Riv. Mat. Univ. Parma (6) **1** (1998), 103-111

A. BENINI and F. MORINI (*)

On the construction of a class of weakly divisible nearrings (**)

1 - Introduction

Weakly divisible nearrings (wd-nearrings) are first defined and studied in [**2**]. Among the zerosymmetric wd-nearrings on the cyclic group $(\mathbb{Z}_{p^n}, +)$, p prime, the class $\mathcal{M}$ of those wd-nearrings in which $p\mathbb{Z}_{p^n}$ is the ideal of all the nilpotent elements is characterized and a construction method is provided in [**1**]. Precisely, if G is a cyclic group of prime power order p^n and Φ is an arbitrary subgroup of $Aut(G)$, all the wd-nearrings of $\mathcal{M}$ are constructible starting from the pair (G, Φ) and from the representatives of orbits of Φ selected in the following way: *if* p^j*,* $j < n$*, is the maximal power of* p *such that any two elements of two orbits belong to the same coset of* $p^j\mathbb{Z}_{p^n}$*, this belonging must also be preserved between the representatives.*

Too many computations are necessary to verify if the above condition holds, even if a computer is used. Therefore, in this paper, using an account of the orbits of an automorphism group of $(\mathbb{Z}_{p^n}, +)$ and calling two orbits *p-equivalent*, when their elements belong to the same cosets of $p\mathbb{Z}_{p^n}$, we prove that the previous condition is automatically guaranteed iff *the selected representatives of p-equivalent orbits belong to the same coset of* $p\mathbb{Z}_{p^n}$ *— if* $p \neq 2$ *or* $p = 2$ *and* Φ *is generated by* $g \to (1 + 2^{n-h})g$ *— otherwise they belong to the same coset of* $4\mathbb{Z}_{2^n}$. Clearly, it is very easy to select the representatives fulfilling this last condition.

(*) Dipartimento di Elettronica per l'Automazione, Facoltà di Ingegneria dell'Università degli Studi di Brescia, Via Branze 38, I-25123 Brescia, Italy.

(**) Received May 5, 1998. AMS classification 16 Y 30. Work carried out on behalf of Italian M.U.R.S.T.

2 - Preliminaries and notations

For details about nearrings we refer to the texts by Pilz [**6**] and Clay [**4**]. Throughout this paper we always consider left zerosymmetric nearrings. We here summarize the results, terminology and notations from [**1**] used in the following. At first we recall:

Definition 1. *A nearring N is weakly divisible (wd-nearring) if, for each x, y belonging to N, there exists an element $z \in N$ such that $xz = y$ or $yz = x$.*

Definition 2. *Let «·» be multiplication* (mod m). *A Clay function is a function π mapping $\mathbb{Z}_m$ in itself and fulfilling the following condition*:

$$\pi(a) \cdot \pi(b) = \pi(a \cdot \pi(b)) \qquad \text{for each } a, b \in \mathbb{Z}_m .$$

Hereinafter «·» will be omitted and, when it will be necessary, $\widehat{a}$ will denote the residue class (mod p^n) containing $a \in \mathbb{Z}$.

In [**3**] it is proved that every nearring whose additive group is finite and cyclic arises from a Clay function. In [**1**] those Clay functions defining wd-nearrings on $(\mathbb{Z}_{p^n}, +)$, whose ideal of all the nilpotent elements coincides with $p\mathbb{Z}_{p^n}$, are investigated. We summarize the construction method of such wd-nearrings here and emphasize that all wd-nearrings of this class are constructed in this way.

To begin with, we need a pair of groups (G, Φ) where G equals $(\mathbb{Z}_{p^n}, +)$ and Φ is an arbitrary subgroup of $Aut(G)$. Hereinafter, K denotes the set $\mathbb{Z}_{p^n} \backslash p\mathbb{Z}_{p^n}$. For all the orbits $\Phi(k)$, $k \in K$, select representatives e_k such that the following condition holds:

Condition 1. *If $e_a - e_b \notin p^j \mathbb{Z}_{p^n}$ ($j < n$), then $x - y \notin p^j \mathbb{Z}_{p^n}$, for all $x \in \Phi(a)$ and for all $y \in \Phi(b)$.*

Fix one of the selected representatives, call it e and denote φ_x the element of Φ such that $\varphi_x(e_x) = x$. Consider the map given by the following:

Definition 3. *For every $\widehat{a} \in \mathbb{Z}_{p^n}$ define*:

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

When the fixed representatives fulfill Condition 1, such a map π is a Clay function, therefore it defines a multiplication « $*$ » on $\mathbb{Z}_{p^n}$ by $x * y = \pi(x)\, y$.

The structure $N = (\mathbb{Z}_{p^n}, +, *)$ is a wd-nearring whose set of the nilpotent elements coincides with $p\mathbb{Z}_{p^n}$ (Th. 2 of [**1**]). Moreover, any such wd-nearring can be constructed by the method described above (Th. 3 of [**1**]).

Now, we are going to describe a method for choosing the representatives of the orbits included in K so that Condition 1 is automatically guaranteed. To our purpose we will use the following:

Definition 4. *Let G be a group. Let $H \leq G$ and $\Phi \leq Aut(G)$. For each orbit $\Phi(g)$, $g \in G$, the set of the cosets of H which contain elements of $\Phi(g)$ is called H-class of $\Phi(g)$, denoted by $[\Phi(g)]_H$.*

Definition 5. *Let G be a group. Let $H \leq G$ and $\Phi \leq Aut(G)$. Two orbits $\Phi(g)$ and $\Phi(g')$, $g, g' \in G$, are called H-equivalent if $[\Phi(g)]_H = [\Phi(g')]_H$.*

To simplify our notations, when H is cyclic we identify H with its generator h and, so, we essentially say h-class (or h-equivalent) and write $[\Phi(g)]_h$.

3 - Case $p \neq 2$

In this section G denotes the additive group of integers (mod p^n) with $p \neq 2$ and Φ a subgroup of $Aut(G)$. It is well known that $|Aut(G)| = (p-1)\,p^{n-1}$ and if the order of Φ is tp^h, with $(p, t) = 1$, then Φ equals the direct product $T \times \Phi_h$, where T is a fixed point free automorphism group of order t and $\Phi_h = \{\alpha_x : g \to xg \mid x = bp^{n-h} + 1,\ 0 \leq b \leq p^h - 1\}$ has order p^h (see [**4**] Chapter 2).

Proposition 1. *Let $G = (\mathbb{Z}_{p^n}, +)$ with $p \neq 2$.*

(1) If β_1 and β_2 are distinct automorphisms of G whose orders divide $p-1$, then $\beta_1(k) - \beta_2(k) \notin p\mathbb{Z}_{p^n}$, for all $k \in K$;

(2) if ϕ_1 and ϕ_2 are automorphisms of G of orders p^r and p^h, $r \leq h$, respectively, then $\phi_1(k) - \phi_2(k) \in p^{n-h}\mathbb{Z}_{p^n}$, for all $k \in K$.

(1) Suppose $\beta_1(k) - \beta_2(k) \in p\mathbb{Z}_{p^n}$, for some $k \in K$. Then $p^{n-1}\beta_1(k) = p^{n-1}\beta_2(k)$, so $(\beta_2^{-1}\beta_1)(p^{n-1}k) = p^{n-1}k$, but this is excluded because otherwise $p^{n-1}k$ should be a fixed point of $\beta_2^{-1}\beta_1$.

(2) It is well known that ϕ_1 and ϕ_2 are determined by elements of the form $bp^{n-h} + 1$, $0 \leq b \leq p^h - 1$. Thus, for all $k \in K$, we have $\phi_1(k) = (b_1 p^{n-h} + 1)\,k$ and $\phi_2(k) = (b_2 p^{n-h} + 1)\,k$ for suitable b_1 and b_2, hence $\phi_1(k) - \phi_2(k)$ belongs to $p^{n-h}\mathbb{Z}_{p^n}$. ■

Corollary 1. *Let* $G = (\mathbb{Z}_{p^n}, +)$, *with* $p \neq 2$, *and* $\Phi = T \times \Phi_h \leqslant Aut(G)$ *of order* tp^h, *where* t *divides* $p-1$.

(1) *For every* $k \in K$, *two elements of* $\Phi(k)$ *belong to the same coset of* $p\mathbb{Z}_{p^n}$ *iff they belong to the same coset of* $p^{n-h}\mathbb{Z}_{p^n}$;

(2) *every orbit* $\Phi(k)$, $k \in K$, *is the union of* t *distinct cosets of* $p^{n-h}\mathbb{Z}_{p^n}$. *Precisely,* $\Phi(k) = \bigcup_{i=1}^{t} (\beta_i \alpha(k) + p^{n-h}\mathbb{Z}_{p^n})$, *where* $T = \{\beta_1, \ldots, \beta_t\}$ *and* $\alpha \in \Phi_h$.

(1) Let $x, y \in \Phi(k)$, that is $x = \beta\alpha(k)$ and $y = \overline{\beta}\overline{\alpha}(k)$, where $\beta, \overline{\beta} \in T$ and $\alpha, \overline{\alpha} \in \Phi_h$. Suppose $x - y \in p\mathbb{Z}_{p^n}$. By Proposition 1(2) $\overline{\alpha}(k) = \alpha(k) + p^{n-h}g$, for some $g \in \mathbb{Z}_{p^n}$, and hence $\beta\alpha(k) - \overline{\beta}(\alpha(k) + p^{n-h}g) = \beta\alpha(k) - \overline{\beta}\alpha(k) - \overline{\beta}(p^{n-h}g)$ belongs to $p\mathbb{Z}_{p^n}$. But, by Proposition 1(1), $\beta\alpha(k) - \overline{\beta}\alpha(k) \in p\mathbb{Z}_{p^n}$ if and only if $\beta = \overline{\beta}$. Now, we can conclude that $x - y = \beta(\alpha(k) - \overline{\alpha}(k)) \in p^{n-h}\mathbb{Z}_{p^n}$.

(2) Suppose $x = \beta_i \overline{\alpha}(k)$ where $\overline{\alpha} \in \Phi_h$ and $\beta_i \in T$. Then, by Proposition 1(2), $\beta_i \alpha(k) - \beta_i \overline{\alpha}(k) = \beta_i(\alpha(k) - \overline{\alpha}(k)) \in p^{n-h}\mathbb{Z}_{p^n}$. It follows that $\Phi(k)$ is included in $\bigcup_{i=1}^{t} (\beta_i \alpha(k) + p^{n-h}\mathbb{Z}_{p^n})$. Since $|\Phi(k)| = |\bigcup_{i=1}^{t} (\beta_i \alpha(k) + p^{n-h}\mathbb{Z}_{p^n})|$ the proof is concluded. ■

Clearly, from Corollary 1 there is always exactly one orbit having a fixed p^{n-h}-class.

Example 1. Take $G = (\mathbb{Z}_{49}, +)$ and $\Phi \leqslant Aut(G)$ generated by the automorphism $\alpha_4 \colon g \to 4g$ of order 21. Using the notations of Corollary 1, Φ equals $T \times \Phi_1$, where $T = \langle \alpha_{18} \rangle = \{id_G, \alpha_{18}, \alpha_{30}\}$ and $\Phi_1 = \langle \alpha_{22} \rangle = \{id_G, \alpha_{22}, \alpha_{43}, \alpha_{15}, \alpha_{36}, \alpha_8, \alpha_{29}\}$. Hence, in this case, $n = 2$, $h = 1$, $t = 3$ and the orbits of K are:

$$\Phi(\widehat{1}) = \{\widehat{1}, \widehat{4}, \widehat{16}, \widehat{15}, \widehat{11}, \widehat{44}, \widehat{29}, \widehat{18}, \widehat{23}, \widehat{43}, \widehat{25}, \widehat{2}, \widehat{8}, \widehat{32}, \widehat{30}, \widehat{22}, \widehat{39}, \widehat{9}, \widehat{36}, \widehat{46}, \widehat{37}\},$$

$$\Phi(\widehat{3}) = \{\widehat{3}, \widehat{12}, \widehat{48}, \widehat{45}, \widehat{33}, \widehat{34}, \widehat{38}, \widehat{5}, \widehat{20}, \widehat{31}, \widehat{26}, \widehat{6}, \widehat{24}, \widehat{47}, \widehat{41}, \widehat{17}, \widehat{19}, \widehat{27}, \widehat{10}, \widehat{40}, \widehat{13}\}.$$

We can observe that in each of these orbits the elements can be gathered in three distinct cosets of $7\mathbb{Z}_{49}$. Precisely, $\Phi(\widehat{1})$ is the union of the following cosets:

$$id_G(\widehat{1}) + 7\mathbb{Z}_{49} = \widehat{1} + 7\mathbb{Z}_{49},$$

$$\alpha_{18}(\widehat{1}) + 7\mathbb{Z}_{49} = \widehat{18} + 7\mathbb{Z}_{49} = \widehat{4} + 7\mathbb{Z}_{49},$$

$$\alpha_{30}(\widehat{1}) + 7\mathbb{Z}_{49} = \widehat{30} + 7\mathbb{Z}_{49} = \widehat{2} + 7\mathbb{Z}_{49}.$$

Similarly, $\Phi(\widehat{3})$ is the union of $(\widehat{3} + 7\mathbb{Z}_{49})$, $(\widehat{5} + 7\mathbb{Z}_{49})$ and $(\widehat{6} + 7\mathbb{Z}_{49})$. Thus $[\Phi(\widehat{1})]_7 \neq [\Phi(\widehat{3})]_7$, that is $\Phi(\widehat{1})$ and $\Phi(\widehat{3})$ are not 7-equivalent.

Proposition 2. *Let* $G = (\mathbb{Z}_{p^n}, +)$, *with* $p \neq 2$, *and* $\Phi = T \times \Phi_h \leq Aut(G)$ *of order* tp^h, *where* t *divides* $p-1$.

(1) *The set* $\{[\Phi(k)]_p \mid k \in K\}$ *of all the* p*-classes under* Φ *determines a partition of* $(\mathbb{Z}_{p^n}/p\mathbb{Z}_{p^n})^*$ *containing* $s = (p-1)/t$ *blocks*;

(2) *in* K *there are* $(p-1)/t = s$ *orbits non* p*-equivalent pairwise*;

(3) *there are exactly* p^{n-h-1} *orbits* p*-equivalent to each orbit of* Φ *included in* K.

(1) We show that distinct blocks are disjoint. Suppose $[\Phi(k)]_p \cap [\Phi(l)]_p \neq \emptyset$. From Corollary 1, there exist $\beta_1, \beta_2 \in T$ such that $\beta_1(k) + p\mathbb{Z}_{p^n} = \beta_2(l) + p\mathbb{Z}_{p^n}$, that is $\beta_1(k) - \beta_2(l) \in p\mathbb{Z}_{p^n}$. Consequently, $\beta(\beta_1(k)) - \beta(\beta_2(l)) \in p\mathbb{Z}_{p^n}$, for any $\beta \in T$, thus $[\Phi(k)]_p = [\Phi(l)]_p$. Again from Corollary 1, $[\Phi(k)]_p$ contains exactly t different elements, hence the partition determined by all the p-classes contains exactly $(p-1)/t = s$ blocks.

(2) From (1), in K there are s distinct orbits having disjoint p-classes to each other.

(3) By Proposition 2(1) two orbits $\Phi(l)$, $\Phi(k)$ are p-equivalent if and only if $\Phi(l) \cap (k + p\mathbb{Z}_{p^n}) \neq \emptyset$. Let $\beta \in T$, $\alpha \in \Phi_h$, $\alpha(l) = bp^{n-h}l + l$. Then $(\beta\alpha)(l) \in k + p\mathbb{Z}_{p^n}$ if and only if $\beta(bp^{n-h}l + l) - k \in p\mathbb{Z}_{p^n}$. By Proposition 1 β is unique, hence there are p^h choices for b which in turn shows that $|\Phi(l) \cap (k + p\mathbb{Z}_{p^n})| = p^h$. Since $|k + p\mathbb{Z}_{p^n}| = p^{n-1}$ it now follows that there are p^{n-h-1} orbits $\Phi(l)$ which are p-equivalent to $\Phi(k)$. ■

Proposition 3. *Let* $G = (\mathbb{Z}_{p^n}, +)$, *with* $p \neq 2$, *and* $\Phi = T \times \Phi_h \leq Aut(G)$ *of order* tp^h, *where* t *divides* $p-1$. *Let* $\Phi(k)$, $\Phi(l)$ *be distinct* p*-equivalent orbits of* Φ *such that* $k - l \in p^j\mathbb{Z}_{p^n}$, $(j < n)$. *Two elements of* $\Phi(k)$ *and* $\Phi(l)$, *respectively, belong to the same coset of* $p\mathbb{Z}_{p^n}$ *iff they belong to the same coset of* $p^j\mathbb{Z}_{p^n}$.

By Corollary 1(2) $k + p^{n-h}\mathbb{Z}_{p^n}$ is included in $\Phi(k)$ and, by the hypothesis, $l \notin \Phi(k)$ and $l \in k + p^j\mathbb{Z}_{p^n}$, thus $j < n - h$.

Let $x \in \Phi(k)$ and $y \in \Phi(l)$. Suppose φ is the automorphism of Φ such that $\varphi(x) = k$. If $x - y \in p\mathbb{Z}_{p^n}$ then $\varphi(x) - \varphi(y) \in p\mathbb{Z}_{p^n}$. Hence $\varphi(y) - l = (k - l) - (\varphi(x) - \varphi(y)) \in p\mathbb{Z}_{p^n}$. Therefore, it follows $\varphi(y) - l \in p^j\mathbb{Z}_{p^n}$ (Corollary 1(1)). Thus $\varphi(y) - \varphi(x) = \varphi(y) - k = (\varphi(y) - l) + (l - k) \in p^j\mathbb{Z}_{p^n}$. ■

The next example shows all the notations and the results presented in this section.

Example 2. Take $G = (\mathbb{Z}_{7^5}, +)$, $T = \{id_G, -id_G\}$ and $\Phi_2 = \langle \alpha_{344} \rangle$. Thus, $\Phi = T \times \Phi_2$ is of order $2 \cdot 7^2$. Here $n = 5$, $h = 2$, $t = 2$, $s = 3$. Therefore, there are $s = 3$ orbits non 7-equivalent, for instance $\Phi(\widehat{1})$, $\Phi(\widehat{2})$ and $\Phi(\widehat{3})$, infact $[\Phi(\widehat{1})]_7 = \{\widehat{1} + 7\mathbb{Z}_{7^5}, \widehat{6} + 7\mathbb{Z}_{7^5}\}$, $[\Phi(\widehat{2})]_7 = \{\widehat{2} + 7\mathbb{Z}_{7^5}, \widehat{5} + 7\mathbb{Z}_{7^5}\}$, $[\Phi(\widehat{3})]_7 = \{\widehat{3} + 7\mathbb{Z}_{7^5}, \widehat{4} + 7\mathbb{Z}_{7^5}\}$. Moreover, there are $p^{n-h-1} = 7^2$ orbits 7-equivalent to $\Phi(\widehat{1})$, $\Phi(\widehat{2})$ and $\Phi(\widehat{3})$ respectively. Using [7] it is possible to verify these results and we can also observe that, for example, $\Phi(\widehat{1})$ and $\Phi(\widehat{50})$ are 7-equivalent and such that $\widehat{1} - \widehat{50} \in 7^2 \mathbb{Z}_{7^5}$, thus, for all $x \in \Phi(\widehat{1})$ and for all $y \in \Phi(\widehat{50})$, $x - y \in 7\mathbb{Z}_{7^5}$ implies $x - y \in 7^2 \mathbb{Z}_{7^5}$ (see Proposition 3).

4 - Case $p = 2$

Let now $G = (\mathbb{Z}_{2^n}, +)$ and $\Phi < Aut(G)$ of order 2^h. The following cases are possible (see [5], Chap. 4) ([1]):

(A) $\Phi = \langle \alpha_{1+2^{n-h}} \rangle = \{\alpha_k : x \to kx \mid k = 1 + b2^{n-h},\ 0 \leq b \leq 2^h - 1\}$ with $0 \leq h \leq n-1$;

(B) $\Phi = \langle \alpha_{-1+2^{n-h}} \rangle = \{\alpha_k : x \to kx \mid k = (-1)^b + b2^{n-h},\ 0 \leq b \leq 2^h - 1\}$ with $0 < h \leq n - 1$;

(C) $\Phi = \langle \alpha_{1+2^{n-h+1}}, -id_G \rangle = \{\alpha_k : x \to kx \mid k = \pm(1 + b2^{n-h+1}),\ 0 \leq b \leq 2^{h-1} - 1\}$ with $0 < h \leq n - 1$.

Case (A). The orbits in K are described by the following:

Proposition 4. *Let $G = (\mathbb{Z}_{2^n}, +)$ and let Φ be a subgroup of $Aut(G)$ having form (A). In K:*

(1) *all the orbits of Φ are 2-equivalent pairwise*;

(2) *every orbit of Φ equals a coset of $2^{n-h}\mathbb{Z}_{2^n}$*;

(3) *if $\Phi(k)$, $\Phi(l)$ are distinct orbits such that k and l belong to the same coset of $2^j\mathbb{Z}_{2^n}$, ($j < n$), then two elements of $\Phi(k)$ and $\Phi(l)$, respectively, belong to that same coset.*

Immediately (1) follows by the definition of 2-equivalent orbits, while the proof

([1]) Here id_G denotes the identity map of G and $-id_G$ is defined by $x \to -x$.

of (2) and (3) is analogous to the case $p \neq 2$, because of the form of the elements of Φ. ■

Cases (B) and (C). The orbits in K are now described by the following:

Proposition 5. *Let $G = (\mathbb{Z}_{2^n}, +)$ and let Φ be a nontrivial subgroup of $Aut(G)$ having form (B) or (C). In K*:

(1) *all the orbits of Φ are 4-equivalent pairwise*;

(2) *let $\Phi(k)$, $\Phi(l)$ be distinct orbits such that $k - l \in 2^j \mathbb{Z}_{2^n} (1 < j < n)$. Two elements of $\Phi(k)$ and $\Phi(l)$, respectively, belong to the same coset of $4\mathbb{Z}_{2^n}$ iff they belong to the same coset of $2^j \mathbb{Z}_{2^n}$.*

(1) It is clear because of the form of elements of Φ.

(2) Let $|\Phi| = 2^h$ and let $x \in \Phi(k)$ and $y \in \Phi(l)$ such that $x - y \in 4\mathbb{Z}_{2^n}$. If $j = 2$, the statement is clear. Furthermore, since the coset $k + 2^{n-h+1}\mathbb{Z}_{2^n}$ contains 2^{h-1} elements and it is included in $\Phi(k)$, it is sufficient to consider $2 < j < n - h + 1$. From the structure of Φ we only have two possibilities.

The first one is $k \pm x, l \pm y \in 2^{n-h}\mathbb{Z}_{2^n} \subseteq 2^j \mathbb{Z}_{2^n}$. By the hypothesis $k - l \in 2^j \mathbb{Z}_{2^n}$, we derive that $k \pm x - (l \pm y) = \pm x \mp y + (k - l) \in 2^j \mathbb{Z}_{2^n}$, and in any case $x - y \in 2^j \mathbb{Z}_{2^n}$.

Otherwise $k \pm x, l \mp y \in 2^{n-h}\mathbb{Z}_{2^n}$. Analogously, we obtain $\pm x \pm y \in 2^j \mathbb{Z}_{2^n}$. Keeping in mind that $x - y \in 4\mathbb{Z}_{2^n}$ we have $x + x \in 4\mathbb{Z}_{2^n}$, but this is false. ■

5 - Conclusion

We are now able to prove a necessary and sufficient condition about the choice of the representatives of the orbits so that π of Definition 3 can be a Clay function.

Theorem 1. *Let $G = (\mathbb{Z}_{p^n}, +)$, p any prime, let Φ be a subgroup of $Aut(G)$ and π as in Definition 3. Condition 1 is fulfilled iff the selected representatives of p-equivalent orbits in K belong*:

$$\begin{cases} \text{to the same coset of } p\mathbb{Z}_{p^n} & \text{if } p \neq 2 \text{ or } p = 2 \text{ and } \Phi = \langle \alpha_{1+2^{n-h}} \rangle, \\ \text{to the same coset of } 4\mathbb{Z}_{2^n} & \text{otherwise}. \end{cases}$$

Suppose that Condition 1 is satisfied, that is π of Definition 3 is a Clay function by Prop. 8 of [**1**].

Assume $p \neq 2$ or $p = 2$ and $\Phi = \langle \alpha_{1+2^{n-h}} \rangle$.

Let e_k and $e_{k'}$ be the selected representatives of two p-equivalent orbits in K and let $k \in \Phi(e_k)$, $k' \in \Phi(e_{k'})$ such that $k - k' \in p\mathbb{Z}_{p^n}$. Clearly, $p^{n-1}(k-k') = 0$, thus the element $a = e^{-(n-1)}kp^{n-1}$ equals $a' = e^{-(n-1)}k'p^{n-1}$. Since π is a function, we have $\pi(a) = \pi(a')$, that is $e^{-(n-1)}p^{n-1}\varphi_k(\widehat{1}) = e^{-(n-1)}p^{n-1}\varphi_{k'}(\widehat{1})$. From the last equality $\varphi_k(\widehat{1}) - \varphi_{k'}(\widehat{1})$ is in $p\mathbb{Z}_{p^n}$, thus $e_k'(\varphi_k(\widehat{1}) - \varphi_{k'}(\widehat{1})) = e_{k'}\varphi_k(\widehat{1}) - k' \in p\mathbb{Z}_{p^n}$. Consequently, $e_{k'}\varphi_k(\widehat{1}) - e_k\varphi_k(\widehat{1}) = e_{k'}\varphi_k(\widehat{1}) - k = (e_{k'}\varphi_k(\widehat{1}) - k') + (k' - k) \in p\mathbb{Z}_{p^n}$. Since $\varphi_k(\widehat{1}) \notin p\mathbb{Z}_{p^n}$, it follows $e_{k'} - e_k \in p\mathbb{Z}_{p^n}$.

Assume $p = 2$ and $\Phi = \langle \alpha_{-1+2^{n-h}} \rangle$ or $\Phi = \langle \alpha_{1+2^{n-h+1}}, -id_G \rangle$.

Since all the orbits have the same 4-class, any two of them contain respectively elements which belong to the same coset of $4\mathbb{Z}_{2^n}$, hence Condition 1 implies that all representatives of the orbits belong to the same coset of $4\mathbb{Z}_{2^n}$.

We can now turn to the converse. Suppose $p \neq 2$ and $\Phi(k)$, $\Phi(k')$ are two distinct orbits in K. If $\Phi(k)$ and $\Phi(k')$ are p-equivalent then $e_k - e_{k'} \in p\mathbb{Z}_{p^n}$. Thus, by Proposition 3, $x - y \in p^j\mathbb{Z}_{p^n}$, for some $x \in \Phi(k)$ and $y \in \Phi(k')$, implies $e_k - e_{k'} \in p^j\mathbb{Z}_{p^n}$ and Condition 1 is fulfilled. If $\Phi(k)$ and $\Phi(k')$ are not p-equivalent, then there are not any $x \in \Phi(k)$, $y \in \Phi(k')$ such that $x - y \in p\mathbb{Z}_{p^n}$ (Proposition 2(1)) and so Condition 1 clearly holds. Finally, if $p = 2$ the converse arises analogously from Propositions 4(3) and 5(2). ■

An application of the above theorem is shown in the following:

Example 3. Take $G = (\mathbb{Z}_{49}, +)$ and $\Phi = \langle \alpha_{18} \rangle = \{id_G, \alpha_{18}, \alpha_{30}\}$. The 7-class of $\Phi(\widehat{1})$, $\Phi(\widehat{2})$, $\Phi(\widehat{4})$, $\Phi(\widehat{8})$, $\Phi(\widehat{9})$, $\Phi(\widehat{16})$ and $\Phi(\widehat{29})$ is $\{\widehat{1} + 7\mathbb{Z}_{49}, \widehat{2} + 7\mathbb{Z}_{49}, \widehat{4} + 7\mathbb{Z}_{49}\}$. The 7-class of $\Phi(\widehat{3})$, $\Phi(\widehat{6})$, $\Phi(\widehat{12})$, $\Phi(\widehat{13})$, $\Phi(\widehat{19})$, $\Phi(\widehat{24})$ and $\Phi(\widehat{26})$ is $\{\widehat{3} + 7\mathbb{Z}_{49}, \widehat{5} + 7\mathbb{Z}_{49}, \widehat{6} + 7\mathbb{Z}_{49}\}$. Thus, in K there are $s = 2$ orbits non 7-equivalent, for instance $\Phi(\widehat{1})$ and $\Phi(\widehat{3})$. There are exactly 7 orbits 7-equivalent to $\Phi(\widehat{1})$ and by Theorem 1 their representatives must be chosen in the same coset of $7\mathbb{Z}_{49}$: choose $\widehat{18}, \widehat{11}, \widehat{4}, \widehat{46}, \widehat{25}, \widehat{39}, \widehat{28}$. There are exactly 7 orbits 7-equivalent to $\Phi(\widehat{3})$ and, for the same reason, their representatives have to be selected in the same coset of $7\mathbb{Z}_{49}$: choose $\widehat{3}, \widehat{10}, \widehat{17}, \widehat{18}, \widehat{37}, \widehat{24}, \widehat{45}$. Fix arbitrarily $e = \widehat{46}$ among the selected representatives and define:

$$\pi(\widehat{a}) = \begin{cases} \widehat{0} & \text{if } a = 0 \\ 7^r \varphi_{ke^r}(e^{-r}) & \text{if } a = k7^r \text{ with } (k, 7) = 1 \text{ and } 0 \leq r < n \end{cases}$$

Because of the choice of the representatives, Theorem 1 and Prop. 8 [**1**] guarantee that π is a Clay function and the structure $(\mathbb{Z}_{49}, +, *)$, where « $*$ » is defined by $x * y = \pi(x)y$, turns out a wd-nearring with $Q = 7\mathbb{Z}_{49}$.

References

[1] A. Benini and F. Morini, *Weakly divisible nearrings on the group of integers* (mod p^n)), Riv. Mat. Univ. Parma (6) 1 (1998), 1-11.

[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] W. J. LeVeque, *Fundamentals of Number Theory*, Addison-Wesley Publishing Company, Philippines 1977.

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

[7] The Sonata Team, *SONATA - Systems Of Nearrings And Their Applications*, Version 1, Institut für Algebra, Stochastik und wissenbasierte mathematische Systeme, University of Linz, Austria 1997.

Abstract

A nearring N is called weakly divisible (wd-nearring) if, for each $x, y \in N$, *there exists an element* $z \in N$ *such that* $xz = y$ *or* $yz = x$. *A method to generate all the zerosymmetric* wd-*nearrings on the cyclic group* $(\mathbb{Z}_{p^n}, +)$ *whose set of the nilpotent elements equals* $p\mathbb{Z}_{p^n}$ *is already known. In this paper we give an account of the orbits of a subgroup of the automorphism group of* $(\mathbb{Z}_{p^n}, +)$ *to provide the guide for improving the construction method of such wd-nearrings.*

* * *