Riv. Mat. Univ. Parma (ser.) **no.** (year), ...-...

Anna Benini and Silvia Pellegrini [1]

Finite weakly divisible nearrings [2]

1 - Introduction

In [5] we defined and studied the algebraic structure called weakly divisible nearring (wd-nearring). In [1, 2] a special class of finite wd-nearrings on $\mathbb{Z}_{p^n}$, p prime, was constructed: on the group $(\mathbb{Z}_{p^n}, +)$ of the residue classes $(mod\ p^n)$ a multiplication "$*$" can be defined in such a way that $(\mathbb{Z}_{p^n}, +, *)$ becomes a wd-nearring. Afterwards, in [3, 4] Partially Balanced Incomplete Block Designs ($PBIBD$s) and codes were obtained starting from the wd-nearrings of [1, 2] and formulae for computing their parameters could be derived just making use of the combinatorial properties of the constructed algebraic structure.
In [9] the construction of [1, 2] was generalized to any wd-nearring. Applying Prop. 1 of [9], in Example 2.1 of this paper a wd-nearring $N = (\mathbb{Z}_7^2, +, *)$ is constructed on the elementary abelian group $(\mathbb{Z}_7^2, +)$ and a $PBIBD$ is obtained from N. Using the algebraic properties of $N = (\mathbb{Z}_7^2, +, *)$, all the parameters of the $PBIBD$ are computed.
Since it seems reasonable to think the construction and the method to compute all the parameters in [3] could be extended to some additional classes of wd-nearrings, the aim of this paper is to study in more depth the algebraic structure of any finite wd-nearring, especially with regard to determining the size of the elements of significant structures in N, as partitions, normal chains and products. In the next paragraph, the main definitions and properties of a finite wd-nearring are recalled (Remark 2.1) and the most significant results presented in this paper are summarized (Remark 2.2).

[1] Via Valotti 9, I-25133 Brescia, Italy, e-mail: firstname.familyname@ing.unibs.it
[2] AMS classification 16Y30. This research was partially supported by italian MIUR.
Keywords: near-rings

2 - Finite weakly divisible nearrings

A *left nearring* is an algebraic structure $(N, +, *)$ such that $(N, +)$ is an additive group, $(N, *)$ is a multiplicative semigroup, and the left distributive low holds (see [6], [10]). An additive normal subgroup I of $(N, +)$ is called *left ideal* if $N * I \subseteq I$, *right ideal* if $(y + i) * x - y * x \in I, \forall x, y \in N, i \in I$. In this paper we always consider left *zerosymmetric* nearrings, that is $0 * x = 0$, for all $x \in N$. In the sequel the subset $\{1, 2, \ldots, m\} \subseteq \mathbb{N}$ could be denoted by I_m and $a|b$ will be sometimes used as a divides b.

D e f i n i t i o n 2.1 *A nearring N is called weakly divisible (wd-nearring) if the following condition is satisfied:*

$$\forall a, b \in N \quad \exists x \in N \quad | \quad a * x = b \quad or \quad b * x = a$$

R e m a r k 2.1 *In [5] it is proved that a finite wd-nearring N is the disjoint union of Q, the set of all the nilpotent elements, and C, the set of all the left cancellable elements, that is $N = C \cup Q$ and $C \cap Q = \emptyset$.*[3] *In the finite case, from Theorem 8 of [5] we know that:*

(a) The set C of the left cancellable elements is the disjoint union of m isomorphic groups. We will call them "the B_{e_i}s", e_i being the identity of B_{e_i} and a left identity of N, for $i \in I_m$. The map $\pi : B_{e_i} \mapsto B_{e_h}$, defined by $\pi(x) = x * e_h$ for $x \in B_{e_i}$, is a (multiplicative) group isomorphism, for $i, h \in I_m$.

(b) The set Q of the nilpotent elements is the prime radical of N, it coincides with the Jacobson radicals and contains every right invariant subset, that is any subset H of N such that $HN \subseteq H$. Obviously, any zero divisor belongs to Q.

R e m a r k 2.2 *In Paragraph 3 we find that, for a finite wd-nearring N, there are integers t and r such that $|N| = t^r$ and $|Q| = t^{r-1}$, so $|C| = (t-1)t^{r-1}$. Moreover, for $j \in I_{r-1}$, we are able to find partitions for the right annihilators of $\boldsymbol{q}^j$, $\boldsymbol{q}$ being any nilpotent such that $\boldsymbol{q} * N = Q$ and $Ann(\boldsymbol{q}^j) = \{y \in N \mid \boldsymbol{q}^j * y = 0\}$. More precisely, we have $Ann(\boldsymbol{q}) = \boldsymbol{q}^{r-1} * C \dot{\cup} \{0\}$ and $Ann(\boldsymbol{q}^j) = \boldsymbol{q}^{r-j} * C \dot{\cup} Ann(\boldsymbol{q}^{j-1})$. So, since Q can be seen as the right annihilator of $\boldsymbol{q}^{r-1}$, it results in $Q = \boldsymbol{q} * C \dot{\cup} \boldsymbol{q}^2 * C \dot{\cup} \ldots \dot{\cup} \boldsymbol{q}^{r-1} * C \dot{\cup} \{0\}$. Also $|Ann(\boldsymbol{q}^j)| = t^j$ and $|\boldsymbol{q}^j * C| = (t-1)t^{r-j-1}$.*

In Paragraph 4 we study the algebraic structure of one of the B_{e_i}s, say B_e. We know that $|B_e| = hk$, where $h|(t-1)$ and $k|t^{r-1}$. We prove that B_e contains two normal chains of subgroups: $F_e(\boldsymbol{q}) \subseteq F_e(\boldsymbol{q}^2) \subseteq \cdots \subseteq F_e(\boldsymbol{q}^{r-1})$ and $U_e(\boldsymbol{q}) \subseteq U_e(\boldsymbol{q}^2) \subseteq \cdots \subseteq U_e(\boldsymbol{q}^{r-1})$, so we investigate the orders of their elements. In particular we obtain $|F_e(\boldsymbol{q}^{r-1})| = h_{r-1}k$, where $h_{r-1}|h$, and $|U_e(\boldsymbol{q}^{r-1})| = k$, thus B_e results in the semidirect product between $U_e(\boldsymbol{q}^{r-1})$ and a suitable complement of order h.

In Paragraph 5, in addition, t is a prime and, consequently, $|B_e| = ht^\alpha$, $|U_e(\boldsymbol{q}^{r-1})| = t^\alpha$ and $|F_e(\boldsymbol{q}^{r-1})| = h_{r-1}t^\alpha$. Hence $U_e(\boldsymbol{q}^{r-1})$ results in the t-Sylow subgroup of both B_e and $F_e(\boldsymbol{q}^{r-1})$ and $\frac{|U_e(\boldsymbol{q}^j)|}{|U_e(\boldsymbol{q}^{j-1})|} \in \{1, t\}$.

[3] In the following, $X \dot{\cup} Y$ will denote the disjoint union of X and Y.

2.1 - *Example*

First step - Construction of a wd-nearring
Here is what we need:

- the elementary abelian group $(\mathbb{Z}_7^2, +)$,
- an automorphism group of $(\mathbb{Z}_7^2, +)$, $\Phi := \{id, \gamma : (x, y) \to (x, -y)\}$,
- a nilpotent endomorphism of $(\mathbb{Z}_7^2, +)$, $\psi : (x, y) \to (y, 0)$.

We begin by choosing the representatives of the Φ-orbits:

Φ-orbits, $x \in \mathbb{Z}_7$	representatives
$\{(x,1),(x,6)\}$	$(x,1)$
$\{(x,2),(x,5)\}$	$(x,2)$
$\{(x,3),(x,4)\}$	$(x,3)$
$\{(x,0)\}$	$(x,0)$

Let E denote the set of the chosen representatives for Φ on $\mathbb{Z}_7^2 \setminus Im\ \psi$. We can verify that all the conditions required in [9] Prop.1 are satisfied, in particular:

$$\text{for all } n \in \mathbb{Z}_7^2 \text{ there are } i = 0, 1,\ \varphi \in \Phi \text{ and } e \in E \text{ such that } n = \psi^i \varphi(e)$$

so that a multiplication " $*$ " on $(\mathbb{Z}_7^2, +)$ can be defined in the following way:

$$n * m = \psi^i \varphi(e) * m = \psi^i \varphi(m)$$

Now $N = (\mathbb{Z}_7^2, +, *)$ results in a wd-nearring with:
the set of the nilpotent elements $Q = Ker\ \psi = Im\ \psi = \{(y, 0) \in \mathbb{Z}_7^2 \mid y \in \mathbb{Z}_7\}$;
the set of the cancellable elements $C = N \setminus Q = \bigcup_{e \in E} \Phi(e)$.
Φ acts fixed point free on C and C is partitioned into Φ-orbits, each of them results in a multiplicative group with the representative as identity.

Second step - Construction of a tactical configuration on N
We will proceed with adapting the method of Hall (see [8]). The raw materials needed are a finite non empty set X, a transitive permutation group G on X with an intransitive subgroup S. Now:

- $X = \mathbb{Z}_7^2$;
- $G = (\mathbb{Z}_7^2, +) \rtimes \Phi$, the natural semidirect sum $((n, \phi_1) +_{\rtimes} (m, \phi_2) = (n + \phi_1(m), \phi_1\phi_2))$;
- $S = \{(0, \phi) \in G \rtimes \Phi, \phi \in \Phi\}$.

We choose an element in E, say $e = (0, 1)$, and we consider the set $N * (0, 1) = \{(0, 1), (0, 6), (1, 0), (6, 0), (0, 0)\}$. It is easy to see that $N * (0, 1)$ is a union of orbits of Φ, being $N * (0, 1) = \Phi((0, 1)) \bigcup \Phi((1, 0)) \bigcup \Phi((6, 0)) \bigcup \Phi((0, 0))$.
A direct computation shows that S results in the stabilizer of $N * (0, 1)$ in G, hence distinct elements of $(\mathbb{Z}_7^2, +)$ determine distinct cosets of S in G. Thereby, when $(x, y) \in \mathbb{Z}_7^2$, the sets $N * (0, 1) + (x, y)$ are the distinct blocks of a tactical configuration whose parameters are $(v, b, r, k) = (49, 49, 5, 5)$.

Third step - Construction of an association scheme on N
We will continue to apply the method of Hall. The raw materials needed are

the stabilizer G_n of any element $n \in N$, the G_n-orbits partitioning N and the sets $U = \Delta \bigcup(-\Delta)$ obtained by forming the union of any orbit Δ and the orbit $-\Delta$. Now:

- $n = (0,0)$ and $G_n = \Phi$;
- $$\begin{array}{lcll} U_1 & = & \{(0,1),(0,6)\} & = \Delta_1 = -\Delta_1 \quad \text{self paired} \\ U_2 & = & \{(0,2),(0,5)\} & = \Delta_2 = -\Delta_2 \quad " \\ U_3 & = & \{(0,3),(0,4)\} & = \Delta_3 = -\Delta_3 \quad " \\ U_4 & = & \{(1,1),(1,6)\}\bigcup\{(6,6),(6,1)\} & = \Delta_4 \bigcup(-\Delta_4) \quad \text{paired} \\ U_5 & = & \{(1,2),(1,5)\}\bigcup\{(6,5),(6,2)\} & = \Delta_5 \bigcup(-\Delta_5) \quad " \\ U_6 & = & \{(1,3),(1,4)\}\bigcup\{(6,4),(6,3)\} & = \Delta_6 \bigcup(-\Delta_6) \quad " \\ U_7 & = & \{(2,1),(2,6)\}\bigcup\{(5,6),(5,1)\} & = \Delta_7 \bigcup(-\Delta_7) \quad " \\ U_8 & = & \{(2,2),(2,5)\}\bigcup\{(5,5),(5,2)\} & = \Delta_8 \bigcup(-\Delta_8) \quad " \\ U_9 & = & \{(2,3),(2,4)\}\bigcup\{(5,4),(5,3)\} & = \Delta_9 \bigcup(-\Delta_9) \quad " \\ U_{10} & = & \{(3,1),(3,6)\}\bigcup\{(4,6),(4,1)\} & = \Delta_{10} \bigcup(-\Delta_{10}) \quad " \\ U_{11} & = & \{(3,2),(3,5)\}\bigcup\{(4,5),(4,2)\} & = \Delta_{11} \bigcup(-\Delta_{11}) \quad " \\ U_{12} & = & \{(3,3),(3,4)\}\bigcup\{(4,4),(4,3)\} & = \Delta_{12} \bigcup(-\Delta_{12}) \quad " \\ U_{13} & = & \{(1,0)\}\bigcup\{(6,0)\} & = \Delta_{13} \bigcup(-\Delta_{13}) \quad " \\ U_{14} & = & \{(2,0)\}\bigcup\{(5,0)\} & = \Delta_{14} \bigcup(-\Delta_{14}) \quad " \\ U_{15} & = & \{(3,0)\}\bigcup\{(4,0)\} & = \Delta_{15} \bigcup(-\Delta_{15}) \quad " \end{array}$$

Two elements will be called ith-associates if their difference belongs to U_i, for $i = 1, \ldots, 15$. Hence, we obtain 15 relations which constitute an Association Scheme whose parameters are

- the numbers n_i of the ith-associates of any element

  $n_1 = n_2 = n_3 = n_{13} = n_{14} = n_{15} = 2, \qquad n_4 = \cdots = n_{12} = 4$
- the numbers p_{ij}^k of the elements which are ith-associates of (a,b) and jth-associates of (c,d) when (a,b) and (c,d) are kth-associates.

These parameters are organized into 15 symmetric squared matrices of order 15, denoted by $P^k = (p_{ij}^k)$ with $k = 1, \ldots, 15$. The values of the p_{ij}^ks were calculated directly, using the algebraic properties of $(\mathbb{Z}_7^2, +, *)$. Below you can find a way to obtain P^k for any $k = 1, \ldots, 15$.

Let O and I denote the zero matrix and the identity matrix of order 3 respectively. Let A^t denote the transpose of A. Moreover, let:

$$\bar{A} = \begin{pmatrix} A & O & O & O & O \\ O & 2A & O & O & 2A_1 \\ O & O & 2A & O & 2A_2 \\ O & O & O & 2A & 2A_3 \\ O & 2A_1^t & 2A_2^t & 2A_3^t & O \end{pmatrix}$$

$$B_1 = \begin{pmatrix} O & A & O & O & A_1 \\ A & O & A & O & A_2 \\ O & A & O & A & A_1 + A_3 \\ O & O & A & A & A_2 + A_3 \\ A_1^t & A_2^t & A_1^t + A_3^t & A_2^t + A_3^t & O \end{pmatrix} \quad C_1 = \begin{pmatrix} O & 2I & O & O & O \\ 2I & O & 2I & O & O \\ O & 2I & O & 2I & O \\ O & O & 2I & 2I & O \\ O & O & O & O & A \end{pmatrix}$$

$$B_2 = \begin{pmatrix} O & O & A & O & A_2 \\ O & A & O & A & A_1 + A_3 \\ A & O & O & A & A_3 \\ O & A & A & O & A_1 + A_2 \\ A_1^t & A_2^t + A_3^t & A_3^t & A_1^t + A_2^t & O \end{pmatrix} \quad C_2 = \begin{pmatrix} O & O & 2I & O & O \\ O & 2I & O & 2I & O \\ 2I & O & O & 2I & O \\ O & 2I & 2I & O & O \\ O & O & O & O & A \end{pmatrix}$$

$$B_3 = \begin{pmatrix} O & O & O & A & A_3 \\ O & O & A & A & A_2+A_3 \\ O & A & A & O & A_1+A_2 \\ A & A & O & O & A_1 \\ A_3^t & A_2^t+A_3^t & A_1^t+A_2^t & A_1^t & O \end{pmatrix} \quad C_3 = \begin{pmatrix} O & O & O & 2I & O \\ O & O & 2I & 2I & O \\ O & 2I & 2I & O & O \\ 2I & 2I & O & O & O \\ O & O & O & O & A \end{pmatrix}$$

Then:
$P^1 = \bar{A}$, $P^4 = B_1$, $P^7 = B_2$, $P^{10} = B_3$, $P^{13} = C_1$ with
$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$, $A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $A_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $A_3 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.
$P^2 = \bar{A}$, $P^5 = B_1$, $P^8 = B_2$, $P^{11} = B_3$, $P^{14} = C_2$ with
$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$, $A_1 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $A_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $A_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.
$P^3 = \bar{A}$, $P^6 = B_1$, $P^9 = B_2$, $P^{12} = B_3$, $P^{15} = C_3$ with
$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, $A_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, $A_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, $A_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Forth step - The partial balance
Finally, from [8] the tactical configuration results in partially balanced with respect to the association scheme, that is any two ith-associate elements belong exactly to λ_i blocks. We can compute easily the parameters of the partial balance: $\lambda_1 = \lambda_4 = \lambda_{13} = 2$, $\lambda_2 = \lambda_{14} = 1$, $\lambda_i = 0$ otherwise. $\diamondsuit$

Notice that our ability to compute the parameters of the $PBIBD$ depends both on the small size and the algebraic properties of the nearring N. The more the size of N increases, the more the knowledge of the algebraic structure becomes essential. This is why we want to know more about the algebraic structure of any finite wd-nearring.

3 - The set Q of the nilpotent elements

Hereinafter N denotes a wd-nearring, Q is the set of its nilpotent elements and C is the set of its cancellable ones. We will always assume $Q \neq \{0\}$.
The smallest positive integer n such that $x^n = 0$ ($H^n = \{0\}$) will be denoted by $\nu(x)$ ($\nu(H)$). From [5] we learn that Q is monogenic, that is there exists $\boldsymbol{q} \in Q$ such that $Q = \boldsymbol{q} * N$. Such an element will be called *generator* of Q. Obviously, if $\nu(\boldsymbol{q}) = n$, for any $\boldsymbol{p} \in Q$ we have $\boldsymbol{p} = \boldsymbol{q}^t * c$, for some $t \in I_n$ and $c \in C$. Following propositions state a lot of useful properties of the generators of Q.

P r o p o s i t i o n 3.1 *Let $\boldsymbol{q}$ be a generator of Q and let $\nu(\boldsymbol{q}) = r$, then $\nu(Q) = r$.*

P r o o f . Consider $\prod_{i=1}^{r} x_i$ where $x_i \in Q$ for all $i \in I_r$. We have $\prod_{i=1}^{r} x_i = \prod_{i=1}^{r} \boldsymbol{q} * n_i$, where $n_i \in N$ for all $i \in I_r$. As $\boldsymbol{q}^r = 0$ and the I.F.P.[4] holds in a

[4] A nearring N has the I.F.P. if for every $a, b, n \in N$, $a * b = 0$ implies $a * n * b = 0$.

finite wd-nearring, we obtain $\prod_{i=1}^{r} x_i = 0$. $\diamondsuit$

P r o p o s i t i o n 3.2 *Let $\boldsymbol{q}$ be a generator of Q and let $\nu(\boldsymbol{q}) = r$, then the following statements are equivalent.*
(a) $\boldsymbol{p}$ is an element of Q and $\nu(\boldsymbol{p}) = r$;
(b) $\boldsymbol{p}$ is of the form $\boldsymbol{q} * c$, where $c \in C$;
(c) $\boldsymbol{p}$ is a generator of Q.

P r o o f . $(a) \Rightarrow (b)$ Let $\boldsymbol{p}$ be an element of Q. Then $\boldsymbol{p} = \boldsymbol{q}^t * c$, for some $t \in I_r$ and $c \in C$. Applying Proposition 3.1 we obtain $\boldsymbol{p}^{r-t+1} = (\boldsymbol{p}^{r-t} * \boldsymbol{q}^t) * c = 0 * c = 0$. Hence it must be $r - t + 1 \geq r$, and this implies $t = 1$.
$(b) \Rightarrow (c)$ Obvious, because $(\boldsymbol{q} * c) * N = \boldsymbol{q} * (c * N) = \boldsymbol{q} * N = Q$, for $c \in C$.
$(c) \Rightarrow (a)$ Let $\boldsymbol{p}$ be a generator of Q and $\nu(\boldsymbol{p}) = s$. Applying Proposition 3.1 we have $\nu(Q) = s$. But we know that $\nu(Q) = r$, so $s = r$. $\diamondsuit$

P r o p o s i t i o n 3.3 *Let $\boldsymbol{p}$ and $\boldsymbol{q}$ be generators of Q and $\nu(\boldsymbol{q}) = \nu(\boldsymbol{p}) = r$, then $\boldsymbol{p}^j * C = \boldsymbol{q}^j * C$, for all $j \in I_r$.*

P r o o f . For every $c \in C$, $\boldsymbol{p}^j * c$ belongs to Q, so $\boldsymbol{p}^j * c = \boldsymbol{q}^t * c'$, for some $t \in I_r$ and $c' \in C$. If $j < t$, $\boldsymbol{p}^{r-t+j} * c = (\boldsymbol{p}^{r-t} * \boldsymbol{q}^t) * c' = 0 * c' = 0$, from previous Proposition 3.1. As a zero divisor of N must belong to Q and $c \notin Q$, it must be $\boldsymbol{p}^{r-(t-j)} = 0$, but this is impossible. Analogously, if $j > t$, $(\boldsymbol{q}^{r-j} * \boldsymbol{p}^j) * c = (\boldsymbol{q}^{r-j} * \boldsymbol{q}^t) * c'$ implies $0 * c = 0 = \boldsymbol{q}^{r-(j-t)} * c'$ and again $\boldsymbol{q}^{r-(j-t)} = 0$ is impossible. So $j = t$.$\diamondsuit$

P r o p o s i t i o n 3.4 *Let $\boldsymbol{q}$ be a generator of Q and $\nu(\boldsymbol{q}) = r$. Then, for $k, j \in I_{r-1}$ with $k \neq j$,*
(a) $C * \boldsymbol{q}^j \subseteq \boldsymbol{q}^j * C$;
(b) $\boldsymbol{q}^j * C \cap \boldsymbol{q}^k * C = \emptyset$;
(c) $Ann(\boldsymbol{q}^j) = \boldsymbol{q}^{r-j} * N = \boldsymbol{q}^{r-j} * C \dot{\cup} \boldsymbol{q}^{r-j+1} * C \dot{\cup} \ldots \dot{\cup} \boldsymbol{q}^{r-1} * C \dot{\cup} \{0\}$[5];
(d) $Q = \boldsymbol{q} * C \dot{\cup} \boldsymbol{q}^2 * C \dot{\cup} \ldots \dot{\cup} \boldsymbol{q}^{r-1} * C \dot{\cup} \{0\}$.

P r o o f . (a) We know that for any $c \in C$ the element $c * \boldsymbol{q}^j$ belongs to Q, so it is of the form $\boldsymbol{q}^k * c'$ for some $k \in I_r$ and $c' \in C$. As in previous Proposition 3.3, from $c * \boldsymbol{q}^j = \boldsymbol{q}^k * c'$ we obtain $j = k$. Hence $C * \boldsymbol{q}^j \subseteq \boldsymbol{q}^j * C$.
(b) If $x \in \boldsymbol{q}^j * C \cap \boldsymbol{q}^k * C$, we have $\boldsymbol{q}^j * c = x = \boldsymbol{q}^k * c'$ for some $c, c' \in C$ and $j = k$ follows as before, but now we have $k \neq j$.
(c) We start showing that $Ann(\boldsymbol{q}^j) = \boldsymbol{q}^{r-j} * N$. Obviously $\boldsymbol{q}^j * (\boldsymbol{q}^{r-j} * N) = 0 * N = \{0\}$, thus $\boldsymbol{q}^{r-j} * N \subseteq Ann(\boldsymbol{q}^j)$. Vice versa, if $x \in Ann(\boldsymbol{q}^j)$ then x must belong to Q, so $x = \boldsymbol{q}^i * c$ for some $i \in I_r$ and $c \in C$. From $\boldsymbol{q}^j * x = \boldsymbol{q}^{j+i} * c = 0$ we have $\boldsymbol{q}^{j+i} = 0$, and this forces $j + i \geq r$. Hence $x = \boldsymbol{q}^{r-j} * \boldsymbol{q}^{i-(r-j)} * c \in \boldsymbol{q}^{r-j} * N$, and this implies $\boldsymbol{q}^{r-j} * N \supseteq Ann(\boldsymbol{q}^j)$. Moreover, $\boldsymbol{q}^{r-j} * N = \boldsymbol{q}^{r-j} * (C \dot{\cup} Q) = \boldsymbol{q}^{r-j} * C \dot{\cup} \boldsymbol{q}^{r-j} * Q = \boldsymbol{q}^{r-j} * C \dot{\cup} \boldsymbol{q}^{r-j+1} * N = \cdots = \boldsymbol{q}^{r-j} * C \dot{\cup} \boldsymbol{q}^{r-j+1} * C \dot{\cup} \ldots \dot{\cup} \boldsymbol{q}^{r-1} * C \dot{\cup} \{0\}$.
(d) Obvious, as $Q = Ann(\boldsymbol{q}^{r-1})$ and we can apply previous point (c). $\diamondsuit$

[5] $Ann(x) = \{y \in N | x * y = 0\}$ is called the right annihilator of x (here it is an ideal of N).

L e m m a 3.1 *Let N be a finite wd-nearring with $|N| = n$ and $|Q| = m$. Let $\boldsymbol{q}$ be any generator of Q and $r = \nu(\boldsymbol{q})$. Then, for $j \in I_{r-1}$,*
(a) $|Ann(\boldsymbol{q}^j)||Ann(\boldsymbol{q}^{r-j})| = n$;
(b) $|\boldsymbol{q}^j * C||Ann(\boldsymbol{q}^j)| = n - m$;
(c) $|Ann(\boldsymbol{q}^j)| = (n/m)^j$.

P r o o f . (*a*) From Proposition 3.4 (*c*), we know that $|Ann(\boldsymbol{q}^j)| = |\boldsymbol{q}^{r-j} * N|$. If $\boldsymbol{q}^{r-j} * n_1 = \boldsymbol{q}^{r-j} * n_2$, then $\boldsymbol{q}^{r-j} * (n_1 - n_2) = 0$ implies $n_1 \in n_2 + Ann(\boldsymbol{q}^{r-j})$ and vice versa. So $|\boldsymbol{q}^{r-j} * N| = |N|/|Ann(\boldsymbol{q}^{r-j})|$, that is $|Ann(\boldsymbol{q}^j)||Ann(\boldsymbol{q}^{r-j})| = n$.
(*b*) Let $c_1, c_2 \in C$. If $\boldsymbol{q}^j * c_1 = \boldsymbol{q}^j * c_2$, then $\boldsymbol{q}^j * (c_1 - c_2) = 0$ implies $c_1 \in c_2 + Ann(\boldsymbol{q}^j)$ and vice versa. Since $c + Ann(\boldsymbol{q}^j) \subseteq C$ for all $c \in C$, we obtain $|\boldsymbol{q}^j * C| = |C|/|Ann(\boldsymbol{q}^j)| = (n - m)/|Ann(\boldsymbol{q}^j)|$.
(*c*) From Proposition 3.4 (*c*), we have $Ann(\boldsymbol{q}^j) = \boldsymbol{q}^{r-j} * C \dot{\cup} Ann(\boldsymbol{q}^{j-1})$, so $|Ann(\boldsymbol{q}^j)| = |\boldsymbol{q}^{r-j} * C| + |Ann(\boldsymbol{q}^{j-1})|$. Applying previous points (*a*) and (*b*), we obtain $|Ann(\boldsymbol{q})| = n/m$, as $Ann(\boldsymbol{q}^{r-1}) = Q$, and $|Ann(\boldsymbol{q}^j)| = (n/m)|Ann(\boldsymbol{q}^{j-1})|$. So $|Ann(\boldsymbol{q}^j)| = (n/m)^j$. ♢

T h e o r e m 3.1 *Let N be a finite wd-nearring with $|N| = n$, $|Q| = m$ and $[N : Q] = n/m = t$. Let $\boldsymbol{q}$ be any generator of Q and $r = \nu(\boldsymbol{q})$, then*
(a) $|N| = t^r$ *and* $|Q| = t^{r-1}$;
(b) $|Ann(\boldsymbol{q}^j)| = t^j$ *and* $|\boldsymbol{q}^j * C| = (t-1)t^{r-j-1}$, *for* $j \in I_{r-1}$.

P r o o f . (*a*) Since $Q = Ann(\boldsymbol{q}^{r-1})$, applying previous Lemma 3.1 (*c*), we obtain $|Q| = |Ann(\boldsymbol{q}^{r-1})| = t^{r-1}$ and $|N| = |Q|[N : Q] = t^r$.
(*b*) From previous Lemma 3.1 (*b*) we know that $|Ann(\boldsymbol{q}^j)| = (n/m)^j = t^j$. Moreover, $|\boldsymbol{q}^j * C| = (n - m)/t^j$ with $n = t^r$ and $m = t^{r-1}$, so $|\boldsymbol{q}^j * C| = (t-1)t^{r-j-1}$, $\forall j \in I_{r-1}$. ♢

Notice that, generally, the set $E = \{e_1, \ldots, e_m\}$ results in the set of the left identities of N and also, from Definition 2.1, every element of N has at least a right identity. Thus, both the set of the left identities of any element of N and the set of the right ones are certainly non empty.

R e m a r k 3.1 In the $\mathbb{Z}_{p^n}$ case (see [1, 2]), if $\boldsymbol{e}$ is an idempotent right identity of any generator of Q, say $\boldsymbol{q}$, *in B_e the sets of the left and right identities of $\boldsymbol{q}$ coincide* and $\boldsymbol{e}$ *is the only left (and right) identity of $\boldsymbol{q}$ in B_e if and only if the order of B_e is a divisor of $t - 1$.* From previous Example 2.1 we can see that it is not always true.

Return to the Example 2.1 *- Now, we have $|Q| = t = 7$ and $t - 1 = 6$. Each non zero element of Q results in a generator of Q itself. So, fixing $\boldsymbol{q} = (1, 0)$ as a generator and without loss of generality, we have*

$$B_{(0,1)} = \Phi((0,1)) = \{(0,1), (0,6)\}$$

$$B_{(0,1)} * (1,0) = \{(1,0)\} \subsetneq \{(1,0), (6,0)\} = (1,0) * B_{(0,1)}$$

Thus, all the elements of $B_{(0,1)}$ are left identities of $(1, 0)$ but the only right identity of $(1, 0)$ in $B_{(0,1)}$ is $(0, 1)$. Moreover, $B_{(0,1)}$ has order 2, but even if 2 is a divisor of $t - 1 = 6$, $(0, 1)$ has more then one left identity.

So, in the following paragraphs 4.1 and 4.2 we are just dealing with the sets of the left or right identities of $\boldsymbol{q}^j$, $j = 1, \ldots, r-1$, where $\boldsymbol{q}$ is a generator of Q and $r = \nu(\boldsymbol{q})$.

4 - The set C of the left cancellable elements

In what follows we will always assume $|N| = t^r$ for some integer $t > 1$. Here we recall again (see Remark 2.1) that C is a multiplicative semigroup, disjoint union of m isomorphic groups, the B_{e_i}s, e_i being the identity of B_{e_i}.

R e m a r k 4.1 *From previous Theorem 3.1 we learn that* $|C| = (t-1)t^{r-1}$, *thus* $|B_{e_i}| = hk$, *where* h *divides* $t-1$ *and* k *divides* t^{r-1}, *for* $i \in I_m$.

4.1 - *Left identities of* $\boldsymbol{q}^j$

D e f i n i t i o n 4.1 *Let* $\boldsymbol{q}$ *be a generator of* Q *and* $\nu(\boldsymbol{q}) = r$. *The set of all the left identities of* $\boldsymbol{q}^j$ *will be denoted by* $F(\boldsymbol{q}^j)$, *that is*

$$F(\boldsymbol{q}^j) = \{x \in N | x * \boldsymbol{q}^j = \boldsymbol{q}^j\}, \quad \text{for } j \in I_{r-1}$$

P r o p o s i t i o n 4.1 *Let* $\boldsymbol{q}$ *be a generator of* Q *and* $\nu(\boldsymbol{q}) = r$. *Then* $F(\boldsymbol{q}) \subseteq F(\boldsymbol{q}^2) \subseteq \cdots \subseteq F(\boldsymbol{q}^{r-1}) \subseteq C$ *is a chain of multiplicative semigroups.*

P r o o f . Obviously, $x, y \in F(\boldsymbol{q}^j)$ implies $x * y \in F(\boldsymbol{q}^j)$. Moreover $F(\boldsymbol{q}^j) \subseteq F(\boldsymbol{q}^{j+1})$, as $x * \boldsymbol{q}^j = \boldsymbol{q}^j$ implies $x * \boldsymbol{q}^{j+1} = \boldsymbol{q}^{j+1}$, $\forall j \in I_{r-1}$. Finally, let $x \in F(\boldsymbol{q}^{r-1})$. If $x \in Q$, then $x = \boldsymbol{q}^s * c$, for some $s \in I_{r-1}$ and $c \in C$. Hence, $\boldsymbol{q}^{r-1} = x * \boldsymbol{q}^{r-1} = \boldsymbol{q}^s * c * \boldsymbol{q}^{r-1} = 0$, because the I.F.P. holds now. But $\boldsymbol{q}^{r-1} = 0$ is clearly impossible, so $x \in C$. ♢

D e f i n i t i o n 4.2 *Let* $\boldsymbol{q}$ *be a generator of* Q *and* $\nu(\boldsymbol{q}) = r$. *The set of all the left identities of* $\boldsymbol{q}^j$ *belonging to* B_{e_i} *will be denoted by* $F_{e_i}(\boldsymbol{q}^j)$, *that is*

$$F_{e_i}(\boldsymbol{q}^j) = F(\boldsymbol{q}^j) \cap B_{e_i} = \{x \in B_{e_i} | x * \boldsymbol{q}^j = \boldsymbol{q}^j\}, \quad \text{for } j \in I_{r-1} \text{ and } i \in I_m$$

R e m a r k 4.2 $F_{e_i}(\boldsymbol{q}^j)$ *is non empty, because* $e_i \in F_{e_i}(\boldsymbol{q}^j)$, $\forall j \in I_{r-1}$, $\forall i \in I_m$.

P r o p o s i t i o n 4.2 *Let* $\boldsymbol{q}$ *be a generator of* Q *and* $\nu(\boldsymbol{q}) = r$. *Then, for* $i, h \in I_m$ *and* $j \in I_{r-1}$,
(*a*) $F_{e_i}(\boldsymbol{q}) \subseteq F_{e_i}(\boldsymbol{q}^2) \subseteq \cdots \subseteq F_{e_i}(\boldsymbol{q}^{r-1}) \subseteq B_{e_i}$ *is a normal chain of multiplicative subgroups of* B_{e_i};
(*b*) $F_{e_i}(\boldsymbol{q}^j)$ *and* $F_{e_h}(\boldsymbol{q}^j)$ *are isomorphic groups.*

P r o o f . (*a*) Previous Proposition 4.1 implies that $F_{e_i}(\boldsymbol{q}) \subseteq \cdots \subseteq F_{e_i}(\boldsymbol{q}^{r-1})$ is a chain of multiplicative subsemigroups of B_{e_i}, $\forall i \in I_m$. Now, let $x \in F_{e_i}(\boldsymbol{q}^j)$ and x^{-1} be the inverse of x in B_{e_i}. From $\boldsymbol{q}^j = x * \boldsymbol{q}^j$ we have $x^{-1} * \boldsymbol{q}^j = x^{-1} * x * \boldsymbol{q}^j = e_i * \boldsymbol{q}^j = \boldsymbol{q}^j$, so $x^{-1} \in F_{e_i}(\boldsymbol{q}^j)$. Hence $F_{e_i}(\boldsymbol{q}^j)$ results in a subgroup of B_{e_i} with e_i as identity. Moreover, from Proposition 3.4(*a*) we learn that for all $c \in C$ there exists $c' \in C$ such that $c * \boldsymbol{q}^j = \boldsymbol{q}^j * c'$. Thus $\forall x \in B_{e_i}, \forall y \in F_{e_i}(\boldsymbol{q}^j)$ we have $x^{-1} * y * x * \boldsymbol{q}^j = x^{-1} * y * \boldsymbol{q}^j * x' = x^{-1} * \boldsymbol{q}^j * x' = x^{-1} * x * \boldsymbol{q}^j = e_i * \boldsymbol{q}^j = \boldsymbol{q}^j$.

Hence $F_{e_i}(\boldsymbol{q}^j)$ is a normal subgroup of B_{e_i}.
(b) It can be easily verified that $\pi(F_{e_i}(\boldsymbol{q}^j)) = F_{e_h}(\boldsymbol{q}^j)$, where π is the isomorphism defined as in Remark 2.1 (a). ♢

P r o p o s i t i o n 4.3 *Let $\boldsymbol{q}$ be a generator of Q, $\nu(\boldsymbol{q}) = r$, $|B_{e_i}| = hk$ and $|F_{e_i}(\boldsymbol{q}^j)| = h_j k_j$, where $h_1 \mid \ldots \mid h_{r-1} \mid h \mid (t-1)$ and $k_1 \mid \ldots \mid k_{r-1} \mid k \mid t^{r-1}$. Then $\frac{k}{k_j}$ divides $t^{r-(j+1)}$ for $j \in I_{r-1}$ and, in particular, $k_{r-1} = k$.*

P r o o f . Firstly, we observe that $C * \boldsymbol{q}^j = C * e_i * \boldsymbol{q}^j = B_{e_i} * \boldsymbol{q}^j$ and, from Proposition 3.4 (a), $B_{e_i} * \boldsymbol{q}^j \subseteq \boldsymbol{q}^j * C$, for $i \in I_m$. Secondly, for any fixed $c \in C$, we can show that the right translation $\delta_c : B_{e_i} * \boldsymbol{q}^j \to B_{e_i} * \boldsymbol{q}^j * c$ is a bijection for all $j \in I_{r-1}$. In fact, let $b_1 * \boldsymbol{q}^j * c = b_2 * \boldsymbol{q}^j * c$, for $b_1, b_2 \in B_{e_i}$. Obviously $c \in B_{e_s}$ for some $s \in I_m$. Let c^{-1} be the inverse of c in B_{e_s}. Then $b_1 * \boldsymbol{q}^j * c * c^{-1} = b_2 * \boldsymbol{q}^j * c * c^{-1}$ implies $b_1 * \boldsymbol{q}^j * e_s = b_2 * \boldsymbol{q}^j * e_s$. Multiplying on the right by an idempotent right identity of $\boldsymbol{q}^j$ and keeping in mind that e_s is a left identity of N, we obtain $b_1 * \boldsymbol{q}^j = b_2 * \boldsymbol{q}^j$, hence δ_c results in injective and hence bijective. Moreover, for any fixed $c \in C$, either $B_{e_i} * \boldsymbol{q}^j \cap B_{e_i} * \boldsymbol{q}^j * c = \emptyset$ or $B_{e_i} * \boldsymbol{q}^j = B_{e_i} * \boldsymbol{q}^j * c$. In fact, if y belongs to $B_{e_i} * \boldsymbol{q}^j \cap B_{e_i} * \boldsymbol{q}^j * c$ we have $y = b_1 * \boldsymbol{q}^j = b_2 * \boldsymbol{q}^j * c$, for some $b_1, b_2 \in B_{e_i}$. Hence $\boldsymbol{q}^j = b_1^{-1} * b_2 * \boldsymbol{q}^j * c$ implies $b * \boldsymbol{q}^j = b * b_1^{-1} * b_2 * \boldsymbol{q}^j * c \in B_{e_i} * \boldsymbol{q}^j * c$, for any $b \in B_{e_i}$. So $B_{e_i} * \boldsymbol{q}^j \subseteq B_{e_i} * \boldsymbol{q}^j * c$ implies $B_{e_i} * \boldsymbol{q}^j = B_{e_i} * \boldsymbol{q}^j * c$. We can deduce that the elements of $\boldsymbol{q}^j * C$ are equally shared in each $B_{e_i} * \boldsymbol{q}^j$, $\forall i \in I_m$, so $|B_{e_i} * \boldsymbol{q}^j| = [B_{e_i} : F_{e_i}(\boldsymbol{q}^j)] = \frac{h}{h_j}\frac{k}{k_j}$ must divide $|\boldsymbol{q}^j * C| = (t-1)t^{r-(j+1)}$ (see Proposition 3.1). In particular, $\frac{k}{k_{r-1}}$ divides 1, so $k_{r-1} = k$. ♢

R e m a r k 4.3 *Since $F(\boldsymbol{q}^j) = \dot{\bigcup}_{i=1}^{m} F_{e_i}(\boldsymbol{q}^j)$, we have that $F(\boldsymbol{q}) \subseteq \cdots \subseteq F(\boldsymbol{q}^{r-1}) \subseteq C$ is a chain of multiplicative subsemigroups of N, each of them results in a disjoint union of m isomorphic groups.*

4.2 - *Right identities of $\boldsymbol{q}^j$*

From Definition 2.1 we know that every element of N has at least a right identity, so the set of all the right identities of any element x of N is certainly non empty. Now we are dealing with the set of all the right identities of $\boldsymbol{q}^j$, $j = 1, \ldots, r-1$, where $\boldsymbol{q}$ is a generator of Q and $\nu(\boldsymbol{q}) = r$.

D e f i n i t i o n 4.3 *Let $\boldsymbol{q}$ be a generator of Q and $\nu(\boldsymbol{q}) = r$. The set of all the right identities of $\boldsymbol{q}^j$ will be denoted by $U(\boldsymbol{q}^j)$, that is*

$$U(\boldsymbol{q}^j) = \{x \in N | \boldsymbol{q}^j * x = \boldsymbol{q}^j\}, \text{ for } j \in I_{r-1}$$

P r o p o s i t i o n 4.4 *Let $\boldsymbol{q}$ be a generator of Q and $\nu(\boldsymbol{q}) = r$. Then, for $j \in I_{r-1}$,*
(a) *$U(\boldsymbol{q}) \subseteq U(\boldsymbol{q}^2) \subseteq \cdots \subseteq U(\boldsymbol{q}^{r-1}) \subseteq C$ is a chain of subsemigroups of C;*
(b) *$U(\boldsymbol{q}^j) = \mathbf{u} + Ann(\boldsymbol{q}^j)$, $\mathbf{u}$ being any right identity of $\boldsymbol{q}^j$;*
(c) *$|U(\boldsymbol{q}^j)| = t^j$.*

P r o o f . (a) Obvious, as in Proposition 4.1.
(b) Let $\mathbf{u}$ be any right identity of $\boldsymbol{q}^j$. Let $x \in U(\boldsymbol{q}^j)$. Then $\boldsymbol{q}^j * x = \boldsymbol{q}^j = \boldsymbol{q}^j * \mathbf{u}$, thus $\boldsymbol{q}^j * (x - \mathbf{u}) = 0$ implies $x - \mathbf{u} \in Ann(\boldsymbol{q}^j)$. Conversely, let y be any element of $Ann(\boldsymbol{q}^j)$, then $\boldsymbol{q}^j * (\mathbf{u} + y) = \boldsymbol{q}^j * \mathbf{u} + \boldsymbol{q}^j * y = \boldsymbol{q}^j$.
(c) From previous point (b) and Theorem 3.1, $|U(\boldsymbol{q}^j)| = |Ann(\boldsymbol{q}^j)| = t^j$. $\diamondsuit$

D e f i n i t i o n 4.4 *Let $\boldsymbol{q}$ be a generator of Q and $\nu(\boldsymbol{q}) = r$. The set of all the right identities of $\boldsymbol{q}^j$ belonging to B_{e_i} will be denoted by $U_{e_i}(\boldsymbol{q}^j)$, that is*
$U_{e_i}(\boldsymbol{q}^j) = U(\boldsymbol{q}^j) \cap B_{e_i} = \{x \in B_{e_i} | \boldsymbol{q}^j * x = \boldsymbol{q}^j\}$, *for $j \in I_{r-1}$ and $i \in I_m$.*

R e m a r k 4.4 *For all $j \in I_{r-1}$, $U_{e_i}(\boldsymbol{q}^j)$ is non empty if and only if $\boldsymbol{q}^j * e_i = \boldsymbol{q}^j$, that is if and only if $e_i \in U_{e_i}(\boldsymbol{q}^j)$.*

R e m a r k 4.5 *If $\boldsymbol{q}^j * e_i \neq \boldsymbol{q}^j$ then $e_i \in U_{e_i}(\boldsymbol{p}^j)$, where $\boldsymbol{p} = \boldsymbol{q} * e_i$ results in a generator of Q.*

P r o p o s i t i o n 4.5 *Let $\boldsymbol{q}$ be a generator of Q and $\nu(\boldsymbol{q}) = r$. Then, for $i, h \in I_m$ and $j \in I_{r-2}$,*
(a) if $\boldsymbol{q}^j * e_i = \boldsymbol{q}^j$, then $U_{e_i}(\boldsymbol{q}^j) \subseteq U_{e_i}(\boldsymbol{q}^{j+1}) \subseteq \cdots \subseteq U_{e_i}(\boldsymbol{q}^{r-1})$ is a normal chain of multiplicative subgroups of B_{e_i};
(b) $U_{e_i}((\boldsymbol{q} * e_i)^j)$ and $U_{e_h}((\boldsymbol{q} * e_h)^j)$ are isomorphic groups;
(c) if $\boldsymbol{q}^j * B_{e_i} \cap \boldsymbol{q}^j * B_{e_h}$ is non empty, then $\boldsymbol{q}^j * B_{e_i} = \boldsymbol{q}^j * B_{e_h}$.

P r o o f . (a) If $\boldsymbol{q}^j * e_i = \boldsymbol{q}^j$, from previous Proposition 4.4(a) we know that $U_{e_i}(\boldsymbol{q}^j)$ is a non empty subsemigroup of $U_{e_i}(\boldsymbol{q}^{j+1})$ with e_i as identity (see Remark 4.4), $\forall j \in I_{r-2}$. Let now $x \in U_{e_i}(\boldsymbol{q}^j)$. The inverse of x in B_{e_i} belongs to $U_{e_i}(\boldsymbol{q}^j)$ because it is an integer power of x (see [5], Th.8), so $U_{e_i}(\boldsymbol{q}^j)$ results in a subgroup of B_{e_i}. In order to show that $U_{e_i}(\boldsymbol{q}^j)$ is normal in B_{e_i}, firstly we prove that an element x of B_{e_i} belongs to $U_{e_i}(\boldsymbol{q}^j)$ if and only if $x * (c + Ann(\boldsymbol{q}^j)) = c + Ann(\boldsymbol{q}^j)$, for all $c \in C$. In fact $x \in U_{e_i}(\boldsymbol{q}^j)$ implies $\boldsymbol{q}^j * x = \boldsymbol{q}^j$. Thus $\boldsymbol{q}^j * x * c = \boldsymbol{q}^j * c$ and this implies $x * c \in c + Ann(\boldsymbol{q}^j)$, $\forall c \in C$. Hence, keeping in mind that $x * Ann(\boldsymbol{q}^j) = Ann(\boldsymbol{q}^j)$ for all $x \in C$ and $j \in I_{r-1}$, $x * (c + Ann(\boldsymbol{q}^j)) = x * c + Ann(\boldsymbol{q}^j) = c + Ann(\boldsymbol{q}^j)$, for all $c \in C$. Conversely, if $x \in B_{e_i}$ and $x * (c + Ann(\boldsymbol{q}^j)) = c + Ann(\boldsymbol{q}^j)$ for all $c \in C$, choosing $c = e_i$ we have $x * (e_i + Ann(\boldsymbol{q}^j)) = e_i + Ann(\boldsymbol{q}^j)$. Hence $\boldsymbol{q}^j * x * (e_i + Ann(\boldsymbol{q}^j)) = \boldsymbol{q}^j * (e_i + Ann(\boldsymbol{q}^j))$ and this implies $\boldsymbol{q}^j * x = \boldsymbol{q}^j$, that is $x \in U_{e_i}(\boldsymbol{q}^j)$.
Applying previous characterization, $\forall y \in B_{e_i}$, $\forall x \in U_{e_i}(\boldsymbol{q}^j)$ and $\forall c \in C$ we have $y^{-1} * x * y * (c + Ann(\boldsymbol{q}^j)) = y^{-1} * x * (y * c + y * Ann(\boldsymbol{q}^j)) = y^{-1} * x * (y * c + Ann(\boldsymbol{q}^j)) = y^{-1} * (y * c + Ann(\boldsymbol{q}^j)) = y^{-1} * y * c + y^{-1} * Ann(\boldsymbol{q}^j) = c + Ann(\boldsymbol{q}^j)$. Thus $y^{-1} * x * y$ belongs to $U_{e_i}(\boldsymbol{q}^j)$ and this implies $U_{e_i}(\boldsymbol{q}^j)$ is normal.
(b) It can be easily verified that $\pi(U_{e_{i_1}}((\boldsymbol{q} * e_{i_1})^j)) = U_{e_{i_2}}((\boldsymbol{q} * e_{i_2})^j)$, where π is the isomorphism defined as in Remark 2.1 (a).
(c) $\boldsymbol{q}^j * B_{e_i} \cap \boldsymbol{q}^j * B_{e_h} \neq \emptyset$ implies $\boldsymbol{q}^j * x = \boldsymbol{q}^j * y$ for some $x \in B_{e_i}$ and $y \in B_{e_h}$. Multiplying by e_i on the right we obtain $\boldsymbol{q}^j * x = \boldsymbol{q}^j * y * e_i$, so $\boldsymbol{q}^j * y * (e_i - e_h) = 0$. Let y^{-1} be the inverse of y in B_{e_h}. Applying the I.F.P. we obtain $\boldsymbol{q}^j * y * y^{-1} * n * (e_i - e_h) = 0$, so $\boldsymbol{q}^j * n * e_i = \boldsymbol{q}^j * n * e_h$ for all $n \in N$. Hence $\boldsymbol{q}^j * B_{e_i} = \boldsymbol{q}^j * B_{e_i} * e_h = \boldsymbol{q}^j * B_{e_h}$. $\diamondsuit$

R e m a r k 4.6 *From what precedes we can say that $U(\boldsymbol{q}^j)$ is a semigroup containing exactly m_j idempotent right identities of $\boldsymbol{q}^j$, say $e_{i_1}, e_{i_2}, \ldots, e_{i_{m_j}}$. Then $U(\boldsymbol{q}^j)$ results in the disjoint union of m_j isomorphic groups, the $U_{e_{i_\lambda}}(\boldsymbol{q}^j)$s, for $\lambda \in I_{m_j}$, that is $U(\boldsymbol{q}^j) = \dot{\bigcup}_{\lambda=1}^{m_j} U_{e_{i_\lambda}}(\boldsymbol{q}^j)$ and $m_j = \frac{|U(\boldsymbol{q}^j)|}{|U_{e_{i_\lambda}}(\boldsymbol{q}^j)|}$, for $j \in I_{r-1}$.*

Now we are able to state a theorem about the algebraic structure of the B_{e_i}s. Since the B_{e_i}s are isomorphic groups, we will confine our attention to one of them, say B_e, $\mathbf{e}$ being its identity. Since each non zero idempotent is a right identity of some generator of Q, let $\boldsymbol{q}$ be a generator of Q such that $\boldsymbol{q} * \mathbf{e} = \boldsymbol{q}$.

Actually, the following Theorem 4.1 could be inferred from Prop. 4 of [9], changing the contest appropriately. Anyway, here we give a short direct proof.

T h e o r e m 4.1 *Let $\boldsymbol{q}$ be a generator of Q and $\nu(\boldsymbol{q}) = r$. Let $\mathbf{e}$ be an idempotent right identity of $\boldsymbol{q}$ and $|B_e| = hk$, where $h \mid (t-1)$ and $k \mid t^{r-1}$. Then*
(a) $U_e(\boldsymbol{q}^{r-1})$ is a normal subgroup of B_e of order k;
(b) B_e results in the semidirect product of $U_e(\boldsymbol{q}^{r-1})$ and a complement U' of order h.

P r o o f . (*a*) From Proposition 4.5 (*a*) we know that $U_e(\boldsymbol{q}^{r-1})$ is a normal subgroup of B_e. Moreover, since the elements of $U(\boldsymbol{q}^{r-1})$ are shared into disjoint subgroups isomorphic to $U_e(\boldsymbol{q}^{r-1})$ (see Proposition 4.5 (*b*)), the order of $U_e(\boldsymbol{q}^{r-1})$ divides $|U(\boldsymbol{q}^{r-1})| = t^{r-1}$ (see Proposition 4.4(*c*)). In addition, the index of $U_e(\boldsymbol{q}^{r-1})$ in B_e equals the cardinality of $\boldsymbol{q}^{r-1} * B_e$ and $|\boldsymbol{q}^{r-1} * B_e|$ must divide $|\boldsymbol{q}^{r-1} * C| = t - 1$ (see Proposition 4.5 (*c*) and Theorem 3.1). Thus, $[B_e : U_e(\boldsymbol{q}^{r-1})]$ divides $t-1$ and $|U_e(\boldsymbol{q}^{r-1})| = k$.
(*b*) $U_e(\boldsymbol{q}^{r-1})$ is a normal subgroup of B_e whose order and index are coprime, so B_e results in the semidirect product between $U_e(\boldsymbol{q}^{r-1})$ and its Schur-Zassenhaus complement (see [7]). ♢

C o r o l l a r y 4.1 *Let $\boldsymbol{q}$ be a generator of Q, $\nu(\boldsymbol{q}) = r$ and $|B_e| = hk$ where h divides $t-1$ and k divides t^{r-1}. The following statements are equivalent.*
(a) $|F_e(\boldsymbol{q}^{r-1})| = 1$;
(b) $|B_e| = h$ and $|F_e(\boldsymbol{q}^j)| = |U_e(\boldsymbol{q}^j)| = 1$, $\forall j \in I_{r-1}$;
(c) $|B_e| = h$ and $B_e * \boldsymbol{q}^j = \boldsymbol{q}^j * B_e$, $\forall j \in I_{r-1}$.

P r o o f . (*a*) $\Rightarrow$ (*b*) Obviously $|F_e(\boldsymbol{q}^{r-1})| = 1$ implies $|F_e(\boldsymbol{q}^j)| = 1$, $\forall j \in I_{r-1}$. Moreover, from Proposition 4.3 we know that $|F_e(\boldsymbol{q}^{r-1})| = h_{r-1}k$, where h_{r-1} divides $t-1$, so $k = h_{r-1} = 1$. Hence $|U_e(\boldsymbol{q}^{r-1})| = 1$ implies both $|B_e| = h$ and $|U_e(\boldsymbol{q}^j)| = 1$, $\forall j \in I_{r-1}$.
(*b*) $\Rightarrow$ (*c*) $|F_e(\boldsymbol{q}^j)| = |U_e(\boldsymbol{q}^j)| = 1$, $\forall j \in I_{r-1}$ implies $|B_e * \boldsymbol{q}^j| = |B_e| = |\boldsymbol{q}^j * B_e|$. Since $B_e * \boldsymbol{q}^j \subseteq \boldsymbol{q}^j * B_e$ (see Proposition 3.4 (*a*)), then $B_e * \boldsymbol{q}^j = \boldsymbol{q}^j * B_e$.
(*c*) $\Rightarrow$ (*a*) $B_e * \boldsymbol{q}^{r-1} = \boldsymbol{q}^{r-1} * B_e$ implies $|F_e(\boldsymbol{q}^{r-1})| = |U_e(\boldsymbol{q}^{r-1})|$. $|B_e| = h$ implies $k = 1$, so $|U_e(\boldsymbol{q}^{r-1})| = 1 = |F_e(\boldsymbol{q}^{r-1})|$. ♢

In the $\mathbb{Z}_{p^n}$ case the equality $B_e * \boldsymbol{q}^j = \boldsymbol{q}^j * B_e$ is always satisfied, so $|B_e| = h$ implies $|F_e(\boldsymbol{q}^j)| = |U_e(\boldsymbol{q}^j)| = 1$, $\forall j \in I_{r-1}$. Generally, it is not true (see the Example in Remark 3.1), anyway we can show the following

P r o p o s i t i o n 4.6 *Let $\boldsymbol{q}$ be a generator of Q and $\nu(\boldsymbol{q}) = r$. If $|B_e| = h$, where h divides $t-1$, then $|U_e(\boldsymbol{q}^j)| = 1$, $|F_e(\boldsymbol{q}^j)| = h_j$ and $h_j|B_e * \boldsymbol{q}^j| = |\boldsymbol{q}^j * B_e| = h$, $\forall j \in I_{r-1}$.*

P r o o f . Since we know that $|B_e| = hk$, where h divides $t-1$ and k divides t^{r-1}, our hypothesis forces $k = 1$, hence $|U_e(\boldsymbol{q}^j)| = 1$ (see Proposition 4.5 and Theorem 4.1) and $|F_e(\boldsymbol{q}^j)| = h_j$, where h_j divides h, $\forall j \in I_{r-1}$ (see Proposition 4.3). So, $|\boldsymbol{q}^j * B_e| = [B_e : U_e(\boldsymbol{q}^j)] = h$ and $|B_e * \boldsymbol{q}^j| = [B_e : F_e(\boldsymbol{q}^j)] = \frac{h}{h_j}$. ♢

5 - Let t be a prime number

If t is a prime number, the orders of N and Q are prime powers, so N and Q are (additive) t-groups. We also know that $|B_e| = hk$, where h divides $t-1$ and k divides t^{r-1}, so $k = t^\alpha$, with $0 \leq \alpha \leq r-1$.

T h e o r e m 5.1 *Let $\boldsymbol{q}$ be a generator of Q and $\nu(\boldsymbol{q}) = r$. Let $\mathbf{e}$ be any idempotent right identity of $\boldsymbol{q}$ and $|B_e| = ht^\alpha$, where t is a prime, h divides $t-1$ and $0 \leq \alpha \leq r-1$. Then $|U_e(\boldsymbol{q}^{r-1})| = t^\alpha$ and $U_e(\boldsymbol{q}^{r-1}) \subseteq F_e(\boldsymbol{q}^{r-1})$.*

P r o o f . From previous Theorem 4.1 we know that $|U_e(\boldsymbol{q}^{r-1})| = t^\alpha$. Moreover, as $|F_e(\boldsymbol{q}^{r-1})| = h_{r-1}t^\alpha$, with t and h_{r-1} relatively prime, we know that $F_e(\boldsymbol{q}^{r-1})$ contains a subgroup of order t^α, say $\bar{F}_e$. Obviously $\bar{F}_e$ is a t-Sylow subgroup of B_e. As $U_e(\boldsymbol{q}^{r-1})$ is normal in B_e, it is the only t-Sylow subgroup of B_e. Hence, $U_e(\boldsymbol{q}^{r-1}) = \bar{F}_e$. ♢

R e m a r k 5.1 *If t is a prime number, from* Propositions 4.4, 4.5 *and previous* Theorem 5.1 *we know that*
(a) $|U_e(\boldsymbol{q}^{r-1})| = t^\alpha$;
(b) $|U_e(\boldsymbol{q})| = 1$ *or* t;
(c) if $|U_e(\boldsymbol{q}^j)| = t^x$ *then* $|U_e(\boldsymbol{q}^{j+1})| = t^x$ *or* t^{x+1}, *for* $j \in I_{r-2}$.

Thus, we can easily deduce the following

P r o p o s i t i o n 5.1 *Let $\boldsymbol{q}$ be a generator of Q and $\nu(\boldsymbol{q}) = r$. Let $\mathbf{e}$ be any idempotent right identity of $\boldsymbol{q}$ and $|B_e| = ht^\alpha$, where t is a prime, h divides $t-1$ and $0 \leq \alpha \leq r-1$. If $|U_e(\boldsymbol{q}^\alpha)| = t^\alpha$ then*
for $j \leq \alpha$ $|U_e(\boldsymbol{q}^j)| = t^j$ *and* $|q^j * B_e| = ht^{\alpha-j}$
for $j \geq \alpha$ $|U_e(\boldsymbol{q}^j)| = t^\alpha$ *and* $|q^j * B_e| = h$
If $|U_e(\boldsymbol{q}^{r-\alpha-1})| = 1$ then
for $j \leq r-\alpha-1$ $|U_e(\boldsymbol{q}^j)| = 1$ *and* $|q^j * B_e| = ht^\alpha$
for $j \geq r-\alpha-1$ $|U_e(\boldsymbol{q}^j)| = t^{j-r+\alpha+1}$ *and* $|q^j * B_e| = ht^{r-j-1}$

♢

References

[1] A. Benini, 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, F. Morini, *On the construction of a class of weakly divisible nearrings*, Riv. Mat. Univ. Parma, (6) **1** (1998) 103-111.

[3] A. Benini, F. Morini, *Partially Balanced Incomplete Block Designs from Weakly Divisible Nearrings*, Discrete Math. **301** (2005) 34-45.

[4] A. Benini, *PBIBDs from weakly divisible nearrings and related codes*, Result. Math. **47** (2005) 6-16.

[5] A. Benini, S. Pellegrini, *Weakly Divisible Nearrings*, Discrete Math. **208/209** (1999) 49-59.

[6] J.R. Clay, *Nearrings: Geneses and Applications*, Oxford Science Publications, Oxford University Press, NY 1992.

[7] D. Gorenstein, *Finite groups*, 2nd. ed., Amer. Math. Soc., Providence, 1980.

[8] M. Hall, *Designs with transitive authomorphism group*, Proc. of Symposia in Pure Math. AMS, T. L. Motzkin, ed., (1971), 109-113.

[9] P. Mayr, F. Morini, *Nearrings whose set of N-subgroups is linearly ordered*, Result. Math. **42** (2002) 339-348.

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

A b s t r a c t

In [5] the algebraic structure called weakly divisible nearring (wd-nearring) was defined and studied. In [1, 2] a special class of wd-nearrings was constructed and its combinatorial properties was investigated. In [3] $PBIBDs$ were derived from a class of wd-nearrings and their parameters were calculated thanks to the knowledge of the algebraic structure. In [9] a generalization of the construction of [1, 2] was given. In order to generalize the construction of [3] to more general cases, this paper is devoted to a more in depth study of the algebraic structure of any finite wd-nearring N, especially with regard to determining the size of the elements of significant structures in N, as partitions, normal chains and products.

***