ISSN 2075-9827 **e-ISSN 2313-0210**
Carpathian Math. Publ. 2020, **12** (1), 199–207
doi:10.15330/cmp.12.1.199-207

http://www.journals.pnu.edu.ua/index.php/cmp
Карпатські матем. публ. 2020, Т.12, №1, С.199–207

RAIEVSKA I.YU., RAIEVSKA M.YU.

LOCAL NEARRINGS ON FINITE NON-ABELIAN 2-GENERATED p-GROUPS

It is proved that for $p > 2$ every finite non-metacyclic 2-generated p-group of nilpotency class 2 with cyclic commutator subgroup is the additive group of a local nearring and in particular of a nearring with identity. It is also shown that the subgroup of all non-invertible elements of this nearring is of index p in its additive group.

Key words and phrases: finite p-group, local nearring.

Institute of Mathematics, National Academy of Sciences of Ukraine, 3 Tereschenkivska str., 01024, Kyiv, Ukraine
E-mail: raeirina@imath.kiev.ua (Raievska I.Yu.), raemarina@imath.kiev.ua (Raievska M.Yu.)

INTRODUCTION

Nearrings are generalizations of associative rings in the sense that with respect to the addition they need not be commutative and only one distributive law is assumed. In this paper the concept "nearring" means a left distributive nearring with a multiplicative identity. The reader is referred to the books by Meldrum [6] or Pilz [8] for terminology, definitions and basic facts concerning nearrings.

Following [3], the nearring with identity will be called local, if the set of all non-invertible elements forms a subgroup of its additive group. The main results concerning local nearrings are summarized in [11].

In [4] it is shown that every non-cyclic abelian p-group of order $p^n > 4$ is the additive group of a zero-symmetric local nearring which is not a ring. As it was noted in [5], neither a generalized quaternion group nor a non-abelian group of order 8 can be the additive group of a local nearring.

Therefore the structure of the non-abelian finite p-groups which are the additive groups of local nearrings is an open problem [2].

It was proved that every non-metacyclic Miller–Moreno p-group of order $p^n > 8$ is the additive group of a local nearring and the multiplicative group of such a nearring is the group of order $p^{n-1}(p-1)$ [9]. In this paper finite non-abelian non-metacyclic 2-generated p-groups ($p > 2$) of nilpotency class 2 with cyclic commutator subgroup are studied.

УДК 512.6
2010 *Mathematics Subject Classification:* 16Y30.
This work was partially supported by the grant 346300 for IMPAN from the Simons Foundation and the matching 2015-2019 Polish MNiSW fund.

1 PRELIMINARIES

Let G be a finite non-abelian non-metacyclic 2-generated p-group ($p > 2$) of nilpotency class 2 with cyclic commutator subgroup.

Denote by G' and $Z(G)$ the commutator subgroup and the centre of G, respectively.

Let a and b be generators for G such that $G/G' = \langle aG' \rangle \times \langle bG' \rangle$, aG' has order p^m and bG' has order p^n. Then $c = [a, b]$ generates G', c has order p^d with $1 \leq d \leq n \leq m$, and $c \in Z(G) = \langle a^{p^m}, b^{p^n}, c \rangle$.

Suppose that $\langle a \rangle \cap G' = \langle b \rangle \cap G' = 1$. Then

$$G = \langle a,\ b,\ c | a^{p^m} = b^{p^n} = c^{p^d} = 1,\ a^b = ac,\ c^a = c^b = c \rangle$$

and each element of G can be uniquely written in the form $a^{x_1} b^{x_2} c^{x_3}$, $x_1 \in C_{p^m}$, $x_2 \in C_{p^n}$, $x_3 \in C_{p^d}$. Therefore the group G with $p > 2$ will be denoted by $G(p^m, p^n, p^d)$.

Lemma 1. *For any natural numbers k and l the equality $[a^k, b^l] = c^{kl}$ holds.*

Proof. Since $b^{-1}ab = ac$, it follows that $b^{-l}ab^l = ac^l$. Therefore, $b^{-l}a^k b^l = (ac^l)^k = a^k c^{kl}$, thus $a^{-k}b^{-l}a^k b^l = c^{kl}$. □

Corollary 1. *Let the group $G(p^m, p^n, p^d)$ be additively written. Then for any natural numbers k and l the equalities $-ak - bl + ak + bl = c(kl)$ and $bl + ak = -c(kl) + ak + bl$ hold.*

Lemma 2. *For any natural numbers k, l and r the equality*

$$(a^k b^l)^r = a^{kr} b^{lr} c^{-kl\binom{r}{2}} \tag{1}$$

holds.

Proof. For $r = 1$, there is nothing to prove. By induction on r, we derive

$$(a^k b^l)^r = a^{kr} b^{lr} c^{-kl\binom{r}{2}}.$$

Replacing r by $r + 1$ in equality (1), we have

$$\begin{aligned}(a^k b^l)^{(r+1)} &= a^{kr} b^{lr} a^k b^l c^{-kl\binom{r}{2}} = a^{k(r+1)} b^{l(r+1)} c^{-klr} c^{-kl\binom{r}{2}} \\ &= a^{k(r+1)} b^{l(r+1)} c^{-kl\left(r+\binom{r}{2}\right)} = a^{k(r+1)} b^{l(r+1)} c^{kl\binom{r+1}{2}}.\end{aligned}$$

Thus, equality (1) holds for an arbitrary r. □

Corollary 2. *Let the group $G(p^m, p^n, p^d)$ be additively written. Then for any natural numbers k, l and r the equality $(ak + bl)r = akr + blr - ckl\binom{r}{2}$ holds.*

Obviously, the exponent of $G(p^m, p^n, p^d)$ is equal to p^m for $1 \leq d \leq n \leq m$.

Lemma 3. *If x is an element of order p^m of $G(p^m, p^n, p^d)$, then there exist generators a, b, c of this group such that $a = x$ and $a^{p^m} = b^{p^n} = c^{p^d} = 1$, $a^b = ac$, $c^a = c^b = c$.*

Proof. Indeed, for each $x \in G(p^m, p^n, p^d)$ there exist positive integers α, β and γ such that $x = a^\alpha b^\beta c^\gamma$. Thus, we have

$$x^{p^m} = (a^\alpha b^\beta c^\gamma)^{p^m} = (a^\alpha b^\beta)^{p^m} c^{\gamma p^m} = a^{\alpha p^m} b^{\beta p^m} c^{\gamma p^m - \alpha\beta\binom{p^m}{2}}$$
$$= a^{p^m \alpha} b^{p^m \beta} c^{p^m(\gamma - \alpha\beta\frac{(p^m-1)}{2})} = 1$$

by Lemma 2. Since $|a| = p^m$ and $1 \leq d \leq n \leq m$, where $m > 1$ and $p > 2$, it follows that the exponent of $G(p^m, p^n, p^d)$ equals p^m.

If

$$x^{p^{m-1}} = a^{p^{m-1}\alpha} b^{p^{m-1}\beta} c^{p^{m-1}(\gamma - \alpha\beta\frac{(p^{m-1}-1)}{2})} \neq 1,$$

then either $(\alpha, p) = 1$, or $(\beta, p) = 1$ for $m = n$, or $(\gamma, p) = 1$ for $m = n = d$. So, without loss of generality, we can assume that $(\alpha, p) = 1$. Then

$$\langle x, b\rangle = \langle a^\alpha b^\beta c^\gamma, b\rangle = \langle a^\alpha, b\rangle = \langle a, b\rangle = G$$

and

$$b^{-1}xb = b^{-1}(a^\alpha b^\beta c^\gamma)b = (ac)^\alpha b^\beta c^\gamma = (a^\alpha b^\beta c^\gamma)c^\alpha = xc^\alpha.$$

Furthermore, substituting c^α instead of c for generators x and b of $G(p^m, p^n, p^d)$, we have similar expressions as for generators a and b, thus replacing the element a by x. □

The following assertion concerning the automorphisms group of $G(p^m, p^n, p^d)$ is a direct consequence of statement (B1) [7].

Lemma 4. *Let $G = G(p^m, p^n, p^d)$ and let $Aut(G)$ be the automorphism group of G. Then the following statements hold*:

1) *if $m = n$, then $|Aut(G)| = p^{2d+4m-5}(p^2-1)(p-1)$;*

2) *if $m > n$, then $|Aut(G)| = p^{2d+3n+m-2}(p-1)^2$.*

An information about a group of automorphisms of $G(p^m, p^m, p^d)$ is given by the following lemma.

Lemma 5. *Let $G = G(p^m, p^m, p^d)$ and let there exist a subgroup A of $Aut(G)$ of order $p^{2m+d-2}(p^2-1)$, where m, $d > 1$ with odd p. If an element $g \in G$ of order p^m and A contains Sylow normal p-subgroup, then $G \neq g^A \cup \Phi(G)$.*

Proof. Assume that $G = g^A \cup \Phi(G)$. Then $G = (\langle a\rangle \times \langle c\rangle) \rtimes \langle b\rangle$ with generators a, b of order p^m and a central commutator $c = [a, b]$ of order p^d by the definition. Hence

$$\Phi(G) = (\langle a^p\rangle \times \langle c\rangle) \rtimes \langle b^p\rangle,$$

and thus all elements of order p^m are contained in g^A. Furthermore, $a = g^u$ for some $u \in A$, hence $g^A = a^A$, i. e. $G = a^A \cup \Phi(G)$. Since $|G| = p^{2m+d}$ and $\Phi(G) = p^{2m+d-2}$, it follows that

$$|a^A| = |G| - |\Phi(G)| = p^{2m+d-2}(p^2-1),$$

and so the centralizer $C_A(a)$ of a in A equals 1. In particular, $(a\langle c^p\rangle)^A = (a\langle c^p\rangle)^B = a\langle c^p\rangle$ for the normal subgroup $B = C_A(a\langle c^p\rangle)$ of order p^{d-1} in A.

Considering the factor-group $\bar{G} = G/\langle c^p\rangle$ and $\bar{A} = A/B$. Taking into consideration, that $|\bar{a}^{\bar{A}}| = p^{2m-1}(p^2-1)$, we have $\bar{G} = \bar{a}^{\bar{A}} \cup \Phi(\bar{G})$. Since $|\Phi(\bar{G})| = |Z(\bar{G})|$ and $xy = yx$ for all $x \in \Phi(\bar{G})$, $y \in \bar{G}$, we have $\Phi(\bar{G}) = Z(\bar{G})$. Therefore, $\bar{G}$ is a Miller–Moreno group. Since $\bar{G} = \bar{a}^{\bar{A}} \cup Z(\bar{G})$, the latter equality is impossible by [9, Lemma 7]. This contradiction completes the proof. □

2 NEARRINGS WITH IDENTITY ON GROUP $G(p^m, p^n, p^d)$

First recall some basic concepts of the theory of nearrings.

Definition 1. *A set R with two binary operations "$+$" and "$\cdot$" is called a (left) nearring if the following statements hold*

(1) $(R, +) = R^+$ is a (not necessarily abelian) group with neutral element 0;

(2) $(R, \cdot)$ is a semigroup;

(3) $x(y + z) = xy + xz$ for all $x, y, z \in R$.

If R is a nearring, then the group R^+ is called the *additive group* of R. If in addition $0 \cdot x = 0$, then the nearring R is called *zero-symmetric* and if the semigroup $(R, \cdot)$ is a monoid, i.e. it has an identity element i, then R is a *nearring with identity* i. In the latter case the group R^* of all invertible elements of the monoid $(R, \cdot)$ is called the *multiplicative group* of R.

The following assertion is well-known.

Lemma 6. *Let R be a finite nearring with identity i. Then the exponent of R^+ is equal to the additive order of i which coincides with additive order of every element of R^*.*

As a direct consequence of Lemmas 3 and 6 we have the following corollary.

Corollary 3. *Let R be a nearring with identity i whose group R^+ is isomorphic to a group $G(p^m, p^n, p^d)$. Then $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ with elements a, b and c, satisfying relations $ap^m = bp^n = cp^d = 0$, $-b + a + b = a + c$ and $-a + c + a = -b + c + b = c$ with $1 \leq d \leq n \leq m$, where $a = i$.*

The following statement [10, Lemma 1] establishes a connection between the automorphism group of the additive group of the nearring with identity and its multiplicative group.

Lemma 7. *Let R be a nearring with identity i. Then there exists a subgroup A of the automorphism group $Aut(R^+)$ which is isomorphic to R^* and satisfying the condition $i^A = \{i^a \mid a \in A\} = R^*$.*

The subgroup A defined in Lemma 7 is called the automorphism group of the group R^+ associated with the group R^*.

The following statement [11, Theorem 54] concerns the structure of L which is the subgroup of all non-invertible elements of finite local nearring R. Let $\Phi(G)$ denote the Frattini subgroup of G.

Theorem 1. *Let R be a local nearring of order p^n and let $G(R) = R^+ \rtimes R^*$ be a group associated with R. Then $H = R^+ \rtimes (i + L)$ is a Sylow normal p-subgroup of $G(R)$ and $L = R^+ \cap \Phi(H)$. In particular, if L is non-abelian, then its center is non-cyclic.*

Considering $\Phi(R^+) \leq \Phi(H)$, we have the following corollary.

Corollary 4. $\Phi(R^+) \leq L = \Phi(H) \cap R^+$.

Let R be a nearring with identity i whose group R^+ is isomorphic to a group $G(p^m, p^n, p^d)$. It follows from Corollary 3 that $R^+ = \langle a\rangle + \langle b\rangle + \langle c\rangle$ with elements a, b and c, satisfying relations $ap^m = bp^n = cp^d = 0$, $-b+a+b = a+c$ and $-a+c+a = -b+c+b = c$ with $1 \le d \le n \le m$, where $a = i$ and each element $x \in R$ is uniquely written in the form $x = ax_1 + bx_2 + cx_3$ with coefficients $0 \le x_1 < p^m$, $0 \le x_2 < p^n$ and $0 \le x_3 < p^d$.

Furthermore, we can assume $xa = ax = x$ for each $x \in R$. Then there exist uniquely defined mappings $\alpha\colon R \to \mathbb{Z}_{p^m}$, $\beta\colon R \to \mathbb{Z}_{p^n}$ and $\gamma\colon R \to \mathbb{Z}_{p^d}$ such that

$$xb = a\alpha(x) + b\beta(x) + c\gamma(x). \tag{2}$$

Lemma 8. *If $x = ax_1 + bx_2 + cx_3$ and $y = ay_1 + by_2 + cy_3$ are arbitrary elements of R, then*

$$\begin{aligned} xy = a(x_1y_1 + y_2\alpha(x)) + b(x_2y_1 + y_2\beta(x)) \\ + c\Big(- x_1x_2\binom{y_1}{2} - \binom{y_2}{2}\alpha(x)\beta(x) - x_2y_1y_2\alpha(x) \\ + x_3y_1 + y_2\gamma(x) + x_1y_3\beta(x) - x_2y_3\alpha(x)\Big), \end{aligned}$$

where mappings $\alpha\colon R \to \mathbb{Z}_{p^m}$, $\beta\colon R \to \mathbb{Z}_{p^n}$ and $\gamma\colon R \to \mathbb{Z}_{p^d}$ satisfy the conditions

(0) $\alpha(0) \equiv 0 \pmod{p^m}$, $\beta(0) \equiv 0 \pmod{p^n}$ *and* $\gamma(0) \equiv 0 \pmod{p^d}$ *if and only if the nearring R is zero-symmetric*;

(1) $\alpha(xy) \equiv x_1\alpha(y) + \alpha(x)\beta(y) \pmod{p^m}$;

(2) $\beta(xy) \equiv x_2\alpha(y) + \beta(x)\beta(y) \pmod{p^n}$;

(3) $\gamma(xy) \equiv -x_1x_2\binom{\alpha(y)}{2} - \alpha(x)\beta(x)\binom{\beta(y)}{2} - x_2\alpha(x)\alpha(y)\beta(y)$

$$+x_3\alpha(y) + \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y) \pmod{p^d}.$$

Proof. If R is a zero-symmetric nearring, then

$$0 = 0 \cdot b = a\alpha(0) + b\beta(0) + c\gamma(0),$$

thus $\alpha(0) \equiv 0 \pmod{p^m}$, $\beta(0) \equiv 0 \pmod{p^n}$ and $\gamma(0) \equiv 0 \pmod{p^d}$. On the other hand, if the last congruences hold, then $0 \cdot b = a \cdot 0 + b \cdot 0 + c \cdot 0 = 0$. Since a is the multiplicative identity in R, we have $0 \cdot a = a \cdot 0 = 0$. Moreover, from the equality $c = -a - b + a + b$ and the left distributive law it follows that $0 \cdot c = -0 \cdot a - 0 \cdot b + 0 \cdot a + 0 \cdot b = 0$, hence

$$0 \cdot x = 0 \cdot (ax_1 + bx_2 + cx_3) = (0 \cdot a)x_1 + (0 \cdot b)x_2 + (0 \cdot c)x_3 = 0.$$

This proves statement (0).

Next, using (2) and Corollary 1, we obtain

$$\begin{aligned} xc &= -xa - xb + xa + xb = -cx_3 - bx_2 - ax_1 - c\gamma(x) - b\beta(x) - a\alpha(x) \\ &\quad + ax_1 + bx_2 + cx_3 + a\alpha(x) + b\beta(x) + c\gamma(x) \\ &= -bx_2 - ax_1 - b\beta(x) - a\alpha(x) + ax_1 + bx_2 + a\alpha(x) + b\beta(x) \\ &= -bx_2 + cx_1\beta(x) - b\beta(x) - ax_1 - a(\alpha(x) - x_1) + bx_2 + a\alpha(x) + b\beta(x) \\ &= cx_1\beta(x) - b(x_2 + \beta(x)) - a\alpha(x) + bx_2 + a\alpha(x) + b\beta(x) \end{aligned}$$

$$= cx_1\beta(x) - b(x_2 + \beta(x)) - a\alpha(x) - cx_2\alpha(x) + a\alpha(x) + bx_2 + b\beta(x)$$
$$= c(x_1\beta(x) - x_2\alpha(x)) - b(x_2 + \beta(x)) + bx_2 + b\beta(x) = c(x_1\beta(x) - x_2\alpha(x)).$$

Therefore

$$xy = (ax_1 + bx_2 + cx_3)y_1 + (a\alpha(x) + b\beta(x) + c\gamma(x))y_2 + (cx_1\beta(x) - x_2\alpha(x))y_3.$$

Corollary 2 implies that

$$(ax_1 + bx_2)y_1 = ax_1y_1 + bx_2y_1 - cx_1x_2\binom{y_1}{2},$$
$$(a\alpha(x) + b\beta(x))y_2 = ay_2\alpha(x) + by_2\beta(x) - c\binom{y_2}{2}\alpha(x)\beta(x)$$

and

$$bx_2y_1 + ay_2\alpha(x) = ay_2\alpha(x) + bx_2y_1 - cx_2y_1y_2\alpha(x).$$

By the left distributive law, we have

$$xy = a(x_1y_1 + y_2\alpha(x)) + b(x_2y_1 + y_2\beta(x)) + c\Big(- x_1x_2\binom{y_1}{2}$$
$$- \binom{y_2}{2}\alpha(x)\beta(x) - x_2y_1y_2\alpha(x) + x_3y_1 + y_2\gamma(x) + x_1y_3\beta(x) - x_2y_3\alpha(x)\Big).$$

Finally, the associativity of multiplication for all $x, y \in R$ implies that

1) $(xy)b = x(yb)$.

Thus

2) $(xy)b = a\alpha(xy) + b\beta(xy) + c\gamma(xy)$

and $yb = a\alpha(y) + b\beta(y) + c\gamma(y)$ by formula (2). Substituting the last expression in the right part of equality 1), we get

3) $x(yb) = a(x_1\alpha(y) + \alpha(x)\beta(y)) + b(x_2\alpha(y) + \beta(x)\beta(y))$
$+ c(-x_1x_2\binom{\alpha(y)}{2} - \alpha(x)\beta(x)\binom{\beta(y)}{2} - x_2\alpha(x)\alpha(y)\beta(y)$
$+ x_3\alpha(y) + \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y)).$

Comparing the coefficients a, b and c in 2) and 3) by equality 1), we derive statements (1)–(3) of the lemma. □

3 LOCAL NEARRINGS ON GROUP $G(p^m, p^n, p^d)$

Let R be a local nearring with identity i, whose group R^+ is isomorphic to the group $G(p^m, p^n, p^d)$. Then $R^+ = \langle a\rangle + \langle b\rangle + \langle c\rangle$ with elements a, b and c, satisfying relations $ap^m = bp^n = cp^d = 0$, $-b + a + b = a + c$ and $-a + c + a = -b + c + b = c$ with $1 \le d \le n \le m$, where $a = i$ and each element $x \in R$ is uniquely written in the form $x = ax_1 + bx_2 + cx_3$ with coefficients $0 \le x_1 < p^m$, $0 \le x_2 < p^n$ and $0 \le x_3 < p^d$.

We show that the set L of all non-invertible elements of R is a subgroup of index p in R^+.

Theorem 2. *The following statements hold*

1) $L = \langle a \cdot p \rangle + \langle b \rangle + \langle c \rangle$ *and, in particular, the subgroup* L *is of index* p *in* R^+ *and* $|R^*| = p^{m+n+d-1}(p-1)$;

2) $x = ax_1 + bx_2 + cx_3$ *is an invertible element if and only if* $x_1 \not\equiv 0 \pmod{p}$.

Proof. Assume that $|R^+ : L| = p^t$, $t > 1$. Since $R = R^* \cup L$, it follows that

$$|R^*| = |R| - |L| = p^{m+n+d} - p^{m+n+d-t} = p^{m+n+d-t}(p^t - 1).$$

According to Lemma 7, the group R^* is isomorphic to the subgroup A of the automorphism group of R^+ and so $|R^*|$ divides $|\mathrm{Aut}(R^+)|$. According to statement 1) of Lemma 4 it is possible only if $t = 2$ and $m = n$.

Assume that $|R^+ : L| = p^2$ and $m = n$. If $d = 1$, then it is impossible because of [9, Theorem 2]. Now let $d > 1$. Since $|R^+ : \Phi(R^+)| = p^2$ and Corollary 4, we have $L = \Phi(R^+)$. Hence by Lemma 7, we get $R^+ = a^A \cup \Phi(R^+)$, which is impossible by Lemma 5. This contradiction shows that our assumption is false and so $|R^+ : L| = p$.

It is clear that R/L is a nearfield and so the factor-group R^+/L^+ is an elementary abelian p-group. Thus for $a \notin L$ we have $ap \in L$ and so $L = \langle a \cdot p \rangle + \langle b \rangle + \langle c \rangle$. Therefore $R^* = R \setminus L$ and hence

$$R^* = \{ax_1 + bx_2 + cx_3 \mid x_1 \not\equiv 0 \ (\mod p)\}.$$

□

Applying statement (1) of Theorem 2 to Lemma 8, we get the following formula for multiplying elements $x = ax_1 + bx_2 + cx_3$ and $y = ay_1 + by_2 + cy_3$ in the local nearring R.

Corollary 5. *If* $x, y \in R$ *with* $1 \le d \le n \le m$ *and* $xb = a\alpha(x) + b\beta(x) + c\gamma(x)$, *then*

$$\begin{aligned} xy = a(x_1y_1 + y_2\alpha(x)) + b(x_2y_1 + y_2\beta(x)) + c\Big(& - x_1x_2\binom{y_1}{2} \\ & - \binom{y_2}{2}\alpha(x)\beta(x) - x_2y_1y_2\alpha(x) + x_3y_1 + y_2\gamma(x) + x_1y_3\beta(x) - x_2y_3\alpha(x)\Big), \end{aligned}$$

where mappings $\alpha\colon R \to \mathbb{Z}_{p^m}$, $\beta\colon R \to \mathbb{Z}_{p^n}$ *and* $\gamma\colon R \to \mathbb{Z}_{p^d}$ *and the following statements hold*

(0) $\alpha(0) \equiv 0 \pmod{p^m}$, $\beta(0) \equiv 0 \pmod{p^n}$ *and* $\gamma(0) \equiv 0 \pmod{p^d}$ *if and only if the nearring* R *is zero-symmetric*;

(1) $\alpha(x) \equiv 0 \pmod{p}$;

(2) *if* $\beta(x) \equiv 0 \pmod{p}$, *then* $x_1 \equiv 0 \pmod{p}$;

(3) $\alpha(xy) \equiv x_1\alpha(y) + \alpha(x)\beta(y) \pmod{p^m}$;

(4) $\beta(xy) \equiv x_2\alpha(y) + \beta(x)\beta(y) \pmod{p^n}$;

(5) $\gamma(xy) \equiv -x_1x_2\binom{\alpha(y)}{2} - \alpha(x)\beta(x)\binom{\beta(y)}{2} - x_2\alpha(x)\alpha(y)\beta(y) + x_3\alpha(y) + \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y) \pmod{p^d}$.

Proof. Indeed, statements (0), (3)–(5) repeat statements (0)–(4) of Lemma 8. Since $L = \langle a \cdot p \rangle + \langle b \rangle + \langle c \rangle$ by Theorem 2 and L is an (R, R)-subgroup in R by statement 2) [1, Lemma 3.2], it follows that $xb \in L$ and hence $\alpha(x) \equiv 0 \pmod{p}$, proving statement (1). Taking $y = c$, we have $xc = c(x_1\beta(x) - x_2\alpha(x))$. Thus, if $\beta(x) \equiv 0 \pmod{p}$, then $xc = 0 \pmod{p}$, and so $x \in L$. Thus $x_1 \equiv 0 \pmod{p}$ by Theorem 2, proving statement (2). □

The following theorem shows the conditions given in Theorem 2 are sufficient for existing of finite local nearrings on $G(p^m, p^n, p^d)$. Moreover, each group $G(p^m, p^n, p^d)$ is the additive group of a nearring with identity.

Theorem 3. *For each prime p and positive integers m, n and d with $1 \leq d \leq n \leq m$ there exists a local nearring R whose additive group R^+ is isomorphic to the group $G(p^m, p^n, p^d)$.*

Proof. Let R be an additively written group $G(p^m, p^n, p^d)$ with generators a, b and c satisfying the relations $|a| = p^m$, $|b| = p^n$, $|c| = p^d$, $b^{-1}ab = ac$ and $a^{-1}ca = b^{-1}cb = c$. Then $G = \langle a \rangle + \langle b \rangle + \langle c \rangle$ and each element $x \in R$ is uniquely written in the form $x = ax_1 + bx_2 + cx_3$ with coefficients $0 \leq x_1 < p^m$, $0 \leq x_2 < p^n$ and $0 \leq x_3 < p^d$. In order to define a multiplication "$\cdot$" on R in such a manner that $(R, +, \cdot)$ is a local nearring.

Assume that $1 \leq d \leq n \leq m$ and let the mappings from Corollary 5 be defined by the congruences $\alpha(x) \equiv 0 \pmod{p^m}$, $\beta(x) \equiv x_1 \pmod{p^n}$ and $\gamma(x) \equiv 0 \pmod{p^d}$ for each $x \in G$. Then

$$x \cdot y = ax_1y_1 + b(x_2y_1 + x_1y_2) + c\Big(- x_1x_2\binom{y_1}{2} + x_3y_1 + x_1^2y_3\Big).$$

It suffices to show that the mappings $\alpha : G \to \mathbb{Z}_{p^m}$, $\beta : G \to \mathbb{Z}_{p^n}$ and $\gamma : G \to \mathbb{Z}_{p^d}$ with respect to the multiplication "$\cdot$" satisfy statements (0)–(5) of Corollary 5.

Indeed, $\alpha(0) \equiv 0 \pmod{p^m}$, $\beta(0) \equiv 0 \pmod{p^n}$ and $\gamma(0) \equiv 0 \pmod{p^d}$ by the definition. Since $0 \cdot y = a \cdot 0 + b \cdot 0 + c \cdot 0 = 0$ for each $y \in G$, this implies that a multiplication "$\cdot$" is zero-symmetric and so, proving statement (0) of Corollary 5. Indeed, we have $\alpha(x) \equiv 0 \pmod{p}$ and $x_1 \equiv 0 \pmod{p}$, if $\beta(x) \equiv 0 \pmod{p}$, so that statements (1) and (2) of Corollary 5 hold. Clearly, we derive statements (3)–(5) of Corollary 5. □

As corollary we have the following assertion.

Corollary 6. *Each group $G(p^m, p^n, p^d)$ is the additive group of a nearring with identity.*

REFERENCES

[1] Amberg B., Hubert P., Sysak Ya. *Local near-rings with dihedral multiplicative group*. J. Algebra 2004, **273**, 700–717.

[2] Feigelstock S. *Additive groups of local near-rings*. Comm. Algebra 2006, **34**, 743–747.

[3] Maxson C.J. *On local near-rings*. Math. Z. 1968, **106**, 197–205.

[4] Maxson C.J. *On the construction of finite local near-rings (I): on non-cyclic abelian p-groups*. Q. J. Math. 1970, **21**, 449–457.

[5] Maxson C.J. *On the construction of finite local near-rings (II): on non-abelian p-groups*. Q. J. Math. 1971, **22**, 65–72.

[6] Meldrum J.D.P. Near-rings and their links with groups. Pitman Publishing Limited, London, 1985, 273 p.

[7] Menegazzo F. *Automorphisms of p-groups with cyclic commutator subgroup*. Rend. Sem. Mat. Univ. Padova 1993, **90**, 81–101.

[8] Pilz G. Near-rings. The theory and its applications. North Holland, Amsterdam, 1977.

[9] Raievska I.Yu., Raievska M.Yu., Sysak Ya.P. *Local nearrings on nonmetacyclic Miller-Moreno groups*. Bulletin Taras Shevchenko National University of Kyiv. Series: Physics and Mathematics 2012, **3**, 39–46. (in Ukrainian)

[10] Raievska M.Yu., Sysak Ya.P. *On local near-rings with Miller-Moreno multiplicative group*. Ukrainian Math. J. 2012, **64** (6), 930–937. doi:10.1007/s11253-012-0688-z (translation of Ukrain. Mat. Zh. 2012, **64** (6), 811–818. (in Ukrainian))

[11] Sysak Ya.P. *Products of groups and local nearrings*. Note Mat. 2008, **28** (2), 179–213.

Received 23.09.2019

Раєвська І.Ю., Раєвська М.Ю. *Локальні майже-кільця на скінченних неабелевих неметациклічних 2-породжених p-групах* // Карпатські матем. публ. — 2020. — Т.12, №1. — С. 199–207.

Доведено, що для $p > 2$ кожна скінченна неметациклічна 2-породжена p-група зі ступенем нільпотентності рівним 2 з циклічним комутантом є адитивною групою деякого локального майже-кільця, зокрема, майже-кільця з одиницею. Показано, що підгрупа всіх необоротних елементів цього локального майже-кільця має індекс p в його адитивній групі.

Ключові слова і фрази: скінченна p-группа, локальне майже-кільце.