Riv. Mat. Univ. Parma (6) **1** (1998), 1-11

A. BENINI and F. MORINI (*)

Weakly divisible nearrings on the group of integers $(\bmod p^n)$ (**)

1 - Introduction

In some papers written from 1964 to 1970 (see [**3**], [**5**]), James Clay began to work on the construction of nearrings on given additive groups. The problem, which was later developed by various authors (see [**7**], [**8**], [**11**], [**1**]), remains substantially open. In fact, except for some general theorems, a method explicitly describing a construction of nearrings on given additive groups is available only for certain specific classes of groups (see [**7**], [**8**], [**9**], [**10**]). This paper, according to Ferrero's work (see [**7**], [**6**]), generalises the method provided in [**2**] for the construction of weakly divisible nearrings, which are left nearrings N fulfilling the following:

$$\forall x, y \in N, \qquad \exists z \in N \,|\, xz = y \text{ or } yz = x .$$

Here we deal with wd-nearrings on a cyclic additive group. Since it has been proved that the residue class rings of order m are wd-rings if, and only if, m is a prime-power, in Section 4 we study and construct wd-nearrings on $(\mathbb{Z}_{p^n}, +)$. Our construction allows the characterisation of all zerosymmetric wd-nearrings on the group $(\mathbb{Z}_{p^n}, +)$ of integers $(\bmod p^n)$, p prime, in which $p\mathbb{Z}_{p^n}$ is the ideal Q of all the nilpotent elements. Even when the order of the additive group is not a prime-power or $p\mathbb{Z}_{p^n}$ is different from Q, it is possible to construct wd-nearrings on $(\mathbb{Z}_{p^n}, +)$ and we have some examples. The characterisation of such cases will be object of further research.

(*) Dipartimento di Elettronica per l'Automazione, Facoltà di Ingegneria dell'Università degli Studi di Brescia, Via Branze 38, I-25123 Brescia, Italy.
(**) Received March 16, 1998. AMS classification 16 Y 30. Work carried out on behalf of Italian M.U.R.S.T.

2 - Preliminaries and notations

Let $(H, +)$ be a finite group and Φ a subgroup of $Aut(H, +)$. Let e be a selected representative of any orbit of Φ. For every h belonging to $\Phi(e)$, φ_h will denote an automorphism of Φ such that $\varphi_h(e) = h$. Obviously φ_h exists for every $h \in H^*$, and, if the automorphisms of Φ are fixed point free, it is the only one.

In the following we refer to zerosymmetric left nearrings, without any explicit recall. For the notations we refer to [**12**]. Here we recall that γ_a denotes the left translation defined by a, for $a \in N$, that is $\gamma_a(x) = ax$, for every $x \in N$. Also recall that γ_a is an endomorphism of N^+ and it turns out to be an automorphism if, and only if, a is a left cancellable element of N. If H is a subset of N, $\Gamma(H)$ denotes the set of the left translations defined by the elements of H. The identity of $Aut(N, +)$ is denoted by id_N.

From Prop. 9 and Th. 6 of [**2**] we know that a finite wd-nearring N is the disjoint union of the nil radical Q (hereinafter simply called *radical*), equal to the prime and the Jacobson radicals, and the multiplicative semigroup C of the left cancellable elements. Moreover, by Th. 8 of [**2**], C is the disjoint union of maximal multiplicative subgroups of C, isomorphic to each other.

As in [**2**], in the following, the maximal subgroup of C containing a will be denoted by B_a and 1_a will be its identity. So $N = Q \cup C$, $C = \bigcup_{a \in C} B_a$ where $B_a = \{x \in C \mid x1_a = x\}$. We recall here that the identities of the B_as $(a \in C)$ are the left identities of N and the only idempotent elements of N. Moreover, every B_a $(a \in C)$ contains only one idempotent element (Th. 7, [**2**]).

3 - Finite wd-nearrings

We now show some further properties of a finite wd-nearring.

Proposition 1. *Let N be a finite wd-nearring and q a nilpotent element of N. The set of the right identities of q is a multiplicative subsemigroup of C which contains at least one idempotent element.*

Let q be a non trivial nilpotent element of N. From Prop. 1 of [**2**] the set $R(q)$ of the right identities of q is a subset of C. Furthermore, $R(q)$ is closed with respect to the multiplication, hence it is a multiplicative semigroup of left cancellable elements. Since each left cancellable element has a power which is a left identity of N ([**2**], Th. 8(b)), $R(q)$ obviously contains some idempotent elements. ■

Proposition 2. *Let N be a finite wd-nearring.*

(1) *The set* $\Gamma(C)$ *is a group o f automorphisms of* N^+.

(2) *For each* $a \in C$, $\Gamma(C) = \Gamma(B_a)$.

(3) *For each* $a \in C$, $B_a = \Gamma(a)$, *where* $\Gamma(a)$ *denotes the orbit of* $\Gamma(C)$ *containing the element* a.

(4) *Let* $c \in C$ *with* $\gamma_c \neq id_N$. *The fixed points of* γ_c *are nilpotent and form an* N*-subgroup of* N.

(1) Obviously, $\Gamma(C)$ is a semigroup of automorphisms of N^+. Furthermore, from Th. 8(b) of [**2**], for each $c \in C$ there is a power c^t which is a left identity of N. Thus $id_N = \gamma_{c^t}$ belongs to $\Gamma(C)$ and $\gamma_c^{t-1} = \gamma_{c^{t-1}}$ is the inverse of γ_c.

(2) For all $a, b \in C$, $\Gamma(B_a) = \Gamma(B_b)$. In fact, for every $h \in B_a$, $\gamma_h(x) = hx = h(1_b x) = (h1_b)x = \gamma_{h1_b}(x)$. From $h1_b \in B_b$ it follows that $\gamma_h \in \Gamma(B_b)$ $\forall h \in B_a$. In the same way we obtain $\gamma_k \in \Gamma(B_a)$ $\forall k \in B_b$.

(3) Clearly, $B_a = \{x \in C \mid x1_a = x\} = \{x \in C \mid \gamma_x(1_a) = x\} = \{\gamma_x(1_a) \mid x \in C\} = \{\gamma_x(1_a) \mid \gamma_x \in \Gamma(C)\} = \Gamma(1_a)$. Since $a \in B_a$, a also belongs to $\Gamma(1_a)$, hence $\Gamma(1_a) = \Gamma(a)$.

(4) Let $c \in C$ and $\gamma_c \neq id_N$. Let h be a fixed point of γ_c, that is $ch = h$. If h is left cancellable, there is a power h^t which is a left identity of N. From $ch^t = h^t$, we obtain $ch^t x = h^t x$, for all $x \in N$, and this implies $cx = x$, now excluded. Therefore h is nilpotent. It is routine to verify that $S(c) = \{x \in N \mid \gamma_c(x) = x\}$ is an N-subgroup of N. ■

4 - Wd-nearrings on $(\mathbb{Z}_{p^n}, +)$

The particular additive structure of a nearring N on the group of integers (mod p^n) acts very strongly to determine the multiplicative structure. For instance, we know that, for any x and y in N, $x \circ y = y \cdot (x \circ 1)$, where «$\circ$» and «$\cdot$» denote the multiplications in N and in the ring of integers (mod p^n) respectively (see [**3**]). As usual, «$\cdot$» will be omitted. In the following $\widehat{a}$ will denote the residue class (mod p^n) containing $a \in \mathbb{Z}$ and $x^{(t)}$, x^t the powers of $x \in \mathbb{Z}_{p^n}$ with respect to «$\circ$» and «$\cdot$». We recall here that every automorphism α_k of $(\mathbb{Z}_{p^n}, +)$ is of the form $\alpha_k \colon x \to kx$, k relatively prime to p. The automorphism group of $(\mathbb{Z}_{p^n}, +)$ is a well known group of order $p^{n-1}(p-1)$ whose subgroups containing only fixed point free automorphisms have order t which divides $p-1$ (see [**4**] Chapter 2).

The following propositions describe some further properties of wd-nearrings with the additive group $G = (\mathbb{Z}_{p^n}, +)$.

Proposition 3. *Let* N *be a wd-nearring on* $G = (\mathbb{Z}_{p^n}, +)$. *If* p *divides the order of* $\Gamma(C)$ *then* $\widehat{p}$ *is nilpotent.*

From Sylow's Theorem if p divides the order of the group $\Gamma(C)$ (Proposition 2(1)), then there exists an element of order p in $\Gamma(C)$: let γ_c be, for some $c \in C$.

Let $p \neq 2$. The elements of $Aut\,(G)$ of order p are those automorphisms of G defined by elements of the form $hp^{n-1}+1$, with $1 \leqslant h \leqslant p-1$, so $\gamma_c(\widehat{p}) = (hp^{n-1}+1)\widehat{p} = \widehat{p}$. From Proposition 2(3) it follows that $\widehat{p}$ is nilpotent.

Let $p = 2$. It is well-known that the elements of $Aut\,(G)$ of order 2 are the automorphisms $\alpha_{a_i} (i = 1, 2, 3)$ defined by the elements $a_1 = 1 + 2^{n-1}$, $a_2 = -1$, $a_3 = -1 + 2^{n-1}$. Obviously, $|\Gamma(C)| \neq 2$ or $|\Gamma(C)| = 2$; when $|\Gamma(C)| = 2$, it results either $\Gamma(C) = \{\mathrm{id}_N, \alpha_{a_1}\}$ or $\Gamma(C) = \{\mathrm{id}_N, \alpha_{a_2}\}$ or $\Gamma(C) = \{\mathrm{id}_N, \alpha_{a_3}\}$, thus we have to examine the following complementary cases:

(1) $|\Gamma(C)| > 2$;
(2) $\Gamma(C) = \{\mathrm{id}_N, \alpha_{a_1}\}$;
(3) $\Gamma(C) = \{\mathrm{id}_N, \alpha_{a_2}\}$;
(4) $\Gamma(C) = \{\mathrm{id}_N, \alpha_{a_3}\}$.

Cases (1) and (2). Now α_{a_1} belongs to $\Gamma(C)$, hence $\widehat{2}$ is nilpotent because it is fixed by α_{a_1}.

Case (3). If $\Gamma(C) = \{\mathrm{id}_N, \alpha_{a_2}\}$ and we suppose $\widehat{2}$ is left cancellable, then $\gamma_{\widehat{2}} \in \Gamma(C)$ and, hence, it must be $\widehat{2} \circ \widehat{1} = \gamma_{\widehat{2}}(\widehat{1}) = \pm \widehat{1}$. In both cases, it cannot be $\widehat{2}^{n-1} \circ \widehat{1} = \widehat{2}^{n-1}$, otherwise $\widehat{2}^{n-1} = \pm \widehat{2}^{n-1} = \widehat{2}^{n-1} \circ (\pm \widehat{1}) = \widehat{2}^{n-1} \circ (\widehat{2} \circ \widehat{1}) = (\widehat{2}^{n-1} \circ \widehat{2}) \circ \widehat{1} = [\widehat{2}(\widehat{2}^{n-1} \circ \widehat{1})] \circ \widehat{1} = \widehat{0}$, and this is absurd. So $\widehat{2}^{n-1} \circ \widehat{1} \neq \widehat{2}^{n-1}$.

Nevertheless, $\widehat{2}^{n-1}$ is always nilpotent, because it is a fixed point of each element of $Aut\,(G)$, hence $\widehat{2}^{n-1} \circ \widehat{1}$ is nilpotent too. Since $Q \subseteq p\mathbb{Z}_{p^n}$, $\widehat{2}^{n-1} \circ \widehat{1} = \widehat{2}^k \widehat{b}$ with $(b, 2) = 1$ and $1 < k < n-1$. A direct verification shows that $\widehat{2}^{n-1-k}$ is a right identity of $\widehat{2}^{n-1}$ and, therefore, it is a left cancellable element of N (see Prop. 1 [**2**]), hence $\gamma_{\widehat{2}^{n-1-k}} \in \Gamma(C)$ and thus $\widehat{2}^{n-1-k} \circ \widehat{1} = \gamma_{\widehat{2}^{n-1-k}}(\widehat{1}) = \pm \widehat{1}$. We examine the two possibilities separately.

Suppose $\widehat{2}^{n-1-k} \circ \widehat{1} = \widehat{1}$. Since $B_{\widehat{2}^{n-1-k}} = \{\widehat{2}^{n-1-k}, -\widehat{2}^{n-1-k}\}$, it follows that $(-\widehat{2}^{n-1-k}) \circ \widehat{1} = -\widehat{1}$. Thus

$$\widehat{2}^k \widehat{b} = \widehat{2}^{n-1} \circ \widehat{1} = (-\widehat{2}^{n-1}) \circ \widehat{1} = [-(\widehat{2}^{n-1} \circ \widehat{2}^{n-1-k})] \circ \widehat{1} = [\widehat{2}^{n-1} \circ (-\widehat{2}^{n-1-k})] \circ \widehat{1}$$

$$= \widehat{2}^{n-1} \circ [(-\widehat{2}^{n-1-k} \circ \widehat{1})] = \widehat{2}^{n-1} \circ (-\widehat{1}) = -(\widehat{2}^{n-1} \circ \widehat{1}) = -\widehat{2}^k \widehat{b},$$

that is $\widehat{2}^k \widehat{b} = -\widehat{2}^k \widehat{b}$, but now this is excluded because of $k < n-1$. Thus $\widehat{2}$ is nilpotent.

Suppose $\widehat{2}^{n-1-k} \circ \widehat{1} = -\widehat{1}$. We have again $B_{\widehat{2}^{n-1-k}} = \{\widehat{2}^{n-1-k}, -\widehat{2}^{n-1-k}\}$, but now $(-\widehat{2}^{n-1-k}) \circ \widehat{1} = \widehat{1}$. As above, it results $-\widehat{2}^k \widehat{b} = \widehat{2}^k \widehat{b}$ which is absurd.

Case (4). If $\Gamma(C) = \{id_N, \alpha_{a_3}\}$, the statement arises analogously to case (3). ■

Proposition 4. *Let N be a wd-nearring on $G = (\mathbb{Z}_{p^n}, +)$. The following statements are equivalent*:

(1) $\widehat{p}$ *is a nilpotent element*;
(2) $p\mathbb{Z}_{p^n}$ *is the radical* Q;
(3) *the right identities of* $\widehat{p}$ *belong to* $\mathbb{Z}_{p^n} \backslash p\mathbb{Z}_{p^n}$.

(1)⇒(2) If $\widehat{p}$ belongs to the subnearring Q, obviously $p\mathbb{Z}_{p^n}$ is included in Q. But $p\mathbb{Z}_{p^n}$ is a maximal subgroup of $(\mathbb{Z}_{p^n}, +)$, so $Q = p\mathbb{Z}_{p^n}$.

(2)⇒(3) The right identities of $\widehat{p}$ are left cancellable (see Proposition 1) and if $Q = p\mathbb{Z}_{p^n}$, the left cancellable elements of N are in $\mathbb{Z}_{p^n} \backslash p\mathbb{Z}_{p^n}$.

(3)⇒(1) Let $\widehat{g}$ be a right identity of $\widehat{p}$. Since g is relatively prime to p, then $\widehat{g}$ is one of the generators of $(\mathbb{Z}_{p^n}, +)$, hence, for some k in $\mathbb{Z}$, it follows that $\widehat{p} = k\widehat{g}$, where p divides k because p and g are relatively prime. By induction, we can show that $\widehat{p}^{(t)} = k^{t-1}\widehat{p}$. In particular, we obtain $\widehat{p}^{(n)} = k^{n-1}\widehat{p} = \widehat{0}$ because k is a multiple of p, hence $\widehat{p}$ is nilpotent. ■

Using Propositions 3 and 4, recalling that $\Gamma(C)$ is the group of the left translations defined by the left cancellable elements, we can derive the following:

Theorem 1. *If N is a wd-nearring on $G = (\mathbb{Z}_{p^n}, +)$ and p divides the order of $\Gamma(C)$, then the set Q of the nilpotent elements coincides with $p\mathbb{Z}_{p^n}$.* ■

Thus all wd-nearrings on $(\mathbb{Z}_{2^n}, +)$ have $Q = 2\mathbb{Z}_{2^n}$, while, if $p \neq 2$, there exist wd-nearrings on $(\mathbb{Z}_{p^n}, +)$ with $Q = p\mathbb{Z}_{p^n}$ and also with $Q \neq p\mathbb{Z}_{p^n}$, when p does not divide the order of $\Gamma(C)$. That is shown by the following example.

Example 1. Let $G = (\mathbb{Z}_{81}, +)$ and define on $\mathbb{Z}_{81}$ the following multiplications: for all $\widehat{a}, x \in \mathbb{Z}_{81}$

$$\widehat{a} \circ x = \begin{cases} \widehat{0} & \text{if } a = 0 \\ x & \text{if } a \equiv_3 1 \text{ or } a = 3k \text{ with } k \equiv_3 1 \\ 80x & \text{if } a \equiv_3 2 \text{ or } a = 3k \text{ with } k \equiv_3 2 \\ 9x & \text{if } a = 27 \text{ or } a = 9k \text{ with } k \equiv_3 1 \\ 72x & \text{if } a = 54 \text{ or } a = 9k \text{ with } k \equiv_3 2 \end{cases}$$

$$\widehat{a} \circ' x = \begin{cases} \widehat{0} & \text{if } a = 0 \\ x & \text{if } a \equiv_3 1 \\ 80x & \text{if } a \equiv_3 2 \\ 3x & \text{if a} = 3\text{k with } k \equiv_3 1 \\ 78x & \text{if } a = 3k \text{ with } k \equiv_3 2 \\ 9x & \text{if } a = 9k \text{ with } k \equiv_3 1 \\ 72x & \text{if } a = 9k \text{ with } k \equiv_3 2 \\ 27x & \text{if } a = 27 \\ 54x & \text{if } a = 54 \end{cases}$$

then $(\mathbb{Z}_{81}, +, \circ')$ turns out to be a wd-nearring with $Q = 3\mathbb{Z}_{81}$, while $(\mathbb{Z}_{81}, +, \circ)$ results a wd-nearring with $Q \neq 3\mathbb{Z}_{81}$. Both these constructions are possible, because $p = 3$ does not divide the order of $\Gamma(C) = \{id_G, -id_G\}$, in according to Theorem 1.

Case $Q = p\mathbb{Z}_{p^n}$.

In this paragraph we collect some further properties about wd-nearrings on $(\mathbb{Z}_{p^n}, +)$ with $Q = p\mathbb{Z}_{p^n}$.

Proposition 5. *Let* $N = (\mathbb{Z}_{p^n}, +, \circ)$ *be a wd-nearring with* $Q = p\mathbb{Z}_{p^n}$. *For every* $k \in \mathbb{Z}$, *it is* $k\widehat{p}^t \circ \widehat{1} = p^t e^{-t}(ke^t \circ \widehat{1})$, *where* $1 \leqslant t < n$ *and* e *is an idempotent right identity of* $\widehat{p}$.

From the hypothesis and Proposition 4, we have $\widehat{p} \circ e = \widehat{p}$ with $e \in \mathbb{Z}_{p^n} \setminus p\mathbb{Z}_{p^n}$, hence e is an invertible element of the ring $(\mathbb{Z}_{p^n}, +, \cdot)$ so $\widehat{p} \circ \widehat{1} = e^{-1}\widehat{p}$. Consequently, $k\widehat{p} = k(\widehat{p} \circ e) = \widehat{p} \circ ke$ and also $\widehat{p}^{(2)} = p^2 e^{-1}$. By induction we can prove $k\widehat{p}^t = \widehat{p}^{(t)} \circ ke^t$ and also $\widehat{p}^{(t)} \circ \widehat{1} = p^t e^{-t}$. Thus, $k\widehat{p}^t \circ \widehat{1} = \widehat{p}^{(t)} \circ ke^t \circ \widehat{1} = (ke^t \circ \widehat{1})(\widehat{p}^{(t)} \circ \widehat{1}) = p^t e^{-t}(ke^t \circ \widehat{1})$. ■

We now establish a congruence between the identities 1_a of the maximal subgroups B_a of C.

Proposition 6. *Let* $N = (\mathbb{Z}_{p^n}, +, \circ)$ *be a wd-nearring with* $Q = p\mathbb{Z}_{p^n}$. *Let* B_x, B_y $(x, y \in C)$ *be two maximal multiplicative subgroups of* C. *If* $\widehat{a} \in B_x$, $\widehat{b} \in B_y$ *and* $\widehat{a} - \widehat{b} \in p^j\mathbb{Z}_{p^n}$, $(j < n)$, *then it is also* $1_{\widehat{a}} - 1_{\widehat{b}} \in p^j\mathbb{Z}_{p^n}$.

Let $\widehat{e}$ be an idempotent right identity of $\widehat{p}$. From $\widehat{a} - \widehat{b} \in p^j\mathbb{Z}_{p^n}$ it derives $p^{n-j}\widehat{a} = p^{n-j}\widehat{b}$ and hence $p^{n-j}e^{-(n-j)}\widehat{a} = p^{n-j}e^{-(n-j)}\widehat{b}$. Clearly, we can also say that $ae^{-(n-j)}\widehat{p}^{n-j} \circ \widehat{1} = be^{-(n-j)}\widehat{p}^{n-j} \circ \widehat{1}$. Using Proposition 5 we obtain

$p^{n-j}\widehat{e}^{-(n-j)}(ae^{-(n-j)}\widehat{e}^{-(n-j)}\circ\widehat{1}) = p^{n-j}\widehat{e}^{-(n-j)}(be^{-(n-j)}\widehat{e}^{-(n-j)}\circ\widehat{1})$. It follows $p^{n-j}(\widehat{a}\circ\widehat{1}) = p^{n-j}(\widehat{b}\circ\widehat{1})$ and $(\widehat{a}\circ\widehat{1})-(\widehat{b}\circ\widehat{1})\in p^j\mathbb{Z}_{p^n}$, hence $(\widehat{a}\circ\widehat{1})^{-1}-(\widehat{b}\circ\widehat{1})^{-1}$ belongs to $p^j\mathbb{Z}_{p^n}$. Keeping in mind that $1_{\widehat{a}} = (\widehat{a}\circ\widehat{1})^{-1}\widehat{a}$ and $1_{\widehat{b}} = (\widehat{b}\circ\widehat{1})^{-1}\widehat{b}$, the statement is clear. ■

In [3], necessary and sufficient conditions are given to construct all the nearrings whose additive group is finite and cyclic. Precisely, Clay proved that a function π of $\mathbb{Z}_m$ in itself such that $\pi(a)\pi(b) = \pi(a\pi(b))$, for all $a, b\in\mathbb{Z}_m$, (hereinafter called *Clay function*), defines a multiplication «$*$» on $(\mathbb{Z}_m, +)$ by $a*b = \pi(a)b$ and $(\mathbb{Z}_m, +, *)$ turns out to be a nearring. Conversely, if «$\circ$» is the multiplication of a nearring $N = (\mathbb{Z}_m, +, \circ)$, then the map π of $\mathbb{Z}_m$ in itself defined by $\pi(a) = a\circ\widehat{1}$ is a Clay function. Clearly, this last function π defines a multiplication which equals «$\circ$» of N.

Using these previous results we can prove the following:

Proposition 7. *Let $N = (\mathbb{Z}_{p^n}, +, \circ)$ be a wd-nearring with $Q = p\mathbb{Z}_{p^n}$. Suppose e is an idempotent right identity of the element $\widehat{p}$. The Clay function π defining the product «$\circ$» of N is such that:*

for each $\widehat{a}\in\mathbb{Z}_{p^n}$, $a = kp^t$, with $k\in\mathbb{Z}$ and $(k, p) = 1$

$$\pi(\widehat{a}) = p^t\gamma_{ke^t}(e^{-t})$$

where γ_{ke^t} is the left translation defined by ke^t.

By [3] $\pi(\widehat{a}) = \widehat{a}\circ\widehat{1}$, $\widehat{a}\in\mathbb{Z}_{p^n}$, defines the Clay function related to the product of N. Therefore, we have to prove that $\widehat{a}\circ\widehat{1} = p^t\gamma_{ke^t}(e^{-t})$, for each $a = kp^t\in\mathbb{Z}$, $(k, p) = 1$. From Proposition 5, $\widehat{a}\circ\widehat{1} = k\widehat{p}^t\circ\widehat{1} = p^te^{-t}(ke^t\circ\widehat{1}) = p^te^{-t}\gamma_{ke^t}(\widehat{1}) = p^t\gamma_{ke^t}(e^{-t})$. ■

Construction.

In [7] Giovanni Ferrero shows how to construct, in the finite case, strongly monogenic nearrings, starting from an additive group G and a subgroup Φ of *Aut* (G). With a suitable choice of Φ, in [8], the author can build a particular class of strongly monogenic nearrings, the planar and specifically integral planar nearrings. It is exactly in [8] that the (G, Φ) pair is introduced, where G is an additive group and Φ is a subgroup of *Aut* (G) which only includes fixed point free automorphisms. This pair (G, Φ) is known in literature as *Ferrero pair*.

Even if according to Ferrero's work, the construction described in this paper starts from a pair (G, Φ) which is not necessarily a Ferrero pair, in fact G equals $(\mathbb{Z}_{p^n}, +)$ and Φ is any subgroup of not necessarily fixed point free automorphisms of G. Beginning with such a pair (G, Φ), now we are able to define a Clay function on $\mathbb{Z}_{p^n}$. The derived nearring results a wd-nearring with $Q = p\mathbb{Z}_{p^n}$, thus, it is non integral nearring but with a trivial left annihilator, therefore, in particular, non integral planar nearring and not even strongly monogenic.

Definition 1. *Let* $G = (\mathbb{Z}_{p^n}, +)$ *and let* Φ *be a subgroup of Aut* (G). *Two elements* a *and* b *of* G *are called* α*-associate if the following condition holds*:

$$(\alpha) \quad \begin{array}{l} \text{if } a - b \notin p^j\mathbb{Z}_{p^n},\ (j < n), \text{ then for all } x \in \Phi(a) \\ \text{and for all } y \in \Phi(b) \text{ it is } x - y \notin p^j\mathbb{Z}_{p^n}. \end{array}$$

A set of representatives of the orbits included in $\mathbb{Z}_{p^n} \backslash p\mathbb{Z}_{p^n}$ *is called* α*-set if its elements are* α*-associate to each other. A subgroup* Φ *of Aut* (G) *with an* α*-set* R_α *will be denoted by* $\langle \Phi, R_\alpha \rangle$.

Definition 2. *Let* $G = (\mathbb{Z}_{p^n}, +)$ *and* $\langle \Phi, R_\alpha \rangle$ *be a subgroup of Aut* (G) *with an* α*-set. Let* e *be a selected element of* R_α. *For every* $\hat{a} \in \mathbb{Z}_{p^n}$ *define* (1):

$$\pi(\hat{a}) = \begin{cases} \hat{0} & \text{if } a = 0\,, \\ p^r \varphi_{ke^r}(e^{-r}) & \text{if } a = kp^r \text{ with } k \in \mathbb{Z},\ (k, p) = 1 \text{ and } 0 \leq r < n\,. \end{cases}$$

Proposition 8. *Let* G, $\langle \Phi, R_\alpha \rangle$ *and* π *be as in Definition* 2. *Then* π *is a Clay function.*

First of all, we prove that π is a function. Clearly, for every $\hat{a} \in \mathbb{Z}_{p^n}$, $\pi(\hat{a})$ exists. Hence it is sufficient to show that $\hat{a} = \hat{b}$ implies $\pi(\hat{a}) = \pi(\hat{b})$.

If $\hat{a}, \hat{b} \in \mathbb{Z}_{p^n} \backslash p\mathbb{Z}_{p^n}$ the statement is clear.

If $\hat{a} \in p\mathbb{Z}_{p^n}$ then $\hat{b} \in p\mathbb{Z}_{p^n}$ too. Denote $a = kp^r$ and $b = (k + tp^{n-r})\, p^r$, for some $t \in \mathbb{Z}$, with $(k, p) = 1$ and $0 \leq r < n$. It follows:

$$(\beta) \quad \pi(\hat{a}) = p^r \varphi_{ke^r}(e^{-r}) = p^r e^{-r} \varphi_{ke^r}(\hat{1})\,,$$

$$(\gamma) \quad \pi(\hat{b}) = p^r \varphi_{(k+tp^{n-r})e^r}(e^{-r}) = p^r e^{-r} \varphi_{(k+tp^{n-r})e^r}(\hat{1})\,.$$

Comparing (β) and (γ), we can see that our statement is true if $\varphi_{ke^r}(\hat{1})$ and

(1) We recall that φ_x denotes the automorphism of Φ such that $\varphi_x(e_x) = x$, where e_x is the selected representative of $\Phi(x)$.

$\varphi_{(k+tp^{n-r})e^r}(\widehat{1})$ are congruent (mod $p^{n-r}\mathbb{Z}_{p^n}$). Let e_1 and e_2 denote the selected representatives of $\Phi(ke^r)$ and $\Phi((k+tp^{n-r})e^r)$ respectively, by the hypothesis e_1 and e_2 are α-associate, it follows that $e_1 - e_2$ belongs to $p^{n-r}\mathbb{Z}_{p^n}$, and this is true for $\varphi_{(k+tp^{n-r})e^r}(e_1) - \varphi_{(k+tp^{n-r})e^r}(e_2)$ too. But $\varphi_{(k+tp^{n-r})e^r}(e_2)$ equals $(k+tp^{n-r})e^r$ which, clearly, belongs to the coset $ke^r + p^{n-r}\mathbb{Z}_{p^n}$, called S. Finally, recalling $ke^r = \varphi_{ke^r}(e_1)$, it results that $\varphi_{(k+tp^{n-r})e^r}(e_1)$ and $\varphi_{ke^r}(e_1)$ are in S. Thus, since $e_1 \in \mathbb{Z}_{p^n}\backslash p\mathbb{Z}_{p^n}$, the proof is complete.

We now show that π is a Clay function, that is π fulfils the following condition $\pi(a)\pi(b) = \pi(a\pi(b))$, for all $a, b \in G$.

Take $\widehat{a}, \widehat{b} \in \mathbb{Z}_{p^n}$ with $a = hp^r$, $b = kp^s$, where h, k are relatively prime to p and $0 \leq r, s < n$. We have:

$$\pi(\widehat{a})\,\pi(\widehat{b}) = p^r \varphi_{he^r}(e^{-r})\, p^s \varphi_{ke^s}(e^{-s}) =$$

$$= p^{r+s} e^{-(r+s)} \varphi_{he^r}(\widehat{1})\, \varphi_{ke^s}(\widehat{1}) = p^{r+s} e^{-(r+s)} \varphi_{ke^s}(\varphi_{he^r}(\widehat{1})),$$

$$\pi(\widehat{a}\pi(\widehat{b})) = \pi(hp^{r+s}\varphi_{ke^s}(e^{-s})) = p^{r+s}\varphi_{h\varphi_{ke^s}(e^{-s})\,e^{r+s}}(e^{-(r+s)}) =$$

$$= p^{r+s} e^{-(r+s)} \varphi_{he^r\varphi_{ke^s}(\widehat{1})}(\widehat{1}) = p^{r+s} e^{-(r+s)} \varphi_{\varphi_{ke^s}(he^r)}(\widehat{1}).$$

Because $\varphi_{\varphi_{x(y)}} = \varphi_x \circ \varphi_y$, for each $x, y \in \mathbb{Z}_{p^n}\backslash p\mathbb{Z}_{p^n}$, then the proof is complete. ■

In the next example we can see that the choice of the representatives of the orbits included in $\mathbb{Z}_{p^n}\backslash pZ_{p^n}$ is essential in order to make π a function.

Example 2. Let $G = (\mathbb{Z}_{16}, +)$ and $\Phi = \{id_G, \alpha_7, \alpha_9, \alpha_{15}\}$. Since $|\Phi| = 4$, there are exactly two orbits of B: $\Phi(\widehat{1}) = \{\widehat{1}, \widehat{7}, \widehat{9}, \widehat{15}\}$ and $\Phi(\widehat{3}) = \{\widehat{3}, \widehat{5}, \widehat{11}, \widehat{13}\}$. Let $\widehat{7}$ and $\widehat{5}$ be the selected representatives of $\Phi(\widehat{1})$ and $\Phi(\widehat{3})$, respectively. Choose $e = \widehat{7}$. In this case, for instance, $\pi(\widehat{4}) = 4\varphi_{e^2}(e^{-2}) = 4\varphi_{\widehat{1}}(\widehat{1}) = \widehat{12}$ while $\pi(\widehat{5\cdot 4}) = 4\varphi_{5e^2}(e^{-2}) = 4\varphi_{\widehat{5}}(\widehat{1}) = \widehat{4}$, hence π is not a function. In fact, $\widehat{7}$ and $\widehat{5}$ are not α-associate.

Theorem 2. *Let G, $\langle \Phi, R_a \rangle$ and π be as in Definition 2. Define $x * y = \pi(x)\,y$, for all $x, y \in G$. The structure $N = (\mathbb{Z}_{p^n}, +, *)$ is a wd-nearring whose radical Q is $p\mathbb{Z}_{p^n}$.*

From Th. II of [3] and Proposition 7, N is a (left) nearring. Now we have to verify that $(\mathbb{Z}_{p^n}, +, *)$ is weakly divisible. Assume $\widehat{x}, \widehat{y} \in N$, with $x = hp^r$ and $y = kp^s$ and suppose $s \leq r$. Take $g = hp^{r-s}(\varphi_{ke^s}(e^{-s}))^{-1}$, it results $\widehat{y} * g = \widehat{x}$. In the same way we can proceed when $r \leq s$. Finally, from Proposition 4, to prove

$Q = p\mathbb{Z}_{p^n}$ can be reduced to show that $\hat{p}$ is nilpotent. Applying the induction principle we can show that $\hat{p}^{(t)} = p^t[\varphi_e(e^{-1})]^{t-1}$. From this it follows $\hat{p}^{(n)} = \hat{0}$, hence $\hat{p}$ is nilpotent. ■

Example 3. Let $G = (\mathbb{Z}_{16}, +)$ and $\langle \Phi, R_\alpha \rangle = (\{id_G, \alpha_7, \alpha_9, \alpha_{15}\}, \{\hat{7}, \widehat{11}\})$. Choose $e = \hat{7}$. Definition 2 provides the following Clay function on G:

$$\pi : \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 0 & 7 & 14 & 9 & 12 & 15 & 2 & 1 & 8 & 15 & 14 & 1 & 4 & 7 & 2 & 9 \end{pmatrix}$$

and this defines a multiplication «$*$» on $\mathbb{Z}_{16}$ by $x * y = \pi(x)\, y$.

Now $N = (\mathbb{Z}_{16}, +, *)$ turns out to be a nearring and, in particular, a wd-nearring with $Q = 2\mathbb{Z}_{16}$. Thus N is a nearring of order 16, non integral, without non trivial left annihilators, and, therefore, non planar and not strongly monogenic.

Theorem 2 summarizes the construction method of wd-nearrings on $(\mathbb{Z}_{p^n}, +)$ with $Q = p\mathbb{Z}_{p^n}$ and the following theorem emphasizes that all such wd-nearrings are constructed in this way.

Theorem 3. *Every wd-nearring* $N = (\mathbb{Z}_{p^n}, +, \circ)$ *with* $Q = p\mathbb{Z}_{p^n}$ *is constructible as in Theorem* 2 *taking*:

(1) $G = (\mathbb{Z}_{p^n}, +)$;
(2) $\Phi = \Gamma(C)$;
(3) *the idempotent elements of* N *as* $\alpha - set$ *of* Φ;
(4) e *equals an idempotent right identity of* $\hat{p}$.

From Proposition 2(1), Proposition 6 and Proposition 1, $\langle \Phi, R_\alpha \rangle$ and e of the hypothesis are suitable to apply Definition 2, that is to define the Clay function π (Proposition 8):

$$\pi(\hat{a}) = \begin{cases} \hat{0} & \text{if } a = 0\,, \\ p^r \varphi_{ke^r}(e^{-r}) & \text{if } a = kp^r \text{ with } k \in \mathbb{Z},\ (k, p) = 1 \text{ and } 0 \le r < n\,. \end{cases}$$

In this case, for all $k \in \mathbb{Z}$, $1 \le r < n$, the automorphism $\varphi_{ke^r} \in \Gamma(C)$ such that $\varphi_{ke^r}(e_{ke^r}) = ke^r$ turns out to be the left translation γ_{ke^r} defined by ke^r, in fact, from the hypothesis, $\gamma_{ke^r}(1_{ke^r}) = ke^r$ and 1_{ke^r} is the fixed representative of $\Gamma(ke^r) = B_{ke^r}$. Therefore, from Proposition 7, the Clay function defining «$\circ$» equals the Clay function π here constructed. Thus, clearly, the multiplication «$\circ$» of N and the one defined by π coincide. ■

References

[1] A. BENINI, *Near-rings on certain groups*, Riv. Mat. Univ. Parma (4) **15** (1989), 149-158.

[2] A. BENINI and S. PELLEGRINI, *Weakly Divisible Nearrings*, Discrete Math. (to appear).

[3] J. R. CLAY, *The near-rings on a finite cyclic group*, Amer. Math. Monthly, **71** (1964), 47-50.

[4] J. R. CLAY, *Nearrings: Geneses and Applications*, Oxford University Press, New York 1992.

[5] J. R. CLAY and J. J. MALONE jr., *The near-rings with identities on certain finite groups*, Math. Scand., **19** (1966), 146-150.

[6] C. COTTI FERRERO and G. FERRERO, *Quasi-anelli con particolari semigruppi di Clay*, Matematiche vol. LI suppl. (1996), 81-89.

[7] G. FERRERO, *Classificazione e costruzione degli stems p-singolari*, Istit. Lombardo Accad. Sci. Lett. Rend. A, **102** (1968), 597-613.

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

[9] G. GALLINA, *Generalizzazioni di quasi-anelli fortemente monogeni*, Riv. Mat. Univ. Parma (4) **12** (1986), 31-34.

[10] S. PELLEGRINI, *Φ-sums: medial, permutable and LRD-near-rings*, Near-rings and Near-fields: Proc. of a Conference held at the Math. Forschungsinstitut, Oberwolfach, 1989, G. Betsch et al. eds., 1995, 152-169.

[11] G. PILZ, *A construction method for near-rings*, Acta Math. Acad. Sci. Hungar. **24** (1973), 97-105.

[12] G. PILZ, *Near-rings* **23** (Revised edition) North Holland Math. Studies, Amsterdam 1983.

Abstract

A nearring N is weakly divisible (wd-nearring) if, for each $x, y \in N$, *there exists an element* $z \in N$ *such that* $xz = y$ *or* $yz = x$. *In this paper we characterise and construct all zerosymmetric wd-nearrings on the group* $(\mathbb{Z}_{p^n}, +)$ *of integers* (mod p^n), *p prime, in which* $p\mathbb{Z}_{p^n}$ *is the set of all the nilpotent elements.*

* * *