Algebra and Discrete Mathematics RESEARCH ARTICLE
Volume **22** (2016). Number 1, pp. 129–152

Finite local nearrings with split metacyclic additive group

I. Yu. Raievska, M. Yu. Raievska and Ya. P. Sysak

Communicated by Yu. A. Drozd

Abstract. In the paper the split metacyclic groups which are the additive groups of finite local nearrings are classified.

Introduction

Nearrings are generalized rings in the sense that the addition need not be commutative and only one distributive law is assumed. For a detailed account of basic concepts concerning the nearrings we refer the reader to the books [12] or [13]. A nearring R with an identity is called local if the set of all non-invertible elements of R forms a subgroup of the additive group of R.

Maxson [9] described all non-isomorphic zero-symmetric local nearrings with non-cyclic additive group of order p^2 which are not nearfields. He also shown in [10] 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. This result was extended to infinite abelian p-groups of finite exponent [5].

However in the case of finite non-abelian p-groups the situation is different. For instance, neither a generalized quaternion group nor a non-abelian group of order 8 can be the additive group of a local nearring [11] (see also [10]).

2010 MSC: 16Y30.
Key words and phrases: nearring with identity, local nearring, additive group, split metacyclic group.

In [14] all minimal non-abelian groups (the Miller–Moreno groups in other words) which are the additive groups of finite nearrings with identity are classified. In this paper the split metacyclic groups which appear as the additive groups of finite local nearrings are considered and their full classification is given.

1. Preliminaries

First we recall some notions and facts concerning nearrings and metacyclic groups.

Definition 1. A (left) nearring is a set $R = (R, +, \cdot)$ with two binary operations, addition " + " and multiplication " $\cdot$ ", such that
1) $(R, +)$ is a group with neutral element 0,
2) $(R, \cdot)$ is a semigroup, and
3) $x(y + z) = xy + xz$ for all x, y, $z \in R$.

The group $(R, +)$ of a nearring R is denoted by R^+ and called the *additive group* of R. It is easy to see that for each subgroup M of R^+ and for each element $x \in R$ the set $xM = \{x \cdot y | y \in M\}$ is a subgroup of R^+ and in particular $x \cdot 0 = 0$. If in addition $0 \cdot x = 0$ for all $x \in R$, then the nearring R is called *zero-symmetric*. In general, the set of all $y \in R$ with $0 \cdot y = 0$ is a subnearring called the *zero-symmetric part* of R. Furthermore, R is a *nearring with an identity* i if the semigroup $(R, \cdot)$ is a monoid with identity element i. In the latter case the group of all invertible elements of the monoid $(R, \cdot)$ is denoted by R^* and called the *multiplicative group* of R. A subgroup M of R^+ is called R^*-*invariant*, if $rM \leqslant M$ for each $r \in R^*$, and (R, R)-*subgroup*, if $xMy \subseteq M$ for arbitrary x, $y \in R$.

As usual, for every element $r \in R$ and each integer $n \in \mathbb{Z}$ we define the element rn of R as follows:

$$rn = \begin{cases} \underbrace{r + \cdots + r}_{n \text{ times}} & \text{if } n > 0, \\ 0 & \text{if } n = 0, \\ \underbrace{(-r) + \cdots + (-r)}_{-n \text{ times}} & \text{if } n < 0. \end{cases}$$

Then $r(m + n) = rm + rn$ for any integers m and n, so that we can identify the neutral element 0 with integer 0. On the other hand, if i is an identity of R, then we will not identify i with integer 1, because in general $(in)r \neq rn = r(in)$ for $n \neq 1$. Thus, to avoid a confusion, we do not use a notation nr with an integer n.

The following two simple assertions are well-known.

Lemma 1. *Let R be a finite nearring R with identity i. Then the exponent of the additive group R^+ is equal to the additive order of i which coincides with additive order of every element of the multiplicative group R^*.*

Proof. Indeed, if $ik = 0$ for some positive integer k, then for each $x \in R$ we have $xk = (xi)k = x(ik) = x0 = 0$. On the other hand, if $y \in R^*$ and $yl = 0$ for a positive integer l, then $il = y^{-1}(yl) = 0$, so that the additive orders of r and i coincide. □

Lemma 2. *Let R be a nearring with identity i and $a \in R^*$. For any elements $x, y \in R$ we put $x \circ y = xa^{-1}y$. Then with respect to the operations "$+$" and "$\circ$" the set $(R, +, \circ)$ is a nearring with identity a which is isomorphic to R.*

Proof. It can be easily verified that the operation "$\circ$" is associative and left distributive with respect to the addition and the mapping $r \mapsto ar$ determines an isomorphism of the nearring R onto $(R, +, \circ)$. □

Definition 2. [8] A nearring R with identity is said to be local if the set $L = R \setminus R^*$ of all non-invertible elements of R is a subgroup of R^+.

As it was shown in [8], Theorem 7.4, the additive group of a finite local nearring is a p-group for a prime p.

The following lemma characterizes the main properties of local nearrings (see [1], Lemma 3.2).

Lemma 3. *Let R be a local nearring with an identity i and L the subgroup of all non-invertible elements of R. Then the following statements hold:*

1) *L is an (R, R)-subgroup of R^+;*
2) *each proper R^*-invariant subgroup of R^+ is contained in L;*
3) *the set $i + L$ forms a subgroup of the multiplicative group R^*.*

Recall that a group G is called *metacyclic* if there exists a cyclic normal subgroup $\langle a \rangle$ such that the factor-group $G/\langle a \rangle$ is cyclic. For a prime p, a metacyclic p-group G is *split* if and only if it is decomposed in a semidirect product $G = \langle a \rangle \rtimes \langle b \rangle$ of the cyclic normal subgroup $\langle a \rangle$ and a cyclic subgroup $\langle b \rangle$.

The following useful characterization of non-abelian split metacyclic p-groups is due to B. King (see [7], Theorem 3.2 and Proposition 4.10).

Proposition 1. *Let $G = \langle a \rangle \rtimes \langle b \rangle$ be a non-abelian split metacyclic p-group with $a^{p^m} = b^{p^n} = 1$ for some positive integers m and n. Then the exponent of G is equal to* $\max\{p^m, p^n\}$ *and one of the following statements holds*:

I. $b^{-1}ab = a^{1+p^{m-r}}$ *with* $1 \leqslant r < \min\{m, n+1\}$ *and* $r < m-1$ *for* $p = 2$;

II. $p = 2$ *and* $b^{-1}ab = a^{-1+2^{m-r}}$ *with* $0 \leqslant r < \min\{m-1, n+1\}$.

Henceforth, a group G satisfying one of statements I or II of Proposition 1 will be denoted by $G(p^m, p^n, r)$ or $G(2^m, 2^n, -r)$, respectively. Furthermore, for any integers v and $w \geqslant 0$ we put $j(v, 0) = 0$ and $j(v, w) = 1 + v + \ldots + v^{w-1}$ for $w \geqslant 1$.

Lemma 4. *Let p be a prime and t, u positive integers. If d, k and l are non-negative integers, then the following statements hold*:

1) $j(t^d, k) + j(t^d, l)t^{dk} = j(t^d, k+l)$;

2) *if* $t \equiv 1 \pmod{p^u}$, *then*

$$t^d \equiv t^{dt} \equiv 1 + d(t-1) \pmod{p^{2u}}$$

and

$$j(t^d, k) \equiv k + \binom{k}{2} d(t-1) \pmod{p^{2u}};$$

3) *if* $t \equiv -1 \pmod{2^u}$, *then*

$$t^{d2^k} \equiv \begin{cases} (-1)^d(1 - d(t+1)) \pmod{2^{2u}} & \text{if } k = 0, \\ 1 - d(t+1)2^k \pmod{2^{2u+k-1}} & \text{if } k > 0, \end{cases}$$

and

$$j(t^d, k) \equiv \begin{cases} \frac{1-(-1)^k}{2} + \frac{(2k-1)(-1)^k+1}{4} d(t+1) & \pmod{2^{2u}} \\ & \text{if } d \equiv 1 \pmod{2}, \\ k - \binom{k}{2} d(t-1) & \pmod{2^{2u}} \\ & \text{if } d \equiv 0 \pmod{2}. \end{cases}$$

Proof. Since all statements are obvious for $d = 0$, we assume that $d > 0$. Clearly statement 1) is trivial if $kl = 0$. In the other case we have

$$\begin{aligned} j(t^d, k) + j(t^d, l)t^{dk} &= (1 + t^d + \cdots + t^{d(k-1)}) + (1 + t^d + \cdots + t^{d(l-1)})t^{dk} \\ &= 1 + t^d + \cdots + t^{d(k+l-1)} = j(t^d, k+l), \end{aligned}$$

as desired.

Statement 2) is easily proved by induction on d. Indeed, we have

$$t^{d-1} \equiv 1 + (d-1)(t-1) \pmod{p^{2u}}$$

and so $t^{d-1}(t-1) \equiv t-1 \pmod{p^{2u}}$. Therefore

$$t^d \equiv t^{d-1} + t - 1 \equiv 1 + d(t-1) \pmod{p^{2u}}.$$

This implies

$$t^{dt} - t^d \equiv 1 + dt(t-1) - (1 + d(t-1)) = d(t-1)^2 \equiv 0 \pmod{p^{2u}}$$

and thus $t^{dt} \equiv t^d \pmod{p^{2u}}$. Furthermore,

$$j(t^d, k) = 1 + t^d + \cdots + t^{d(k-1)} \equiv 1 + (1 + d(t-1)) + \cdots + (1 + d(k-1)(t-1))$$

$$= k + (1 + \cdots + (k-1))d(t-1) = k + \binom{k}{2} d(t-1) \pmod{p^{2u}},$$

which proves statement 2).

For proving statement 3), we put $v = t+1$. Then $v \equiv 0 \pmod{2^u}$ and

$$t^{d2^k} = (-1+v)^{d2^k} = (-1)^{d2^k} + (-1)^{d2^k-1}\binom{d2^k}{1} v$$

$$+(-1)^{d2^k-2}\binom{d2^k}{2} v^2 + \cdots + v^{d2^k}.$$

Since $\binom{d2^k}{2} \equiv 0 \pmod{2^{k-1}}$, the congruence for t^{d2^k} follows from this equality. Therefore

$$j(t^d, k) = 1 + t^d + \cdots + t^{(k-1)d} \equiv 1 + (-1)^d(1-v)$$

$$+(-1)^{2d}(1-2dv) + \cdots + (-1)^{(k-1)d}(1-(k-1)dv) \pmod{2^{2u}}.$$

In particular, for odd d we have

$$j(t^d, k) \equiv 1 + (-1+dv) + (1-2dv) + \cdots + ((-1)^{k-1} + (-1)^{k-2}(k-1)dv)$$

$$= \frac{1-(-1)^k}{2} + (1 - 2 + 3 - \cdots + (-1)^{k-2}(k-1))dv$$

$$= \frac{1-(-1)^k}{2} + \frac{(2k-1)(-1)^k + 1}{4} dv \pmod{2^{2u}}.$$

If d is even, then

$$j(t^d,k) \equiv 1+(1-dv)+(1-2dv)+\cdots+(1-(k-1)dv)$$

$$= k-(1+2+\cdots+(k-1))dv = k-\binom{k}{2}dv \pmod{2^{2u}},$$

as claimed. □

Lemma 5. *Let G be an additively written group whose elements a and b satisfy the relation $a+b=b+as$ for some natural number s. If t is the least natural number such that $ast=0$, then for any non-negative integers d, k and u the equalities $au+bd=bd+as^du$, $bd+au=aut^d+bd$, $(au+bd)k=auj(t^d,k)+bdk$ and $(bd+au)k=bdk+auj(s^d,k)$ hold.*

Proof. Since $-b+a+b=as$ and $-b+at+b=(-b+a+b)t=ast=a$, we have $b+a=at+b$ and so $b+au=atu+b$. By induction on d, we derive $au+bd=bd+as^du$ and $bd+au=at^du+bd$. Therefore

$$(au+bd)k = au(1+t^d+\ldots+t^{d(k-1)})+bdk = auj(t^d,k)+bdk$$

and hence

$$(bd+au)k = bdk+au(1+s^d+\ldots+s^{d(k-1)}) = bdk+auj(s^d,k).$$

□

The following proposition on the automorphism group of a non-abelian split metacyclic p-group can be found in [2], Theorem 3.1, for $p>2$ and in [4], Theorem 3.5, for $p=2$.

Proposition 2. *Let G be a split non-abelian metacyclic p-group and let S be a Sylow p-subgroup of the automorphism group Aut(G). Then S is a normal subgroup of index $p-1$ in Aut(G). In particular, if $p=2$, then Aut(G) is a 2-group.*

An information about orbits of the group G under the action of its automorphism group $\mathrm{Aut}(G)$ is given by the following lemma.

Lemma 6. *Let $G=G(p^m,p^n,r)$ with $m\leqslant n+r$, $A=$ Aut(G) and let $\langle x\rangle$ be a cyclic subgroup of G. Then the following statements hold:*

1) *if $\langle x\rangle$ is a normal subgroup of order p^m in G, then*

$$|x^A| \leqslant p^{2m-r-1}(p-1);$$

2) *if* $p > 2$, $m \leqslant n$ *and* $\langle x\rangle$ *is a non-normal subgroup of order* p^n, *then* $x^{-1} \notin x^A$.

Proof. If $G = \langle a\rangle \rtimes \langle b\rangle$ with $b^{-1}ab = a^{1+p^{m-r}}$ and $\langle x\rangle$ is a normal subgroup of order p^m in G, then either $\langle a\rangle \cap \langle x\rangle = 1$ and so $\langle x\rangle$ centralizes the subgroup $\langle a\rangle$, or $a^{p^{m-1}} \in \langle x\rangle$. Since $G' = \langle a^{p^{m-r}}\rangle$ is a characteristic subgroup of G, it follows that in the first case $\langle a\rangle \cap \langle x^\alpha\rangle = 1$ for each $\alpha \in A$. Hence $x^A \subseteq C_G(a) = \langle a\rangle \times \langle b^{p^r}\rangle$ and so $|x^A| \leqslant p^{2m-r-1}(p-1)$. In the second case $G = \langle x\rangle \rtimes \langle b\rangle$ and so $G' = \langle a^{p^{m-r}}\rangle \leqslant \langle x\rangle$. Then $|\langle x\rangle\langle x^\alpha\rangle| = \frac{|x||x^\alpha|}{|\langle x\rangle\cap\langle x\rangle^\alpha|} \leqslant p^{2m-r}$, whence $\langle x\rangle\langle x^\alpha\rangle \leqslant \langle x\rangle \rtimes \langle b^{p^{n+r-m}}\rangle$ and in particular $x^\alpha \in \langle x\rangle \rtimes \langle b^{p^{n+r-m}}\rangle$. Taking into account that the number of elements of order p^m in $\langle x\rangle$ is equal to $p^{m-1}(p-1)$, we have $|x^A| \leqslant p^{2m-r-1}(p-1)$, which proves statement 1).

Now let $p > 2$, $m \leqslant n$ and let $\langle x\rangle$ be a non-normal subgroup of order p^n in G. Since $G' = \langle a^{p^{m-r}}\rangle$, it follows that $\langle a\rangle \cap \langle x\rangle = \langle a^{p^s}\rangle$ for some integer s such that $m \geqslant s > m-r$ and so $\langle a^{p^s}\rangle = \langle x^{p^{n-m+s}}\rangle$. Therefore $x = a^u b^{vp^{m-s}}$ for some integers u and v with $(v,p) = 1$ and hence $[a,x] = [a, b^{vp^{m-s}}] = a^{wp^{2m-r-s}}$, where

$$w = \frac{(1+p^{m-r})^{vp^{m-s}-1}}{p^{2m-r-s}}$$

and in particular $(w,p) = 1$.

Assume that $x^\alpha = x^{-1}$ for some automorphism $\alpha \in A$. As it was shown above, $a^\alpha \in \langle a\rangle \rtimes \langle b^{p^{n+r-m}}\rangle$, whence $a^\alpha = a^k b^{lp^{n+r-m}}$ for some integers k and l with $(k,p) = 1$. Furthermore, $\langle a^{p^{m-r}}\rangle^\alpha = \langle a^{p^{m-r}}\rangle$ and so $(a^{p^{m-r}})^\alpha = (a^k b^{lp^{n+r-m}})^{p^{m-r}} = a^{kp^{m-r}} b^{lp^n} = a^{kp^{m-r}}$. Thus $(a^{p^{m-r}})^\alpha = a^{kp^{m-r}}$. On the other hand, because of $m \leqslant n$ it follows that $b^{lp^{n+r-m}} \in \langle b^r\rangle \leqslant Z(G)$. Therefore $a^{kwp^{m-r}} = (a^{wp^{m-r}})^\alpha = [a,x]^\alpha = [a^\alpha, x^{-1}] = [a^k b^{lp^{n+r-m}}, x^{-1}] = [a^k, x^{-1}] = [a, x^{-1}]^k = ([a,x]^{-k})^{x^{-1}} = (a^{-kwp^{m-r}})^{x^{-1}}$ and hence $(a^{kwp^{m-r}})^x = a^{-kwp^{m-r}}$. However for $p > 2$ the last equality holds only in the case where $a^{kwp^{m-r}} = 1$. Since $(kw,p) = 1$, this means that $a^{p^{m-r}} = 1$, contrary to the hypothesis of the lemma. Therefore, $x^{-1} \notin x^A$, as claimed in statement 2). □

Lemma 7. *Let* R *be a local nearring whose additive group* R^+ *is a split non-abelian metacyclic* p*-group and let* L *be the subgroup of all non-invertible elements of* R*. Then* L *is a subgroup of index* p *in* R^+.

Proof. Indeed, we have the index $|R^+ : L| = p^k$ for some $k \geqslant 1$ and so $|R| = p^k|L|$. Since $R = R^* \cup L$ with $R^* \cap L = \varnothing$, it follows that

$|R^*| = p^k|L| - |L| = (p^k - 1)|L|$ and thus the order of R^* is divisible by $p^k - 1$. On the other hand, for each element $r \in R^*$ the mapping $x \mapsto rx$ with $x \in R$ is an automorphism of R^+, because of $r(x + y) = rx + ry$ for all x, $y \in R$. Therefore R^* can be viewed as a subgroup of $\mathrm{Aut}(R^+)$. Furthermore, it follows from Proposition 2 that the order of $\mathrm{Aut}(R^+)$ is divisible by $p^k - 1$ only if $k = 1$. Hence $|R^+ : L| = p$, as desired. □

As a direct consequence of Lemmas 1, 2 and 7 we have the following assertion.

Corollary 1. *Let R be a local nearring whose additive group R^+ is a non-abelian split metacyclic p-group. Then the group R^+ is generated by elements a and b of orders p^m and p^n, respectively, one of which coincides with identity element of R and $a+b = b+a(1+p^{m-r})$, if R^+ is isomorphic to the group $G(p^m, p^n, r)$, and $a+b = b+a(-1+2^{m-r})$, if R^+ is isomorphic to the group $G(2^m, 2^n, -r)$.*

2. Nearrings with identity on non-abelian split metacyclic p-groups

Let R be a nearring with identity whose additive group R^+ is a split non-abelian metacyclic p-group with $p \geqslant 2$. Then $R^+ = \langle a \rangle + \langle b \rangle$ for some elements a and b of R satisfying the relations $ap^m = bp^n = 0$ and $b+a = at+b$ with $(p, t) = 1$. In particular, each element $x \in R$ is uniquely written in the form $x = ax_1 + bx_2$ with coefficients $0 \leqslant x_1 < p^m$ and $0 \leqslant x_2 < p^n$. In this section we will consider the cases when at least one of the elements a or b is invertible in R, i. e. it belongs to the multiplicative group R^*.

Assume first that $a \in R^*$. Then R^+ is a group of exponent p^m by Lemma 1 and so $m \geqslant n$. Furthermore, according to Lemma 2, without loss of generality we can assume that a is an identity of R, i. e. $ax = xa = x$ for each $x \in R$. Moreover, for each $x \in R$ there exist coefficients $\alpha(x)$ and $\beta(x)$ such that $xb = a\alpha(x) + b\beta(x)$. It is clear that they are uniquely defined modulo p^m and p^n, respectively, so that some mappings $\alpha : R \to Z_{p^m}$ and $\beta : R \to Z_{p^n}$ are determined.

Lemma 8. *Let $x = ax_1 + bx_2$ and $y = ay_1 + by_2$ be elements of the nearring R. If a is an identity of R, then $m \geqslant n$ and the following statements hold*:

(0) $\alpha(0) = \beta(0) = 0$ *if and only if the nearring R is zero-symmetric*;
(1) $\alpha(a) = 0$ *and* $\beta(a) = 1$;

(2) $xy = a(x_1 j(t^{x_2}, y_1) + \alpha(x) j(t^{\beta(x)}, y_2) t^{x_2 y_1}) + b(x_2 y_1 + \beta(x) y_2)$;
(3) $\alpha(x)(t^{x_2 t} - 1) \equiv x_1(t^{\beta(x)} - j(t^{x_2}, t)) \ (\bmod p^m)$;
(4) $x_2(t-1) \equiv 0 \ (\bmod p^n)$.

Proof. Since $0 \cdot a = a \cdot 0 = 0$, it follows that R is a zero-symmetric nearring if and only if $0 = 0 \cdot b = a\alpha(0) + b\beta(0)$ or equivalently $\alpha(0) = \beta(0) = 0$. Moreover, since $b = ab = a\alpha(a) + b\beta(a)$, we have $\alpha(a) = 0$ and $\beta(a) = 1$, so that statements (0) and (1) hold.

Further, using the left distributive law, we derive

$$xy = (xa)y_1 + (xb)y_2 = (ax_1 + bx_2)y_1 + (a\alpha(x) + b\beta(x))y_2.$$

Applying Lemma 5, we have also

$$(ax_1 + bx_2)y_1 = ax_1 j(t^{x_2}, y_1) + bx_2 y_1,$$

$$(a\alpha(x) + b\beta(x))y_2 = a\alpha(x) j(t^{\beta(x)}, y_2) + b\beta(x) y_2$$

and

$$bx_2 y_1 + a\alpha(x) j(t^{\beta(x)}, y_2) = a\alpha(x) j(t^{\beta(x)}, y_2) t^{x_2 y_1} + bx_2 y_1.$$

Thus

$$xy = a(x_1 j(t^{x_2}, y_1) + \alpha(x) j(t^{\beta(x)}, y_2) t^{x_2 y_1}) + b(x_2 y_1 + \beta(x) y_2)$$

and so statement (2) holds. Setting in this formula $y = at + b$, we derive

$$xy = a(x_1 j(t^{x_2}, t) + \alpha(x) t^{x_2 t}) + b(x_2 t + \beta(x)).$$

On the other hand, $y = b + a$ and so

$$xy = xb + x = a(\alpha(x) + x_1 t^{\beta(x)}) + b(x_2 + \beta(x))$$

by Lemma 5. Comparing the coefficients under a and b in the latter two expressions for xy, we get for each $x \in R$ the equalities

$$\alpha(x)(t^{x_2 t} - 1) \equiv x_1(t^{\beta(x)} - j(t^{x_2}, t)) \ (\bmod p^m)$$

and

$$x_2(t-1) \equiv 0 \ (\bmod p^n),$$

i. e. statements (3) and (4), as desired. □

Consider now the case when $b \in R^*$.

Lemma 9. *If $b \in R^*$, then $m \leqslant n$, $a \notin R^*$ and $p = 2$.*

Proof. Since b is of order p^n, the group R^+ is of exponent p^n by Lemma 1 and so $m \leqslant n$. Let A denote the automorphism group $\mathrm{Aut}(R^+)$ of R^+. Considering R^* as a subgroup of A, we have $R^*x \subseteq x^A$ for each $x \in R$ and in particular $R^* = R^*b \subseteq b^A$. If $a \in b^A$, then $a = b^\phi$ for some automorphism $\phi \in A$ and so $\langle a\rangle^\phi = \langle b\rangle$. Since the subgroup $\langle a\rangle$ is normal in R^+ and the subgroup $\langle b\rangle$ is not, the latter equality is impossible. Therefore $a \notin b^A$ and hence $a \notin R^*$.

Assume that $p > 2$. Then $-b \notin b^A$ by Lemma 6 and so $-b \notin R^*$. On the other hand, if i is an identity of R, then $b^{-1}(-b) = -(b^{-1}b) = -i$. Since $(-i)^2 = -(-i) = i$, this implies $b^{-1}(-b) = -i \in R^*$ and so $-b \in bR^* = R^*$. This contradiction shows that $p = 2$ and completes the proof. □

As above, according to Lemma 2, in the case $b \in R^*$ we can assume that b is an identity of R and for each $x \in R$ there exist the coefficients $\alpha(x)$ and $\beta(x)$ which are uniquely determined modulo 2^m and 2^n, respectively, such that $xa = a\alpha(x) + b\beta(x)$.

Lemma 10. *Let $x = ax_1 + bx_2$ and $y = ay_1 + by_2$ be elements of the nearring R. If b is an identity of R, then $p = 2$, $m \leqslant n$ and the following statements hold*:

(0) $\alpha(0) = \beta(0) = 0$ *if and only if the nearring R is zero-symmetric*;
(1) $\alpha(b) = 1$ *and* $\beta(b) = 0$;
(2) $xy = a(\alpha(x)j(t^{\beta(x)}, y_1) + x_1 j(t^{x_2}, y_2)t^{\beta(x)y_1}) + b(\beta(x)y_1 + x_2y_2)$;
(3) $\alpha(x)(j(t^{\beta(x)}, t) - t^{x_2}) \equiv x_1(1 - t^{\beta(x)t}) \pmod{2^m}$;
(4) $\beta(x)(t - 1) \equiv 0 \pmod{2^n}$.

Proof. Observe first that $p = 2$ and $m \leqslant n$ by Lemma 9. Since $0 \cdot b = b \cdot 0 = 0$, the nearring R is zero-symmetric if and only if $0 = 0 \cdot a = a\alpha(0) + b\beta(0)$, whence $\alpha(0) = \beta(0) = 0$. Similarly, the equality $a = ba = a\alpha(b) + b\beta(b)$ implies that $\alpha(b) = 1$ and $\beta(b) = 0$, i. e. statements (0) and (1) hold. Further, applying the left distributive law, we obtain

$$xy = (xa)y_1 + (xb)y_2 = (a\alpha(x) + b\beta(x))y_1 + (ax_1 + bx_2)y_2.$$

Using Lemma 5, we have also

$$(a\alpha(x) + b\beta(x))y_1 = a\alpha(x)j(t^{\beta(x)}, y_1) + b\beta(x)y_1,$$

$$(ax_1 + bx_2)y_2 = ax_1 j(t^{x_2}, y_2) + bx_2y_2$$

and

$$b\beta(x)y_1 + ax_1j(t^{x_2}, y_2) = ax_1j(t^{x_2}, y_2)t^{\beta(x)y_1} + b\beta(x)y_1.$$

Therefore

$$xy = a(\alpha(x)j(t^{\beta(x)}, y_1) + x_1j(t^{x_2}, y_2)t^{\beta(x)y_1}) \\ + b(\beta(x)y_1 + x_2y_2),$$

which proves statement (2). Substituting $y = at + b$ in this equality, we get

$$xy = a(\alpha(x)j(t^{\beta(x)}, t) + x_1t^{\beta(x)t}) + b(x_2 + \beta(x)t).$$

On the other hand, $y = b + a$ and thus

$$xy = x + xa = a(x_1 + \alpha(x)t^{x_2}) + b(x_2 + \beta(x)).$$

Comparing the coefficients under a and b in the latter two expressions for xy, we obtain the congruences

$$\alpha(x)j(t^{\beta(x)}, t) + x_1t^{\beta(x)t} \equiv x_1 + \alpha(x)t^{x_2} \pmod{2^m}$$

and

$$x_2 + \beta(x)t \equiv x_2 + \beta(x) \pmod{2^n},$$

from which statements (3) and (4) follow directly. □

2.1. Nearrings with identity on the group $G(p^m, p^n, r)$

Assume now that m, n and r are positive integers satisfying statement I of Proposition 1, and let t be the least natural number such that $(1 + p^{m-r})t \equiv 1 \pmod{p^m}$. It is easy to see that $t = 1 + hp^{m-r}$ for some h with $0 < h < p^r$ and $(h, p) = 1$.

The following two lemmas describe the multiplication in a nearring R whose additive group R^+ is isomorphic to the group $G(p^m, p^n, r)$, i. e. R^+ is generated by elements a and b satisfying the relations $ap^m = bp^n = 0$ and $b + a = at + b$. As it was mentioned above, we restrict ourselves to the cases when one of the generators a or b is an identity of R. In what follows $x = ax_1 + bx_2$ and $y = ay_1 + by_2$ are arbitrary elements of R.

Lemma 11. *If a is an identity of R, then $m \geqslant n + r \geqslant 2r$ and*

$$xy = a(x_1y_1 + \alpha(x)y_2 - x_1x_2\binom{y_1}{2}p^{m-r}) + b(x_2y_1 + \beta(x)y_2).$$

Moreover, the following statements hold:

(1) $\alpha(x) \equiv 0 \pmod{p^{m-n}}$;
(2) *either* $x_1(\beta(x) - 1) \equiv 0 \pmod{p^r}$ *or* $p = 2$, $m > 2r$ *and* $x_1(\beta(x) - 1) \equiv 0 \pmod{2^r}$;
(3) $\alpha(xy) = x_1\alpha(y) + \alpha(x)\beta(y) - x_1x_2\binom{\alpha(y)}{2}p^{m-r}$;
(4) $\beta(xy) = x_2\alpha(y) + \beta(x)\beta(y)$.

Proof. Since $x_2(t-1) \equiv 0 \pmod{p^n}$ by statement (4) of Lemma 8 and $t - 1 = hp^{m-r}$ with $(h, p) = 1$, we have $m - r \geqslant n$. Therefore

$$m \geqslant n + r \geqslant 2r \tag{i}$$

and in particular $2(m - r) \geqslant m$. Furthermore, since $(1 + p^{m-r})t \equiv 1 \pmod{p^m}$, it follows that

$$t - 1 \equiv -p^{m-r} \pmod{p^m}. \tag{ii}$$

Using this and statement 2) of Lemma 4, we obtain the congruences

$$j(t^{x_2}, y_1) \equiv y_1 - x_2\binom{y_1}{2}p^{m-r} \pmod{p^m}, \tag{iii}$$

$$j(t^{\beta(x)}, y_2) \equiv y_2 - \beta(x)\binom{y_2}{2}p^{m-r} \pmod{p^m} \tag{iv}$$

and

$$t^{x_2y_1} \equiv 1 - x_2y_1p^{m-r} \pmod{p^m}. \tag{v}$$

Substituting now in formula (2) of Lemma 8 instead of the left parts of congruences (iii)–(v) their right parts, we derive the equality

$$\begin{aligned} xy = a((x_1y_1 + \alpha(x)y_2) - (x_1x_2\tbinom{y_1}{2} + \alpha(x)\beta(x)\tbinom{y_2}{2} \\ + \alpha(x)x_2y_1y_2)p^{m-r}) + b(x_2y_1 + \beta(x)y_2). \end{aligned} \tag{$*$}$$

Setting in this equality $y = bp^n = 0$, we have

$$0 = x(bp^n) = a(\alpha(x)p^n - \alpha(x)\beta(x)\binom{p^n}{2}p^{m-r})$$

$$= a\alpha(x)p^n(1 - \beta(x)\binom{p^n}{2}p^{m-r-n}).$$

As $m-r \geqslant 1$ for $p>2$ and $m-r \geqslant 2$ for $p=2$, it follows that $1-\beta(x)\binom{p^n}{2}p^{m-r-n} \equiv 1 \ (\bmod p\,)$ and so $a\alpha(x)p^n = 0$. Therefore

$$\text{(vi)} \qquad \alpha(x) \equiv 0 \ (\bmod p^{m-n}),$$

i.e. statement (1) holds. Moreover, since $m-n \geqslant r$ by (i), it follows that $a\alpha(x)p^{m-r} = 0$ and hence equality (*) can be rewritten in the form

$$xy = a(x_1y_1 + \alpha(x)y_2 - x_1x_2\binom{y_1}{2}p^{m-r}) + b(x_2y_1 + \beta(x)y_2),$$

as claimed.

Replacing in this equality y by $yb = a\alpha(y) + b\beta(y)$ and taking into account that $x(yb) = (xy)b = a\alpha(xy) + b\beta(xy)$, we obtain two expressions for the element $x(yb)$. Comparing the coefficients at a and b in these expressions, we derive the equalities

$$\alpha(xy) = x_1\alpha(y) + \alpha(x)\beta(y) - x_1x_2\binom{\alpha(y)}{2}p^{m-r}$$

and

$$\beta(xy) = x_2\alpha(y) + \beta(x)\beta(y)$$

of statements (3) and (4) of the lemma.

Furthermore, using statement 2) of Lemma 4, we have also

$$\text{(vii)} \qquad t^{x_2t} \equiv 1 - x_2p^{m-r} \ (\bmod p^m),$$

$$\text{(viii)} \qquad t^{\beta(x)} \equiv 1 - \beta(x)p^{m-r} \ (\bmod p^m)$$

and

$$\text{(ix)} \quad j(t^{x_2}, t) \equiv \begin{cases} 1 - p^{m-r} & (\bmod p^m) \quad \text{if} \quad p>2, \\ 1 - 2^{m-r}(1 - x_22^{m-r-1}) & (\bmod 2^m) \quad \text{if} \quad p=2. \end{cases}$$

Substituting the right parts of congruences (vi)–(viii) in congruence (3) of Lemma 8, we get the congruences

$$\text{(x)} \qquad \alpha(x)x_2 \equiv x_1(\beta(x) - 1) \ (\bmod p^r\,)$$

for $p>2$ and

$$\text{(xi)} \qquad \alpha(x)x_2 \equiv x_1(\beta(x) - 1 + x_22^{m-r-1}) \ (\bmod 2^r\,)$$

for $p=2$. Since $m-n \geqslant r$ by (i), it follows from conditions (vi), (x) and (xi) that $x_1(\beta(x)-1) \equiv 0 \ (\bmod p^r\,)$ for $p>2$ and $x_1(\beta(x)-1+x_22^{m-r-1}) \equiv 0 \ (\bmod 2^r\,)$ for $p=2$. In the latter case $m>2r$ and this implies $x_1(\beta(x)-1) \equiv 0 \ (\bmod 2^r\,)$, so that statement (2) holds. □

Lemma 12. *If b is an identity of R, then $p = 2 < m \leqslant n$, $r = 1$ and*

$$xy = a(\alpha(x)y_1 + x_1 j(t^{x_2}, y_2)) + b(\beta(x)y_1 + x_2y_2).$$

Moreover, the following statements hold:

(0) $\alpha(0) = \beta(0) = 0$;
(1) $\beta(x) \equiv 0 \pmod{2^{n-m+1}}$;
(2) $\alpha(x)(1 - x_2) \equiv 0 \pmod{2}$;
(3) $\alpha(xy) = \alpha(x)\alpha(y) + x_1 j(t^{x_2}, \beta(y))$;
(4) $\beta(xy) = \beta(x)\alpha(y) + x_2\beta(y)$.

Proof. It follows from Lemma 10 that $p = 2$ and $m \leqslant n$. Furthermore, statement (4) of this lemma and the equality $t-1 = h2^{m-r}$ with $(h, 2) = 1$ imply that

$$\beta(x) \equiv 0 \pmod{2^{n-m+r}}.$$

Therefore it follows from statement 2) of Lemma 4 that for each integer $k \geqslant 0$ the congruences

$$t^{\beta(x)k} \equiv 1 \pmod{2^n} \tag{i}$$

and

$$j(t^{\beta(x)}, k) \equiv k \pmod{2^n} \tag{ii}$$

hold. In particular, taking $k = y_1$ and applying these congruences to formula (2) of Lemma 10, we get for R the multiplication formula

$$xy = a(\alpha(x)y_1 + x_1 j(t^{x_2}, y_2)) + b(\beta(x)y_1 + x_2y_2), \tag{**}$$

as claimed. Furthermore, expressing the left part of the equality $x(ya) = (xy)a$ by formula (**) and taking into consideration that $ya = a\alpha(y) + b\beta(y)$ and $(xy)a = a\alpha(xy) + b\beta(xy)$, we derive the formulas for $\alpha(xy)$ and $\beta(xy)$, i. e. statements (3) and (4) of the lemma.

Next, setting $k = t$ in congruences (i) and (ii), we have

$$1 - t^{\beta(x)t} \equiv 0 \pmod{2^n} \tag{iii}$$

and

$$j(t^{\beta(x)}, t) - t^{x_2} \equiv t - t^{x_2} \pmod{2^n}. \tag{iv}$$

Since $m \leqslant n$, it follows from congruences (iii), (iv) and statement (3) of Lemma 10 that

$$\alpha(x)(t - t^{x_2}) \equiv 0 \pmod{2^m}. \tag{v}$$

On the other hand,

$$t^{x_2} \equiv 1 + x_2 h 2^{m-r} \ (\mod 2^{2(m-r)}\ )$$

by statement 2) of Lemma 4 and hence

$$\text{(vi)} \qquad t - t^{x_2} \equiv (1 - x_2) h 2^{m-r} \ (\mod 2^{2(m-r)}\ ).$$

Therefore congruences (v) and (vi) imply that

$$\alpha(x)(1 - x_2) \equiv 0 \ (\mod 2^{\min\{r,m-r\}}\ ).$$

In particular, $\alpha(-b)(1 + 1) \equiv 0$ (mod $2^{\min\{r,m-r\}}$) and hence

$$\text{(vii)} \qquad \alpha(-b) \equiv 0 \ (\mod 2^{\min\{r,m-r\}-1}\ ).$$

Finally, since $b = (-b)^2$ and $\alpha(b) = 1$ by statement (1) of Lemma 10, it follows that $\alpha((-b)^2) = 1$. However, $\alpha((-b)^2) = \alpha(-b)^2$ by statement (3) of the lemma, so that $\alpha(-b) \equiv \pm 1$ (mod 2). Comparing this congruence with congruence (vii), we conclude that $\min\{r, m - r\} = 1$ and

$$\alpha(x)(1 - x_2) \equiv 0 \ (\mod 2\ ),$$

i. e. statement (2) of the lemma holds. Moreover, as $r < m - 1$ by Proposition 1, it follows that $r = 1$ and thus $\beta(x) \equiv 0$ (mod 2^{n-m+1}). In particular, if $x = 0$, then both $\alpha(0)$ and $\beta(0)$ are even integers. Since $\alpha(0) = \alpha(0)^2$ and $\beta(0) = \beta(0)\alpha(0)$ by statements (3) and (4) of the lemma, we get $\alpha(0) = \beta(0) = 0$. This proves statements (0) and (1) of the lemma and completes the proof. □

2.2. Nearrings with identity on the group $G(2^m, 2^n, -r)$

In this subsection the integers m, n and r satisfy statement *II* of Proposition 1 and t is the least natural number satisfying the congruence $(-1 + 2^{m-r})t \equiv 1$ (mod 2^m). It is easy to check that $t = -1 + h2^{m-r}$ for some odd h with $0 < h < 2^r$.

We describe the multiplication in a nearring R whose additive group R^+ is isomorphic to the group $G(2^m, 2^n, -r)$ and one of two generators a and b of this group is an identity of R. Recall that the generators a and b of R^+ satisfy the relations $a2^m = b2^n = 0$ and $b + a = at + b$. As before, $x = ax_1 + bx_2$ and $y = ay_1 + by_2$ denote arbitrary elements of R.

Lemma 13. *If a is an identity of R, then $m = 2$, $n = 1$ and $r = 0$, i. e., R^+ is the dihedral group of order* 8.

Proof. Since $x_2(-2+h2^{m-r}) \equiv 0(\bmod 2^n)$ by statement (4) of Lemma 8, it follows that $-1 + h2^{m-r-1} \equiv 0 \pmod{2^{n-1}}$ and so $n = 1$. Hence $0 \leqslant r \leqslant 1$ and thus either $r = 0$ and $t = -1 + 2^m$ or $r = 1$ and $t = -1 + 2^{m-1}$. But if $t = -1 + 2^m$, then $R^+ = \langle a \rangle + \langle b \rangle$ is isomorphic to the dihedral group of order 2^{m+1} and this is possible only if $m = 2$ by [6], Proposition 4.4.

Let $t = -1 + 2^{m-1}$. Then $m \geqslant 3$ and statement (3) of Lemma 8 implies that

$$\alpha(x)(t^{x_2 t} - 1) \equiv x_1(t^{\beta(x)} - j(t^{x_2}, t)) \pmod{2^m}$$

for each $x = ax_1 + bx_2$ of R. In particular, if $x = a + b$, then

$$\alpha(x)(t^t - 1) \equiv t^{\beta(x)} - j(t, t) \pmod{2^m}.$$

Moreover, $t^t \equiv -1 + 2^{m-1} \pmod{2^m}$, $j(t,t) \equiv 1 + 2^{m-1} \pmod{2^m}$ and $t^{\beta(x)} \equiv (-1)^{\beta(x)}(1 - \beta(x)2^{m-1}) \pmod{2^m}$ by statement 3) of Lemma 4. Therefore

$$\alpha(x)(-2-2^{m-1}) \equiv ((-1)^{\beta(x)} - 1) - ((-1)^{\beta(x)}\beta(x) - 1)2^{m-1} \pmod{2^m}$$

and hence either

(i) $$\alpha(x) \equiv 1 \pmod{2^{m-1}}$$

if $\beta(x) \equiv 1 \pmod 2$ or

(ii) $$\alpha(x) \equiv 2^{m-2} \pmod{2^{m-1}}$$

if $\beta(x) \equiv 0 \pmod 2$.

On the other hand, we have $b2 = 0$ and $xb = a\alpha(x) + b\beta(x)$, so that $0 = (xb)2 = a\alpha(x)j(t^{\beta(x)}, 2)$ by Lemma 5. Since

$$j(t^{\beta(x)}, 2) = 1 + t^{\beta(x)} \equiv \begin{cases} 2^{m-1} \pmod{2^m} & \text{if } \beta(x) \equiv 1 \pmod 2, \\ 2 \pmod{2^m} & \text{if } \beta(x) \equiv 0 \pmod 2, \end{cases}$$

it follows that $a\alpha(x)2^{m-1} = 0$ in the case (i) and $a\alpha(x)2 = 0$ in the case (ii). But then in both cases $a2^{m-1} = 0$ and this contradiction completes the proof. □

It should be noted that the nearrings with identity on the dihedral group of order 8 were firstly classified by J. Clay in [3]. He shown in particular that there exist exactly 7 non-isomorphic such nearrings.

Lemma 14. *If b is an identity of R, then $r+1 < m \leqslant n$, $0 \leqslant r \leqslant 1$ and*

$$xy = a(\alpha(x)y_1 + x_1 j(t^{x_2}, y_2)) + b(\beta(x)y_1 + x_2y_2).$$

Moreover, the following statements hold:
(0) $\alpha(0) = \beta(0) = 0$;
(1) $\beta(x) \equiv 0 \pmod{2^{n-1}}$;
(2) $\alpha(xy) = \begin{cases} \alpha(x)\alpha(y) + x_1\beta(y), \text{ if } m = n \text{ and } x_2 \equiv 0 \pmod 2, \text{ and} \\ \alpha(x)\alpha(y), \text{ in the other cases}; \end{cases}$
(3) $\beta(xy) = \beta(x)\alpha(y) + x_2\beta(y)$.

Proof. Note first that $r+1 < m$ by Proposition 1, $m \leqslant n$ by Lemma 9 and $\beta(x)(t-1) \equiv 0 \pmod{2^n}$ by statement (4) of Lemma 10. Since $t = -1 + h2^{m-r}$ for some odd integer h, we have $\beta(x)(-2 + h2^{m-r}) \equiv 0 \pmod{2^n}$ and so $\beta(x) \equiv 0 \pmod{2^{n-1}}$, i. e., statement (1) of the lemma holds. As $2(m-r)+n-2 \geqslant m+n-r$ and $t^{\beta(x)} \equiv 1 + h2^{m+n-r-1} \pmod{2^{m+n-r}}$ by statement 3) of Lemma 4, it follows that $t^{\beta(x)k} \equiv 1 \pmod{2^m}$ and so $j(t^{\beta(x)}, k) \equiv k \pmod{2^m}$ for every integer $k \geqslant 0$. In particular, setting $k = y_1$ and using the latter two congruences in statement (2) of Lemma 10, we can rewrite the formula for xy in the form

$$(***) \qquad xy = a(\alpha(x)y_1 + x_1 j(t^{x_2}, y_2)) + b(\beta(x)y_1 + x_2y_2),$$

as claimed.

Next, if $k = t$, then the above-mentioned congruences and statement (3) of Lemma 10 imply that $\alpha(x)(t - t^{x_2}) \equiv 0 \pmod{2^m}$. In particular, if $x = -b = b(2^n - 1)$, then $x_2 = 2^n - 1$ and $t - t^{x_2} = t - t^{2^n-1} \equiv t^2 - t^{2^n} \pmod{2^m}$. Since $t^{2^{m-1}} \equiv 1 \pmod{2^m}$ and $m \leqslant n$, it follows that $t - t^{x_2} \equiv t^2 - 1 = h2^{m-r+1}(-1 + h2^{m-r-1}) \pmod{2^m}$. Thus $\alpha(-b)2^{m-r+1} \equiv 0 \pmod{2^m}$, so that either $r = 0$ or $r \geqslant 1$ and

$$\text{(i)} \qquad \alpha(-b) \equiv 0 \pmod{2^{r-1}}.$$

Now, expressing both parts of the equality $x(ya) = (xy)a$ by formula (***) and comparing the coefficients at a and b, we derive

$$\text{(ii)} \qquad \alpha(xy) = \alpha(x)\alpha(y) + x_1 j(t^{x_2}, \beta(y))$$

and

$$\text{(iii)} \qquad \beta(xy) = \beta(x)\alpha(y) + x_2\beta(y).$$

In particular, if $x = y = -b$, then $x_1 = 0$ and from equality (ii) it follows that $\alpha((-b)^2) = \alpha(-b)^2$. As $(-b)^2 = -(-b) = b$ and $\alpha(b) = 1$ by statement (1) of Lemma 10, this implies $\alpha(-b) \equiv \pm 1 \pmod{2^m}$ and hence congruence (i) holds if and only if $r = 1$.

Finally, it follows from statement 3) of Lemma 4 that $j(t^{x_2}, \beta(x)) \equiv 0 \pmod{2^{n-1}}$ for $x_2 \equiv 0 \pmod 2$ and $j(t^{x_2}, \beta(x)) \equiv 0 \pmod{2^n}$ for $x_2 \equiv 1 \pmod 2$. Therefore statements (2) and (3) of the lemma follow directly from equalities (ii) and (iii). Furthermore, if $x = y = 0$, then $\alpha(0) = \alpha(0)^2$ by equality (ii) and $\beta(0) = \beta(0)\alpha(0)$ by equality (iii), so that either $\alpha(0) = \beta(0) = 0$ or $\alpha(0) = 1$. Since in the latter case $0 \cdot y = ay_1 + b\beta(0)y_1$ by formula (***), it follows that $0 \cdot y = 0$ if and only if $y_1 = 0$ and hence $y \in \langle b \rangle$. But then, as the zero-symmetric part of R, the subgroup $\langle b \rangle$ is normal in R^+ by [12], Theorem 1.15, and thus the group R^+ is abelian, contrary to the assumption. This proves statement (0) of the lemma and completes the proof. □

3. Local nearrings on the groups $G(p^m, p^n, r)$ and $G(2^m, 2^n, -r)$

Now we apply the results of the previous section for describing local nearrings whose additive groups are non-abelian split metacyclic. Recall that if R is such a local nearring, then the additive group R^+ is a p-group for some prime number p and so it is isomorphic to one of the groups $G(p^m, p^n, r)$ or $G(2^m, 2^n, -r)$ by Proposition 1. Furthermore, the set L of all non-invertible elements of R is a subgroup of index p in R^+ by Lemma 7.

Our first theorem concerns local nearrings on the group $G(p^m, p^n, r)$.

Theorem 1. *Let R be a local nearring whose additive group R^+ is isomorphic to the group $G(p^m, p^n, r)$. Then $R^+ = \langle a \rangle + \langle b \rangle$, one of the elements a or b coincides with an identity of R and the following statements hold:*

1) *$ap^m = bp^n = 0$ and $a + b = b + a(1 + p^{m-r})$ with $1 \leqslant r < \min\{m, n+1\}$ and $r < m - 1$ for $p = 2$;*
2) *if a is an identity of R, then $m \geqslant n + r \geqslant 2r + [\frac{2}{p}]$, $L = \langle ap \rangle + \langle b \rangle$ and $R^* = \{ax_1 + bx_2 \mid x_1 \not\equiv 0 \pmod p\}$;*
3) *if b is an identity of R, then $p = 2 < m \leqslant n$, $r = 1$, $L = \langle a \rangle + \langle b2 \rangle$ and $R^* = \{ax_1 + bx_2 \mid x_2 \equiv 1 \pmod 2\}$.*

Proof. It follows from Corollary 1 that $R^+ = \langle a \rangle + \langle b \rangle$ for some elements a and b one of which coincides with an identity of R and that statement 1) of the theorem holds.

If a is an identity of R, then $m \geqslant n + r \geqslant 2r + [\frac{2}{p}]$ by Lemma 11. In particular, $m > n$ and so $b \in L$ by Lemma 1. Therefore $L = \langle ap \rangle + \langle b \rangle$. Since $R^* = R \setminus L$, an element $x = ax_1 + bx_2$ belongs to R^* if and only if $x_1 \not\equiv 0 \pmod{p}$.

Similarly, if b is an identity of R, then Lemmas 9 and 12 imply that $a \in L$, $p = 2 < m \leqslant n$ and $r = 1$. Hence $L = \langle a \rangle + \langle b2 \rangle$ and so an element $x = ax_1 + bx_2$ belongs to R^* if and only if $x_2 \equiv 1 \pmod{2}$. □

Applying now statements 2) and 3) of Theorem 1 to Lemmas 11 and 12, respectively, we obtain the following formulas for multiplying any two elements $x = ax_1 + bx_2$ and $y = ay_1 + by_2$ in a local nearring R whose additive group is isomorphic to $G(p^m, p^n, r)$.

Corollary 2. *If a is an identity of R and $xb = a\alpha(x) + b\beta(x)$, then $m \geqslant n + r \geqslant 2r > 0$ and*

$$xy = a(x_1y_1 + \alpha(x)y_2 - x_1x_2\binom{y_1}{2}p^{m-r}) + b(x_2y_1 + \beta(x)y_2)$$

with coefficients $\alpha(x)$ and $\beta(x)$ satisfying the following conditions:

(0) $\alpha(0) = \beta(0) = 0$ *if and only if the nearring R is zero-symmetric*;
(1) $\alpha(a) = 0$ *and* $\beta(a) = 1$;
(2) $\alpha(x) \equiv 0 \pmod{p^{m-n}}$;
(3) $x_1(\beta(x) - 1) \equiv 0 \pmod{p^r}$ *and* $m \geqslant 2r + [\frac{2}{p}]$;
(4) $\alpha(xy) = x_1\alpha(y) + \alpha(x)\beta(y) - x_1x_2\binom{\alpha(y)}{2}p^{m-r}$;
(5) $\beta(xy) = x_2\alpha(y) + \beta(x)\beta(y)$.

Corollary 3. *If b is an identity of R and $xa = a\alpha(x) + b\beta(x)$, then $p = 2 < m \leqslant n$, $r = 1$ and*

$$xy = a(\alpha(x)y_1 + x_1j(t^{x_2}, y_2)) + b(\beta(x)y_1 + x_2y_2)$$

with coefficients $\alpha(x)$ and $\beta(x)$ satisfying the following conditions:

(0) $\alpha(0) = \beta(0) = 0$;
(1) $\alpha(b) = 1$ *and* $\beta(b) = 0$;
(2) $\beta(x) \equiv 0 \pmod{2^{n-m+1}}$;
(3) $\alpha(x)(1 - x_2) \equiv 0 \pmod{2}$;
(4) $\alpha(xy) = \alpha(x)\alpha(y) + x_1j(t^{x_2}, \beta(y))$;
(5) $\beta(xy) = \beta(x)\alpha(y) + x_2\beta(y)$.

We now turn to local nearrings on the group $G(2^m, 2^n, -r)$.

Theorem 2. *Let R be a local nearring whose additive group R^+ is isomorphic to the group $G(2^m, 2^n, -r)$. Then $R^+ = \langle a\rangle + \langle b\rangle$, the element b is an identity of R and the following statements hold*:

1) $r + 1 < m \leqslant n$ *and* $0 \leqslant r \leqslant 1$;
2) $a2^m = b2^n = 0$ *and* $a + b = b + a(-1 + 2^{m-r})$;
3) $L = \langle a\rangle + \langle b2\rangle$ *and* $R^* = \{ax_1 + bx_2 \mid x_2 \equiv 1 \pmod{2}\}$.

Proof. As in the proof of Theorem 1, it follows from Corollary 1 that there exists a decomposition $R^+ = \langle a\rangle + \langle b\rangle$ in which one of the elements a or b is an identity of R and that statement 2) of the theorem holds. But if a is an identity of R, then the group R^+ is dihedral of order 8 by Lemma 13 and so it cannot be the additive group of a local nearring by [11]. Hence the element b is an identity of R. Then $r + 1 < m \leqslant n$ and $0 \leqslant r \leqslant 1$ by Lemma 14 and $a \in L$ by Lemma 9. Therefore $L = \langle a\rangle + \langle b2\rangle$ by Lemma 1 and thus $R^* = \{ax_1 + bx_2 \mid x_2 \equiv 1 \pmod{2}\}$, as claimed. □

As a consequence of Lemmas 10, 14 and Theorem 2, we have the following formula for multiplying any two elements in a local nearring R whose additive group is isomorphic to $G(2^m, 2^n, -r)$.

Corollary 4. *If $x = ax_1 + bx_2$ and $y = ay_1 + by_2$ are elements of R, then*

$$xy = a(\alpha(x)y_1 + x_1 j(t^{x_2}, y_2)) + b(\beta(x)y_1 + x_2y_2)$$

with coefficients $\alpha(x)$ and $\beta(x)$ satisfying the following conditions:

(0) $\alpha(0) = \beta(0) = 0$;
(1) $\alpha(b) = 1$ *and* $\beta(b) = 0$;
(2) $\beta(x) \equiv 0 \pmod{2^{n-1}}$;
(3) $\alpha(xy) = \begin{cases} \alpha(x)\alpha(y) + x_1\beta(y), \text{ if } m = n \text{ and } x_2 \equiv 0 \pmod{2}, \text{ and} \\ \alpha(x)\alpha(y), \text{ in the other cases}; \end{cases}$
(4) $\beta(xy) = \beta(x)\alpha(y) + x_2\beta(y)$.

4. Groups $G(p^m, p^n, r)$ and $G(2^m, 2^n, -r)$ as the additive groups of local nearrings

The following two theorems show that the conditions given in Theorems 1 and 2 are also sufficient for existing finite local nearrings on groups $G(p^m, p^n, r)$ and $G(2^m, 2^n, -r)$. Therefore this completes our classification of all non-abelian split metacyclic p-groups which are the additive groups of local nearrings.

Theorem 3. *For each prime p and positive integers m, n and r such that either $m \geqslant n + r \geqslant 2r + [\frac{2}{p}]$ or $p = 2$, $2 < m \leqslant n$ and $r = 1$ there exists a local nearring R whose additive group R^+ is isomorphic to the group $G(p^m, p^n, r)$.*

Proof. Let G be an additively written group $G(p^m, p^n, r)$ with generators a, b satisfying the relations $ap^m = 0$, $bp^n = 0$ and $a + b = b + a(1 + p^{m-r})$. Then $G = \langle a \rangle + \langle b \rangle$ and each element $x \in G$ is uniquely written in the form $x = ax_1 + bx_2$ with coefficients $0 \leqslant x_1 < p^m$ and $0 \leqslant x_2 < p^n$.

We assume first that $m \geqslant n + r \geqslant 2r > 0$ and put $x \cdot b = b$ for each $x \in G$. Then the coefficients $\alpha(x) = 0$ and $\beta(x) = 1$ satisfy the conditions (1) - (5) of Corollary 2 and so the formula

$$x \cdot y = a(x_1 y_1 - x_1 x_2 \binom{y_1}{2} p^{m-r}) + b(x_2 y_1 + y_2)$$

determines a multiplication "$\cdot$" on G such that the system $R = (G, +, \cdot)$ is a nearring with identity element a. Furthermore, it is easy to check that an element $x = ax_1 + bx_2 \in G$ is invertible in R if and only if $x_1 \equiv 1 \pmod{p}$. Therefore the set of all non-invertible elements of R coincides with the subgroup $L = \langle ap \rangle + \langle b \rangle$ of index p in G, so that the nearring R is local. Moreover, it is also easily verified that the zero-symmetric part of R coincides with the subgroup $\langle a \rangle$ and the constant part $0 \cdot R = \langle b \rangle$.

In the other case, if $p = 2$, $2 < m \leqslant n$ and $r = 1$, then G is a metacyclic Miller-Moreno p-group, so that G is the additive group of a zero-symmetric local nearring with identity element b by [15], Theorem 2. $\square$

Theorem 4. *If m, n and r are integers such that $r + 1 < m \leqslant n$ and $0 \leqslant r \leqslant 1$, then there exists a local nearring R whose additive group R^+ is isomorphic to the group $G(2^m, 2^n, -r)$.*

Proof. Let G be an additively written group $G(2^m, 2^n, -r)$ with generators a, b satisfying the relations $a2^m = 0$, $b2^n = 0$ and $a + b = b + at$ with $t = -1 + 2^{m-r}$. Then $G = \langle a \rangle + \langle b \rangle$ and each element $x \in G$ is uniquely written in the form $x = ax_1 + bx_2$ with coefficients $0 \leqslant x_1 < 2^m$ and $0 \leqslant x_2 < 2^n$.

In order to define a required multiplication "$\cdot$" on G, for each $x \in G$ we put $x \cdot a = a\alpha(x)$ with

$$\alpha(x) = \begin{cases} 1, \text{if } x_2 \equiv 1 \pmod{2}, \text{and} \\ 0, \text{ if } x_2 \equiv 0 \pmod{2}. \end{cases}$$

Then the coefficients $\alpha(x)$ and $\beta(x) = 0$ satisfy the conditions (0) - (4) of Corollary 4 and so the formula

$$x \cdot y = a(\alpha(x)y_1 + x_1 j(t^{x_2}, y_2)) + b(x_2 y_2)$$

determines multiplication "$\cdot$" on G such that the system $R = (G, +, \cdot)$ is a nearring with identity element b.

Indeed, it is easy to see that $x \cdot b = a(\alpha(x) \cdot 0 + x_1 j(t^{x_2}, 1)) + bx_2 = ax_1 + bx_2 = x = b \cdot x$, so that b is the identity of R.

We show further that $x \cdot (y+z) = x \cdot y + x \cdot z$ for arbitrary $y = ay_1 + by_2$ and $z = az_1 + bz_2$ of G. Since $y + z = a(y_1 + z_1 t^{y_2}) + b(y_2 + z_2)$ by Lemma 5, we have

$$(i) \quad x \cdot (y+z) = a(\alpha(x)(y_1 + z_1 t^{y_2}) + x_1 j(t^{x_2}, y_2 + z_2)) + bx_2(y_2 + z_2).$$

On the other hand,

$$x \cdot z = a(\alpha(x)z_1 + x_1 j(t^{x_2}, z_2)) + b(x_2 z_2)$$

and

$$b(x_2 y_2) + a(\alpha(x)z_1 + x_1 j(t^{x_2}, z_2)) = a(\alpha(x)z_1 + x_1 j(t^{x_2}, z_2))t^{x_2 y_2}) + b(x_2 y_2)$$

by Lemma 5. Therefore

$$(ii) \qquad x \cdot y + x \cdot z = a(\alpha(x)(y_1 + z_1 t^{x_2 y_2})$$
$$+ x_1(j(t^{x_2}, y_2) + j(t^{x_2}, z_2)t^{x_2 y_2})) + bx_2(y_2 + z_2).$$

Subtracting equality (ii) from (i), we obtain

$$x \cdot (y+z) - (x \cdot y + x \cdot z) = a(\alpha(x)(y_1 + z_1 t^{y_2}) + x_1 j(t^{x_2}, y_2 + z_2))$$
$$-a(\alpha(x)(y_1 + z_1 t^{x_2 y_2}) + x_1(j(t^{x_2}, y_2) + j(t^{x_2}, z_2)t^{x_2 y_2})$$
$$= a(\alpha(x)(y_1 + z_1 t^{y_2}) + x_1 j(t^{x_2}, y_2 + z_2) - x_1(j(t^{x_2}, y_2) + j(t^{x_2}, z_2)t^{x_2 y_2})$$
$$-(\alpha(x)(y_1 + z_1 t^{x_2 y_2})) = a(\alpha(x)(y_1 + z_1 t^{y_2} - z_1 t^{x_2 y_2} - y_1)),$$

because

$$j(t^{x_2}, y_2 + z_2) = j(t^{x_2}, y_2) + j(t^{x_2}, z_2)t^{x_2 y_2})$$

by statement 1) of Lemma 4. Thus

$$x \cdot (y+z) - (x \cdot y + x \cdot z) = a(\alpha(x)(y_1 + z_1 t^{y_2} - z_1 t^{x_2 y_2} - y_1))$$

and since $\alpha(x) = 0$ for $x_2 \equiv 0 \,(\bmod\, 2\,)$, it remains to consider the case $\alpha(x) = 1$ in which $x_2 \equiv 1 \,(\bmod\, 2\,)$. But then $t^{x_2} \equiv t \,(\bmod\, 2^m\,)$ by statement 3) of Lemma 4 and so $t^{x_2 y_2} \equiv t^{y_2} \,(\bmod\, 2^m\,)$. Therefore $(y_1 + z_1 t^{y_2} - z_1 t^{x_2 y_2} - y_1) \equiv 0 \,(\bmod\, 2^m\,)$ and hence $a(y_1 + z_1 t^{y_2} - z_1 t^{x_2 y_2} - y_1) = 0$, as claimed.

It is also clear that the associativity of multiplication "$\cdot$" follows from its left distributivity and the equality $x \cdot (y \cdot a) = (x \cdot y) \cdot a$. Indeed, since $y \cdot a = a\alpha(y)$ and $(x \cdot y) \cdot a = a\alpha(x \cdot y)$ by definition, we have $x \cdot (y \cdot a) = x \cdot (a\alpha(y)) = (x \cdot a)\alpha(y) = (a\alpha(x))\alpha(y) = a(\alpha(x)\alpha(y)) = a\alpha(x \cdot y)$.

Finally, we show that an element $x = ax_1 + bx_2 \in G$ is invertible if and only if $x_2 \equiv 1 \,(\bmod\, 2\,)$. This means that we need to find an element $y = ay_1 + by_2$ such that $x \cdot y = y \cdot x = b$. Clearly there exists an odd integer y_2 such that $x_2 y_2 \equiv 1 \,(\bmod\, 2^n\,)$. Thus if we put $y_1 = -x_1 j(t^{x_2}, y_2)$, then it easy to see that $x \cdot y = y \cdot x = b$. Therefore $R^* = \{ax_1 + bx_2 \mid x_2 \equiv 1 \,(\bmod\, 2)\}$ and hence the set of all non-invertible elements of R coincides with the subgroup $L = \langle a \rangle + \langle b2 \rangle$ of G. Thus $R = (G, +, \cdot)$ is a local nearring, as desired. $\square$

References

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

[2] J. N. S. Bidwell, M. J. Curran, *The automorphism group of a split metacyclic p-group*, Arch. Math., **87**, 2006, pp. 488–497.

[3] J. R. Clay *Research in near-ring theory using a digital computer* // BIT, **10** (1970), pp. 249–265.

[4] M. J. Curran, *The automorphism group of a split metacyclic* 2*-group*, Arch. Math., **89**, 2007, pp. 10–23.

[5] S. Feigelstock. *Additive Groups of Local Near-Rings*, Comm. Algebra, **34**, 2006, pp. 743–747.

[6] M. J. Johnson, *Near-rings with identities on dihedral groups*, Proc. Edinburgh Math. Soc. (2), **18**, 1972/73, pp. 219–228.

[7] B. W. King, *Presentations of metacyclic groups*, Bul. Austral. Math. Soc., **8**, 1973, pp. 103–131.

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

[9] C. J. Maxson, *Local near-rings of cardinality* p^2, Canad. Math. Bull., **11**, 1968, no 4.

[10] C. J. Maxson, *On the construction of finite local near-rings (I): on non-cyclic abelian p-groups*, Quart. J. Math. Oxford (2), **21**, 1970, pp. 449–457.

[11] C. J. Maxson, *On the construction of finite local near-rings (II): on non-abelian p-groups*, Quart. J. Math. Oxford (2), **22**, 1971, pp. 65–72.

[12] J. D. P. Meldrum, *Near-rings and their links with groups*, PPL, 1985, 273 p.

[13] G. Pilz, *Near-rings. The theory and its applications* (Second edition), North-Holland, Amsterdam, 1983, 470 p.

[14] I. Yu. Raievska, M. Yu. Raievska, *Finite nearrings with identity on Miller–Moreno groups*, Mat. Stud., **42**, no 1, 2014, pp. 15–20.

[15] I. Yu. Raievska, Ya. P. Sysak, *Finite local nearrings on metacyclic Miller–Moreno p-groups*, Algebra and Discrete Math., **13**, no 1, 2012, pp. 111–127.

Contact information

I. Raievska, M. Raievska, Ya. Sysak

Institute of Mathematics, National Academy of Sciences of Ukraine, 3 Tereshchenkivs'ka Str., Kyiv, Ukraine, 01004

E-Mail(s): raeirina@imath.kiev.ua, raemarina@imath.kiev.ua, sysak@imath.kiev.ua

Received by the editors: 07.09.2016
and in final form 12.09.2016.