

ANNA BENINI and SILVIA PELLEGRINI

## Finite weakly divisible nearrings

**Abstract.** 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.

**Keywords.** Near-rings.

**Mathematics Subject Classification (2000):** 16Y30.

### 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 (*PBIBDs*) 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

---

Received: May 28, 2009; accepted in revised form: August 26, 2009.

This research was partially supported by italian MIUR.

Prop. 1 of [9], in Example 2.1 of this paper a wd-nearring  $N = (\mathbb{Z}_{r_7}^2, +, *)$  is constructed on the elementary abelian group  $(\mathbb{Z}_{r_7}^2, +)$  and a *PBIBD* is obtained from  $N$ . Using the algebraic properties of  $N = (\mathbb{Z}_{r_7}^2, +, *)$ , 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).

## 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 law 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  $\{1, 2, \dots, m\} \subseteq \mathbb{N}$  could be denoted by  $I_m$  and  $a|b$  will be sometimes used as  $a$  divides  $b$ .

**Definition 2.1.** *A nearring  $N$  is called weakly divisible (wd-nearring) if the following condition is satisfied:*

$$\forall a, b \in N \quad \exists x \in N \quad | \quad a * x = b \quad \text{or} \quad b * x = a.$$

**Remark 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  $C \cap Q = \emptyset$ .<sup>1</sup> 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  $i, h \in I_m$ .*

---

<sup>1</sup> In the following,  $X \dot{\cup} Y$  will denote the disjoint union of  $X$  and  $Y$ .

(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  $Q$ .

**Remark 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  $\mathbf{q}^j$ ,  $\mathbf{q}$  being any nilpotent such that  $\mathbf{q} * N = Q$  and  $\text{Ann}(\mathbf{q}^j) = \{y \in N \mid \mathbf{q}^j * y = 0\}$ . More precisely, we have  $\text{Ann}(\mathbf{q}) = \mathbf{q}^{r-1} * C \dot{\cup} \{0\}$  and  $\text{Ann}(\mathbf{q}^j) = \mathbf{q}^{r-j} * C \dot{\cup} \text{Ann}(\mathbf{q}^{j-1})$ . So, since  $Q$  can be seen as the right annihilator of  $\mathbf{q}^{r-1}$ , it results in  $Q = \mathbf{q} * C \dot{\cup} \mathbf{q}^2 * C \dot{\cup} \dots \dot{\cup} \mathbf{q}^{r-1} * C \dot{\cup} \{0\}$ . Also  $|\text{Ann}(\mathbf{q}^j)| = t^j$  and  $|\mathbf{q}^j * C| = (t-1)t^{r-j-1}$ .

In Paragraph 4 we study the algebraic structure of one of the  $B_e$ '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:  $F_e(\mathbf{q}) \subseteq F_e(\mathbf{q}^2) \subseteq \dots \subseteq F_e(\mathbf{q}^{r-1})$  and  $U_e(\mathbf{q}) \subseteq U_e(\mathbf{q}^2) \subseteq \dots \subseteq U_e(\mathbf{q}^{r-1})$ , so we investigate the orders of their elements. In particular we obtain  $|F_e(\mathbf{q}^{r-1})| = h_{r-1}k$ , where  $h_{r-1}|h$ , and  $|U_e(\mathbf{q}^{r-1})| = k$ , thus  $B_e$  results in the semidirect product between  $U_e(\mathbf{q}^{r-1})$  and a suitable complement of order  $h$ .

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

**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  $(\mathbb{Z}_7^2, +)$ ,  $\Phi := \{id, \gamma : (x, y) \rightarrow (x, -y)\}$ ,
- a nilpotent endomorphism of  $(\mathbb{Z}_7^2, +)$ ,  $\psi : (x, y) \rightarrow (y, 0)$ .

We begin by choosing the representatives of the  $\Phi$ -orbits:

$\Phi$ -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  $\Phi$  on  $\mathbb{Z}_7^2 \setminus \text{Im } \psi$ . We can verify that all the conditions required in [9] Prop.1 are satisfied, in particular:

for all  $n \in \mathbb{Z}_7^2$  there are  $i = 0, 1$ ,  $\varphi \in \Phi$  and  $e \in E$  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  $Q = \text{Ker } \psi = \text{Im } \psi = \{(y, 0) \in \mathbb{Z}_7^2 \mid y \in \mathbb{Z}_7\}$ ;

the set of the cancellable elements  $C = N \setminus Q = \bigcup_{e \in E} \Phi(e)$ .

$\Phi$  acts fixed point free on  $C$  and  $C$  is partitioned into  $\Phi$ -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

$$((n, \phi_1) +_{\times} (m, \phi_2)) = (n + \phi_1(m), \phi_1 \phi_2);$$

- $S = \{(0, \phi) \in G \rtimes \Phi, \phi \in \Phi\}$ .

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  $\Phi$ , being  $N * (0, 1) = \Phi((0, 1)) \cup \Phi((1, 0)) \cup \Phi((6, 0)) \cup \Phi((0, 0))$ .

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  $U = \Delta \cup (-\Delta)$  obtained by forming the union of any orbit  $\Delta$  and the orbit  $-\Delta$ .

Now:

- $n = (0, 0)$  and  $G_n = \Phi$ ;
- $U_1 = \{(0, 1), (0, 6)\} = \mathcal{A}_1 = -\mathcal{A}_1$  self paired
- $U_2 = \{(0, 2), (0, 5)\} = \mathcal{A}_2 = -\mathcal{A}_2$  ”
- $U_3 = \{(0, 3), (0, 4)\} = \mathcal{A}_3 = -\mathcal{A}_3$  ”
- $U_4 = \{(1, 1), (1, 6)\} \cup \{(6, 6), (6, 1)\} = \mathcal{A}_4 \cup (-\mathcal{A}_4)$  paired
- $U_5 = \{(1, 2), (1, 5)\} \cup \{(6, 5), (6, 2)\} = \mathcal{A}_5 \cup (-\mathcal{A}_5)$  ”
- $U_6 = \{(1, 3), (1, 4)\} \cup \{(6, 4), (6, 3)\} = \mathcal{A}_6 \cup (-\mathcal{A}_6)$  ”
- $U_7 = \{(2, 1), (2, 6)\} \cup \{(5, 6), (5, 1)\} = \mathcal{A}_7 \cup (-\mathcal{A}_7)$  ”
- $U_8 = \{(2, 2), (2, 5)\} \cup \{(5, 5), (5, 2)\} = \mathcal{A}_8 \cup (-\mathcal{A}_8)$  ”
- $U_9 = \{(2, 3), (2, 4)\} \cup \{(5, 4), (5, 3)\} = \mathcal{A}_9 \cup (-\mathcal{A}_9)$  ”
- $U_{10} = \{(3, 1), (3, 6)\} \cup \{(4, 6), (4, 1)\} = \mathcal{A}_{10} \cup (-\mathcal{A}_{10})$  ”
- $U_{11} = \{(3, 2), (3, 5)\} \cup \{(4, 5), (4, 2)\} = \mathcal{A}_{11} \cup (-\mathcal{A}_{11})$  ”
- $U_{12} = \{(3, 3), (3, 4)\} \cup \{(4, 4), (4, 3)\} = \mathcal{A}_{12} \cup (-\mathcal{A}_{12})$  ”
- $U_{13} = \{(1, 0)\} \cup \{(6, 0)\} = \mathcal{A}_{13} \cup (-\mathcal{A}_{13})$  ”
- $U_{14} = \{(2, 0)\} \cup \{(5, 0)\} = \mathcal{A}_{14} \cup (-\mathcal{A}_{14})$  ”
- $U_{15} = \{(3, 0)\} \cup \{(4, 0)\} = \mathcal{A}_{15} \cup (-\mathcal{A}_{15})$  ”

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

- the numbers  $n_i$  of the  $i$ th-associates of any element

$$n_1 = n_2 = n_3 = n_{13} = n_{14} = n_{15} = 2, \quad n_4 = \dots = n_{12} = 4$$

- the numbers  $p_{ij}^k$  of the elements which are  $i$ th-associates of  $(a, b)$  and  $j$ th-associates of  $(c, d)$  when  $(a, b)$  and  $(c, d)$  are  $k$ th-associates.

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

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:

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

$$\begin{aligned}
B_1 &= \begin{pmatrix} O & A & O & O & A_1 \\ A & O & A & O & A_2 \\ O & A & O & A & A_1 + A_3 \\ O & O & A & A & A_2 + A_3 \\ A_1^t & A_2^t & A_1^t + A_3^t & A_2^t + A_3^t & O \end{pmatrix} & C_1 &= \begin{pmatrix} O & 2I & O & O & O \\ 2I & O & 2I & O & O \\ O & 2I & O & 2I & O \\ O & O & 2I & 2I & O \\ O & O & O & O & A \end{pmatrix} \\
B_2 &= \begin{pmatrix} O & O & A & O & A_2 \\ O & A & O & A & A_1 + A_3 \\ A & O & O & A & A_3 \\ O & A & A & O & A_1 + A_2 \\ A_2^t & A_2^t + A_3^t & A_3^t & A_1^t + A_2^t & O \end{pmatrix} & C_2 &= \begin{pmatrix} O & O & 2I & O & O \\ O & 2I & O & 2I & O \\ 2I & O & O & 2I & O \\ O & 2I & 2I & O & O \\ O & O & O & O & A \end{pmatrix} \\
B_3 &= \begin{pmatrix} O & O & O & A & A_3 \\ O & O & A & A & A_2 + A_3 \\ O & A & A & O & A_1 + A_2 \\ A & A & O & O & A_1 \\ A_3^t & A_2^t + A_3^t & A_1^t + A_2^t & A_1^t & O \end{pmatrix} & C_3 &= \begin{pmatrix} O & O & O & 2I & O \\ O & O & 2I & 2I & O \\ O & 2I & 2I & O & O \\ 2I & 2I & O & O & O \\ O & O & O & O & A \end{pmatrix}.
\end{aligned}$$

Then:

$$P^1 = \bar{A}, P^4 = B_1, P^7 = B_2, P^{10} = B_3, P^{13} = C_1 \text{ with}$$

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, A_3 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

$$P^2 = \bar{A}, P^5 = B_1, P^8 = B_2, P^{11} = B_3, P^{14} = C_2 \text{ with}$$

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, A_1 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, A_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

$$P^3 = \bar{A}, P^6 = B_1, P^9 = B_2, P^{12} = B_3, P^{15} = C_3 \text{ with}$$

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, A_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, A_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

### ***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  $i$ th-associate elements belong exactly to  $\lambda_i$  blocks. We can compute easily the parameters of the partial balance:

$$\lambda_1 = \lambda_4 = \lambda_{13} = 2, \lambda_2 = \lambda_{14} = 1, \lambda_i = 0 \text{ otherwise.} \quad \square$$

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  $\mathbf{q} \in Q$  such that  $Q = \mathbf{q} * N$ . Such an element will be called *generator* of  $Q$ . Obviously, if  $\nu(\mathbf{q}) = n$ , for any  $\mathbf{p} \in Q$  we have  $\mathbf{p} = \mathbf{q}^t * c$ , for some  $t \in I_n$  and  $c \in C$ . Following propositions state a lot of useful properties of the generators of  $Q$ .

**Proposition 3.1.** *Let  $\mathbf{q}$  be a generator of  $Q$  and let  $\nu(\mathbf{q}) = r$ , then  $\nu(Q) = r$ .*

**Proof.** Consider  $\prod_{i=1}^r x_i$  where  $x_i \in Q$  for all  $i \in I_r$ . We have  $\prod_{i=1}^r x_i = \prod_{i=1}^r \mathbf{q} * n_i$ , where  $n_i \in N$  for all  $i \in I_r$ . As  $\mathbf{q}^r = 0$  and the I.F.P.<sup>2</sup> holds in a finite wd-nearring, we obtain  $\prod_{i=1}^r x_i = 0$ . □

**Proposition 3.2.** *Let  $\mathbf{q}$  be a generator of  $Q$  and let  $\nu(\mathbf{q}) = r$ , then the following statements are equivalent*

- (a)  $\mathbf{p}$  is an element of  $Q$  and  $\nu(\mathbf{p}) = r$ ;
- (b)  $\mathbf{p}$  is of the form  $\mathbf{q} * c$ , where  $c \in C$ ;
- (c)  $\mathbf{p}$  is a generator of  $Q$ .

**Proof.** (a)  $\Rightarrow$  (b) Let  $\mathbf{p}$  be an element of  $Q$ . Then  $\mathbf{p} = \mathbf{q}^t * c$ , for some  $t \in I_r$  and  $c \in C$ . Applying Proposition 3.1 we obtain  $\mathbf{p}^{r-t+1} = (\mathbf{p}^{r-t} * \mathbf{q}^t) * c = 0 * c = 0$ . Hence it must be  $r - t + 1 \geq r$ , and this implies  $t = 1$ .

(b)  $\Rightarrow$  (c) Obvious, because  $(\mathbf{q} * c) * N = \mathbf{q} * (c * N) = \mathbf{q} * N = Q$ , for  $c \in C$ .

(c)  $\Rightarrow$  (a) Let  $\mathbf{p}$  be a generator of  $Q$  and  $\nu(\mathbf{p}) = s$ . Applying Proposition 3.1 we have  $\nu(Q) = s$ . But we know that  $\nu(Q) = r$ , so  $s = r$ . □

---

<sup>2</sup> A nearring  $N$  has the I.F.P. if for every  $a, b, n \in N$ ,  $a * b = 0$  implies  $a * n * b = 0$ .

**Proposition 3.3.** *Let  $\mathbf{p}$  and  $\mathbf{q}$  be generators of  $Q$  and  $v(\mathbf{q}) = v(\mathbf{p}) = r$ , then  $\mathbf{p}^j * C = \mathbf{q}^j * C$ , for all  $j \in I_r$ .*

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

**Proposition 3.4.** *Let  $\mathbf{q}$  be a generator of  $Q$  and  $v(\mathbf{q}) = r$ . Then, for  $k, j \in I_{r-1}$  with  $k \neq j$ ,*

- (a)  $C * \mathbf{q}^j \subseteq \mathbf{q}^j * C$ ;
- (b)  $\mathbf{q}^j * C \cap \mathbf{q}^k * C = \emptyset$ ;
- (c)  $\text{Ann}(\mathbf{q}^j) = \mathbf{q}^{r-j} * N = \mathbf{q}^{r-j} * C \dot{\cup} \mathbf{q}^{r-j+1} * C \dot{\cup} \dots \dot{\cup} \mathbf{q}^{r-1} * C \dot{\cup} \{0\}$ <sup>3</sup>;
- (d)  $Q = \mathbf{q} * C \dot{\cup} \mathbf{q}^2 * C \dot{\cup} \dots \dot{\cup} \mathbf{q}^{r-1} * C \dot{\cup} \{0\}$ .

*Proof.* (a) We know that for any  $c \in C$  the element  $c * \mathbf{q}^j$  belongs to  $Q$ , so it is of the form  $\mathbf{q}^k * c'$  for some  $k \in I_r$  and  $c' \in C$ . As in previous Proposition 3.3, from  $c * \mathbf{q}^j = \mathbf{q}^k * c'$  we obtain  $j = k$ . Hence  $C * \mathbf{q}^j \subseteq \mathbf{q}^j * C$ .

(b) If  $x \in \mathbf{q}^j * C \cap \mathbf{q}^k * C$ , we have  $\mathbf{q}^j * c = x = \mathbf{q}^k * c'$  for some  $c, c' \in C$  and  $j = k$  follows as before, but now we have  $k \neq j$ .

(c) We start showing that  $\text{Ann}(\mathbf{q}^j) = \mathbf{q}^{r-j} * N$ . Obviously  $\mathbf{q}^j * (\mathbf{q}^{r-j} * N) = 0 * N = \{0\}$ , thus  $\mathbf{q}^{r-j} * N \subseteq \text{Ann}(\mathbf{q}^j)$ . Vice versa, if  $x \in \text{Ann}(\mathbf{q}^j)$  then  $x$  must belong to  $Q$ , so  $x = \mathbf{q}^i * c$  for some  $i \in I_r$  and  $c \in C$ . From  $\mathbf{q}^j * x = \mathbf{q}^{j+i} * c = 0$  we have  $\mathbf{q}^{j+i} = 0$ , and this forces  $j + i \geq r$ . Hence  $x = \mathbf{q}^{r-j} * \mathbf{q}^{i-(r-j)} * c \in \mathbf{q}^{r-j} * N$ , and this implies  $\mathbf{q}^{r-j} * N \supseteq \text{Ann}(\mathbf{q}^j)$ . Moreover,  $\mathbf{q}^{r-j} * N = \mathbf{q}^{r-j} * (C \dot{\cup} Q) = \mathbf{q}^{r-j} * C \dot{\cup} \mathbf{q}^{r-j} * Q = \mathbf{q}^{r-j} * C \dot{\cup} \mathbf{q}^{r-j+1} * N = \dots = \mathbf{q}^{r-j} * C \dot{\cup} \mathbf{q}^{r-j+1} * C \dot{\cup} \dots \dot{\cup} \mathbf{q}^{r-1} * C \dot{\cup} \{0\}$ .

(d) Obvious, as  $Q = \text{Ann}(\mathbf{q}^{r-1})$  and we can apply previous point (c).  $\square$

**Lemma 3.1.** *Let  $N$  be a finite wd-nearring with  $|N| = n$  and  $|Q| = m$ . Let  $\mathbf{q}$  be any generator of  $Q$  and  $r = v(\mathbf{q})$ . Then, for  $j \in I_{r-1}$ ,*

- (a)  $|\text{Ann}(\mathbf{q}^j)| |\text{Ann}(\mathbf{q}^{r-j})| = n$ ;
- (b)  $|\mathbf{q}^j * C| |\text{Ann}(\mathbf{q}^j)| = n - m$ ;
- (c)  $|\text{Ann}(\mathbf{q}^j)| = (n/m)^j$ .

---

<sup>3</sup>  $\text{Ann}(x) = \{y \in N | x * y = 0\}$  is called the right annihilator of  $x$  (here it is an ideal of  $N$ ).



**Proof.** (a) From Proposition 3.4 (c), we know that  $|Ann(\mathbf{q}^j)| = |\mathbf{q}^{r-j} * N|$ . If  $\mathbf{q}^{r-j} * n_1 = \mathbf{q}^{r-j} * n_2$ , then  $\mathbf{q}^{r-j} * (n_1 - n_2) = 0$  implies  $n_1 \in n_2 + Ann(\mathbf{q}^{r-j})$  and vice versa. So  $|\mathbf{q}^{r-j} * N| = |N|/|Ann(\mathbf{q}^{r-j})|$ , that is  $|Ann(\mathbf{q}^j)||Ann(\mathbf{q}^{r-j})| = n$ .

(b) Let  $c_1, c_2 \in C$ . If  $\mathbf{q}^j * c_1 = \mathbf{q}^j * c_2$ , then  $\mathbf{q}^j * (c_1 - c_2) = 0$  implies  $c_1 \in c_2 + Ann(\mathbf{q}^j)$  and vice versa. Since  $c + Ann(\mathbf{q}^j) \subseteq C$  for all  $c \in C$ , we obtain  $|\mathbf{q}^j * C| = |C|/|Ann(\mathbf{q}^j)| = (n - m)/|Ann(\mathbf{q}^j)|$ .

(c) From Proposition 3.4 (c), we have  $Ann(\mathbf{q}^j) = \mathbf{q}^{r-j} * C \dot{\cup} Ann(\mathbf{q}^{j-1})$ , so  $|Ann(\mathbf{q}^j)| = |\mathbf{q}^{r-j} * C| + |Ann(\mathbf{q}^{j-1})|$ . Applying previous points (a) and (b), we obtain  $|Ann(\mathbf{q})| = n/m$ , as  $Ann(\mathbf{q}^{r-1}) = Q$ , and  $|Ann(\mathbf{q}^j)| = (n/m)|Ann(\mathbf{q}^{j-1})|$ . So  $|Ann(\mathbf{q}^j)| = (n/m)^j$ .  $\square$

**Theorem 3.1.** *Let  $N$  be a finite wd-nearring with  $|N| = n$ ,  $|Q| = m$  and  $[N : Q] = n/m = t$ . Let  $\mathbf{q}$  be any generator of  $Q$  and  $r = v(\mathbf{q})$ , then*

(a)  $|N| = t^r$  and  $|Q| = t^{r-1}$ ;

(b)  $|Ann(\mathbf{q}^j)| = t^j$  and  $|\mathbf{q}^j * C| = (t - 1)t^{r-j-1}$ , for  $j \in I_{r-1}$ .

**Proof.** (a) Since  $Q = Ann(\mathbf{q}^{r-1})$ , applying previous Lemma 3.1 (c), we obtain  $|Q| = |Ann(\mathbf{q}^{r-1})| = t^{r-1}$  and  $|N| = |Q|[N : Q] = t^r$ .

(b) From previous Lemma 3.1 (b) we know that  $|Ann(\mathbf{q}^j)| = (n/m)^j = t^j$ . Moreover,  $|\mathbf{q}^j * C| = (n - m)/t^j$  with  $n = t^r$  and  $m = t^{r-1}$ , so  $|\mathbf{q}^j * C| = (t - 1)t^{r-j-1}$ ,  $\forall j \in I_{r-1}$ .  $\square$

Notice that, generally, the set  $E = \{e_1, \dots, e_m\}$  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.

**Remark 3.1.** *In the  $\mathbb{Z}_p$  case (see [1, 2]), if  $e$  is an idempotent right identity of any generator of  $Q$ , say  $\mathbf{q}$ , in  $B_e$  the sets of the left and right identities of  $\mathbf{q}$  coincide and  $e$  is the only left (and right) identity of  $\mathbf{q}$  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  $\mathbf{q} = (1, 0)$  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 than 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  $\mathbf{q}^j$ ,  $j = 1, \dots, r - 1$ , where  $\mathbf{q}$  is a generator of  $Q$  and  $r = v(\mathbf{q})$ .

#### 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  $B_{e_i}$ .

Remark 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 $\mathbf{q}^j$

Definition 4.1. Let  $\mathbf{q}$  be a generator of  $Q$  and  $v(\mathbf{q}) = r$ . The set of all the left identities of  $\mathbf{q}^j$  will be denoted by  $F(\mathbf{q}^j)$ , that is

$$F(\mathbf{q}^j) = \{x \in N \mid x * \mathbf{q}^j = \mathbf{q}^j\}, \text{ for } j \in I_{r-1}.$$

Proposition 4.1. Let  $\mathbf{q}$  be a generator of  $Q$  and  $v(\mathbf{q}) = r$ . Then  $F(\mathbf{q}) \subseteq F(\mathbf{q}^2) \subseteq \dots \subseteq F(\mathbf{q}^{r-1}) \subseteq C$  is a chain of multiplicative semigroups.

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

Definition 4.2. Let  $\mathbf{q}$  be a generator of  $Q$  and  $v(\mathbf{q}) = r$ . The set of all the left identities of  $\mathbf{q}^j$  belonging to  $B_{e_i}$  will be denoted by  $F_{e_i}(\mathbf{q}^j)$ , that is

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

Remark 4.2.  $F_{e_i}(\mathbf{q}^j)$  is non empty, because  $e_i \in F_{e_i}(\mathbf{q}^j)$ ,  $\forall j \in I_{r-1}$ ,  $\forall i \in I_m$ .

Proposition 4.2. Let  $\mathbf{q}$  be a generator of  $Q$  and  $v(\mathbf{q}) = r$ . Then, for  $i, h \in I_m$  and  $j \in I_{r-1}$ ,

(a)  $F_{e_i}(\mathbf{q}) \subseteq F_{e_i}(\mathbf{q}^2) \subseteq \dots \subseteq F_{e_i}(\mathbf{q}^{r-1}) \subseteq B_{e_i}$  is a normal chain of multiplicative subgroups of  $B_{e_i}$ ;

(b)  $F_{e_i}(\mathbf{q}^j)$  and  $F_{e_h}(\mathbf{q}^j)$  are isomorphic groups.

*Proof.* (a) Previous Proposition 4.1 implies that  $F_{e_i}(\mathbf{q}) \subseteq \dots \subseteq F_{e_i}(\mathbf{q}^{r-1})$  is a chain of multiplicative subsemigroups of  $B_{e_i}$ ,  $\forall i \in I_m$ . Now, let  $x \in F_{e_i}(\mathbf{q}^j)$  and  $x^{-1}$  be the inverse of  $x$  in  $B_{e_i}$ . From  $\mathbf{q}^j = x * \mathbf{q}^j$  we have  $x^{-1} * \mathbf{q}^j = x^{-1} * x * \mathbf{q}^j = e_i * \mathbf{q}^j = \mathbf{q}^j$ , so  $x^{-1} \in F_{e_i}(\mathbf{q}^j)$ . Hence  $F_{e_i}(\mathbf{q}^j)$  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  $c * \mathbf{q}^j = \mathbf{q}^j * c'$ . Thus  $\forall x \in B_{e_i}, \forall y \in F_{e_i}(\mathbf{q}^j)$  we have  $x^{-1} * y * x * \mathbf{q}^j = x^{-1} * y * \mathbf{q}^j * x' = x^{-1} * \mathbf{q}^j * x' = x^{-1} * x * \mathbf{q}^j = e_i * \mathbf{q}^j = \mathbf{q}^j$ . Hence  $F_{e_i}(\mathbf{q}^j)$  is a normal subgroup of  $B_{e_i}$ .

(b) It can be easily verified that  $\pi(F_{e_i}(\mathbf{q}^j)) = F_{e_h}(\mathbf{q}^j)$ , where  $\pi$  is the isomorphism defined as in Remark 2.1 (a).  $\square$

**Proposition 4.3.** *Let  $\mathbf{q}$  be a generator of  $\mathcal{Q}$ ,  $v(\mathbf{q}) = r$ ,  $|B_{e_i}| = hk$  and  $|F_{e_i}(\mathbf{q}^j)| = h_j k_j$ , where  $h_1 | \dots | h_{r-1} | h | (t-1)$  and  $k_1 | \dots | k_{r-1} | k | t^{r-1}$ . Then  $\frac{k}{k_j}$  divides  $t^{r-(j+1)}$  for  $j \in I_{r-1}$  and, in particular,  $k_{r-1} = k$ .*

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

**Remark 4.3.** *Since  $F(\mathbf{q}^j) = \dot{\bigcup}_{i=1}^m F_{e_i}(\mathbf{q}^j)$ , we have that  $F(\mathbf{q}) \subseteq \dots \subseteq F(\mathbf{q}^{r-1}) \subseteq C$  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 $\mathbf{q}^j$

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  $\mathbf{q}^j, j = 1, \dots, r-1$ , where  $\mathbf{q}$  is a generator of  $\mathbf{Q}$  and  $v(\mathbf{q}) = r$ .

**Definition 4.3.** *Let  $\mathbf{q}$  be a generator of  $\mathbf{Q}$  and  $v(\mathbf{q}) = r$ . The set of all the right identities of  $\mathbf{q}^j$  will be denoted by  $U(\mathbf{q}^j)$ , that is*

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

**Proposition 4.4.** *Let  $\mathbf{q}$  be a generator of  $\mathbf{Q}$  and  $v(\mathbf{q}) = r$ . Then, for  $j \in I_{r-1}$ ,*

- (a)  $U(\mathbf{q}) \subseteq U(\mathbf{q}^2) \subseteq \dots \subseteq U(\mathbf{q}^{r-1}) \subseteq C$  is a chain of subsemigroups of  $C$ ;
- (b)  $U(\mathbf{q}^j) = \mathbf{u} + \text{Ann}(\mathbf{q}^j)$ ,  $\mathbf{u}$  being any right identity of  $\mathbf{q}^j$ ;
- (c)  $|U(\mathbf{q}^j)| = t^j$ .

**Proof.** (a) Obvious, as in Proposition 4.1.

(b) Let  $\mathbf{u}$  be any right identity of  $\mathbf{q}^j$ . Let  $x \in U(\mathbf{q}^j)$ . Then  $\mathbf{q}^j * x = \mathbf{q}^j = \mathbf{q}^j * \mathbf{u}$ , thus  $\mathbf{q}^j * (x - \mathbf{u}) = 0$  implies  $x - \mathbf{u} \in \text{Ann}(\mathbf{q}^j)$ . Conversely, let  $y$  be any element of  $\text{Ann}(\mathbf{q}^j)$ , then  $\mathbf{q}^j * (\mathbf{u} + y) = \mathbf{q}^j * \mathbf{u} + \mathbf{q}^j * y = \mathbf{q}^j$ .

(c) From previous point (b) and Theorem 3.1,  $|U(\mathbf{q}^j)| = |\text{Ann}(\mathbf{q}^j)| = t^j$ . □

**Definition 4.4.** *Let  $\mathbf{q}$  be a generator of  $\mathbf{Q}$  and  $v(\mathbf{q}) = r$ . The set of all the right identities of  $\mathbf{q}^j$  belonging to  $B_{e_i}$  will be denoted by  $U_{e_i}(\mathbf{q}^j)$ , that is*

$$U_{e_i}(\mathbf{q}^j) = U(\mathbf{q}^j) \cap B_{e_i} = \{x \in B_{e_i} \mid \mathbf{q}^j * x = \mathbf{q}^j\}, \text{ for } j \in I_{r-1} \text{ and } i \in I_m.$$

**Remark 4.4.** *For all  $j \in I_{r-1}$ ,  $U_{e_i}(\mathbf{q}^j)$  is non empty if and only if  $\mathbf{q}^j * e_i = \mathbf{q}^j$ , that is if and only if  $e_i \in U_{e_i}(\mathbf{q}^j)$ .*

**Remark 4.5.** *If  $\mathbf{q}^j * e_i \neq \mathbf{q}^j$  then  $e_i \in U_{e_i}(\mathbf{p}^j)$ , where  $\mathbf{p} = \mathbf{q} * e_i$  results in a generator of  $\mathbf{Q}$ .*

**Proposition 4.5.** *Let  $\mathbf{q}$  be a generator of  $\mathbf{Q}$  and  $v(\mathbf{q}) = r$ . Then, for  $i, h \in I_m$  and  $j \in I_{r-2}$ ,*

- (a) if  $\mathbf{q}^j * e_i = \mathbf{q}^j$ , then  $U_{e_i}(\mathbf{q}^j) \subseteq U_{e_i}(\mathbf{q}^{j+1}) \subseteq \dots \subseteq U_{e_i}(\mathbf{q}^{r-1})$  is a normal chain of multiplicative subgroups of  $B_{e_i}$ ;
- (b)  $U_{e_i}((\mathbf{q} * e_i)^j)$  and  $U_{e_h}((\mathbf{q} * e_h)^j)$  are isomorphic groups;
- (c) if  $\mathbf{q}^j * B_{e_i} \cap \mathbf{q}^j * B_{e_h}$  is non empty, then  $\mathbf{q}^j * B_{e_i} = \mathbf{q}^j * B_{e_h}$ .

**Proof.** (a) If  $\mathbf{q}^j * e_i = \mathbf{q}^j$ , from previous Proposition 4.4(a) we know that  $U_{e_i}(\mathbf{q}^j)$  is a non empty subsemigroup of  $U_{e_i}(\mathbf{q}^{j+1})$  with  $e_i$  as identity (see Remark 4.4),  $\forall j \in I_{r-2}$ . Let now  $x \in U_{e_i}(\mathbf{q}^j)$ . The inverse of  $x$  in  $B_{e_i}$  belongs to  $U_{e_i}(\mathbf{q}^j)$  because it is an integer power of  $x$  (see [5], Th.8), so  $U_{e_i}(\mathbf{q}^j)$  results in a subgroup of  $B_{e_i}$ . In order to show that  $U_{e_i}(\mathbf{q}^j)$  is normal in  $B_{e_i}$ , firstly we prove that an element  $x$  of  $B_{e_i}$  belongs to  $U_{e_i}(\mathbf{q}^j)$  if and only if  $x * (c + \text{Ann}(\mathbf{q}^j)) = c + \text{Ann}(\mathbf{q}^j)$ , for all  $c \in C$ . In fact  $x \in U_{e_i}(\mathbf{q}^j)$  implies  $\mathbf{q}^j * x = \mathbf{q}^j$ . Thus  $\mathbf{q}^j * x * c = \mathbf{q}^j * c$  and this implies  $x * c \in c + \text{Ann}(\mathbf{q}^j)$ ,  $\forall c \in C$ . Hence, keeping in mind that  $x * \text{Ann}(\mathbf{q}^j) = \text{Ann}(\mathbf{q}^j)$  for all  $x \in C$  and  $j \in I_{r-1}$ ,  $x * (c + \text{Ann}(\mathbf{q}^j)) = x * c + \text{Ann}(\mathbf{q}^j) = c + \text{Ann}(\mathbf{q}^j)$ , for all  $c \in C$ . Conversely, if  $x \in B_{e_i}$  and  $x * (c + \text{Ann}(\mathbf{q}^j)) = c + \text{Ann}(\mathbf{q}^j)$  for all  $c \in C$ , choosing  $c = e_i$  we have  $x * (e_i + \text{Ann}(\mathbf{q}^j)) = e_i + \text{Ann}(\mathbf{q}^j)$ . Hence  $\mathbf{q}^j * x * (e_i + \text{Ann}(\mathbf{q}^j)) = \mathbf{q}^j * (e_i + \text{Ann}(\mathbf{q}^j))$  and this implies  $\mathbf{q}^j * x = \mathbf{q}^j$ , that is  $x \in U_{e_i}(\mathbf{q}^j)$ .

Applying previous characterization,  $\forall y \in B_{e_i}$ ,  $\forall x \in U_{e_i}(\mathbf{q}^j)$  and  $\forall c \in C$  we have  $y^{-1} * x * y * (c + \text{Ann}(\mathbf{q}^j)) = y^{-1} * x * (y * c + y * \text{Ann}(\mathbf{q}^j)) = y^{-1} * x * (y * c + \text{Ann}(\mathbf{q}^j)) = y^{-1} * (y * c + \text{Ann}(\mathbf{q}^j)) = y^{-1} * y * c + y^{-1} * \text{Ann}(\mathbf{q}^j) = c + \text{Ann}(\mathbf{q}^j)$ . Thus  $y^{-1} * x * y$  belongs to  $U_{e_i}(\mathbf{q}^j)$  and this implies  $U_{e_i}(\mathbf{q}^j)$  is normal.

(b) It can be easily verified that  $\pi(U_{e_{i_1}}((\mathbf{q} * e_{i_1})^j)) = U_{e_{i_2}}((\mathbf{q} * e_{i_2})^j)$ , where  $\pi$  is the isomorphism defined as in Remark 2.1 (a).

(c)  $\mathbf{q}^j * B_{e_i} \cap \mathbf{q}^j * B_{e_h} \neq \emptyset$  implies  $\mathbf{q}^j * x = \mathbf{q}^j * y$  for some  $x \in B_{e_i}$  and  $y \in B_{e_h}$ . Multiplying by  $e_i$  on the right we obtain  $\mathbf{q}^j * x = \mathbf{q}^j * y * e_i$ , so  $\mathbf{q}^j * y * (e_i - e_h) = 0$ . Let  $y^{-1}$  be the inverse of  $y$  in  $B_{e_h}$ . Applying the I.F.P. we obtain  $\mathbf{q}^j * y * y^{-1} * n * (e_i - e_h) = 0$ , so  $\mathbf{q}^j * n * e_i = \mathbf{q}^j * n * e_h$  for all  $n \in N$ . Hence  $\mathbf{q}^j * B_{e_i} = \mathbf{q}^j * B_{e_i} * e_h = \mathbf{q}^j * B_{e_h}$ .  $\square$

**Remark 4.6.** *From what precedes we can say that  $U(\mathbf{q}^j)$  is a semigroup containing exactly  $m_j$  idempotent right identities of  $\mathbf{q}^j$ , say  $e_{i_1}, e_{i_2}, \dots, e_{i_{m_j}}$ . Then  $U(\mathbf{q}^j)$  results in the disjoint union of  $m_j$  isomorphic groups, the  $U_{e_{i_\lambda}}(\mathbf{q}^j)$ s, for  $\lambda \in I_{m_j}$ , that is  $U(\mathbf{q}^j) = \bigcup_{\lambda=1}^{m_j} U_{e_{i_\lambda}}(\mathbf{q}^j)$  and  $m_j = \frac{|U(\mathbf{q}^j)|}{|U_{e_{i_\lambda}}(\mathbf{q}^j)|}$ , 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  $B_e$ ,  $e$  being its identity. Since each non zero idempotent is a right identity of some generator of  $Q$ , let  $\mathbf{q}$  be a generator of  $Q$  such that  $\mathbf{q} * e = \mathbf{q}$ .

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.

**Theorem 4.1.** *Let  $\mathbf{q}$  be a generator of  $\mathbf{Q}$  and  $v(\mathbf{q}) = r$ . Let  $e$  be an idempotent right identity of  $\mathbf{q}$  and  $|B_e| = hk$ , where  $h \mid (t-1)$  and  $k \mid t^{r-1}$ . Then*

- (a)  $U_e(\mathbf{q}^{r-1})$  is a normal subgroup of  $B_e$  of order  $k$ ;
- (b)  $B_e$  results in the semidirect product of  $U_e(\mathbf{q}^{r-1})$  and a complement  $U'$  of order  $h$ .

**Proof.** (a) From Proposition 4.5 (a) we know that  $U_e(\mathbf{q}^{r-1})$  is a normal subgroup of  $B_e$ . Moreover, since the elements of  $U(\mathbf{q}^{r-1})$  are shared into disjoint subgroups isomorphic to  $U_e(\mathbf{q}^{r-1})$  (see Proposition 4.5 (b)), the order of  $U_e(\mathbf{q}^{r-1})$  divides  $|U(\mathbf{q}^{r-1})| = t^{r-1}$  (see Proposition 4.4(c)). In addition, the index of  $U_e(\mathbf{q}^{r-1})$  in  $B_e$  equals the cardinality of  $\mathbf{q}^{r-1} * B_e$  and  $|\mathbf{q}^{r-1} * B_e|$  must divide  $|\mathbf{q}^{r-1} * C| = t-1$  (see Proposition 4.5 (c) and Theorem 3.1). Thus,  $[B_e : U_e(\mathbf{q}^{r-1})]$  divides  $t-1$  and  $|U_e(\mathbf{q}^{r-1})| = k$ .

(b)  $U_e(\mathbf{q}^{r-1})$  is a normal subgroup of  $B_e$  whose order and index are coprime, so  $B_e$  results in the semidirect product between  $U_e(\mathbf{q}^{r-1})$  and its Schur-Zassenhaus complement (see [7]).  $\square$

**Corollary 4.1.** *Let  $\mathbf{q}$  be a generator of  $\mathbf{Q}$ ,  $v(\mathbf{q}) = r$  and  $|B_e| = hk$  where  $h$  divides  $t-1$  and  $k$  divides  $t^{r-1}$ . The following statements are equivalent*

- (a)  $|F_e(\mathbf{q}^{r-1})| = 1$ ;
- (b)  $|B_e| = h$  and  $|F_e(\mathbf{q}^j)| = |U_e(\mathbf{q}^j)| = 1, \forall j \in I_{r-1}$ ;
- (c)  $|B_e| = h$  and  $B_e * \mathbf{q}^j = \mathbf{q}^j * B_e, \forall j \in I_{r-1}$ .

**Proof.** (a)  $\Rightarrow$  (b) Obviously  $|F_e(\mathbf{q}^{r-1})| = 1$  implies  $|F_e(\mathbf{q}^j)| = 1, \forall j \in I_{r-1}$ . Moreover, from Proposition 4.3 we know that  $|F_e(\mathbf{q}^{r-1})| = h_{r-1}k$ , where  $h_{r-1}$  divides  $t-1$ , so  $k = h_{r-1} = 1$ . Hence  $|U_e(\mathbf{q}^{r-1})| = 1$  implies both  $|B_e| = h$  and  $|U_e(\mathbf{q}^j)| = 1, \forall j \in I_{r-1}$ .

(b)  $\Rightarrow$  (c)  $|F_e(\mathbf{q}^j)| = |U_e(\mathbf{q}^j)| = 1, \forall j \in I_{r-1}$  implies  $|B_e * \mathbf{q}^j| = |B_e| = |\mathbf{q}^j * B_e|$ . Since  $B_e * \mathbf{q}^j \subseteq \mathbf{q}^j * B_e$  (see Proposition 3.4 (a)), then  $B_e * \mathbf{q}^j = \mathbf{q}^j * B_e$ .

(c)  $\Rightarrow$  (a)  $B_e * \mathbf{q}^{r-1} = \mathbf{q}^{r-1} * B_e$  implies  $|F_e(\mathbf{q}^{r-1})| = |U_e(\mathbf{q}^{r-1})|$ .  $|B_e| = h$  implies  $k = 1$ , so  $|U_e(\mathbf{q}^{r-1})| = 1 = |F_e(\mathbf{q}^{r-1})|$ .  $\square$

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

**Proposition 4.6.** *Let  $\mathbf{q}$  be a generator of  $\mathbf{Q}$  and  $v(\mathbf{q}) = r$ . If  $|B_e| = h$ , where  $h$  divides  $t-1$ , then  $|U_e(\mathbf{q}^j)| = 1, |F_e(\mathbf{q}^j)| = h_j$  and  $h_j|B_e * \mathbf{q}^j| = |\mathbf{q}^j * B_e| = h, \forall j \in I_{r-1}$ .*

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

### 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  $k = t^a$ , with  $0 \leq a \leq r - 1$ .

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

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

**Remark 5.1.** *If  $t$  is a prime number, from Propositions 4.4, 4.5 and previous Theorem 5.1 we know that*

- (a)  $|U_e(\mathbf{q}^{r-1})| = t^a$ ;
- (b)  $|U_e(\mathbf{q})| = 1$  or  $t$ ;
- (c) if  $|U_e(\mathbf{q}^j)| = t^x$  then  $|U_e(\mathbf{q}^{j+1})| = t^x$  or  $t^{x+1}$ , for  $j \in I_{r-2}$ .

Thus, we can easily deduce the following

**Proposition 5.1.** *Let  $\mathbf{q}$  be a generator of  $Q$  and  $v(\mathbf{q}) = r$ . Let  $\mathbf{e}$  be any idempotent right identity of  $\mathbf{q}$  and  $|B_e| = ht^a$ , where  $t$  is a prime,  $h$  divides  $t - 1$  and  $0 \leq a \leq r - 1$ . If  $|U_e(\mathbf{q}^a)| = t^a$  then*

$$\begin{aligned} \text{for } j \leq a \quad & |U_e(\mathbf{q}^j)| = t^j \quad \text{and} \quad |\mathbf{q}^j * B_e| = ht^{a-j} \\ \text{for } j \geq a \quad & |U_e(\mathbf{q}^j)| = t^a \quad \text{and} \quad |\mathbf{q}^j * B_e| = h. \end{aligned}$$

If  $|U_e(\mathbf{q}^{r-a-1})| = 1$  then

$$\begin{aligned} \text{for } j \leq r - a - 1 \quad & |U_e(\mathbf{q}^j)| = 1 \quad \text{and} \quad |\mathbf{q}^j * B_e| = ht^a \\ \text{for } j \geq r - a - 1 \quad & |U_e(\mathbf{q}^j)| = t^{j-r+a+1} \quad \text{and} \quad |\mathbf{q}^j * B_e| = ht^{r-j-1}. \end{aligned}$$

### 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 F. MORINI, *On the construction of a class of weakly divisible nearrings*, Riv. Mat. Univ. Parma (6) **1** (1998), 103-111.
- [3] A. BENINI and 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*, Results Math. **47** (2005), 6-16.
- [5] A. BENINI and 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, New York 1992.
- [7] D. GORENSTEIN, *Finite groups*, 2nd ed., Chelsea Publishing Co., New York 1980.
- [8] M. HALL, *Designs with transitive automorphism groups*, in Combinatorics, Proc. Sympos. Pure Math., Vol. XIX, T. S. Motzkin, ed., AMS, Providence 1971, pp.109-113.
- [9] P. MAYR and F. MORINI, *Nearrings whose set of  $N$ -subgroups is linearly ordered*, Results Math. **42** (2002), 339-348.
- [10] G. PILZ, *Near-rings*, 2nd ed., North-Holland Math. Studies 23, North-Holland Publishing Co., Amsterdam 1983.

ANNA BENINI, SILVIA PELLEGRINI  
Dipartimento di Matematica  
Università di Brescia  
Via Valotti 9, I-25133 Brescia, Italy  
e-mail: anna.benini@ing.unibs.it  
e-mail: silvia.pellegrini@ing.unibs.it