LE MATEMATICHE
Vol. LI (1996) – Supplemento, pp. 159-166

STRONGLY MONOGENIC A-RIGID NEARRINGS

FIORENZA MORINI

To the memory of Umberto Gasapina

1. Introduction.

The study of the automorphism group of a nearring allows to derive properties of nearrings, but, above all, that often provides a link between nearrings and combinatorial structures.

For instance, the planar nearrings define in a natural way some interesting geometries and their automorphism group has remarkable influences on these geometries ([1], [4]).

In this paper the A-rigid nearrings - that is those which have no automorphism except the identity - are studied.

Rigidity in other algebraic structures has also been the object of previous research ([9], [2]). C. J. Maxson, in [5] and [6], first introduced and investigated the class of rigid rings in which, namely, the only ring endomorphisms are the trivial ones. Moreover, there, he gave a complete characterization of rigid left artinian rings (also see [7]).

In the present paper the automorphisms of a strongly monogenic finite nearring N with $Aut(N^+)$ abelian are characterized through the behaviour of their left identities. Consequently we prove that a finite planar nearring N with $Aut(N^+)$ abelian is A-rigid if, and only if, every non identical automorphism of N^+ maps a left identity to an element of N which is not a left identity.

Work carried out on behalf of Italian M.U.R.S.T.

Moreover, we obtain some specific properties about an A-rigid nearring whose additive group is cyclic of prime order.

2. Preliminaries.

For the notations and the basic results, we refer to [8] without any explicit recall. Precisely for a (left) nearring N, let N^+ denote its additive group and $Aut(N^+)$ denote the automorphism group of N^+. For $a \in N$, define $\gamma_a : N \to N$ by $\gamma_a(x) = ax$.

Definition 1. *A nearring N is A-rigid if the unique nearring automorphism $\alpha : N \to N$ is the identity map.*

If N is a trivial (1) A-rigid nearring, we obtain an analogous result as described in ring theory ([6], [7]).

Proposition 1. *A trivial nearring is A-rigid if, and only if, it only contains two elements.*

Proof. Let N be a A-rigid constant nearring. Then every automorphism of N^+ is a nearring automorphism. In particular for $a \in N$ α_a defined by $x \to a+x-a$ is an automorphism of N and hence, by the assumption, the map α_a must be the identity map of N. It follows N^+ is abelian. Therefore, similarly, $\beta : N \to N$ such that $\beta(x) = -x$ is an automorphism of N and the condition $\beta = \mathrm{id}_N$ implies N^+ is an elementary abelian 2-group. Moreover, N^+ is finite, because if it was infinite, any permutation of a basis of N^+ would be an automorphism of N contradicting the A-rigidity of N.

Let $N^+ = \bigoplus_{i=1}^{m} \mathbb{Z}_2^i$, where $m \in \mathbb{N}$.

Since it is well known that $|Aut(N^+)| = (2^m - 1)(2^m - 2) \cdots (2^m - 2^{m-1})$, the rigidity of N implies $m = 1$ and $|N| = 2$.

A similar argument applies in the case when N is a zero nearring.

The converse is trivial, because every nearring on $\mathbb{Z}_2$ has only one automorphism, the identity map. $\square$

3. Strongly monogenic nearrings.

A nearring N is A-rigid when none of the non identical automorphisms of N^+ preserves the multiplication of N.

---

(1) A nearring N is said trivial if N is a zero nearring or a constant one.

Clearly, if $\alpha : N \to N$ is a nearring automorphism, then α maps left identities to left identities of N, but in general an automorphism of N^+ satisfying the above property is not necessarily a nearring automorphism.

In Theorem 1 we prove that if N is a strongly monogenic ([2]) finite nearring with $Aut(N^+)$ abelian, then every automorphism of N^+ which transforms left identities in left identities is a nearring automorphism.

On the other hand the following examples show that nearrings exist which admit automorphisms of the additive group with the property described above, but such maps do not preserve multiplication. In the first case, N is a nearring with $Aut(N^+)$ abelian but N is not strongly monogenic, while in the other case the nearring is strongly monogenic with $Aut(N^+)$ non abelian.

Example 1. Let $\mathbb{Z}_8$ with addition modulo 8 and whith multiplication defined by

$\cdot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	0	0	0	0	0	0	0
3	0	5	2	7	4	1	6	3
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	4	0	4	0	4	0	4
7	0	1	2	3	4	5	6	7

Of course, $N = (\mathbb{Z}_8, +, \cdot)$ is a nearring which is not strongly monogenic.
The map $\alpha : x \to 7x$ is an element of $Aut(N^+)$ which permutes the left identities of N, but α is not an automorphism of N because, for instance, $\alpha(6 \cdot 3) \neq \alpha(6) \cdot \alpha(3)$.

Example 2. Let $(S_3, +)$ be the symmetric group on three letters.
Define multiplication on S_3 by

([2]) A nearring N is strongly monogenic if there exists $y \in N$ such that $yN = N$ and, for each $x \in N$, $xN = \{0\}$ or $xN = N$.

$\cdot$	0	a	b	c	x	y
0	0	0	0	0	0	0
a	0	0	0	0	0	0
b	0	0	0	0	0	0
c	0	0	0	0	0	0
x	0	a	c	b	y	x
y	0	a	b	c	x	y

It is easily checked that $N = (S_3, +, \cdot)$ is strongly monogenic, but it is known that $Aut(N^+)$ is not abelian. The map

$$\alpha = \begin{pmatrix} 0 & a & b & c & x & y \\ 0 & b & c & a & x & y \end{pmatrix} \in Aut(N^+)$$

fixes y, the unique left identity of N, but α fails to be an automorphism of N, since $\alpha(x \cdot a) \neq \alpha(x) \cdot \alpha(a)$.

We now recall that in [3] G. Ferrero proved the following properties concerning a strongly monogenic finite nearring N:

a) the set $\{\gamma_a | a \in N, \gamma_a \neq 0_N\}$ is a subgroup of $Aut(N^+)$;
b) N has at least one left identity.

Theorem 1. *Let N be a strongly monogenic finite nearring with $Aut(N^+)$ abelian. Suppose $\alpha \in \mathrm{Aut}(N^+)$. The following statements are equivalent:*

(a) α is an automorphism of N;
(b) for each $x \in N$, $\gamma_x = \gamma_{\alpha(x)}$;
(c) if, for $x \in N$, $\gamma_x = \mathrm{id}_N$ then $\gamma_{\alpha(x)} = \mathrm{id}_N$.

Proof. Let α be an automorphism of N^+. The definition implies that α is an automorphism of N if, and only if, $\alpha \circ \gamma_x = \gamma_{\alpha(x)} \circ \alpha$, for all $x \in N$. Clearly, by that and by the hypothesis, (a) and (b) result to be equivalent.

Of course, (b) implies (c).

To complete the proof we have to show the inverse implication: if α permutes each other the left identities of N, then α is an automorphism of N. If α is the identity map, the implication is clear.

Suppose $\alpha \in \mathrm{Aut}(N^+)$ of order $r > 1$. Let Φ be the subgroup of $\mathrm{Aut}(N^+)$ generated by α and let L denote the set of the left identities of N. By hypothesis $\alpha(L) = L$; if for each $y \in N \setminus L$, y is a left annihilator of N, then the orbits of

Φ contain or left identities or left annihilators.
In this case $\gamma_x = \gamma_{\alpha(x)}$, for all $x \in N$, and the proof is complete.

Suppose, indeed, there exists an element of N which is neither a left identity nor a left annihilator and K denotes the set of these elements.

First of all, we note that the set $K \cup L$ is closed with respect to multiplication in N and, for every $x \in K$, there exists $x' \in K$ such that $x'x = u_x$, where $u_x \in L$. In fact, now, N is strongly monogenic; for $x \in K$, γ_x is an automorphism of N^+ and, consequently, there exists $h \in \mathbb{N}$ such that $\gamma_x^h = \gamma_{x^h} = \mathrm{id}_N$. It means that every $x \in K$ has a left inverse, denoted by x'.

Moreover, it is possible to prove that for each $x \in K$, there exist $z \in K$ and $u_x \in L$ such that $x = zu_x$.
Suppose $x \in K$. If we take $z = (x')'$ then we have $x = (x')'x'x = zx'x = zu_x$.
Lastly, given $z \in K$, we note that for $i = 1, 2, \dots, r$ and $u \in L$ the following equalities $\alpha^i(zu) = (\alpha^i \circ \gamma_z)(u) = (\gamma_z \circ \alpha^i)(u) = z\alpha^i(u)$ hold, since $\gamma_z \in \mathrm{Aut}(N^+)$ and $\mathrm{Aut}(N^+)$ is abelian.

From the above observations, we see that the set $\{zu_1, zu_2, \dots, zu_r\}$ where $z \in K$ and $u_i = \alpha^i(u)$ ($u \in L$ and $i = 1, 2, \dots, r$) is an orbit of Φ and the union of these orbits exhaust K.

Now L and K are a union of orbits of Φ and so is $N \setminus (L \cup K)$, namely, the set of the left annihilators of N. It follows that α maps every left annihilator to a left annihilator.

To conclude the proof we show that for all $x \in N$, for all $n \in N$, $xn = \alpha(x)n$. The result is clear if $x \in L$ or $x \in N \setminus (L \cup K)$.
Suppose $x \in K$, we know that $x = zu_x$, where $z \in K$ and $u_x \in L$, and $\alpha(x) = z\alpha(u_x)$; thus, keeping in mind $\alpha(u_x) \in L$, we have $\alpha(x)n = z\alpha(u_x)n = zn = zu_xn = xn$, for any $n \in N$. □

Corollary 1. *A strongly monogenic finite nearring N with* $\mathrm{Aut}(N^+)$ *abelian is A-rigid if, and only if, every non identical automorphism of N^+ maps a left identity of N to an element which is not a left identity.*

In particular, since a planar nearring N is strongly monogenic, when N is finite and $\mathrm{Aut}(N^+)$ is abelian, it results an A-rigid nearring if, and only if, it satisfies the condition of Corollary 1.

The following examples show that integral or not A-rigid planar nearrings exist.

Example 3. Let $(\mathbb{Z}_{p^k}, +)$ be the additive group of integers modulo p^k with p prime and $k \in \mathbb{N}$. Let a be a fixed element of $\mathbb{Z}_{p^k}$ relatively prime to p.

Define multiplication by

$$x \cdot y = \begin{cases} y & \text{if } x = a \\ -y & \text{if } x = -a \\ 0 & \text{otherwise} \end{cases}$$

It is clear that $N = (\mathbb{Z}_{p^k}, +, \cdot)$ is a non integral planar nearring. Moreover, since no automorphism of N^+, except the identity, fixes a, N results A-rigid by Corollary 1.

Example 4. Let $\mathbb{Z}_9$ with addition modulo 9 and with multiplication defined by

$\cdot$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	8	7	6	5	4	3	2	1
3	0	1	2	3	4	5	6	7	8
4	0	8	7	6	5	4	3	2	1
5	0	1	2	3	4	5	6	7	8
6	0	8	7	6	5	4	3	2	1
7	0	1	2	3	4	5	6	7	8
8	0	8	7	6	5	4	3	2	1

Clearly $N = (\mathbb{Z}_9, +, \cdot)$ is a planar integral nearring and by Theorem 1, N is A-rigid because no $\alpha \in \mathrm{Aut}(\mathbb{Z}_9)$ preserves all the left identities.

We see that the condition described in Corollary 1 defines the A-rigidity for any nearring whose additive group is cyclic of prime order. In fact, if N is a nearring whose additive group is cyclic of prime order then N is strongly monogenic and $\mathrm{Aut}(N^+)$ is abelian.

In this case we can show the following

Proposition 2. *Let N be a nearring whose additive group is cyclic of prime order. If N has exactly one left identity, then N is A-rigid.*

Proof. This is immediate from Corollary 1 since any non identical automorphism of N^+ is fixed point free. □

Proposition 3. *Let N be a nearring whose additive group is cyclic of prime order. Suppose that N has exactly two left identities u_1, u_2 then N is A-rigid if, and only if, $u_1 + u_2 \neq 0$.*

Proof. Since N^+ is abelian, the map $\alpha : N \to N$ defined by $x \to -x$ is an element of $\mathrm{Aut}(N^+)$.

By Theorem 1, α is an automorphism of N if, and only if, $u_1 + u_2 = 0$. Consequently, by the hypothesis of A-rigidity of N, we have $u_1 + u_2 \neq 0$.

Conversely, let N be a non A-rigid nearring and let $\alpha \neq \mathrm{id}_N$ in $\mathrm{Aut}(N^+)$. Using Theorem 1 and the fact that, all the automorphisms of N^+, except the identity map, are fixed point free, we have $\alpha^2(u_1) = \alpha(u_2) = u_1$. This means that α has order 2. But in $\mathrm{Aut}(N^+)$ the only automorphism of order 2 is defined by $x \to -x$, hence $u_1 + u_2 = 0$. □

Proposition 4. *Let N be a nearring whose additive group is cyclic of prime order p. If N has exactly a prime number q of left identities and q is relatively prime to $p - 1$, then N is A-rigid nearring.*

Proof. Since $|\mathrm{Aut}(N^+)| = p - 1$ and $\mathrm{Aut}(N^+)$ is cyclic generated by the cycle $(1\varepsilon\varepsilon^2 \ldots \varepsilon^{p-2})$, where ε is a primitive root of p, every element α of $\mathrm{Aut}(N^+)$, $\alpha \neq \mathrm{id}_N$, is the product of disjoint cycles of equal lengths and α is fixed point free. Consequently, using Theorem 1, if α preserves multiplication then the q left identities of N form a cycle of length q: that is α has order q. But this is a contradiction because q does not divide $p - 1$. □

REFERENCES

[1] J.R. Clay, *Nearrings,* Oxford Science Publications, Oxford University Press, 1992.

[2] V. Dlab - B.H. Neumann, *Semigroups with few endomorphisms,* J. Aust. Math. Soc., 10 (1969), pp. 162-168.

[3] G. Ferrero, *Struttura degli stems p-singolari,* Riv. Mat. Univ. Parma, (2) 7 (1966), pp. 243-254.

[4] G. Ferrero, *Stems planari e BIB-Disegni,* Riv. Mat. Univ. Parma, (2) 11 (1970), pp. 79-96.

[5] C.J. Maxson, (0, 1)*-matrices and semigroups of ring endomorphisms,* Semigroup Forum, 5 (1972), pp. 160-166.

[6] C.J. Maxson, *Rigid rings,* Proc. Edimb. Math. Soc., 21 (1978), pp. 95-101.

[7] K.R. McLean, *Rigid Artinian rings,* Proc. Edimb. Math. Soc., 25 (1982), pp. 97-99.

[8] G. Pilz, *Near-rings,* 2nd. ed., North Holland Math. Studies 23, Amsterdam, 1983.

[9] P. Volpenka - A. Pultr - Z. Hedrlin, *A rigid relation exists on any set,* Comment. Math. Univ. Carolinae, 6 (1965), pp. 149-155.

Dipartimento di Elettronica per l'Automazione,
Facoltà di Ingegneria,
Università di Brescia,
Via Branze 38,
25123 Brescia (ITALY)