**, p. 65–66] for a discussion of these groups.

If a has finite order n and $C(a) = \langle a \rangle$, Proposition 2(ii) says that $x^4 = e$ if $x \in B(a)$. Essentially two different cases arise:

(a) If $x^2 = e$, then $E(a) \cong D_n$.
(b) If $x^2 \neq e$, then $x^2 = a^{n/2}$. In particular, n is even and $E(a)$ is a dicyclic group of order $2n$.

As a concrete example, consider the smallest of the dicyclic groups, the quarternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with multiplication given by $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, and $ji = -k$, $kj = -i$, $ik = -j$ and the usual rules for multiplying by ± 1. Then $C(i) = \{\pm 1, \pm i\}$ and $B(i) = \{\pm j, \pm k\}$. Since $C(i) = \langle i \rangle$ is a cyclic group, $\{x^2 : x \in B(i)\} = \{-1\}$ is a singleton set.

(ii) Permutation Groups. Every element of the permutation group S_n on n symbols is conjugate to its inverse. This is because any permutation in S_n can be resolved into a product of disjoint cycles in a unique manner except for the order in which the cycles appear. Two permutations are in the same conjugacy class if they have the same cycle pattern. For example, in S_8 the permutations

$$x = (3,5,6)(2,4)(7,1) \quad \text{and} \quad y = (2,4,1)(3,5)(6,7)$$

have the same cycle pattern, so they lie in the same conjugacy class. It is clear that every permutation and its inverse have the same cycle pattern.

Not every element of the alternating group A_n need be conjugate to its inverse. For example in A_4, the cycles $(1,2,3)$ and $(1,2,3)^{-1}$ are not conjugate. This is because $B((1,2,3))$ (in S_4) consists solely of odd permutations. However, every element of A_5 is conjugate to its inverse ([**12**, p. 60]). Examples of infinite groups with this property are given in [**7**].

Note that the element $\sigma = (1,2)(3,4)$ of S_4 has order 2, so $C(\sigma) = B(\sigma)$. Also, $\tau = (2,3,4) \in C(\sigma)$ is of order 3 and $\tau\sigma = \sigma^{-1}\tau$.

(iii) An Infinite Group. Let $G = \langle a, k \rangle$ be the finitely generated group subject to the relations $kak^{-1} = a^{-1}$ and $k^4 = e$. Then $C(a) = \langle a, k^2 \rangle$, and if $x \in B(a)$ then for some $n \in \mathbb{Z}$ either $x = ka^n$ or $x = k^{-1}a^n$. Now

$$(ka^n)^2 = k^2(k^{-1}a^n k)a^n = k^2 a^{-n} a^n = k^2 \neq e,$$

and similarly for $k^{-1}a^n$. It follows that there are no involutions in $B(a)$. However, $|ka^n| = 4$ and $\{x^2 : x \in B(a)\}$ is a singleton set. It follows that $B(a)$ conjugates $C(a)$ to $C(a)^{-1}$.

(iv) Group Rotations. Let G be a compact *monothetic* topological group: there exists some $a \in G$ for which the set $\{a^n : n \in \mathbb{Z}\}$ is dense in G. In this case G is abelian, and we assume that $a^2 \neq e$. A nice example is the unit circle S^1 in the complex plane, with $a \in S^1$ chosen so that it is not a root of unity.

Let $\mathcal{G}$ be the group of all homeomorphisms $h : G \to G$, a subgroup of the permutation group of G. If we define $\phi_a : G \to G$ by $\phi_a(g) = a \cdot g$ for some fixed $a \in G$, then ϕ_a is a *rotation* of G and $\phi_a \in \mathcal{G}$.

We claim that $C(\phi_a) = \{\phi_b : b \in G\}$, for if $\psi \in C(\phi_a)$, then

$$\psi \circ \phi_a = \phi_a \circ \psi \Rightarrow \psi(ag) = a\psi(g), \quad \text{for all} \quad g \in G.$$

If $\psi(e) = b$, then $\psi(a) = a \cdot b$ and $\psi(a^n) = a^n \cdot b$ for all $n \in \mathbb{Z}$. Continuity of ψ now implies that $\psi(g) = b \cdot g$ for all $g \in G$, or $\psi = \phi_b$.

Note that $\phi_a^{-1}(g) = a^{-1}g$, so if we define $S: G \to G$ by $S(g) = g^{-1}$, then

$$S \circ \phi_a(g) = S(ag) = (ag)^{-1} = a^{-1}g^{-1} = \phi_a^{-1}(g^{-1}) = \phi_a^{-1} \circ S(g),$$

or $S \in B(\phi_a)$. It follows that every member of $B(\phi_a)$ is of the form $R = S \circ \phi_b$ for some $b \in G$. Now

$$R^2 = S \circ \phi_b \circ S \circ \phi_b = S \circ \phi_b \circ \phi_b^{-1} \circ S = S^2 = \mathrm{Id},$$

where Id is the identity in $\mathscr{G}$. We conclude that every member of $B(\phi_a)$ is an involution.

(v) Automorphism Groups. Let X be a group and let $\mathscr{G} = \mathrm{Aut}(X)$ be the automorphism group of X. If $\mathscr{G}$ is abelian (for example if X is cyclic, or is the p-adic integers) then $B(\phi) \neq \varnothing$ if and only if $\phi \in \mathscr{G}$ is an involution. In the general case there is a simple way to construct automorphisms conjugate to their inverses: Let $\phi \in \mathrm{Aut}(X)$. Then $\phi \times \phi^{-1} \in \mathrm{Aut}(X \times X)$. Define $\psi_0 \in \mathrm{Aut}(X \times X)$ by $\psi_0(x, y) = (y, x)$. Then $\psi_0 \in B(\phi \times \phi^{-1})$ and $\psi_0^2 = \mathrm{Id}$.

Other less-trivial members of $B(\phi \times \phi^{-1})$ can be described. For example, define $\psi \in \mathrm{Aut}(X \times X)$ by $\psi(x, y) = (y, \phi(x))$. We can verify directly that $(\phi \times \phi^{-1}) \circ \psi = \psi \circ (\phi^{-1} \times \phi)$, and ψ has infinite order if ϕ has infinite order.

Related examples can be given using countable direct products. Let X be a group and write $G = \Pi_{i=-\infty}^{\infty} X_i$, where $X_i = X$ for all $i \in \mathbb{Z}$. Define $\Phi: G \to G$ by $[\Phi(g)]_n = g_{n+1}$, where the subscript n denotes the nth coordinate. Then Φ is just the familiar shift automorphism.

Define automorphisms P and Q of G by $[P(g)]_n = g_{-n}$ and $[Q(g)]_n = g_{1-n}$. Then $\Phi = PQ$ is a product of two involutions. It follows from the last paragraph of Section 1 that Φ is conjugate to its inverse by an involution.

In a similar way we can construct other automorphisms of the product space that are conjugate to their inverses. Let $U: G \to G$ be defined by

$$U(\ldots, g_{-1}, \overset{*}{g}_0, g_1, g_2, \ldots) = \left(\ldots, \phi^{-1}(g_{-1}), \phi(g_0), \overset{*}{\phi}{}^{-1}(g_1), \phi(g_2), \ldots\right),$$

where the $*$ denotes the 0th coordinate and ϕ is an automorphism of X.

Note that $U^2 = \Phi^2$, where Φ is the shift map, so if we let $V = \Phi$ and $A = UV^{-1}$, that is,

$$A(\ldots, g_{-1}, \overset{*}{g}_0, g_1, \ldots) = \left(\ldots, \phi(g_{-1}), \overset{*}{\phi}{}^{-1}(g_0), \phi(g_1), \ldots\right),$$

then the same reasoning as in the preceding example implies that A is conjugate to A^{-1} and $U \in B(A)$.

5. DYNAMICAL ORIGINS. Let $T{:}X \to X$ be an *invertible measure-preserving transformation* on a Borel probability space $(X, \mathscr{F}, \mu)$. This means that $T^{-1}B \in \mathscr{F}$ and $\mu(T^{-1}B) = \mu(B)$ for all $B \in \mathscr{F}$. If T_1 and T_2 are two such transformations on corresponding probability spaces, T_1 is *conjugate* to T_2 if there is an invertible measure-preserving transformation $S: X_1 \to X_2$ such that $ST_1 = T_2S$ (when we write $f = g$ in this section, we mean $f(x) = g(x)$ for all $x \in X$ except possibly for a set of μ-measure zero). With every measure-preserving transformation T we associate a unitary operator

$$U_T: L^2(X, \mu) \to L^2(X, \mu); \quad U_T f(x) = f(Tx).$$

A measure-preserving transformation T is said to have *discrete spectrum* if U_T has discrete spectrum, i.e., there is a complete orthonormal sequence

$\{f_n\} \subset L^2(X, \mu)$ and a sequence $\{\lambda_n\}$ of complex numbers (of absolute value one) such that $f_n(Tx) = \lambda_n f_n(x)$ for all $n = 1, 2, \ldots$. More generally, T is said to have *simple spectrum* if there exists some $h \in L^2(X, \mu)$ such that the closed linear span of $\{U_T^n h : n \in \mathbb{Z}\}$ is all of $L^2(X, \mu)$.

A transformation T is *ergodic* if for any measurable function f, the condition $f(Tx) = f(x)$ implies $f =$ constant. This is equivalent to the condition: if $A \in \mathscr{F}$, then $T^{-1}A = A$ implies $\mu(A) = 0$ or 1.

Suppose G is a compact topological group with Haar measure λ, and whose measurable sets are the Borel subsets of G. If $a \in G$, the *rotation* $\phi_a : G \to G$ given by $\phi_a(g) = a \cdot g$ is a Haar measure-preserving transformation. The transformation ϕ_a is ergodic if and only if $\langle a \rangle$ is dense in G. A celebrated result of Halmos and von Neumann [**6**, Theorem 4] says that an ergodic transformation T with discrete spectrum is conjugate to an ergodic rotation $\phi_a : G \to G$ for some compact topological group G and some $a \in G$.

The characters of G have the property

$$\chi(\phi_a(g)) = \chi(a \cdot g) = \chi(a)\chi(g),$$

i.e., they are eigenfunctions of ϕ_a. Conversely, every eigenfunction of ϕ_a is a character of G. It is a consequence of Pontryagin duality theory that the characters constitute a complete orthonormal basis for $L^2(G, \lambda)$.

Let T be an ergodic transformation with discrete spectrum. The discrete spectrum theorem of Halmos and von Neumann implies that T is conjugate to its inverse. Also, if S is measure-preserving and $ST = T^{-1}S$, then $S^2 = I$. Furthermore, the centralizer of T (with a suitable topology) is a compact abelian group that is isomorphic to G in a natural way. Conversely, any ergodic T for which $C(T)$ is compact must have discrete spectrum.

Halmos and von Neumann asked whether every ergodic transformation is conjugate to its inverse via an involution. In 1951, Anzai showed that there is an ergodic transformation that is not conjugate to its inverse. As a consequence, this type of inverse-conjugacy problem lay dormant for some years. Recently it was shown that if a transformation T has simple spectrum and is conjugate to its inverse, then every conjugation is an involution. This generalizes aspects of the Halmos–von Neumann theorem [**3**, Theorem 1]. In addition, in [**3**], [**4**], [**8**], and [**9**] one finds many examples of transformations whose centralizers and skew centralizers have group theoretic properties similar to those discussed in this paper. Ergodic transformations with a wide variety of centralizers are now known. For an ergodic T, $C(T)$ can be a compact abelian group, a countable cyclic group, an uncountable monothetic group (hence abelian, but not locally compact), as well as many other abelian and non-abelian groups. A nice treatment of certain examples arising in this theory is given in [**2**].

6. CONCLUDING REMARKS. In the dynamical systems literature there has been some confusion about the role of involutory time-reversal systems. Some authors seem to believe that the set of reversing symmetries $B(a)$ (if non empty) must always contain an involution. Our examples show that this is not generally the case, although it is true in certain special contexts. For example, if $G = GL(n, \mathbf{R})$ then for all $a \in G$ such that $B(a) \neq \emptyset$, $B(a)$ contains an involution; see [**13**, Chapter 2]. Related results are given in [**5**], where properties of real orthogonal matrices are studied in this context. A survey of time-reversal symmetry in dynamical systems is given in [**11**].

ACKNOWLEDGMENTS. I thank Jay Zimmerman of Towson University and Jeroen Lamb of Warwick University for carefully reading the manuscript, suggesting many improvements, and providing additional references.

REFERENCES

1. H. S. M. Coxeter and W. O. J. Moser, *Generators and Relations for Discrete Groups*. Springer-Verlag, Berlin Heidelberg New York, 1984.
2. N. A. Friedman, Replication and stacking in ergodic theory, *Amer. Math. Monthly* **99** (1992) 31–41.
3. G. R. Goodson, A. del Junco, M. Lemańczyk, and D. J. Rudolph, Ergodic transformations conjugate to their inverses by involutions, *Ergodic Theory Dynamical Systems* **16** (1996) 97–124.
4. G. R. Goodson and M. Lemańczyk, Transformations conjugate to their inverses have even essential values, *Proc. Amer. Math. Soc.* **124** (1996) 2703–2710.
5. G. R. Goodson, The inverse-similarity problem for real orthogonal matrices, *Amer. Math. Monthly* **104** (1997) 223–230.
6. P. R. Halmos and J. von Neumann, Operator methods in classical mechanics II, *Annals Math.* **43** (1941) 332–350.
7. P. Hall, Some constructions for locally finite groups, *J. London Math. Soc.* **34** (1959) 305–319.
8. J. S. W. Lamb, Reversing symmetries in dynamical systems, *J. Phys. A: Math. Gen.* **25** (1992) 925–937.
9. J. S. W. Lamb, Reversing symmetries in dynamical systems, Ph.D. Thesis, University of Amsterdam, 1994.
10. J. S. W. Lamb and G. R. W. Quispel, Reversing *k*-symmetries in dynamical systems, *Phys. Rev. D* **73** (1994) 277–304.
11. J. S. W. Lamb and J. A. G. Roberts, Time-reversal in dynamical systems: a survey, University of Warwick preprint 34/1997.
12. W. Lederman, *Introduction to Group Characters*, Cambridge University Press, Cambridge, 1976.
13. M. B. Sevryuk, *Reversible systems*. Lecture Notes in Math. 1211, Springer-Verlag, Berlin Heidelberg New York, 1986.

GEOFFREY GOODSON was born in Cape Town, South Africa and was educated in Great Britain. He now teaches at Towson University (previously Towson State University) in Maryland. His interests include ergodic theory and mathematical exposition at the undergraduate level.
Towson University, Towson, MD 21252
ggoodson@towson.edu