Mathematica Pannonica
3/1 (1992), 3 – 17

SEMI-HOMOMORPHISMS OF NEAR-RINGS

Y. **Fong**

Department of Mathematics, National Cheng Kung University, Tainan 70102, Taiwan, Republic of China.

L. **van Wyk**

Department of Mathematics, University of Stellenbosch, 7600 Stellenbosch, Republic of South Africa.

Received September 1990

AMS Subject Classification: 16 A 76, 16 A 72

Keywords: Semi-homomorphisms, semi-subgroups, finite abelian groups, near-rings, Dickson near-fields.

Abstract: The semi-subgroups of finite abelian groups are characterized and comparisons are made between semi-homomorphisms of rings and near-rings. This study leads to an alternative proof of a result by Zassenhaus in 1936, viz. that the automorphism group of the smallest Dickson non-field is isomorphic to the symmetric group of degree 3.

1. Introduction

Projectivity in classical projective geometry led to a study of semi-automorphisms of rings (see [1] and [3]). In [2] and [8] it was proven that every semi-automorphism of a division ring is either an automorphism or an anti-automorphism, and similarly for a matrix ring over a division ring.

Huq [9] presented a general study of semi-homomorphisms of rings, following the mentioned papers and, amongst others, Herstein's study of semi-homomorphisms of groups in [7]. In [4] the authors introduced semi-subgroups of groups and provided counterexamples to some of the assertions in [9]. The purpose of this paper is, on the one hand, to continue the investigation of the structure of semi-subgroups.

In Section 2 we characterize the semi-subgroups of finite abelian groups and the semi-subrings of $\mathbb{Z}_n$, the ring of integers modulo n, which shows that the notions semi-subgroup and semi-subring are not equivalent in $\mathbb{Z}_n$, unlike the case of subgroups and subrings of $\mathbb{Z}_n$.

In Section 3 we initiate a study of semi-homomorphisms of near-rings, although th first part applies to groups in general. Herstein [7] calls a mapping $\varphi : G \to H$ between groups (written additively) a *semi-homomorphism* if

$$\varphi(a + b + a) = \varphi(a) + \varphi(b) + \varphi(a) \tag{1}$$

for all $a, b \in G$. By taking $b = -a$, it follows that

$$\varphi(-a) = -\varphi(a) \tag{2}$$

for every $a \in G$; in particular we have $2\varphi(0) = 0$, where 0 denotes the neutral elements of G and H. Herstein showed that if the centralizer of $\varphi(G)$ in H is 0, then (2) can be generalized to

$$\varphi(na) = n\varphi(a) \tag{3}$$

for every integer n and every $a \in G$. We prove that the condition that the subset $\{\varphi(2a) - 2\varphi(a) : a \in G\}$ of H contains no elements of order 2, is also sufficient for (3). This result strengthens [4, Corollary 3.4] in which G and H are assumed to be abelian.

We use Huq's definition of a semi-homomorphism of rings as the definition of a semi-homomorphism of near-rings, i.e. a mapping $\varphi : R \to S$ between near-rings satisfying (1) and the condition

$$\varphi(aba) = \varphi(a)\varphi(b)\varphi(a) \tag{4}$$

for all $a, b \in R$. The left hand mapping convention is used for near-rings, since we shall be dealing with right near-rings. For details about near-rings we refer the reader to the books by Meldrum [11] or Pilz [12].

The image T of a semi-homomorphism φ of groups (rings, near-rings) is easily seen to be a *semi-subgroup* (*semi-subring, semi-subnear-ring*) of the codomain of φ, i.e.

$$(5) \qquad a+b+a \in T \quad (\text{and } aba \in T)$$

for all $a, b \in T$. Note that a semi-subnear-ring in general does not concern a semi-near-ring (see e.g. Weinert [15]).

As far as semi-homomorphisms of near-rings in particular are concerned, we show that there are many similarities to the ring case when the near-rings under consideration happen to be abelian (e.g. in the case of near-fields), but that there are in general also some striking differences. (Recall that abelian near-rings can still be very much "non-ring-like".) During the investigation of the problem whether every semi-automorphism of a near-field is an automorphism, we obtained a surprising result, viz. that every automorphism φ of $(GF(3^2), +)$ satisfying $\varphi(1) = 1$ is an automorphism of $(GF(3^2), +, \circ)$, the smallest Dickson near-field which is not a field. Hence every semi-automorphism of $(GF(3^2), +, \circ)$ is an automorphism, and so the automorphism group of $(GF(3^2), +, \circ)$ comprises 6 elements (and is isomorphic to S_3, the symmetric group of degree 3). This provides an alternative proof of a special case of [16, Theorem 18].

Throughout the paper the symbol $\subset$ denotes strict inclusion and all near-rings are associative.

2. A characterization of the semi-subgroups of finite abelian groups

Let $(G, +)$ be a (not necessarily abelian of finite) group. Every subgroup of G is obviously a semi-subgroup, but the converse need not be true. The term *non-subgroup* will be used for a semi-subgroup which is not a subgroup. Our purpose in this section is to give a characterization of the semi-subgroups of finite abelian groups.

We denote the semi-subgroup of G generated by a subset $\{a_1, a_2, \ldots, a_n\}$, $n \geq 1$, of G by $(a_1, a_2, \ldots, a_n)_s$ and we stick to the usual notation $(a_1, a_2, \ldots, a_n)$ for the subgroup of G generated by $\{a_1, a_2, \ldots, a_n\}$. The order of an element a of G will be denoted by

$o(a)$, and $|X|$ will stand for the number of elements of a subset X of G.

The first two results describe the semi-subgroup of a group generated by a singleton.

Proposition 2.1. *If $o(a)$, $a \in G$, is even or infinite, then $(a)_s$ is a non-subgroup of G.*

Proof. Firstly, let $o(a) = 2k$ for some $k > 0$. We assert that $|(a)_s| = k$; to be more precise, $(a)_s$ comprises the following different elements: $a, 3a, 5a, \ldots, (2(k-1)+1)a$. For if $(2i+1)a = (2j+1)a$ for some i and j, $0 \leq i, j \leq k-1$, then $2(i-j)a = 0$. But $2(i-j) \leq 2k-2 < k$, which contradicts the assumption that $o(a) = 2k$. It is easily verified that these elements compose a semi-subgroup of G which is contained in $(a)_s$, and so our assertion is valid. Furthermore, $0 \notin (a)_s$, otherwise the assumption that $o(a) = 2k$ is contradicted again. Hence $(a)_s$ is not a subgroup of G. The case where $o(a)$ is infinite, is dealt with similarly. $\diamondsuit$

Proposition 2.2. *If $o(a)$, $a \in G$, is odd, then $(a)_s = (a)$.*

Proof. Let $o(a) = 2l+1$ for some $l > 0$. (If $l = 0$, then $a = 0$, and the result is trivial.) Consider the subset $T := \{a, 3a, 5a, \ldots, (2(l-1)+1)a, (2l+1)a, (2(l+1)+1)a, \ldots, (2(2l)+1)a\}$ of $(a)_s$. Clearly $T = \{a, 3a, 5a, \ldots, (2l-1)a, 0, 2a, 4a, \ldots, 2la\} = (a)$, and so $(a)_s = a(a)$. $\diamondsuit$

Henceforth in this section G will be a finite abelian group.

Theorem 2.3. *If $|G|$ is odd, then G has no non-subgroups.*

Proof. By Proposition 2.2 it clearly suffices to show that $(a,b)_s = (a,b)$ for all $a, b \in G$, since the order of every element of G is odd. Let $o(a) = 2k+1$ and $o(b) = 2l+1$ for some $k, l \geq 0$. Since $(2m+1)a + nb = (k+m+1)a + nb + (k+m+1)a$ and $2ma + nb = ma + nb + ma$ for every $m, n \geq 0$, it follows from Proposition 2.2 that $(a,b) \subseteq (a,b)_s$, and so $(a,b)_s = (a,b)$. $\diamondsuit$

As a result of Theorem 2.3 and the Fundamental Theorem on finite abelian groups, we study now the semi-subgroups of $\mathbb{Z}_{2^i}$, $i \geq 1$. The greatest common divisor of $m, n \in \mathbb{Z}$ will be denoted by $\gcd(m,n)$.

Proposition 2.4. *If $0 \neq a \in \mathbb{Z}_{2^i}$, $i \geq 1$, then $(a)_s = \{g, 3g, 5g, \ldots, (2^i/g - 1)g\}$, where $g = \gcd(a, 2^i)$.*

Proof. Since $a \neq 0$ and $o(a)$ divides 2^i, it follows that $o(a)$ is even, and so by Proposition 2.1 $(a)_s = \{a, 3a, 5a, \ldots, (2(2^{j-1}-1)+1)a\}$, where $o(a) = 2^j$ for some j, $1 \leq j \leq i$. But $o(a) = 2^i/g$, and so $g = 2^{i-j}$. Therefore $2^{j-1} = 2^i/2g$, which implies that the $2^i/2g$ elements of $(a)_s$

are all the odd multiples of $g(\text{mod } 2^i)$, because a is an odd multiple of g. Hence $(a)_s = \{g, 3g, 5g, \ldots, (2(2^i/2g-1)+1)g\}$. ◇

Theorem 2.5. *The semi-subgroups in Proposition 2.4 are precisely the non-subgroups of $\mathbb{Z}_{2^i}$, $i \geq 1$.*

Proof. We show that, for $a, b \in \mathbb{Z}_{2^i}$, either $(a,b)_s = (a)_s = (b)_s$ or $(a,b)_s = (g)$, where $g := \min(\gcd(a, 2^i), \gcd(b, 2^i))$. Firstly, if $\gcd(a, 2^i) = \gcd(b, 2^i)$, then either $a = 0 = b$, in which case $(a,b)_s = = (0) = (a)_s = (b)_s$, or $a \neq 0$ and $b \neq 0$, in which case by Proposition 2.4 we have $(a)_s = (b)_s = \{g, 3g, 5g, \ldots, (2^i/g - 1)g\}$, and so $(a,b)_s = = (a)_s = (b)_s$. Secondly, let $\gcd(a, 2^i) < \gcd(b, 2^i) =: h$. Then $h = 2^k g$ for some $k \geq 1$, since g and h are powers of 2. It follows from Proposition 2.4 that $(a)_s$ comprises all the odd multiples of g, and $(b)_s$ comprises all the odd multiples of h (mod 2^i). Hence $(a,b)_s$ contains $(a)_s$ as well as at least one even multiple of g. It can now be readily seen that $(a,b)_s = (g)$, since $x + y + x \in (a,b)_s$ for all $x \in (a)_s$, $y \in (b)_s$. ◇

As in the case of subgroups, it is easy to see that if K is a semi-subgroup of the direct sum of two (not necessarliy abelian of finite) groups G_1 and G_2, then $\pi_i K$ is semi-subgroup of G_i, $i = 1, 2$, where π_i denotes the i-th coordinate projection.

The foregoing results lead to a characterization of the semi-subgroups and non-subgroups of a finite abelian group:

Theorem 2.6. (a) *If $H : \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ is a finite abelian group, with m_k an odd prime for $k = 1, 2, \ldots, n, n \geq 1$, then H has no non-subgroups.*

(b) *If $G := \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_s} \oplus H$ is a finite abelian group, with n_k a power of 2 for $k = 1, 2, \ldots, s$, $s \geq 1$, and where $H = 0$ or H is as in (a), then:*

(i) If G_{j_q}, $q = 1, 2, \ldots, r$, $1 \leq r \leq s$, is a non-subgroup of $\mathbb{Z}_{n_{j_q}}$, where $j_q \in \{1, 2, \ldots, s\}$, G_t is a subgroup of $\mathbb{Z}_{n_t}$ for $t \in \{1, 2, \ldots, s\} \setminus \{j_1, j_2, \ldots, j_r\}$, and K is a subgroup of H, then the direct sum of these G_{j_q}'s, G_t's and K is a non-subgroup of G.

(ii) If A is a semi-subgroup of G, then $\pi_j A$ is a semi-subgroup of $\mathbb{Z}_{n_j}$ for $j = 1, 2, \ldots, s$, and $\pi_{s+1} A$ is a subgroup of H; furthermore, if A is a non-subgroup of G, then $\pi_t A$ is a non-subgroup of $\mathbb{Z}_{n_t}$ for some t, $1 \leq t \leq s$.

We have seen that $0 \in S$, S a semi-subgroup of a finite abelian group H, if and only if S is a subgroup of H. Also, every semi-subgroup of $\mathbb{Z}_n$ is "cyclic" in the sense that it is generated by a single element of $\mathbb{Z}_n$. The picture might be much more different in general, even in finitely generated abelian groups; e.g. $\{2k : k \geq 0\}$ and $(2,5)_s = = \{2,5,6,9,10\} \cup \{m : m \geq 12\}$ are non-subgroups of $\mathbb{Z}$.

Although every subgroup of $\mathbb{Z}_n$, $n > 1$, is a subring of $\mathbb{Z}_n$ (and vice versa), the same is not for semi-subgroups and semi-subrings, e.g. it follows from Proposition 2.4 that $\{2,6\}$ is a semi-subgroup of $\mathbb{Z}_8$, but is not a semi-subring of $\mathbb{Z}_8$, since $2^3 = 0 \notin \{2,6\}$. However, $\mathbb{Z}_n$ may contain semi-subrings which are not subrings, and which we call *non-subrings*. We make this scheme of affairs precise in the last part of this section, in which we show that the results about the semi-subring of $\mathbb{Z}_n$ generated by an element a of $\mathbb{Z}_n$, denoted by $(a)_{sr}$, are surprisingly different form those about the semi-subgroups as far as $o(a)$ is concerned, in the sense that if $o(a)$ is even, then it does not necessarily follow that $(a)_{sr}$ is a non-subring of $\mathbb{Z}_n$.

Lemma 2.7. *If n is odd and $n > 1$, then $\mathbb{Z}_n$ has no non-subrings.*

Proof. Let S be a semi-subring of $\mathbb{Z}_n$. Then $(S,+)$ is a semi-subgroup of $(\mathbb{Z}_n,+)$, and so the result follows from Theorem 2.3.

For the rest of this section n will be even.

Proposition 2.8. *If a is odd and $a < n$, then $(a)_{sr} = (a)_s$, a non-subring of $\mathbb{Z}_n$.*

Proof. First note that $o(a)$ is even, because $o(a) = n/g$ and g is odd, where $g := \gcd(a,n)$. Hence by Proposition 2.1 $(a)_s$ comprises the odd multiples of a (mod n). Furthermore, $(2i+1)a(2j+1)a(2i+1)a$ is an odd multiple of a for all i and j, because a is odd, and so $(a)_{sr} = (a)_s$, a non-subring of $\mathbb{Z}_n$, since it follows from Proposition 2.1 that $(a)_s$ is a non-subgroup of $\mathbb{Z}_n$. ♢

Proposition 2.9. *Let b be even, $b < n$. If*

(i) $o(b)$ is odd, then $(b)_{sr} = (b)_s$, a subring (subgroup) of $\mathbb{Z}_n$.

(ii) $o(b)$ is even, then $(b)_{sr}$ is a subring (subgroup) of $\mathbb{Z}_n$, and $(b)_s \subset (b)_{sr}$.

Proof. (i) By Proposition 2.2.

(ii) Since $(b)_s \subseteq (b)_{sr}$, it follows from Proposition 2.1 that $(b)_{sr}$ contains the odd multiples of b(mod n). But b^3 is a multiple of b and b is even, and so it can be seen, as in the last part of the proof of Theorem 2.5, that $(b)_{sr}$ contains all the even multiples of b(mod n) as well. Hence $(b)_s \subset (b)_{sr} = (b)$. ♢

The foregoing results lead to

Theorem 2.10. *The semi-subrings in Proposition 2.8 are precisely the*

non-subrings of $\mathbb{Z}_n$.
Proof. Very much similar to that of Theorem 2.5. ◇

3. Semi-homomorphisms of near-rings

Recall form Section 2 that we deal with right near-rings, i.e. the left distributive law is not required.

Proposition 2.4 provides a host of *non-subnear-rings* of near-rings, i.e. semi-subnear-rings which are not subnear-rings, viz. for any non-subgroup T of $\mathbb{Z}_{2^i}$, $i \geq 1$, as in Proposition 2.4, $\{f \in M(\mathbb{Z}_{2^i}) : f(T) \subseteq \subseteq T\}$ is a non-subnear-ring of the full near-ring $M(\mathbb{Z}_{2^i})$ of mappings on $\mathbb{Z}_{2^i}$.

The following two results, which explore properties of semi-homomorphisms of restricted classes of near-rings, can be proved exactly as in the ring case (see [4, Lemma 3.3] and [9, Proposition 8] respectively):
Lemma 3.1. *A semi-homomorphism* $\varphi : R \to S$ *of abelian near-rings is a homomorphism of the underlying additive groups if and only if the semi-subgroup* $\{\varphi(a+b) - \varphi(b) - \varphi(a) : a, b \in R\}$ *of* $(S, +)$ *contains no elements of order 2.*
Lemma 3.2. *Let* $\varphi : F \to F'$ *be a semi-homomorphism of near-fields. If* $\varphi(a) \neq 0$ *for some* $0 \neq a \in F$, *then* $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

Herstein [7] showed that if the centralizer of $\varphi(G)$ in H is 0, where $\varphi : G \to H$ is a semi-homomorphism of groups, then (3) holds. The authors [4] showed that if G and H are abelian and the semi-subgroup $\{\varphi(2a) - 2\varphi(a) : a \in G\}$ of H contains no element of order 2, then (3) also holds. However, G and H need not be abelian, as will be shown shortly. We first need
Lemma 3.3. *Let* $\varphi : R \to S$ *be a semi-homomorphism of near-rings. Then* $\varphi(a+b) - \varphi(a) - \varphi(b) = \varphi(a) + \varphi(b) - \varphi(b+a)$ *for all* $a, b \in R$.
Proof. For $a, b \in R$ we have by (1) and (2):

$$\begin{aligned}\varphi(a+b) &= \varphi(a + b + (-(b+a)) + b + a) \\ &= \varphi(a) + \varphi(b + (-(b+a)) + b) + \varphi(a) \\ &= \varphi(a) + \varphi(b) + \varphi(-(b+a)) + \varphi(b) + \varphi(a) \\ &= \varphi(a) + \varphi(b) - \varphi(b+a) + \varphi(b) + \varphi(a),\end{aligned}$$

from which the result follows. ◇

Proposition 3.4. *If $\varphi : R \to S$ is semi-homomorphism of near-rings such that the set $\{\varphi(2a) - 2\varphi(a) : a \in R\}$ contains no elements of order 2, then $\varphi(na) = n\varphi(a)$ for every integer n and every $a \in R$.*

Proof. Firstly, since $2\varphi(0) = 0$, it follows that $\varphi(0) \in \{\varphi(2a) - 2\varphi(a) : a \in R\}$, and so the result holds for $n = 0$. The case $n = 1$ is trivial. Next, let $a = b$ in Lemma 3.3. Then $\varphi(2a) - 2\varphi(a) = 2\varphi(a) - \varphi(2a)$, and so $2(\varphi(2a) - 2\varphi(a)) = 0$, and so the result holds for $n = 2$. Using induction on n and assuming that $n > 2$, we get $\varphi(na) = \varphi(a + (n-2)a + a) = \varphi(a) + n(n-2)\varphi(a) + \varphi(a) = n\varphi(a)$, which establishes the result for every $n \geq 0$. Finally, by (2) and since $(-n)a = n(-a)$, the result also holds for $n < 0$. $\diamondsuit$

Note that the above two results hold merely in the presence of a semi-homomorphism of groups, since the multiplicative structure of the near-rings has not been invoked at all.

The multiplicative version of $2\varphi(0) = 0$ is, of course, $(\varphi(1))^2 = 1$, where 1 denotes the identities of the domain and codomain of φ. Huq [9] proved that if $\varphi : R \to S$ is a semi-homomorphism of rings with identities such that $1 \in \varphi(R)$ and S is a non-trivial ring without non-zero divisors of zero, then $\varphi(1) = 1$ of -1. We shall show in Example 3.7 that this result does not extend to near-rings in general, not even if φ is also a homomorphism of the underlying additive groups. However, we still have

Proposition 3.5. *If $\varphi : R \to S$ is a semi-homomorphism of near-rings with identities such that $\varphi(R)$ is a near-field and $1 \in \varphi(R)$, then $(\varphi(1))^2 = 1$ and $\varphi(1) = 1$ or -1.*

Proof. That $(\varphi(1))^2 = 1$, follows as in [9, Proposition 6]. A non-trivial near-ring-theoretic result states that if $r^2 = 1$ in a near-field, then $r = 1$ or -1 (see e.g. [12, Proposition 8.10]). $\diamondsuit$

The following example shows that it is possible that $\varphi(1) = -1$ under the conditions of Proposition 3.5. The reason for exhibiting this example must be seen against the background of the conjecture before Example 3.10.

Example 3.6. Let $(F, +, \circ)$ be the (infinite) Dickson near-field arising from $\mathrm{Q}(x)$, the field of rational functions over the rationals, by defining multiplication as follows:

$$g(x)/h(x) \circ p(x)/q(x) = \begin{cases} 0, \text{ if } p(x)/q(x) = 0 \\ (g(x+d)/h(x+d)) \cdot (p(x)/qx)), \text{ otherwise,} \end{cases}$$

where $d := \deg(p(x)) - \deg(q(x))$ and $\cdot$ is the familiar multiplication in $Q(x)$. (See [11, Example 8.29] for more details.) Then F is not a division ring, since the left distributive law does not hold. Define $\varphi : F \to F$ by $\varphi(g(x)/h(x)) = -g(x)/h(x)$. It can be verified that φ is a semi-homomorphism of near-fields (and an endomorphism of the underlying additive group). Furthermore, $\varphi(1) = -1$.

As in Heatherly and Olivier [5,6] we define a *near integral domain* as a (right) zerosymmetric near-ring having no non-zero divisors of zero and having at least one nonzero element which is not a right identity. (Note that some near-ringers call these nontrivial near integral domains "integral near-rings"). McQuarrie [10] originally devised the following (infinite) near integral domain which was later used by Heatherly and Olivier [6] to show that the additive group of a near integral domain may not be nilpotent. It is not only a near integral domain, but it is also a distributively generated (dg) near-ring with identity.

Let G_2 be the free (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 Γ_n is an element of the full near-ring $M(G_2)$ of mappings on G_2; in fact, the Γ_n's are distributive elements of $M(G_2)$. Let R be the subnear-ring of $M(G_2)$ generated by $\{\Gamma_n : n \in \mathbb{Z}\}$, i.e. $(R, \{\Gamma_n : n \in \mathbb{Z}\})$ is a dg near-ring. Then by [11, Lemma 9.11] $(R, +)$ is generated as a group by $\{\Gamma_n : n \in \mathbb{Z}\}$.

We use the above near integral domain in the following example, in which we show that Huq's result, which was mentioned just before Proposition 3.5, does not extend to near-rings.

Example 3.7. Define $\varphi : R \to R$ by

$$\varphi(\sum_{i=1}^{k} \varepsilon_{n_i}, \Gamma_{n_i}) = \sum_{i=1}^{k} \varepsilon_{n_i} \Gamma_{-n_i},$$

where $\varepsilon_{n_i} = \pm 1$ and $n_i \in \mathbb{Z}$ for $i = 1, 2, \ldots, k$. We show that φ 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. Suppose now that $\sum_{i=1}^{k} \varepsilon_{n_i} \Gamma_{n_i} = \sum_{j=1}^{l} \varepsilon_{m_j} \Gamma_{m_j}$. Then

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

and so

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

Hence, by the above remark

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

i.e. $\sum_{i=1}^{k} \varepsilon_{n_i}\Gamma_{-n_i} = \sum_{j=1}^{l} \varepsilon_{m_j}\Gamma_{-m_j}$.

It is now obvious that φ is an endomorphism of $(R,+)$. Also, since $\varphi(\Gamma_n\Gamma_m\Gamma_n) = \varphi(\Gamma_{nmn}) = \Gamma_{-nmn} = \Gamma_{-n}\Gamma_{-m}\Gamma_{-n} = \varphi(\Gamma_n)\varphi(\Gamma_m)\varphi(\Gamma_n)$ for all $n,m \in \mathbb{Z}$, it follows easily that φ is a semi-homomorphism of near-rings.

The identity of R is Γ_1, and $\varphi(\Gamma_1) = \Gamma_{-1}$. Furthermore, $\Gamma_{-1} \neq -\Gamma_1$, because $\Gamma_{-1}(x+y) = -x + (-y) \neq (-y) + (-x) = -(x+y) = -\Gamma_1(x+y)$. Hence $\varphi(\Gamma_1) \neq -\Gamma_1$, and $\varphi(\Gamma_1) \neq \Gamma_1$.

It is well known that if F is a near-field, then either $F \cong M_c(\mathbb{Z}_2)$, the near-field of constant functions on $\mathbb{Z}_2$, or F is zero-symmetric (see e.g. [11, Proposition 8.1]). So if we exclude this "silly" near-field $M_c(\mathbb{Z}_2)$ (see Example 3.9), then the proof of [9, Proposition 9] serves to a great extent as the proof of the following proposition.

Let $Z(R)$ denote the center of a near-ring R.

Proposition 3.8. *If $\varphi : F \to F'$ is a semi-homomorphism of near-fields, then $\varphi(1) \in Z(\varphi(F))$.*

Proof. If φ is the zero map, then by the above remark $\varphi(1) = 0 \in Z(\varphi(F))$, since F' is zero-symmetric. If $\varphi(F) \neq 0$, then $\varphi(1) \neq 0$, otherwise $\varphi(a) = \varphi(1a1) = \varphi(1)\varphi(a)\varphi(1) = 0$ for all $a \in F$. Since $\varphi(a) = \varphi(1)\varphi(a)\varphi(1)$, the result follows from Lemma 3.3. ◇

Example 3.9. Let $\varphi : M_c(\mathbb{Z}_2) \to M_c(\mathbb{Z}_2)$ be the identity map. Then φ is an isomorphism of "near-fields" (in the sense of the remark preceding Proposition 3.8), but $\varphi(1) \notin Z(M_c(\mathbb{Z}_2))$, the empty set.

Hua [8] proved that every *semi-automorphism* of a division ring R, i.e. an automorphism φ of $(R,+)$ satisfying $\varphi(1) = 1$ and

$$\varphi(aba) = \varphi(a)\varphi(b)\varphi(a) \tag{6}$$

for all $a,b \in R$, is an automorphism of an anti-automorphism.

We have been unable to determine whether Hua's result can be "extended" to near-fields, i.e. whether every semi-automorphism of a near-field (where semi-automorphism is defined as above) is an automorphism. Notice that the lack of one distributive law should prevent a semi-automorphism from being an anti-automorphism, as is shown in [13] for finite simple near-rings with associated idempotents $e_1, e_2, \ldots, e_t$, where $t \geq 2$. (The case $t = 1$ produces the near-fields.)

After examining numerous examples, including the exceptional finite near-fields, i.e. the seven finite near-fields which are not Dickson near-fields (see e.g. [14, Chapter 4], where the structure of theses seven near-fields, which was originally determined by Zassenhaus [16], is made clear), we arrived at the following:

Conjecture. Every semi-automorphism of a near-field is an automorphism.

The examination of this problem yields a surprising result, the significance of which the authors do not understand fully at present and which perhaps has independent interest. It is well known that there are only two automorphisms of the Galois field $(GF(3^2), +, \cdot)$, viz. the (identity-preserving) automorphisms of $\mathbb{Z}_3[i]$ mapping i onto i and $2i$ respectively, where i is a root of the irreducible polynomial $x^2 + 1$ in $\mathbb{Z}_3[x]$. The term *non-field* is widely used in near-ring circles for a near-field which is not a field. The smallest (Dickson) non-field is given by $(GF(3^2), +, \circ)$, where $\circ$ is defined by

$$x \circ y = \begin{cases} x \cdot y, & \text{if } y \text{ is a square in the Galois field } (GF(3^2), +, \cdot) \\ x^3 \cdot y, & \text{otherwise.} \end{cases}$$

(See e.g. [12] for more details.) We show in the following example that every automorphism φ of $(GF(3^2), +)$ satisfying $\varphi(1) = 1$ is an automorphism of $(GF(3^2), +, \circ)$, and so every semi-automorphism of $(GF(3^2), +, \circ)$ is an automorphism. Hence there are precisely 6 automorphisms of $(GF(3^2), +, \circ)$ and the automorphism group of $(GF(3^2), +, \circ)$ is isomorphic to S_3. This provides an alternative proof of a special case of [16, Theorem 18].

Example 3.10. Let $(GF(3^2), +, \circ)$ be the smallest Dickson non-field as defined above, and let $a + bi$, $a, b \in \mathbb{Z}_3$, be the elements of $GF(3^2)$, with $i^2 = -1 = 2$. If φ is an automorphism of $(\mathbb{Z}_3[i], +)$ and $\varphi(1) = 1$, then $\varphi(a + bi) = a + b\varphi(i)$, and so $\varphi(i) \in \{i, 2i, 1 + i, 1 + 2i, 2 + i, 2 + 2i\}$. Since $k^3 = k$ and $3k = k$ and $3k = 0$ for every $k \in \mathbb{Z}_3$, we have, for all

$a + bi$ and $c + di$, the following:

$$(7) \qquad \begin{aligned} \varphi((a+bi)\circ(c+di)) &= \varphi((a+bi)\cdot(c+di)) \\ &= \varphi(ac+2bd+(ad+bc)i) \\ &= ac+2bd+(ad+bc)\varphi(i) \end{aligned}$$

if $c + di$ is a square in $(\mathbb{Z}_3[i], +, \cdot)$, and

$$(8) \qquad \begin{aligned} \varphi((a+bi)\circ(c+di)) &= \varphi((a+bi)^3\cdot(c+di)) \\ &= \varphi(ac+2bi)\cdot(c+di)) \\ &= \varphi(ac+bd+(ad+2bc)i) \\ &= ac+bd+(ad+2bc)\varphi(i) \end{aligned}$$

if $c + di$ is not a square in $(\mathbb{Z}_3[i], +, \cdot)$. Also,

$$(9) \qquad \begin{aligned} \varphi(a+bi)\circ\varphi(c+di) &= (a+b\varphi(i))\circ(c+d\varphi(i)) \\ &= ac+bd(\varphi(i))^2+(ad+bc)\varphi(i) \end{aligned}$$

if $c + d\varphi(i)$ is a square in $(\mathbb{Z}_3[i], +, \cdot)$, and

$$(10) \qquad \begin{aligned} \varphi(a+bi)\circ\varphi(c+di) &= (a+b\varphi(i))^3\cdot(c+d\varphi(i)) \\ &= (a+b(\varphi(i))^3)\cdot(c+d\varphi(i)) \\ &= ac+bd(\varphi(i))^4+ad\varphi(i)+bc(\varphi(i))^3 \end{aligned}$$

if $c + d\varphi(i)$ is not a square in $(\mathbb{Z}_3[i], +, \cdot)$.
It can be verified that $c + di$ is a square in $(\mathbb{Z}_3[i], +, \cdot)$ if and only if $cd = 0$, and so we consider the following cases:

(I) $c + di$ is a square in $(\mathbb{Z}_3[i], +, \cdot)$and $d = 0$:

We have $c + di = c$, and so it follows from (7) and (9) that

$$\varphi((a+bi)\circ(c+di)) = \varphi(a+bi)\circ\varphi(c+di).$$

(II) $c + di$ is a square in $(\mathbb{Z}_3[i], +, \cdot)$and $d \neq 0$:

In this case $c = 0$, but $c + d\varphi(i)$ may be or may not be a square in $(\mathbb{Z}_3[i], +, \cdot)$. The conditions on φ imply that $\varphi(k) = k$ for every $k \in \mathbb{Z}_3$, and so $\varphi(i) \notin \{0, 1, 2\}$. Therefore $\varphi(i) = k + li$ for some $k, l \in \mathbb{Z}_3$, $l \neq 0$.

If $k = 0$, then $c + d\varphi(i) = dli$, which is a square in $(\mathbb{Z}_3[i], +, \cdot)$, and so by (7) and (9) we have

$$\varphi((a+bi)\circ(c+di)) = \varphi(a+bi)\circ\varphi(c+di),$$

because $(\varphi(i))^2 = (li)^2 = 2l^2 = 2$. Suppose now that $k \neq 0$. Then $c + d\varphi(i) = d(k+li) = dk + dli$, which is not a square in $(\mathbb{Z}_3[i], +, \cdot)$. A direct calculation shows that $(k+li)^4 = 2$ in $(\mathbb{Z}_3[i], +, \cdot)$if $kl \neq 0$, and so the desired equality now follows from (7) and (10).

(III) $c + di$ is not a square in $(\mathbb{Z}_3[i], +, \cdot)$, and $\varphi(i) = li$ for some $l \in \mathbb{Z}_3$, $l \neq 0$:

Since $cd \neq 0$, it follows that $c + d\varphi(i)$ is not a square in $(\mathbb{Z}_3[i], +, \cdot)$. Furthermore, in this case $(\varphi(i))^2 = 2$ and $(\varphi(i))^4 = 1$ in $(\mathbb{Z}_3[i], +, \cdot)$, and so by (8) and (10) we have

$$\varphi((a+bi)\circ(c+di)) = \varphi(a+bi)\circ\varphi(c+di).$$

(IV) $c + di$ is not a square in $(\mathbb{Z}_3[i], +, \cdot)$, and $\varphi(i) = k + li$ for some $k, l \in \mathbb{Z}_3$, with $kl \neq 0$:

Now $c + d\varphi(i) = c + dk + dli$, which may be or may not be a square in $(\mathbb{Z}_3[i], +, \cdot)$. Firstly, suppose it is a square, i.e. $c + dk = 0$. Then $d + c\varphi(i) = d + c(k+li) = d + ck + cli$, and $d(\varphi(i))^2 = d(k^2 - l^2 + 2kli) = = 2dkli$, since $k^2 = l^2 = 1$. But $c = 2dk$ and $d + ck = dk^2 + ck = = (c+dk)k = 0$, and so $d + c\varphi(i) = d(\varphi(i))^2$. Hence by (8) and (9) we have

$$\begin{aligned}\varphi((a+bi)\circ(c+di)) &= ac + ad\varphi(i) + bc\varphi(i) + bd(\varphi(i))^2\\ &= \varphi(a+bi)\circ\varphi(c+di),\end{aligned}$$

Secondly, suppose $c + d\varphi(i)$ is not a square in $(\mathbb{Z}_3[i], +, \cdot)$, i.e. $c + dk \neq 0$. Then $c = dk$, since $cdk \neq 0$ and $c, d, k \in \mathbb{Z}_3$. Therefore $2c\varphi(i) = = 2ck + 2cli = d + ck + 2cli = d + c(k + 2li) = d + c(\varphi(i))^3$. Also, $(\varphi(i))^4 = 2$, and so by (8) and (10) we have

$$\begin{aligned}\varphi((a+bi)\circ(c+di)) &= ac + bd + ad\varphi(i) + b(2c\varphi(i))\\ &= ac + bd + ad\varphi(i) + b(d + c(\varphi(i))^3)\\ &= ac + 2bd + ad\varphi(i) + bc(\varphi(i))^3\end{aligned}$$

$$= ac + bd(\varphi(i))^4 + ad\varphi(i) + bc(\varphi(i))^3$$
$$= \varphi(a+bi) \circ \varphi(c+di).$$

This proves the assertion that every automorphism φ of $(GF(3^2),+)$ satisfying $\varphi(1) = 1$ is an automorphism of the smallest Dickson non-field $(GF(3^2),+,\circ)$.

Unfortunately(?) the above result does not hold for the Dickson non-field $(GF(5^2),+,\circ)$, where $\circ$ is defined by

$$x \circ y = \begin{cases} x \cdot y, & \text{if } y \text{ is a square in the Galois field } (GF(5^2),+,\cdot) \\ x^5 \cdot y, & \text{otherwise,} \end{cases}$$

as can be verified easily. However, as mentioned before, every semi-automorphism of this near-field and of all others investigated by us, is an automorphism.

Acknowledgements

1. Portions of this work were done while the second author was visiting the National Cheng Kung University in accordance with a bilateral exchange agreement between the NSC of the Republic of China and the CSIR of the Republic of South Africa. He wishes to express his appreciation for the financial assistance provided by the latter two bodies and for the hospitality bestowed upon him by the National Cheng Kung University.
2. Helpful discussions with Jim Clay during his visit to the National Cheng Kung University on the possibly significance of the result in Example 3.10, and on directions for future research in this regard, are gratefully acknowledged.

References

[1] ANCOCHEA, G.: Le Théorème de von Staudt en géométrie projective quaternionienne, *J. Reine Angew. Math.* **184** (1942), 192 – 198.

[2] ANCOCHEA, G.: On semi-automorphisms of division algebras, *Ann. of Math. (2)* **48** (1947), 147 – 153.

[3] ARTIN, E.: Geometric Algebra, Interscience, New York, 1957.

[4] FONG, Y. and VAN WYK, L.: A note on semi-homomorphisms of rings, *Bull. Austral. Math. Soc.* **40** (1989), 481 – 486.

[5] HEATHERLY, H. and OLIVIER, H.: Near integral domains, *Monatsh. Math.* **78** (1974), 215 – 222.

[6] HEATHERLY, H. and OLIVIER, H.: Near integral domains II, *Monatsh. Math.* **80** (1975), 85 – 92.

[7] HERSTEIN, I.N.: Semi-homomorphisms of groups, *Canad. J. Math.* **20** (1968), 384 – 388.

[8] HUA, L.K.: On the automorphisms of as field, *Proc. Nat. Acad. Sci. U.S.A.* **35** (1949), 386 – 389.

[9] HUQ, S.A.: Semi-homomorphisms of rings, *Bull. Austral. Math. Soc.* **36** (1987), 121 – 125.

[10] McQUARRIE, B.: A non-abelian near-ring in which $(-1)r=r$ implies $r=0$, *Canad. Math. Bull.* **17** (1974), 73 – 75.

[11] MELDURM, J.D.P.: Near-rings and their links with groups, *Res. Notes in Math.* **134**, Pitman, London, 1986.

[12] PILZ, G.: Near-Rings, Revised edition, North-Holland, Amsterdam, 1983.

[13] SMITH, K.C. and VAN WYK, L.: Semi-endomorphisms of finite simple centralizer near-rings, manuscript.

[14] WÄHLING, H.: Theorie der Fastkörper, Thales Verlag, Essen, 1987.

[15] WEINERT, H.J.: Related representation theorems for rings, semi-rings, near-rings and semi-near-rings by partial transformations and partial endomorphisms, *Proc. Edinburgh Math. Soc. (2)* **20** (1976-77), 307 – 315.

[16] ZASSENHAUS, H.: Über endliche Fastkörper, *Abh. Math. Sem. Univ. Hamburg* **11** (1936), 187 – 220.