SEMIENDOMORPHISMS OF SIMPLE NEAR-RINGS

KIRBY C. SMITH AND LEON VAN WYK

(Communicated by Maurice Auslander)

Abstract. Let \( N \) be a finite simple centralizer near-ring that is not an exceptional near-field. A semiendomorphism of \( N \) is a map \( \varphi \) from \( N \) into \( N \) such that \( (a + b)' = a' + b', \ (aba)' = a'b'a' \), and \( 1' = 1 \) for all \( a, b \in N \). It is shown that every semiendomorphism of \( N \) is an automorphism of \( N \). A Jordan-endomorphism of \( N \) is a map \( \varphi \) from \( N \) into \( N \) such that \( (a + b)' = a' + b' \), \( (ab + ba)' = a'b' + b'a' \), and \( 1' = 1 \) for all \( a, b \in N \). It is shown that every Jordan-endomorphism of \( N \) is an automorphism assuming \( 2 \in N \) is invertible. The above results imply that every semiendomorphism (Jordan-endomorphism) of a “special” class of semisimple near-rings is an automorphism. These results are in contrast to the ring situation where semiendomorphisms tend to be either an automorphism or an antiautomorphism.

1. Introduction

Let \( R \) be a ring with 1. By a semiendomorphism of \( R \) we mean a map \( \varphi \) from \( R \) into \( R \) such that \( (a + b)' = a' + b', \ (aba)' = a'b'a' \), and \( 1' = 1 \) for all \( a, b \) in \( R \). Semiendomorphisms of rings arose in connection with a fundamental theorem in projective geometry [2, pp. 37–40, 79–85]. In [1, 4] it was proven that every semiendomorphism of a division ring is either an automorphism or an antiautomorphism, and it was proven similarly for a complete matrix ring over a division ring.

Semiendomorphisms of rings found a new home in the study of Jordan rings. For if \( R \) is a ring with 1, then \( R \) can be made into a Jordan ring \( R^J \) using a new multiplication \( * \) defined by \( a*b = ab + ba \) where \( a, b \) are in \( R \). A Jordan automorphism of \( R^J \) is easily seen to be a semiendomorphism of the ring \( R \). Jordan automorphisms of rings (or more generally Jordan homomorphisms of rings) have been extensively studied, especially by Herstein [3, Chapter 3].

It is the goal of this work to initiate a study of semiendomorphisms of near-rings \( N \) with 1 that are not rings. So a semiendomorphism of \( N \) is a map \( \varphi \) from \( N \) into \( N \) such that \( (a + b)' = a' + b', \ (aba)' = a'b'a' \), and \( 1' = 1 \) for all \( a, b \) in \( N \). Unlike the ring case where a semiendomorphism normally turns out to be either an automorphism or an antiautomorphism, the lack of one distributive law in \( N \) should prevent a semiendomorphism from being an

Received by the editors October 2, 1990 and, in revised form, December 10, 1990.
1980 Mathematics Subject Classification (1985 Revision). Primary 16A76; Secondary 16A72.
antiautomorphism of \( N \). This will be seen to be the case for finite simple near-rings with 1 that are neither rings nor exceptional near-fields. In fact we prove that every semiendomorphism of such a near-ring is an automorphism.

2. Preliminaries

Let \( N \) be a (right) near-ring isomorphic to a near-ring of mappings \( M_A(G) \), where \( G \) is a finite group and \( A \) is a group of automorphisms of \( G \). (Recall that \( M_A(G) \) is the set of mappings \( f: G \to G \) such that \( f\alpha = \alpha f \) for every automorphism \( \alpha \in A \) and \( f(0) = 0 \) where 0 is the identity element of \( G \). The set \( M_A(G) \) forms a near-ring under the operations of function addition and function composition. \( M_A(G) \) is a “centralizer near-ring” as studied in [6].) We note that if \( A \) is a fixed point free group of automorphisms of \( G \) then \( M_A(G) \) is simple, and conversely any finite simple near-ring with 1 that is not a ring is isomorphic to a near-ring \( M_A(G) \) where \( A \) is fixed point free (see [6] and the references given there). An element \( e \) in \( N \) is idempotent if \( e \) is nonzero and \( e^2 = e \). If \( e_i \) and \( e_j \) are idempotents in \( N \), let \( N_{ij} \) denote the set \( e_i N e_j = \{ e_i n e_j | n \text{ is in } N \} \), a subset of \( N \). We recall some elementary properties of \( N \) (see [10]).

(i) There is a finite number of idempotents \( e_1, \ldots, e_t \) in \( N \) such that \( 1 = e_1 + \cdots + e_t \), \( e_i e_j = 0 \) for all \( i, j \) with \( i \neq j \) and \( e_i + e_j = e_j + e_i \) for all \( i, j \).

(ii) For \( i = 1, \ldots, t \) the set \( (e_i N e_i)^* = N_{ii}^* = N_{ii} \setminus \{0\} \) is a group under multiplication with identity \( e_i \).

(iii) If \( n_{i j i} \) is in \( N_{i j i} \), \ldots, \( n_{i j t} \) is in \( N_{i j t} \) with \( \{ j_1, \ldots, j_t \} = \{1, \ldots, t\} \), then for every \( f \) in \( N \), \( f(n_{i j 1} + \cdots + n_{i j t}) = f n_{i j 1} + \cdots + f n_{i j t} \).

(iv) For every \( f \) in \( N \) and for every \( n_{ij} \in N_{ij} \), \( f n_{ij} \) belongs to \( N_{kj} \) for some \( k \) (\( k \) depends on \( f \) and \( n_{ij} \)).

(v) For every \( n_{ij} \) in \( N_{ij} \) and for every \( n_{kj} \) in \( N_{kj} \), \( n_{ij} + n_{kj} \) belongs to \( N_{s j} \) for some \( s \) (\( s \) depends on \( n_{ij} \) and \( n_{kj} \)).

(vi) If \( N_{ij} \neq \{0\} \) and \( N_{jk} \neq \{0\} \), then \( N_{ik} \neq \{0\} \).

We note that the set of idempotents \( \{ e_i \} \) referred to in (i)-(vi) is unique and each \( e_i \) is a primitive idempotent (see [10]). Moreover, the centralizer near-ring \( N \) is simple if and only if \( N_{ij} \) is nonzero for all \( i, j \). In this case we have the following:

(vii) If \( N \) is simple, then for every nonzero \( n_{ij} \) in \( N_{ij} \) there exists an element \( m_{ji} \) in \( N_{ji} \) such that \( n_{ij} m_{ji} = e_i \) and \( m_{ji} n_{ij} = e_j \).

3. Semiendomorphisms of finite simple centralizer near-rings

In §§3, 4 we assume that \( N \) is a finite simple centralizer near-ring with associated idempotents \( e_1, \ldots, e_t \) where \( t \geq 2 \).

Let \( ' \) be a semiendomorphism of \( N \). So \( (a + b)' = a' + b' \), \( (a b a)' = a' b' a' \), and \( ' 1 = 1 \) for all \( a, b \) in \( N \). If \( b = 1 \) then \( (a^2)' = (a 1 a)' = a' 1' a' = (a')^2 \), and so \( ' \) preserves squares of elements.

Lemma 3.1. For each \( i \), \( e_i' \neq 0 \).

Proof. Suppose \( e_i' = 0 \). Let \( j \neq i \), and choose \( n_{ij} \) in \( N_{ij} \) and \( n_{ji} \) in \( N_{ji} \) such that \( n_{ij} n_{ji} = e_i \) and \( n_{ji} n_{ij} = e_j \). Then \( e_j = (n_{ij} + n_{ji}) e_i (n_{ij} + n_{ji}) \) and \( e_j' = (n_{ij} + n_{ji}) e_i' (n_{ij} + n_{ji})' = 0 \). Thus \( e_i' = 0 \) implies \( e_j' = 0 \) for all \( j \), but
this is impossible since \( 0 \neq 1 = 1' = e'_i + \cdots + e'_t \).

Since \( ' \) preserves squares, Lemma 3.1 implies that \( e'_i \) is an idempotent for every \( i \). In Proposition 3.5 we will show that \( ' \) simply permutes the \( e_i \)'s. Toward this goal we need some preliminary results.

If \( f \) is an element in \( N \), then \( f = f(e_1 + \cdots + e_t) = fe_1 + \cdots + fe_t \). By (iv) each \( fe_i \) belongs to \( N_{k_i} \) for some \( k_i \). This means \( f \) has the form \( f = n_{k_1} + \cdots + n_{k_t} \) where \( n_{k_i} \) belongs to \( N_{k_i} \). Moreover this form for \( f \) is easily seen to be unique. We call \( n_{k_1}, \ldots, n_{k_t} \) the summands of \( f \). Henceforth the notation for \( n_{ij} \) will mean \( n_{ij} \) is an element of \( N_{ij} \).

The next lemma describes the form of those elements in \( N \) that are idempotent.

**Lemma 3.2.** An element \( f \neq 0 \) in \( N \) is idempotent if and only if whenever \( n_{ij} \) is a nonzero summand of \( f \) then \( e_i \) is also a summand of \( f \).

**Proof.** Assume \( f \) is idempotent and \( f = n_{k_1} + \cdots + n_{ij} + \cdots + n_{k_t} \) where \( n_{ij} \) is nonzero. Since \( f \) is idempotent, \( f = f^2 = f(n_{k_1} + \cdots + n_{ij} + \cdots + n_{k_t}) = f_n_{k_1} + \cdots + f_{n_{ij}} + \cdots + f_{n_{k_t}} \). Using (iv) and the uniqueness of the form for \( f \), we have \( f_{n_{ij}} = n_{ij} \). Therefore the \( i \)th summand of \( f \) must be \( e_i \).

Now assume \( n_{ij} \), a nonzero summand of \( f \), means \( e_i \) is also a summand of \( f \). Then \( f_{n_{ij}} = n_{ij} \). Since this is true for every nonzero summand of \( f \), \( ff = f \), i.e. \( f \) is idempotent.

Since \( e'_i \) is a nonzero idempotent for all \( i \), Lemma 3.2 implies that \( e'_i \) has at least one summand of the form \( e_k \). The next lemma says there is exactly one such summand.

**Lemma 3.3.** There is a permutation \( \mu \) of \( \{1, \ldots, t\} \) such that for each \( i \), \( e'_i = e_{\mu(i)} + \sum_{k \neq \mu(i)} n_{\mu(i)k} \) where \( n_{\mu(i)k} \) belongs to \( N_{\mu(i)k} \).

**Proof.** Assume \( e_k \) is a summand of both \( e'_i \) and \( e'_j \). Then \( e'_i e'_j e'_i \neq 0 \), but \( e'_i e'_j e'_j = (e_i e_j e_j)' = 0 \), a contradiction. So each \( e'_i \) has exactly one idempotent summand, and no two have the same idempotent summand. Hence there exists a permutation \( \mu \) of \( \{1, \ldots, t\} \) such that \( e'_i = e_{\mu(i)} + \sum_{k \neq \mu(i)} n_{\mu(i)k} \).

**Lemma 3.4.** If \( i \neq j \) then \( e'_i e'_j = 0 \).

**Proof.** If follows from (iii) that \( e'_i = (e'_i + e'_j) e'_j (e'_i + e'_j) \). Also, \( e'_i + e'_j \) is idempotent since \( e_i + e_j \) is idempotent. Multiply the above equation on the left by \( e'_i + e'_j \), and obtain \( (e'_i + e'_j) e'_j = e'_j \) or \( e'_i e'_j + e'_j = e'_j \). This means \( e'_i e'_j = 0 \).

Henceforth, \( \mu \) will be the permutation obtained in Lemma 3.3.

**Proposition 3.5.** For each \( i \), \( e'_i = e_{\mu(i)} \).

**Proof.** Suppose \( e'_i \) has \( n_{\mu(i)k} \) as a nonzero summand where \( k \neq \mu(i) \). Since \( k \neq \mu(i) \), \( k = \mu(s) \) for some \( s \neq i \). By Lemma 3.4, \( e'_i e'_s = 0 \), and by Lemma 3.3, \( e'_s = e_{\mu(s)} + \sum_{j \neq \mu(s)} m_{\mu(s)j} \). This means \( e'_i e'_s \neq 0 \), since \( e'_i e'_s \) has the nonzero summand \( n_{\mu(i)\mu(s)} e_{\mu(s)} \), a contradiction. So \( n_{\mu(i)k} = 0 \) for all \( k \neq \mu(i) \). This means \( e'_i = e_{\mu(i)} \).

Our next goal is to show that for each \( i \) and \( j \), the image of \( N_{ij} \) under \( ' \) is either \( N_{\mu(i)\mu(j)} \) or \( N_{\mu(j)\mu(i)} \). This will be shown in Proposition 3.9.
Lemma 3.6. If \( n_{ij} \neq 0 \) then \( n'_{ij} \neq 0 \).

Proof. First, suppose \( n_{ij} \neq 0 \) and \( n'_{ij} = 0 \). Since \( N'_{ii}^* \) is a group under multiplication, \( n_{ij} \) has an inverse \( n_{ij}^{-1} \) in \( N_{ii} \). We have \( e_i = n_{ii}^{-1}n_{ii}^1n_{ii}^{-1} \) and \( e'_i = (n_{ii}^{-1})'(n_{ii}^1)^2(n_{ii}^{-1})' = 0 \), which contradicts Lemma 3.1.

Second, let \( i \neq j \), \( n_{ij} \neq 0 \), and suppose \( n'_{ij} = 0 \). Then there exists \( n_{jj} \) in \( N_{jj} \) such that \( n_{ij}n_{jj} = e_i \) and \( n_{jj}n_{ij} = e_j \). We have \( (n_{ij} + n_{jj})^2 = e_i + e_j \), but then \( e_{\mu(i)} + e_{\mu(j)} = ((n_{ij} + n_{jj})')^2 = (n'_{ij} + n'_{jj})^2 = (n_{jj}^2)' = 0' = 0 \), which is not true. Therefore \( n'_{ij} \neq 0 \).

Lemma 3.6 implies that the map \( ' \) is one-to-one on \( N_{ij} \) for all \( i \) and \( j \).

We will show in Theorem 3.1 that \( ' \) is one-to-one on \( N \).

We note that if \( i \neq j \) then \( (n'_{ij})^2 = 0 \). The following lemma characterizes those elements in \( N \) that are nilpotent of index 2.

Lemma 3.7. Let \( f \) be an element of \( N \). Then \( f^2 = 0 \) if and only if \( f \) has the property that if \( n_{ij} \neq 0 \) is a summand of \( f \) then \( n_{ki} \) is not a summand of \( f \) for any \( n_{ki} \) in \( N_{kj}^* \), \( k = 1, \ldots, t \).

Proof. Assume \( f \) in \( N \) is such that \( f^2 = 0 \) and \( f \) has a summand \( n_{ij} \neq 0 \). If \( f \) has a summand of the form \( n_{ki} \neq 0 \) then \( f^2 \) has \( n_{ki} \) as a summand, contradicting \( f \) having index 2.

Conversely assume that if \( n_{ij} \neq 0 \) is a summand of \( f \), then \( n_{ki} \neq 0 \) is not a summand for any \( k \). Then clearly \( f^2 = 0 \).

Lemma 3.8. For all \( i \) and \( j \), either \( n'_{ii} \) is in \( N_{\mu(i)\mu(j)} \) or \( n'_{ij} \) is in \( N_{\mu(j)\mu(i)} \).

Proof. If \( i = j \) then \( n'_{ii} = e_i n'_{ii} e_i = e_{\mu(i)} n'_{ii} e_{\mu(i)} \), which means \( n'_{ii} \) belongs to \( N_{\mu(i)\mu(i)} \).

If \( i \neq j \) then \( n_{ij} = (e_i + e_j)n_{ij}(e_i + e_j) \), and so \( n'_{ij} = (e_i + e_j)'n_{ij}'(e_i + e_j)' = (e_{\mu(i)} + e_{\mu(j)})n'_{ii}(e_{\mu(i)} + e_{\mu(j)}) \). Since \( (n_{ij}^2)' = 0 \), Lemma 3.7 implies that the possible nonzero summands of \( n'_{ij} \) are of the form \( m_{\mu(i)\mu(j)} \) or \( m_{\mu(j)\mu(i)} \); that is, \( n'_{ij} = m_{\mu(i)\mu(j)} + m_{\mu(j)\mu(i)} \). But again since \( (n'_{ij})^2 = 0 \), it follows from Lemma 3.7 that either \( n'_{ij} = m_{\mu(i)\mu(j)} \) is in \( N_{\mu(i)\mu(j)} \) or \( n'_{ij} = m_{\mu(j)\mu(i)} \) is in \( N_{\mu(j)\mu(i)} \).

Proposition 3.9. For all \( i \) and \( j \), either \( N'_{ij} = N_{\mu(i)\mu(j)} \) or \( N'_{ij} = N_{\mu(j)\mu(i)} \).

Proof. Suppose there exist nonzero \( n_{ij} \), \( m_{ij} \) in \( N_{ij} \) such that \( n'_{ij} \) is in \( N_{\mu(i)\mu(j)} \) and \( m'_{ij} \) is in \( N_{\mu(j)\mu(i)} \). We have \( n_{ij} + m_{ij} \) is in \( N_{kj} \) for some \( k \) by (v). If \( k \neq j \) then \( (n_{ij} + m_{ij})^2 = 0 \), so \( (n'_{ij} + m'_{ij})^2 = 0 \), which is not true by Lemma 3.7. If \( k = j \) then \( (n_{ij} + m_{ij})^2 \) is in \( N_{jj} \), so \( (n'_{ij} + m'_{ij})^2 \) is in \( N_{\mu(j)\mu(j)} \). But it follows from (vi) that \( (n'_{ij} + m'_{ij})^2 \) belongs to \( N_{\mu(i)\mu(i)} + N_{\mu(j)\mu(j)} \) and does not belong to \( N_{\mu(j)\mu(j)} \). Hence the uniqueness of summands of \( (n'_{ij} + m'_{ij})^2 \) leads to a contradiction, and so \( N'_{ij} \) is a subset of \( N_{\mu(i)\mu(i)} \) or a subset of \( N_{\mu(j)\mu(j)} \). But \( ' \) is one-to-one on \( N_{ij} \) and all the \( N_{ij} \)'s have the same (finite) cardinality, and so the desired result follows.

In Proposition 3.11 we will show that \( N'_{ij} = N_{\mu(i)\mu(j)} \) for all \( i \) and \( j \).

Lemma 3.10. If \( N'_{ij} = N_{\mu(i)\mu(j)} \) for one pair \( i, j \) with \( i \neq j \), then \( N'_{uk} = N_{\mu(u)\mu(k)} \) for all \( k, u \).

Proof. First suppose that \( N'_{ji} = N_{\mu(i)\mu(j)} \), and let \( 0 \neq n_{ij} \) be in \( N_{ij} \) and \( 0 \neq m_{ji} \) be in \( N_{ji} \). By Lemma 3.6, \( 0 \neq n'_{ij} \) is in \( N_{\mu(i)\mu(j)} \), and \( 0 \neq m'_{ji} \) is in...
N_{\mu(j,\mu(i))} \cdot \text{Since } 0 \neq (n_{ij} + m_{ji})e_j(n_{ij} + m_{ji}) \in N_{ji}, \text{ by Lemma 3.6, } 0 \neq (n_{ij}' + m_{ji}')e_j(n_{ij}' + m_{ji}'). \text{ But } n_{ij}' \in N_{\mu(i,\mu(j))} \text{ and } m_{ji}' \in N_{\mu(i,\mu(j))} \text{ so } (n_{ij}' + m_{ji}')e_j(n_{ij}' + m_{ji}') = 0, \text{ a contradiction. This means } N_{ji} = N_{\mu(i,\mu(j))}.

Second, choose any } k \text{ such that } k \neq i \text{ and } k \neq j \text{ (if such a } k \text{ exists). Then } 0 \neq (n_{ki} + n_{jk}m_{ij}(n_{ki} + n_{jk})) = (n_{ki}' + n_{jk}'m_{ij}(n_{ki}' + n_{jk}')) \text{ where } n_{ki}, n_{jk}, \text{ and } m_{ij} \text{ are nonzero. Since } m_{ij}' \in N_{\mu(i,\mu(j))}, j \neq i, \text{ and } k \neq i, \text{ we have } n_{jk}'m_{ij}' = 0 \text{ by Lemma 3.8. So we must have } n_{jk}'m_{ij}' \neq 0. \text{ Since } k \neq i, \text{ it follows from Lemma 3.8 that } n_{ki}' \text{ belongs to } N_{\mu(k,\mu(i))}, \text{ and so by Proposition 3.9, } N_{ki} = N_{\mu(k,\mu(i))} \text{ for all } k. \text{ Fix } k \text{ and repeat the above argument, giving } N_{uk}' = N_{\mu(\mu(i,\mu(k)))} \text{ for all } u.

**Proposition 3.11.** \( N_{ij}' = N_{\mu(i,\mu(j))} \) \text{ for all } i \text{ and } j.

**Proof.** Suppose \( N_{ij}' = N_{\mu(i,\mu(j))} \). Then by Proposition 3.9 and Lemma 3.10, this is true for all \( i \) and \( j \). Choose \( k \neq j \), and select a nonzero \( n_{kj} \) in \( N_{kj} \). We have \( e_j = (e_j - n_{kj}) + n_{kj} \). By (v), \( e_j - n_{kj} = m_{uj} \) is in \( N_{uj} \) for some \( u \). Then \( e_j = m_{uj} + n_{kj} \), and so \( e_j' = m_{uj}(\mu(u)) + n_{\mu(j,\mu(k))} \). If \( u = k \) then by (v), \( m_{uj}(\mu(u)) + n_{\mu(j,\mu(k))} \in N_{\mu(\mu(k,\mu(i)))} \text{ for some } s. \text{ But since } \mu(k) \neq \mu(j), \text{ this is impossible. If } u \neq k, \text{ then } \mu(u) \neq \mu(k), \text{ and } e_j' \text{ would not be idempotent. Hence } N_{ij}' = N_{\mu(i,\mu(j))} \text{ for all } i, j.

**Lemma 3.12.** If \( j \neq k \) then \( (n_{ij}m_{uk} + m_{uk}n_{ij})' = n_{ij}'m_{uk}' + m_{uk}'n_{ij}' \) for all \( n_{ij} \in N_{ij} \text{ and } m_{uk} \in N_{uk} \).

**Proof.** Using Lemmas 3.10 and 3.11 and distributivity as in (iii), we have
\[
((n_{ij} + m_{uk})^2)' = (n_{ij}' + m_{uk}')^2 = (n_{ij}')^2 + n_{ij}'m_{uk}' + m_{uk}'n_{ij}' + (m_{uk}')^2.
\]
On the other hand
\[
((n_{ij} + m_{uk})^2)' = (n_{ij}' + n_{ij}m_{uk} + m_{uk}n_{ij} + m_{uk}^2)' = (n_{ij}')^2 + (n_{ij}m_{uk} + m_{uk}n_{ij})' + (m_{uk}')^2.
\]
Comparing the two results gives \( (n_{ij}m_{uk} + m_{uk}n_{ij})' = n_{ij}'m_{uk}' + m_{uk}'n_{ij}' \).

**Theorem 3.1.** If \( N \) is a finite simple centralizer near-ring with \( 1 = e_1 + \cdots + e_t \) where \( t \geq 2 \) and if \( ' \) is a semiendomorphism of \( N \), then \( ' \) is an automorphism of \( N \).

**Proof.** Let \( i \neq j \), and let \( n_{ji} \text{ be in } N_{ji} \text{ and } n_{ii} \text{ be in } N_{ii} \). It follows from Lemma 3.12 that \( (n_{ji}n_{ii})' = (n_{ji}n_{ii} + n_{ii}n_{ji})' = n_{ji}'n_{ii}' + n_{ii}'n_{ji}' = n_{ji}'n_{ij}' \text{ since } n_{ii}'n_{ij}' = 0 \text{ by Proposition 3.11. Since } n_{ii}m_{ii} \in N_{ii} \text{ and } n_{ji}m_{ii} \in N_{ji} \text{ for every } m_{ii} \text{ in } N_{ii}, \text{ the above argument shows that } n_{ji}'(n_{ii}m_{ii})' = (n_{ji}n_{ii}m_{ii})' = (n_{ji}n_{ii})'m_{ii}' = n_{ji}'n_{ii}'m_{ii}' \text{. Hence it follows from (vii) that } (n_{ii}m_{ii})' = n_{ji}'m_{ii}'.

By Lemma 3.12, \( (n_{ij}n_{ji} + n_{ji}n_{ij})' = n_{ij}'n_{ji}' + n_{ji}'n_{ij}' \). Then \( e_{ij}'(n_{ij}n_{ji} + n_{ji}n_{ij})'e_{ij}' = e_{ij}'(n_{ij}'n_{ji}' + n_{ji}'n_{ij}')e_{ij}' \text{ or } (e_{ij}(n_{ij}n_{ji} + n_{ji}n_{ij})e_{ij})' = e_{ij}'n_{ij}'n_{ji}'e_{ij}'. \text{ This implies that } (n_{ij}m_{ij})' = n_{ij}'m_{ij}'.

If \( k \neq i \), then by Lemma 3.12, \( (n_{ij}m_{jk} + m_{jk}n_{ij})' = (n_{ij}m_{jk} + m_{jk}n_{ij})' = n_{ij}'m_{jk}' + m_{jk}'n_{ij}' \text{ since } m_{jk}'n_{ij}' = 0 \text{ by Proposition 3.11.}

We now have \( (n_{ij}m_{uk})' = n_{ij}'m_{uk}' \text{ for all } i, j, k, u \) and \( n_{ij} \text{ in } N_{ij} \text{, } m_{uk} \text{ in } N_{uk} \).

Suppose \( f \) belongs to \( N \) with \( f' = 0 \). We can uniquely write \( f = n_{k_1} + \cdots + n_{k_t} \). Then \( 0 = f' = n_{\mu(k_1)\mu(1)} + \cdots + n_{\mu(k_t)\mu(i)} \), which means \( n_{k_t} = n_{\mu(k_t)\mu(i)} = 0 \).
for all $i$. By Lemma 3.6, $n_{ki} = 0$ for all $i$. Hence $\varphi$ is one-to-one on $N$. Since $N$ is finite, $\varphi$ is onto.

Let $f = \sum_i n_{ki}$ and $g = \sum_j m_{kj}$ be in $N$. Then $fg = \sum_j(\sum_i(n_{ki}m_{kj}))$ using (iii). But then $(fg)^\prime = \sum_j(\sum_i(n_{ki}m_{kj})) = f^\prime g^\prime$, and $\varphi$ is an automorphism of $N$.

4. JORDAN-ENDOMORPHISMS OF FINITE SIMPLE CENTRALIZER NEAR-RINGS

It was shown in [5] that in the ring case the condition

$$(aba)^\prime = a'b'a'$$

is equivalent to the condition

$$(ab + ba)^\prime = a'b' + b'a'$$

for characteristic different from 2 (and otherwise stronger). This is not true for near-rings, however, as Example 4.1 shows.

McQuarrie [7] originally devised the following (infinite) distributively generated (dg) near-ring with identity. Let $G_2$ be the (additive) group on two generators $x$ and $y$, and define for every integer $n$ the mapping $\Gamma_n : G_2 \to G_2$ by

$$\Gamma_n(h(x, y)) = h(nx, ny),$$

where $h(x, y)$ is an arbitrary word in $G_2$. Every $\Gamma_n$ is an element of the full near-ring $M(G_2)$ of mappings on $G_2$; in fact, the $\Gamma_n$'s form a semigroup of monomorphisms of $G_2$. Hence [8, Lemma 9.6], the $\Gamma_n$'s are distributive elements of $M(G_2)$. Let $N$ be the subnear-ring of $M(G_2)$ generated by $\{\Gamma_n : n \in \mathbb{Z}\}$ where $\mathbb{Z}$ is the set of integers, i.e., $(N, \{\Gamma_n : n \in \mathbb{Z}\})$ is a dg near-ring. By [8, Lemma 9.11], $(N, +)$ is generated as a group by $\{\Gamma_n : n \in \mathbb{Z}\}$. We use this near-ring in the following example.

**Example 4.1.** Define $\varphi$ from $N$ into $N$ by

$$\left(\sum_{i=1}^{k} e_{n_i} \Gamma_{n_i}\right)^{\prime} = \sum_{i=1}^{k} e_{n_i} \Gamma_{-n_i},$$

where $e_{n_i} = \pm 1$ and $n_i \in \mathbb{Z}$ for $i = 1, 2, \ldots, k$. We show that $\varphi$ is well defined. First note that $\Gamma_n(h(-x, -y)) = h(n(-x), n(-y)) = h((-n)x, (-n)y) = \Gamma_{-n}(h(x, y))$ for every $n \in \mathbb{Z}$ and every word $h(x, y)$ in $G_2$. Now suppose that $\sum_{i=1}^{k} e_{n_i} \Gamma_{n_i} = \sum_{j=1}^{\prime} e_{m_j} \Gamma_{m_j}$. Then

$$e_{n_1} \Gamma_{n_1} + \cdots + e_{n_k} \Gamma_{n_k} - e_{m_1} \Gamma_{m_1} - \cdots - e_{m_1} \Gamma_{m_1} \equiv 0,$$

and so

$$(e_{n_1} \Gamma_{n_1} + \cdots + e_{n_k} \Gamma_{n_k} - e_{m_1} \Gamma_{m_1} - \cdots - e_{m_1} \Gamma_{m_1})(h(-x, -y)) = 0.$$

Hence, by the above remark,

$$(e_{n_1} \Gamma_{-n_1} + \cdots + e_{n_k} \Gamma_{-n_k} - e_{m_1} \Gamma_{-m_1} - \cdots - e_{m_1} \Gamma_{-m_1})(h(x, y)) = 0,$$

i.e., $\sum_{i=1}^{k} e_{n_i} \Gamma_{-n_i} = \sum_{j=1}^{\prime} e_{m_j} \Gamma_{-m_j}$. It is now obvious that $\varphi$ is an endomorphism of $(N, +)$. Also, since $(\Gamma_{n} \Gamma_{m} \Gamma_{n})^\prime = \Gamma_{nmn}^\prime = \Gamma_{mnm}^\prime = \Gamma_{-n} \Gamma_{-m} \Gamma_{-n} = \Gamma_{n} \Gamma_{m} \Gamma_{n}^\prime$ for all $m, n \in \mathbb{Z}$, it follows easily that

$$(fgf)^\prime = f^\prime g^\prime f^\prime$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
for all \( f, g \in N \). \( (\Gamma_1 \Gamma_1 + \Gamma_1 \Gamma_1)' \neq \Gamma_1 \Gamma_1 + \Gamma_1 \Gamma_1', \) however, since \( (\Gamma_1 \Gamma_1 + \Gamma_1 \Gamma_1)'(x + y) = (\Gamma_1 \Gamma_1 + \Gamma_1 \Gamma_1)(x + y) = (\Gamma_1 \Gamma_1 + \Gamma_1 \Gamma_1)(x + y) = (\Gamma_1 \Gamma_1 + \Gamma_1 \Gamma_1'(x + y) = x + y + x + y \).

Henceforth \( N \) will be a finite simple centralizer near-ring with associated idempotents \( e_1, e_2, \ldots, e_t \) where \( t \geq 2 \), as in \( \S 3 \). Let \( ' \) be a Jordan-endomorphism of \( N \), and so \( (a + b)' = a' + b' \), \( (ab + ba)' = a'b' + b'a' \), and \( 1' = 1 \). Our goal in this section is to show in Theorem 4.1 that every Jordan-endomorphism of \( N \) is an automorphism of \( N \) in the case \( 2(= 1 + 1) \) is invertible in \( N \). To this end we pursue the same path as in \( \S 3 \), although some of the proofs are completely different. For the ease of the reader we state all the relevant results.

**Lemma 4.2.** For each \( i \), \( e_i' \neq 0 \).

*Proof.* If \( e_i' = 0 \), then for \( j \neq i \), \( n_{ij}' = (e_i n_{ij} + n_{ij} e_i)' = e_i n_{ij}' + n_{ij}' e_i' = 0 \). Similarly \( n_{ji}' = 0 \). By (vii) there exist elements \( m_{ij}, m_{ji} \) such that \( e_i = m_{ij} m_{ji} \) and \( e_j = m_{ji} m_{ij} \). Then \( (e_i + e_j)' = e_i' + e_j' = (m_{ij} m_{ji} + m_{ji} m_{ij})' = m_{ij}' m_{ji}' + m_{ji}' m_{ij}' = 0 \). Since \( e_i' = 0 \), \( e_j' = 0 \). This being true for every \( j \) implies \( 1' = 0 \), a contradiction. So \( e_i' \neq 0 \).

Now assume that \( N \) has the property that \( 2a = 2b \) implies \( a = b \), i.e., assume 2 is invertible in \( N \). Note that \( ' \) preserves squares, since for every \( n \in N \), \( 2(n^2)' = (2n^2)' = (nn + nn)' = n'n' + n'n' = 2(n')^2 \), and so \( (n^2)' = (n')^2 \).

The proof of the following lemma is identical to that of Lemma 3.2.

**Lemma 4.3.** An element \( f \neq 0 \in N \) is idempotent if and only if whenever \( n_{ij} \) is a nonzero summand of \( f \), \( e_i \) is also a summand of \( f \).

**Lemma 4.4.** There is a permutation \( \mu \) of \( \{1, 2, \ldots, t\} \) such that for each \( i \), \( e_i' = e_i + \sum_{k \neq \mu(i)} n_{\mu(i)k} \) where \( n_{\mu(i)k} \in N_{\mu(i)k} \).

*Proof.* Assume \( e_k \) is a summand of both \( e_i' \) and \( e_j' \) where \( i \neq j \). Then \( 0 = (e_i e_j + e_j e_i)' = e_i e_j' + e_i' e_j' \). This means \( 0 = 0 e_k = (e_i e_j' + e_i' e_j') e_k = e_i' e_j' e_k + e_j' e_i' e_k = e_i' e_k + e_j' e_k = e_k + e_k = 2e_k \), so \( e_k = 0 \), which is not true. Hence each \( e_i' \) has exactly one idempotent summand, and no two have the same idempotent summand. This proves the assertion.

Henceforth \( \mu \) will be the permutation obtained in Lemma 4.4. We need the following lemma to show that \( ' \) permutes the \( e_i \)'s.

**Lemma 4.5.** If \( m_{ij} + n_{kj} = r_{ij} + s_{ij} = 0 \) with \( k \neq l \), then \( m_{ij} = n_{kj} = 0 \) or \( r_{ij} = s_{ij} = 0 \).

*Proof.* Suppose \( m_{ij} \neq 0 \). Then \( n_{kj} \neq 0 \), and there exists \( \overline{m}_{ji} \in N_{ji} \) with \( m_{ij} \overline{m}_{ji} = e_i \). So \( e_i + n_{kj} \overline{m}_{ji} = 0 \). If \( r_{ij} \neq 0 \) then there exists \( \overline{r}_{ji} \in N_{ji} \) such that \( r_{ij} \overline{r}_{ji} = e_i \), and so \( e_i + s_{ij} \overline{r}_{ji} = 0 \). This means \( n_{kj} \overline{m}_{ji} = s_{ij} \overline{r}_{ji} \). Since \( k \neq l \), \( n_{kj} \overline{m}_{ji} = e_k n_{kj} \overline{m}_{ji} = e_k s_{ij} \overline{r}_{ji} = 0 \). This means either \( n_{kj} = 0 \) or \( \overline{m}_{ji} = 0 \), which is impossible. So \( r_{ij} = 0 = s_{ij} \).

**Proposition 4.6.** For each \( i \), \( e_i' = e_{\mu(i)} \).

*Proof.* From Lemma 4.4, we have \( e_i' = e_{\mu(i)} + \sum_{k \neq \mu(i)} n_{\mu(i)k} \). Without loss of generality we may assume that \( \mu \) is the identity permutation on \( \{1, 2, \ldots, t\} \), and so
\[ e_i' = e_i + n_{12} + n_{13} + \cdots + n_{1t} \]
Now assume that \( t > 2 \), and let \( i \neq 1, 2 \). We have
\[
e'_2 = m_{21} + e_2 + m_{23} + \cdots + m_{2t}\]
and
\[
e'_i = s_{i1} + s_{i2} + \cdots + e_i + \cdots + s_{it}.
\]
The equations \( e'_1e'_2 + e'_2e'_1 = 0 \), \( e'_1e'_i + e'_ie'_1 = 0 \), and \( e'_2e'_1 + e'_1e'_2 = 0 \) imply the following equations:

(1) \( n_{12} + m_{21}n_{12} = 0 \),
(2) \( n_{11}s_{12} + s_{11}n_{12} = 0 \),
(3) \( n_{11} + s_{11}n_{11} = 0 \),
(4) \( m_{21}s_{11} + s_{12}m_{21} = 0 \),
(5) \( m_{2i} + s_{i2}m_{2i} = 0 \).

If \( n_{12} \neq 0 \), then using Lemma 4.5 and the fact that \( i \neq 2 \), it follows from (1) and (2) that \( n_{22}s_{12} = s_{11}n_{12} = 0 \). Hence \( s_{11} = 0 \), because \( n_{12} \neq 0 \). Therefore by (3) \( n_{11} = 0 \). Since \( n_{12} \neq 0 \), it follows from (1) that \( m_{21} \neq 0 \), and so by (4) and the fact that \( s_{11} = 0 \), we have \( s_{12} = 0 \). Hence by (5) \( m_{2i} = 0 \). We now have
\[
e'_1 = e_1 + n_{12} + n_{13} + \cdots + n_{1i} + 0 + n_{1i} + \cdots + n_{1t},
\]
\[
e'_2 = m_{21} + e_2 + m_{23} + \cdots + m_{2i} + 0 + m_{2i} + \cdots + m_{2t},
\]
\[
e'_i = 0 + 0 + s_{i3} + \cdots + s_{i2} + e_i + s_{ii} + \cdots + s_{it},
\]
where \( i^* = i - 1 \) and \( \tilde{i} = i + 1 \). Therefore, since \( 1 = 1' = e'_1 + e'_2 + \cdots + e'_i \), we have
\[
e_1 = (e'_1 + e'_2 + \cdots + e'_i)e_1 = e'_1e_1 + e'_2e_1 + \cdots + e'_ie_1 = e_1 + m_{21},
\]
which is not true because \( m_{21} \neq 0 \). So our assumption that \( n_{12} \neq 0 \) is false, and hence \( n_{12} = 0 \). A similar argument shows that \( n_{ij} = 0 \) for all \( i, j \) with \( i \neq j \).

Finally, if \( t = 2 \), then \( 1 = 1' = e'_1 + e'_2 \), and so \( e'_1 = (e'_1 + e'_2)e'_1 = (e'_1)^2 + e'_2e'_1 = (e'_1)^2 + e'_2e'_1 = e'_1 + e'_2e'_1 \). Hence \( e'_2e'_1 = 0 \). Similarly, \( e'_1e'_2 = 0 \). The argument in the proof of Lemma 3.5 now establishes the desired result.

**Lemma 4.7.** If \( n_{ij} \neq 0 \) then \( n'_{ij} \neq 0 \).

**Proof.** Suppose \( n_{ii} \neq 0 \) but \( n'_{ii} = 0 \). Then \( 2e_i = n_{ii}n_{ii}^{-1} + n_{ii}^{-1}n_{ii} \), and so \( 2e'_i = 0 \). Hence \( e'_i = 0 \), which is not true, and so \( n_{ii} \neq 0 \). Next, let \( i \neq j \), and suppose \( n_{ij} \neq 0 \) but \( n'_{ij} = 0 \). Then there exists \( m_{ji} \) such that \( m_{ji}n_{ij} = e_j \) and \( n_{ij}m_{ji} = e_i \). So \( e_i + e_j = n_{ij}m_{ji} + m_{ji}n_{ij} \), which implies \( e'_i + e'_j = n'_{ij}m'_{ji} + m'_{ji}n'_{ij} = 0 \). Then \( 0 = (e'_i + e'_j)e'_i = e'_i + e'_j e'_i = e'_i \), since by Proposition 4.6, \( e'_j e'_i = 0 \). But \( e'_i = 0 \) gives our contradiction. So \( n'_{ij} \neq 0 \).

The proof of the following lemma is identical to that of Lemma 3.7.

**Lemma 4.8.** Let \( f \in \mathcal{N} \). Then \( f^2 = 0 \) if and only if \( f \) has the property that if \( n_{ij} \neq 0 \) is a summand of \( f \), then \( n_{ki} \) is not a summand of \( f \) for any \( n_{ki} \) in \( \mathcal{N}_{nk}^* \), \( k = 1, 2, \ldots, t \).

**Lemma 4.9.** If \( n \in \mathcal{N} \) is such that \( e_in + ne_i = 2n \), then \( n \in \mathcal{N}_{ni} \).
Proof. Let $n_{j_1} + n_{j_2} + \cdots + n_{j_t}$. Then $ne = n_{j_i}$ and $e_in = e_in_{j_1} + e_in_{j_2} + \cdots + e_in_{j_t}$. Since $ne + e_in = 2n$, we must have $n_{j_i} + e_in_{j_1} + e_in_{j_2} + \cdots + e_in_{j_t} = 2n$.

Equating components gives

$$e_in_{j_1} = n_{j_1} + n_{j_1}$$

$$e_in_{j_{i-1}} = n_{j_{i-1}} + n_{j_{i-1}}$$

$$e_in_{j_t} = n_{j_t} + n_{j_t}$$

Suppose $k \neq i$ and $e_in_{j_k} \neq 0$. Then $j_k = i$, and there exists $n_{k_i}$ such that $n_{j_k}n_{k_i} = e_i$. So $e_in_{j_k} = n_{j_k} + n_{j_k}$ implies $e_in_{j_k}n_{k_i} = n_{j_k}n_{k_i} + n_{j_k}n_{k_i}$ or $e_i = e_i + e_i$. This implies $e_i = 0$, which is not true. So if $k \neq i$, then $n_{j_k} = 0$. Finally, $n_{j_i} + e_in_{j_i} = n_{j_i} + n_{j_i}$ implies $e_in_{j_i} = n_{j_i}$. So either $j_i = i$ or $n_{j_i} = 0$. In either case $n = n_{j_i}$ is in $N_{ii}$.

Proposition 4.10. For all $i$ and $j$, either $n_{ij} \in N_{\mu(i)\mu(j)}$ or $n_{ij} \in N_{\mu(j)\mu(i)}$.

Proof. First, since $n_{ii}e_i + e_in_{ii} = 2n_{ii}$, it follows from Proposition 4.6 that $n'_{ij}e_{\mu(i)} + e_{\mu(i)}n'_{ii} = 2n'_{ii}$, and so by Lemma 4.9, $n'_{ij} \in N_{\mu(i)\mu(i)}$.

Second, let $i \neq j$, and let $k$ be distinct from $i$ and $j$. Then $0 = (n_{ij}e_k + e_kn_{ij})' = n'_{ij}e_{\mu(k)} + e_{\mu(k)}n'_{ij}$. Assume $e_{\mu(k)}n'_{ij} \neq 0$. Then $n'_{ij}$ has a nonzero summand in $N_{\mu(k)s}$ for some $s$. Since $n'_{ij}$ is nilpotent of index 2, by Lemma 4.8, $n'_{ij}$ cannot have a nonzero summand in $N_x\mu(k)$ for any $x$. So in particular $n'_{ij}e_{\mu(k)} = 0$, but then $e_{\mu(k)}n'_{ij} = 0$. So $n'_{ij}e_{\mu(k)} = e_{\mu(k)}n'_{ij} = 0$ for all $k \neq i, j$. Also, since $n_{ii}e_{j} + e_in_{ij} = n_{ij}$, $n_{ij} = e_{\mu(i)}n_{ij} + n'_{ij}e_{\mu(i)}$. Since $n'_{ij} \neq 0$, either $e_{\mu(j)}n'_{ij} = 0$ or $n'_{ij}e_{\mu(j)} \neq 0$. Since $(n'_{ij})^2 = 0$, then, as above, if $n'_{ij}e_{\mu(j)} = 0$ then $e_{\mu(j)}n'_{ij} = 0$ and if $e_{\mu(j)}n'_{ij} = 0$ then $n'_{ij}e_{\mu(j)} = 0$. Similarly, if $e_{\mu(i)}n'_{ij} = 0$ then $e_{\mu(i)}n'_{ij} = 0$, and conversely. Since $e_{\mu(k)}n'_{ij} = n'_{ij}e_{\mu(k)} = 0$ for every $k \neq i, j$, then the nonzero summands of $n'_{ij}$ are of the form $N_{\mu(i)\mu(j)}$ or $N_{\mu(j)\mu(i)}$. If $e_{\mu(j)}n'_{ij} = 0$ then $n_{\mu(j)\mu(i)} = 0$ and $n'_{ij} \in N_{\mu(i)\mu(j)}$. If $n'_{ij}e_{\mu(j)} = 0$, then $n_{\mu(i)\mu(j)} = 0$ and $n'_{ij} \in N_{\mu(j)\mu(i)}$.

The proof of the following proposition is identical to that of Proposition 3.9.

Proposition 4.11. For all $i$ and $j$, either $N'_{ij} = N_{\mu(i)\mu(j)}$ or $N'_{ij} = N_{\mu(j)\mu(i)}$.

Lemma 4.12. If $N'_{ij} = N_{\mu(i)\mu(j)}$ for one pair $i, j$ with $i \neq j$, then $N'_{uk} = N_{\mu(u)\mu(k)}$ for all $u, k$.

Proof. Suppose $n'_{ij} \in N_{\mu(i)\mu(j)}$ and $m'_{ji} \in N_{\mu(i)\mu(j)}$ with $n_{ij}$ and $m_{ji}$ being nonzero. We have $n_{ij}m_{ji} \neq 0$ and $m_{ji}n_{ij} \neq 0$. So $0 \neq (n_{ij}m_{ji} + m_{ji}n_{ij})' = n'_{ij}m'_{ji} + m'_{ji}n'_{ij} = 0$, since $n'_{ij}m'_{ji} = 0$ and $m'_{ji}n'_{ij} = 0$, a contradiction. So $m'_{ji} \in N_{\mu(j)\mu(i)}$ and $N'_{ij} = N_{\mu(i)\mu(j)}$.

Next choose $k$ such that $k \neq i, k \neq j$ (if such a $k$ exists). Then $0 \neq (n_{ki}m_{ij} + m_{ij}n_{ki})' = n'_{ki}m'_{ij} + m'_{ij}n'_{ki}$. Since $m'_{ij} \in N_{\mu(i)\mu(j)}$, $n'_{ki} \in N_{\mu(k)\mu(i)} \cup N_{\mu(i)\mu(k)}$, and $k \neq i, j$, $n'_{ki} \in N_{\mu(k)\mu(i)}$ (because $m'_{ij}n'_{ki} = 0$). Hence by Proposition 4.11, $N'_{ij} = N_{\mu(i)\mu(j)}$. Fix $k$, and repeat the above argument, giving $N'_{uk} = N_{\mu(u)\mu(k)}$ for all $u$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
The proofs of Proposition 4.13 and Theorem 4.1 are identical to those of Proposition 3.11 and Theorem 3.1 respectively.

**Proposition 4.13.** \( N_{ij}' = N_{\mu(i)\mu(j)} \) for all \( i \) and \( j \).

**Theorem 4.1.** Let \( N \) be a finite simple centralizer near-ring with \( 1 = e_1 + e_2 + \cdots + e_t \) where \( t \geq 2 \). If \( 2 \in N \) is invertible, then every Jordan-endomorphism of \( N \) is an automorphism of \( N \).

5. **Semiendomorphisms and Jordan-endomorphisms of finite Dickson near-fields**

It is the goal of this section to prove that if \( N \) is a finite Dickson near-field, then every semiendomorphism and every Jordan-endomorphism (characteristic of \( N \) not 2 in the Jordan case) is an automorphism. The reader is referred to the book by Pilz [9, pp. 254-258] for background on Dickson near-fields.

We begin by establishing a result about finite fields that will be needed later in this section.

**Lemma 5.1.** Let \( K = GF(p^t) \) be the finite field of order \( p^t \) where \( p \) is a prime. Let \( n \) be a positive integer less than \( t \), and let \( w \) be a generator of the multiplicative cyclic group \( K^* \). Then \( K \) is the smallest extension field of the prime field \( F = GF(p) \) that contains \( w^n \), that is, \( K = F(w^n) \).

**Proof.** Let \( L \) be a proper subfield of \( K \). Then \( L = GF(p^u) \) where \( u \) is a proper divisor of \( t \). So \( t = uv \) with \( v > 1 \). It suffices to show that \( w^n \) does not belong to \( L \).

If \( w^n \) belongs to \( L \), then \( 1 = (w^n)^{p^u-1} = w^n(p^u-1) \). Since the order of \( w \) in \( K^* \) is \( p^t-1 \), this order must divide \( n(p^u-1) \). We have \( p^t-1 = p^u-1 = (p^u-1)((p^u)^{-1} + \cdots + p^u+1) \). This means that \( (p^u)^{-1} + \cdots + p^u+1 \) divides \( n \).

If \( u > 1 \), then \( p^u+1 \geq 2^u+1 > 2u \), and so \( (p^u)^{-1} + \cdots + p^u+1 > (v-2)u+2u = vu = t > n \), which is not possible. If \( u = 1 \), then \( (p^u)^{-1} + \cdots + p^u+1 > v = t > n \), again not possible.

This shows that \( w^n \) does not belong to any proper subfield of \( K \), and hence \( K = F(w^n) \) as desired.

Now we set some of the concepts and notation for the rest of this section. Let \( (q, n) \) be a Dickson pair of positive integers. This means

(a) \( q = p^l \) for some prime \( p \),
(b) each prime divisor of \( n \) divides \( q-1 \),
(c) if \( q \equiv 3 \pmod{n} \) then \( 4 \) does not divide \( n \).

Recall [9, pp. 254-258] that for a Dickson pair \( (q, n) \), a finite near-field \( N \) having \( q^n \) elements and center \( F = GF(q) \) may be constructed from the field \( K = GF(q^n) \) as follows. Let \( w \) be a generator of the multiplicative cyclic group \( K^* \), and let \( H = \langle w^n \rangle \), the cyclic subgroup of \( K^* \) generated by \( w^n \). The cosets of \( H \) in \( K^* \) turn out to be \( wH, w^2H, \ldots, w^{q^n-1}H = H \), a cyclic group of order \( n \). For \( i = 1, \ldots, n \) let \( H_i = w^{(q^i-1)/(q-1)}H \) (so \( H_1 = wH \) and \( H_n = H \)). Associate the automorphism \( a \to a^q \) of \( K \) with
Let \((N, +)\) be the group \((K, +)\), and define multiplication \(\circ\) on \(N\) in terms of that in \(K\),
\[
a \circ b = a^d b \quad \text{if } b \in H_i,
\]
\[
a \circ b = 0 \quad \text{if } b = 0.
\]

Using addition and multiplication as defined above, \(N(+, \circ)\) forms a near-field. Finite near-fields formed in this way are called Dickson near-fields. With seven exceptions, all having order \(p^2\) for some prime \(p\), all finite near-fields are Dickson near-fields.

The next four lemmas will be used to show that if \('\) is a semiendomorphism or a Jordan-endomorphism of \(N\) and \((q, n) \neq (3, 2)\), then \('\) must preserve the set \(H_n = H\), that is, \(H' = H\).

**Lemma 5.2.** Let \(i\) and \(n\) be relatively prime positive integers. Then the polynomial \(f(x) = (x^i - 1)/(x - 1)\) divides the polynomial \(g(x) = (x^{in} - 1)/(x^n - 1)\) in \(\mathbb{C}[x]\), \(\mathbb{C}\) the field of complex numbers.

**Proof.** Let \(\alpha\) be a root of \(f(x)\). Then \(\alpha \neq 1\), and \(\alpha\) is an \(i\)th root of unity. The complex number \(\alpha^n\) is also an \(i\)th root of unity. Since \((i, n) = 1\), \(\alpha^n \neq 1\). This means \(\alpha\) is also a root of \(g(x)\). Since every root of \(f(x)\) is also a root of \(g(x)\) and \(f(x)\) has no repeated roots, \(f(x)\) divides \(g(x)\).

**Lemma 5.3.** Let \(\gcd(i, n) = d\). The order of \((w^n)(q^{in} - 1)/(q^d - 1)\) in \(N^*\) divides \(q^d - 1\).

**Proof.** We have
\[
\frac{q^{in} - 1}{q^d - 1} = \left(\frac{q^{in} - 1}{q^{in/d} - 1}\right) \left(\frac{q^{in/d} - 1}{q^d - 1}\right) = \left(\frac{q^n - 1}{q^{n/d} - 1}\right) \left(\frac{q^{dn} - 1}{q^{dn/d} - 1}\right) \left(\frac{q^n - 1}{q^d - 1}\right).
\]

Since \(\gcd(\frac{i}{d}, \frac{n}{d}) = 1\), Lemma 5.2 implies \((q^{dn/d} - 1)^{i/d - 1}\) divides \((q^{dn/d} - 1)^{i/d - 1}\). But \(q^{dn/d} - 1\) divides \(q^n - 1\), and \(w^{q^n - 1} = 1\), and so \((w^n)(q^{in} - 1)/(q^d - 1)\) raised to the power \(q^d - 1\) gives 1.

**Lemma 5.4.** If \(d\) divides \(n\) with \(d \neq n\) and \((q, n) \neq (3, 2)\) is a Dickson pair, then \(n^2(q^d - 1) < q^n - 1\).

**Proof.** Since \((q^n - 1)/(q^d - 1) = q^{n-d} + q^{n-2d} + \cdots + q^d + 1\), it is enough to show that \(q^{n-d} + q^{n-2d} + \cdots + q^d + 1 > n^2\). The conditions on the pair \((q, n)\) imply that \(q \geq 3\) and \(n \geq 2\). Let \(f\) be the function defined by \(f(n) = 3n^2 + 1 - n^2\). Elementary calculus shows that \(f\) is an increasing function on \([7, \infty)\). Since \(f(8) > 0\), \(f(n) > 0\) for all \(n \geq 8\). Since \(d\) divides \(n\) and \(d \neq n\), \(d \leq n/2\), and so \(q^{n-d} + q^{n-2d} + \cdots + q^{d+1} \geq q^{n-d} + 1 \geq q^q + 1 \geq 3^q + 1 > n^2\) if \(n > 8\).

We now consider the cases \(n = 2, 3, \ldots, 7\). If \(n = 2, 4, 5, 6, 7\), then the conditions on \((q, n)\) imply that \(q \geq 5\). Using the function \(g(n) = 5n^2 + 1 - n^2\) and an argument similar to the above shows that \(5n^2 + 1 > n^2\) if \(n \geq 2\). Hence \(q^{n-2d} + q^{n-2d} + \cdots + 1 \geq q^{n-d} + 1 \geq q^{n/2} + 1 \geq q^{n/2} + 1 > n^2\). If \(n = 3\) then \(q \geq 4\), and the previous argument is valid if \(q \geq 5\). If \(q = 4\) and \(n = 3\), then \(d = 1\), and direct verification gives the result.
Lemma 5.5. Let \((q, n)\) be a Dickson pair different from \((3, 2)\), and let \(N\) be a corresponding near-field of order \(q^n\). If \(v\) is an element of \(H_i\) with \(H_i \neq H\) then the order of \(v\) in the group \(N^*\) is less than \((q^n - 1)/n\).

Proof. Since \(v \in H_i\) with \(H_i \neq H\), \(v = u^{(q^i-1)/(q-1)}w^{nr}\) for some integer \(r\) where \(i < n\). Letting \(v^{on}\) denote the product of \(v\) \(n\)-times in \(N^*\), we have

\[
v^{on} = \left( w^{\frac{q^n-1}{q-1} w^{nr}} \right)^{\frac{q^n-1}{q-1}} = w^{\frac{q^n-1}{q-1} (w^{nr})^{\frac{q^n-1}{q-1}}}.
\]

By Lemma 5.3, the order of \(v^{on}\) divides \(q^d - 1\) where \(d = \gcd\{z, n\}\). Hence the order of \(v\) in \(N^*\) divides \(n(q^d - 1)\), which is less than \((q^n - 1)/n\) by Lemma 5.4.

Let \(\sigma\) be a group endomorphism of \((N, +)\) that also preserves powers of elements in \(N\); that is,

\[
(a + b)' = a' + b', \quad (a^{ot})' = (a')^{ot}
\]

for all \(a, b \in N\) and all integers \(t\). (We note that such a map \(\sigma\) includes semiendomorphisms of \(N\) and Jordan endomorphisms of \(N\) assuming the characteristic of \(N\) is not 2.) Using \(t = 0\) we get \(1' = 1\) or \(1' = 0\). If \(1' = 0\) then \(\sigma\) is the zero map. We assume henceforth that \(1' = 1\). If \(a \neq 0\) is in \(N\) then some power of \(a\) is 1, which means \(a' \neq 0\). This shows \(\sigma\) is one-to-one.

Lemma 5.6. Let \(N\) be a Dickson near-field of order \(q^n\) with center \(GF(q)\), where \(q = p^l\) for some prime \(p\) and \((q, n) \neq (3, 2)\). Then there are at most \(ln\) group endomorphisms of \((N, +)\) that preserve powers of elements in \(N\).

Proof. Let \(w\) be the generator of \(K^*\), \(K = GF(q^n)\), used in the construction of \(N\). The order of \(w^n\) in \(N^*\) is \((q^n - 1)/n\). If \(\sigma\) is a nonzero power preserving map on \(N\) then \(\sigma\) is one-to-one, and so \((w^n)\)' has order \((q^n - 1)/n\) in \(N^*\) because \(\sigma\) preserves orders of elements in \(N^*\). By Lemma 5.5, if \(v \notin H = \langle w^n \rangle\) then the order of \(v\) is less than \((q^n - 1)/n\). This means \((w^n)\)' belongs to \(H\) since \(H\) is the unique cyclic subgroup of \(N^*\) of order \((q^n - 1)/n\). Since \((w^n)\)' \(\in H\), we must have \(H' = H\), i.e., \(H\) is invariant under the map \(\sigma\).

By Lemma 5.1, \(K = F(w^n)\) where \(F = GF(p)\). Since \(w^n\) belongs to \(H\), for every \(m \in N\) we have \(m \circ w^n = mw^n\), so as an element of \(N\), \(w^n\) multiplies as it does in \(K\). In particular, powers of \(w^n\) in \(N\) are identical to those in \(K\). Since \(K = F(w^n)\), every element in \(K\) is a polynomial in \(w^n\) with coefficients from the prime field \(F\); that is, each element in \(K\) has the form

\[
c_{r-1}(w^n)^{r-1} + c_{r-2}(w^n)^{r-2} + \cdots + c_1w^n + c_0,
\]

where \(r = ln\) and each \(c_i \in F\). Since \(\sigma\) preserves powers, we have \((w^n)^k\)' = \((w^n)\)'\(^k\) for all \(k\). If \(c \in F\) then \(cw^n\) can be viewed as repeated addition, and since \(\sigma\) preserves addition, \((cw^n)\)' = \(c(w^n)\)'\(^k\). We now see that the image of (6) under \(\sigma\) is

\[
c_{r-1}(v)^{r-1} + c_{r-2}(v)^{r-2} + \cdots + c_1v + c_0,
\]

where \(v = (w^n)\)' and \(v\) belongs to \(H\). So \(\sigma\) is completely determined on \(N\) once \((w^n)\) is known. Since \((w^n)\)' = \(v\) belongs to \(H\), \(v\) must be a root of the minimal polynomial for \(w^n\) in \(F[x]\). Since the dimension of \(K\) over \(F\) is \(ln\) and \(K = F(w^n)\), there are at most \(ln\) possibilities for \((w^n)\)'.
Corollary. If \( \sigma \) is a semiautomorphism (Jordan-automorphism) of the near-field \( N \) of order \( q^n \), \( \sigma \) is an automorphism of the field \( K = GF(q^n) \).

Proof. Every semiautomorphism (Jordan-automorphism) of the near-field \( N \) is a power preserving map. By Lemma 5.6, power preserving maps of \( N \) are automorphisms of \( K \).

Lemma 5.7. If \( \sigma \) is a semiautomorphism (Jordan-automorphism) of the near-field \( N \) then \( \sigma \) preserves \( H_i \) for every \( i \).

Proof. By Corollary, we know that \( \sigma \) is an automorphism of the associated field \( K \), so \( \sigma \) has the form \( a^\lambda = a^k \) for some \( k \geq 0 \). Now assume that \( \sigma \) is a semiautomorphism of \( N \). We have
\[
(w^n \circ w \circ w^n)' = (w^n \circ w \circ w^n)' = (w^nq \circ w \circ w^n)' = (w^nq \circ w \circ w^n)' = (w^nq \circ (w^np^k + np^k)) = (w^np^k + np^k).
\]
Also,
\[
(w^n)' \circ w \circ (w^n)' = w^np^k \circ w^np^k = w^np^k \circ w^np^k = w^np^k \circ w^np^k.
\]
Since \( \sigma \) is a semiautomorphism,
\[
w^np^k \circ w^np^k = (w^np^k)^q \circ w^np^k + np^k,
\]
which means \( w^np^k + np^k \) belongs to \( wH = H_1 \), and so \( w^np^k = w' \) belongs to \( wH = H_1 \). This means \( \sigma \) preserves \( H_1 \). Since \( \sigma \) is an automorphism of \( K \), \( \sigma \) preserves each \( H_1 \).

Now assume \( \sigma \) is a Jordan-automorphism of \( N \). Then
\[
(w^n \circ w + w \circ w^n)' = (w^nq \circ w \circ w^n)' = (w^nq \circ w \circ w^n)' = (w^nq \circ w \circ w^n)' = (w^nq \circ (w^np^k + np^k)) = (w^np^k + np^k).
\]
Also,
\[
(w^n)' \circ w \circ (w^n)' = w^np^k \circ w^np^k = w^np^k \circ w^np^k = w^np^k \circ w^np^k.
\]
This means \( w^np^k \circ w^np^k = (w^np^k)^q \circ w^np^k \), and so \( w^np^k \) belongs to \( wH = H_1 \). As above, \( \sigma \) preserves each \( H_i \).

Lemma 5.8. Let \( N \) be a near-field corresponding to the Dickson pair \( (q, n) \) where \( (q, n) \neq (3, 2) \). The automorphisms of \( N \) are precisely those automorphisms of the associated field \( K \) that preserve the \( H_i \)'s.

Proof. By Zassenhaus [11] every automorphism of \( N \) is an automorphism of \( K \), but not conversely. If \( \sigma \) is an automorphism of \( N \) then in particular \( \sigma \) is a semiautomorphism of \( N \). By Lemma 5.7, \( \sigma \) preserves each \( H_i \).

It remains to show that if \( \sigma \) is an automorphism of \( K \) that preserves each set \( H_i \) then \( \sigma \) is an automorphism of \( N \). Let \( r \in H_i \) and \( m \in H_j \). Then
\[
r \circ m = r^q \circ m.
\]
Let \( \sigma(a) = a^p^k \). Then we have
\[
\sigma(r \circ m) = \sigma(r^q \circ m) = (r^q \circ m)^p^k,
\]
and
\[
\sigma(r) \circ \sigma(m) = \sigma(r)^q \circ \sigma(m) \quad \text{(since } \sigma(m) \in H_j) \]
\[
= (r^p^k)^{q^j} \circ m^p^k = \sigma(r \circ m).
\]
This shows \( \sigma \in \text{Aut}(N) \).
Theorem 5.1. Let \((q, n)\) be a Dickson pair, and let \(N\) be a Dickson near-field of order \(q^n\). If \(\psi\) is a semiendomorphism (Jordan-endomorphism) of \(N\) then \(\psi\) is an automorphism of \(N\).

Proof. Assume \((q, n) \neq (3, 2)\). By the corollary to Lemma 5.6, \(\psi\) is an automorphism of the associated field \(K\). By Lemma 5.7, \(\psi\) preserves \(H_i\) for every \(i\). By Lemma 5.8, \(\psi\) is an automorphism of \(N\).

If \((q, n) = (3, 2)\) then \(N\) has six automorphisms (see Zassenhaus [11]). If \(\psi\) is a semiendomorphism (Jordan-automorphism) of \(N\) then \(\psi\) preserves \(0, 1,\) and \(2\). Hence there are six possibilities for \(\omega^2\), each giving an automorphism of \(N\).

6. Semiendomorphisms and Jordan-endomorphisms of special finite semisimple near-rings

Let \(N\) be a finite semisimple near-ring with \(1\). Then \(N\) is a direct sum of simple near-rings \(N_1, \ldots, N_s\). We call \(N\) a special semisimple near-ring if each \(N_i\) is a simple finite centralizer near-ring and not a near-field. (So each \(N_i\) is a simple near-ring of the type discussed in §§2–4 above.)

Since \(N = N_1 \oplus \cdots \oplus N_s\) and \(N\) is special, \(N\) has primitive idempotents \(e_1, \ldots, e_t\) such that \(1 = e_1 + \cdots + e_t\) and they satisfy properties (i)–(vi) of §2 (see [6]). Moreover \(N\) semisimple is equivalent to the property that \(N_{ij}\) is nonzero iff \(N_{ji}\) is nonzero. So property (vii) is replaced by the following.

(vii)' If \(N\) is special semisimple and \(N_{ij} \neq \{0\}\) then for every nonzero \(n_{ij}\) in \(N_{ij}\) there exists an element \(m_{ji}\) in \(N_{ji}\) such that \(n_{ij}m_{ji} = e_i\) and \(m_{ji}n_{ij} = e_j\).

Now let \(\psi\) be either a semiendomorphism or a Jordan-endomorphism of the special semisimple near-ring \(N\). Since \(N\) is special, for each index \(i\) there exists at least one index \(j, j \neq i\) such that both \(N_{ij}\) and \(N_{ji}\) are nonzero. This and the fact that properties (i)–(vi), (vii)' are satisfied ensures that the lemmas and propositions of §§3 and 4 are true when \(N\) is special semisimple. (If \(\psi\) is a Jordan-endomorphism we assume \(2 \in N\) is invertible.) Thus we have Theorem 6.1 whose proof is identical to that of Theorem 3.1.

Theorem 6.1. Let \(N\) be a special finite semisimple near-ring. If \(\psi\) is a semiendomorphism of \(N\) then \(\psi\) is an automorphism of \(N\). If \(\psi\) is a Jordan-endomorphism of \(N\) and \(2 \in N\) is invertible then \(\psi\) is an automorphism of \(N\).

We remark that if \(N\) is a finite semisimple near-ring that is not simple or special then Theorem 6.1 is not true. Let \(N = N_1 \oplus \cdots \oplus N_s\) where \(N_1\) is a simple ring that is not commutative and \(N_2, \ldots, N_s\) are simple centralizer near-rings as in §§3 and 4. Let \(\sigma_1\) be an antiautomorphism of \(N_1\), and for \(i = 2, \ldots, s\) let \(\sigma_i\) be an automorphism of \(N_i\). Then \(\sigma = \sigma_1 + \sigma_2 + \cdots + \sigma_s\) is a semiendomorphism (or a Jordan-endomorphism) of \(N\) that is not an automorphism of \(N\).

Acknowledgment

Parts of this work were done while the second author was visiting the Department of Mathematics at Texas A&M University. He wishes to express his gratitude to the CSIR of South Africa for financial assistance and to Texas A&M University for their generous hospitality.
REFERENCES


DEPARTMENT OF MATHEMATICS, TEXAS A&M UNIVERSITY, COLLEGE STATION, TEXAS 77843

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF STellenbosch, STellenbosch 7600, SOUTH AFRICA