Lower bounds for the number of local nearrings on groups of $\operatorname{order} \, p^{3*}$

Iryna Raievska and Maryna Raievska†

Institute of Mathematics, University of Warsaw, 2 Banacha St., 02-097 Warsaw, Poland Department of Algebra and Topology, Institute of Mathematics of NAS of Ukraine, 3 Tereshchenkivs'ka St., 01 024 Kyiv, Ukraine

Received May 10, 2022; accepted January 30, 2024

Abstract. Lower bounds for the number of local nearrings on groups of order p^3 are obtained. On each non-metacyclic non-abelian or metacyclic abelian groups of order $p³$ there exist at least $p + 1$ non-isomorphic local nearrings.

AMS subject classifications: 16Y30, 20D15

Keywords: local nearring, p-group, metacyclic group, non-metacyclic group

1. Introduction

A study of local nearrings was first initiated in [11] and it was found that the additive group of a finite zero-symmetric local nearring is a p -group. In [12], it is shown that, up to isomorphism, there exist $p-1$ local zero-symmetric nearrings with elementary abelian additive groups of order p^2 in which the subgroups of non-invertible elements have order p , that is, those nearrings which are not nearfields. Together with the fundamental paper [22] and [5], a complete description of all zero-symmetric local nearrings of order p^2 is obtained. For instance, every nearring with identity on a cyclic group is a commutative ring.

Note that there is no nearring with identity whose additive group is isomorphic to the quaternion group Q_8 [4]. The dihedral group D_4 of order 8 cannot be the additive group of local nearrings $[14]$. The existence of local nearrings on finite abelian p groups is proved in [13], i.e. 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. Also, it is established in [18] that an arbitrary non-metacyclic Miller–Moreno p-group of order $p^{n} > 8$ is the additive group of some local nearring, and the multiplicative group of such nearring has order $p^{n-1}(p-1)$. All nearrings with identity up to the order of 31 are contained in the package SONATA [1] of the computer algebra system GAP [21].

In $[17]$, it is proved that, up to an isomorphism, there exist at least p local nearrings on elementary abelian additive groups of order p^3 which are not nearfields. Lower bounds for the number of local nearrings on groups of order p^3 are obtained.

https://www.mathos.unios.hr/mc

[∗]This work was partially supported by the Polish Academy of Sciences (PAN) and the National Academy of Sciences (NAS).

[†]Corresponding author. $Email \text{address:}$ raeirina@imath.kiev.ua (I. Raievska), raemarina@imath.kiev.ua (M. Raievska)

c 2024 School of Applied Mathematics and Informatics, University of Osijek

It is established that on each non-metacyclic non-abelian or metacyclic abelian groups of order p^3 there exist at least $p+1$ non-isomorphic local nearrings.

2. Preliminaries

We will give the basic definitions.

Definition 1. A non-empty set R with two binary operations " $+$ " and " \cdot " is a nearring if:

- 1) $(R,+)$ is a group with neutral element 0;
- 2) (R, \cdot) is a semigroup:
- 3) $x \cdot (y + z) = x \cdot y + x \cdot z$ for all $x, y, z \in R$.

Such a nearring is called a left nearring. If axiom 3) is replaced by an axiom $(x +$ $y) \cdot z = x \cdot z + y \cdot z$ for all $x, y, z \in R$, then we get a right nearring.

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*. Furthermore, R is a nearring with 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 $rM \leq M$ for each $r \in R^*$, and (R, R) -subgroup if $xMy \subseteq M$ for arbitrary $x, y \in R$.

The following assertion is well-known (see, for instance, [5], Theorem 3).

Lemma 1. The exponent of the additive group of a finite nearring R with identity i is equal to the additive order of i which coincides with the additive order of every invertible element of R.

Definition 2. A nearring R with identity is called **local** if the set L of all noninvertible elements of R forms a subgroup of the additive group R^+ .

Throughout this paper, L will denote the subgroup of non-invertible elements of R.

The following lemma characterizes the main properties of finite local nearrings (see [2], Lemma 3.2).

Lemma 2. Let R be a local nearring with identity i. 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^* .

Finite local nearrings with a cyclic subgroup of non-invertible elements are described in [16, Theorem 1].

Theorem 1. Let R be a local nearring of order p^n with $n > 1$, whose subgroup L is cyclic and non-trivial. Then the additive group R^+ is either cyclic or an elementary abelian group of order p^2 . In the first case, R is a commutative local ring, which is isomorphic to the residual ring $\mathbb{Z}/p^n\mathbb{Z}$ with $n \geq 2$; in the other case, there exist p non-isomorphic such nearrings R with $|L| = p$, from which p-1 are zero-symmetric nearrings and their multiplicative groups R^* are isomorphic to a semidirect product of two cyclic subgroups of orders p and $p-1$.

As a direct consequence of Theorem 1, we have the following result.

Corollary 1. Let R be a local nearring of order p^3 which is not isomorphic to $\mathbb{Z}/p^3\mathbb{Z}$ or is not a nearfield. Then the subgroup of non-invertible elements L is an elementary abelian group of order p^2 .

The following statement contains a classification of groups of order p^3 (see [6]).

Proposition 1. Let G be a group of order p^3 . The defining relations of such nonisomorphic groups are given:

Abelian groups:

- 1) $a^{p3} = 1$.
- 2) $a^{p^2} = 1$, $b^p = 1$, $ab = ba$.
- 3) $a^p = b^p = c^p = 1$, $ab = ba$, $ac = ca$, $cb = bc$.

Non-abelian groups of order $2^3 = 8$:

- 4) a dihedral group, $a^4 = 1$, $b^2 = 1$, $a^{-1}b = ba$.
- 5) a quaternion group, $a^4 = 1$, $b^2 = a^2$, $a^{-1}b = ba$.

Non-abelian groups of order p^3 , p is odd:

- 6) $a^{p^2} = 1$, $b^p = 1$, $b^{-1}ab = a^{1+p}$.
- 7) $a^p = 1$, $b^p = 1$, $c^p = 1$, $ab = bac$, $ac = ca$, $bc = cb$.

Next, we denote by G_1 a group with relations 7), by G_2 a group with relations 6), and by G_3 a group with relations 2) of Proposition 1.

We define group G_1 to be the additively written group generated by a, b, c subject to the relations $ap = bp = cp = 0, a + b = b + a + c, a + c = c + a, b + c = c + b.$

The following two lemmas are given in [18].

Lemma 3. Let k, $l \in \mathbb{N}$. Then in G_1 , the equalities $-ak - bl + ak + bl = c(kl)$ and $bl + ak = -c(kl) + ak + bl \text{ hold.}$

Proof. Since $-b + a + b = a + c$, we have $-bl + a + bl = a + cl$. Then

$$
-bl + ak + bl = (a + cl)k = ak + ckl.
$$

Therefore, $-ak - bl + ak + bl = ckl$.

 \Box

Lemma 4. Let k, $l, r \in \mathbb{N}$. Then in G_1 , we have $(ak+bl)r = akr + blr - ckl{r \choose 2}$.

Proof. The proof will be carried out by induction on r. For $r = 1$, the equality is valid. Let for r the equality hold, i.e.,

$$
(ak+bl)r = akr + blr - ckl\binom{r}{2}.
$$

r

Let us prove the equality for $r + 1$:

$$
(ak+bl)(r+1) = akr + blr + ak + bl - ckl\binom{r}{2}
$$

$$
= ak(r+1) + bl(r+1) - cklr - ckl\binom{r}{2}
$$

$$
= ak(r+1) + bl(r+1) - ckl(r + \binom{r}{2})
$$

$$
= ak(r+1) + bl(r+1) - ckl\binom{r+1}{2}.
$$

Therefore, the equality is valid for any r.

Let additively written groups of type H have a finite representation in the form

$$
\langle a, b|ap^k, bp, -b+a+b-a(1+p^{k-1})\rangle,
$$

where $k > 2$ and p is prime (see [8]).

The number of non-isomorphic nearrings with identity on groups of type H is given in [8]. It is obvious that for $k = 2$ and $p > 2$ a group of type H will be isomorphic to the group G_2 .

As noted above, there exist local nearrings on all abelian groups. Also, according to [18] and [8], there exist local nearrings on G_1 and G_2 , respectively. So, we have the following result.

Proposition 2. On each group of order p^3 with $p > 2$ there exists a local nearring.

Denote by $n(G)$ the number of all non-isomorphic local nearrings on the group G.

3. Nearrings with identity whose additive groups are isomorphic to G_1

Let R be a nearring with identity whose additive group of R^+ is isomorphic to G_1 . Then $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ for some elements a, b and c of R satisfying the relations $ap = 0, bp = 0, cp = 0, a + b = b + a + c, a + c = c + a$ and $b + c = c + b$. In particular, each element $x \in R$ is uniquely written in the form $x = ax_1 + bx_2 + cx_3$ with coefficients $0 \le x_1 < p$, $0 \le x_2 < p$ and $0 \le x_3 < p$.

We will show that there does not exist a nearring in which the identity is in the center of the additive group G_1 . Note that the subgroup $\langle c \rangle$ is the center of G_1 .

 \Box

Remark 1. Let c be an identity of R, i. e. $xc = cx = x$ for each $x \in R$. Furthermore, for each $x \in R$ there exist coefficients $\alpha(x)$, $\beta(x)$, $\gamma(x)$, $\lambda(x)$, $\mu(x)$ and $\nu(x)$ such that $xb = a\alpha(x) + b\beta(x) + c\gamma(x)$ and $xa = a\lambda(x) + b\mu(x) + c\nu(x)$. It is clear that they are uniquely defined modulo p, so that some mappings $\alpha : R \to \mathbb{Z}_p$, $\beta: R \to \mathbb{Z}_p$, $\gamma: R \to \mathbb{Z}_p$, $\lambda: R \to \mathbb{Z}_p$, $\mu: R \to \mathbb{Z}_p$ and $\nu: R \to \mathbb{Z}_p$ are determined.

Further, using Lemma 3, we derive

$$
xc = -xa - xb + xa + xb = -c\nu(x) - b\mu(x) - a\lambda(x) - c\gamma(x) - b\beta(x) - a\alpha(x)
$$

+ $a\lambda(x) + b\mu(x) + c\nu(x) + a\alpha(x) + b\beta(x) + c\gamma(x)$
= $-b\mu(x) - a\lambda(x) - b\beta(x) - a\alpha(x) + a\lambda(x) + b\mu(x) + a\alpha(x) + b\beta(x)$
= $-b\mu(x) + c\lambda(x)\beta(x) - b\beta(x) - a\lambda(x) - a(\alpha(x) - \lambda(x))$
+ $b\mu(x) + a\alpha(x) + b\beta(x) = c\lambda(x)\beta(x) - b(\mu(x) + \beta(x)) - a\alpha(x)$
+ $b\mu(x) + a\alpha(x) + b\beta(x) = c\lambda(x)\beta(x) - b(\mu(x) + \beta(x))$
- $a\alpha(x) - c\mu(x)\alpha(x) + a\alpha(x) + b\mu(x) + b\beta(x)$
= $c(\lambda(x)\beta(x) - \mu(x)\alpha(x)) - b(\mu(x) + \beta(x)) + b\mu(x) + b\beta(x)$
= $c(\lambda(x)\beta(x) - \mu(x)\alpha(x)) \neq x$.

Therefore, there does not exist a nearring in which the identity is in the center of the additive group G_1 .

Since the order of the element a is equal to the exponent of group G , then by Lemma 1 we can assume that a is an identity of R, i.e. $ax = xa = x$ for each $x \in R$. Furthermore, for each $x \in R$ there exist coefficients $\alpha(x)$, $\beta(x)$ and $\gamma(x)$ such that $xb = a\alpha(x) + b\beta(x) + c\gamma(x)$. It is clear that they are uniquely defined modulo p, so that some mappings $\alpha: R \to \mathbb{Z}_p$, $\beta: R \to \mathbb{Z}_p$ and $\gamma: R \to \mathbb{Z}_p$ are determined.

Nearrings with identity and local nearrings on non-metacyclic Miller–Moreno groups were studied in [18] and [15]. Lemmas 5, 6, 9 are based on the results of these papers.

Lemma 5. Let R be a nearring whose additive group is G_1 with identity a. If $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in R$, $xb = a\alpha(x) + b\beta(x) + c\gamma(x)$, then

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

- $\alpha(x)\beta(x)\binom{y_2}{2} - x_2\alpha(x)y_1y_2 + x_3y_1 + \gamma(x)y_2 + x_1\beta(x)y_3 - x_2\alpha(x)y_3).$

Moreover, for the mappings $\alpha: R \to \mathbb{Z}_p$, $\beta: R \to \mathbb{Z}_p$ and $\gamma: R \to \mathbb{Z}_p$ the following statements hold:

- (0) $\alpha(0) \equiv 0 \pmod{p}$, $\beta(0) \equiv 0 \pmod{p}$ and $\gamma(0) \equiv 0 \pmod{p}$ if and only if the nearring R is zero-symmetric;
- (1) $\alpha(xy) \equiv x_1 \alpha(y) + \alpha(x)\beta(y) \pmod{p}$,
- (2) $\beta(xy) \equiv x_2 \alpha(y) + \beta(x)\beta(y) \pmod{p}$,

(3)
$$
\gamma(xy) \equiv -x_1 x_2 {\alpha(y) \choose 2} - \alpha(x)\beta(x){\beta(y) \choose 2} - x_2 \alpha(x)\alpha(y)\beta(y) + x_3 \alpha(y) + \gamma(x)\beta(y) + x_1 \beta(x)\gamma(y) - x_2 \alpha(x)\gamma(y) \pmod{p}.
$$

Proof. Since $0 \cdot a = a \cdot 0 = 0$, it follows that R is a zero-symmetric nearring if and only if

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

or equivalently $\alpha(0) \equiv 0 \pmod{p}$, $\beta(0) \equiv 0 \pmod{p}$ and $\gamma(0) \equiv 0 \pmod{p}$. Moreover, since $c = -a - b + a + b$ and due to the left distributive law we have $0 \cdot c =$ $-0 \cdot a - 0 \cdot b + 0 \cdot a + 0 \cdot b = 0$, whence

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

so that statement (0) holds.

Further, using Lemma 3, we derive

$$
xc = -xa - xb + xa + xb = -cx3 - bx2 - ax1 - c\gamma(x) - b\beta(x) - a\alpha(x) + ax1 + bx2 + cx3 + a\alpha(x) + b\beta(x) + c\gamma(x) = -bx2 - ax1 - b\beta(x) - a\alpha(x) + ax1 + bx2 + a\alpha(x) + b\beta(x) = -bx2 + cx1\beta(x) - b\beta(x) - ax1 - a(\alpha(x) - x1) + bx2 + a\alpha(x) + b\beta(x) = cx1\beta(x) - b(x2 + \beta(x)) - a\alpha(x) + bx2 + a\alpha(x) + b\beta(x) = cx1\beta(x) - b(x2 + \beta(x)) - a\alpha(x) - cx2\alpha(x) + a\alpha(x) + bx2 + b\beta(x) = c(x1\beta(x) - x2\alpha(x)) - b(x2 + \beta(x)) + bx2 + b\beta(x) = c(x1\beta(x) - x2\alpha(x)).
$$

Further, using the left distributive law, we obtain

$$
xy = (ax_1 + bx_2 + cx_3)y_1 + (a\alpha(x) + b\beta(x) + c\gamma(x))y_2
$$

+ $(cx_1\beta(x) - x_2\alpha(x))y_3$.

By Lemma 4, we get

$$
(ax_1 + bx_2)y_1 = ax_1y_1 + bx_2y_1 - cx_1x_2\binom{y_1}{2},
$$

$$
(a\alpha(x) + b\beta(x))y_2 = a\alpha(x)y_2 + b\beta(x)y_2 - c\alpha(x)\beta(x)\binom{y_2}{2}
$$

and

$$
bx_2y_1 + a\alpha(x)y_2 = a\alpha(x)y_2 + bx_2y_1 - cx_2\alpha(x)y_1y_2.
$$

Hence and using the left distributive law, we have

$$
xy = a(x_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2) + c(-x_1x_2 \binom{y_1}{2} -\alpha(x)\beta(x) \binom{y_2}{2} - x_2\alpha(x)y_1y_2 + x_3y_1 + \gamma(x)y_2 + x_1\beta(x)y_3 - x_2\alpha(x)y_3).
$$

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

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

According to $xb = a\alpha(x) + b\beta(x) + c\gamma(x)$, we obtain

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

and $yb = a\alpha(y) + b\beta(y) + c\gamma(y)$. Substituting the last equation into the right part of equality 1), we also have

$$
x(yb) = a(x_1\alpha(y) + \alpha(x)\beta(y)) + b(x_2\alpha(y) + \beta(x)\beta(y))
$$

+
$$
c(-x_1x_2\begin{pmatrix} \alpha(y) \\ 2 \end{pmatrix} - \alpha(x)\beta(x)\begin{pmatrix} \beta(y) \\ 2 \end{pmatrix} - x_2\alpha(x)\alpha(y)\beta(y)
$$

+
$$
x_3\alpha(y) + \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) - x_2\alpha(x)\gamma(y)).
$$

Since equality 1) implies the congruence of the corresponding coefficients in formulas 2) and 3), we obtain statements (1) – (3) . \Box

4. Local nearrings whose additive groups are isomorphic to G_1

Let R be a local nearring whose additive group of R^+ is isomorphic to G_1 . Then $R^+ = \langle a \rangle + \langle b \rangle + \langle c \rangle$ for some elements a, b and c of R satisfying the relations $ap = 0$, $bp = 0, cp = 0, a + b = b + a + c, a + c = c + a$ and $b + c = c + b$. In particular, each element $x \in R$ is uniquely written in the form $x = ax_1 + bx_2 + cx_3$ with coefficients $0 \leq x_1 < p, \, 0 \leq x_2 < p \text{ and } 0 \leq x_3 < p.$

Since order of the element a is equal to the exponent of group G , then by Lemma 1 we can assume that a is an identity of R, i.e., $ax = xa = x$ for each $x \in R$. Furthermore, for each $x \in R$ there exist coefficients $\alpha(x)$, $\beta(x)$ and $\gamma(x)$ such that $xb = a\alpha(x) + b\beta(x) + c\gamma(x)$. It is clear that they are uniquely defined modulo p, so that some mappings $\alpha: R \to \mathbb{Z}_p$, $\beta: R \to \mathbb{Z}_p$ and $\gamma: R \to \mathbb{Z}_p$ are determined.

By Corollary 1, L is the normal subgroup of order p^2 in R. Since L contains the derived subgroup of R^+ , it follows that $L = \langle b \rangle + \langle c \rangle$ and subgroup $\langle c \rangle$ is the center of R^+ . Since $R^* = R \setminus L$, it follows that $R^* = \{ax_1 + bx_2 + cx_3 \mid x_1 \not\equiv 0 \pmod{p}\}$ and $x = ax_1 + bx_2 + cx_3$ is invertible if and only if $x_1 \not\equiv 0 \pmod{p}$.

Lemma 6. Let R be a local nearring whose additive group is G_1 with identity a. If $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in R$, $xb = a\alpha(x) + b\beta(x) + c\gamma(x)$, then

$$
x \cdot y = ax_1y_1 + b(x_2y_1 + \beta(x)y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + \gamma(x)y_2 + x_1\beta(x)y_3).
$$
 (*)

Moreover, for the mappings $\beta: R \to \mathbb{Z}_p$ and $\gamma: R \to \mathbb{Z}_p$ the following statements hold:

- (0) $\alpha(0) \equiv 0 \pmod{p}$, $\beta(0) \equiv 0 \pmod{p}$ and $\gamma(0) \equiv 0 \pmod{p}$ 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 $x_1 \equiv 0 \pmod{p}$;

$$
(3) \ \beta(xy) \equiv \beta(x)\beta(y) \pmod{p};
$$

(4) $\gamma(xy) \equiv \gamma(x)\beta(y) + x_1\beta(x)\gamma(y) \pmod{p}$.

Proof. Since $L = \langle b \rangle + \langle c \rangle$ and L is the (R, R) -subgroup in R^+ , by statement 1) of Lemma 2 it follows that $xb \in L$, hence $a\alpha(x) \in L$ for each $x \in R$. Thus $\alpha(x) \equiv 0$ (mod p) and we get statement (1). Substituting the obtained value of $\alpha(x) \equiv 0$ \pmod{p} into the formulas from Lemma 5, we obtain statements (3) and (4) of the lemma and the formula for the product xy. Putting $y = c$, we get $xc = c(x_1\beta(x))$. Hence, if $\beta(x) \equiv 0 \pmod{p}$, then $xc = 0$, and so $x \in L$. Therefore, $x_1 \equiv 0$ p , as claimed in statement (2). Indeed, statement (0) repeats statement (0) of Lemma 5. \Box

It is known that for such groups the commutator $D(R^+)$ coincides with the center $Z(R^+)$ and has the order p.

Lemma 7. The commutator $D(R^+)$ is an ideal in the local nearring R.

Proof. Let $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in R$, $z = cz_3 \in D(R^+)$. Let us check whether $D(R^+)$ is an ideal in R, i.e., $(z+x)y - xy \in D(R^+)$. To do this, we use formula $(*)$ for multiplying elements in R. We obtain

$$
(z+x)y - xy
$$

\n
$$
= (cz_3 + ax_1 + bx_2 + cx_3)(ay_1 + by_2 + cy_3) - (ax_1 + bx_2 + cx_3)(ay_1 + by_2 + cy_3)
$$

\n
$$
= (ax_1 + bx_2 + c(x_3 + z_3))(ay_1 + by_2 + cy_3) - (ax_1 + bx_2 + cx_3)(ay_1 + by_2 + cy_3)
$$

\n
$$
= ax_1y_1 + b(x_2y_1 + \beta(x)y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + z_3y_1 + \gamma(z+x)y_2 + x_1\beta(x)y_3)
$$

\n
$$
- ax_1y_1 - b(x_2y_1 + \beta(x)y_2) - c(-x_1x_2\binom{y_1}{2} + x_3y_1 + \gamma(x)y_2 + x_1\beta(x)y_3)
$$

\n
$$
= ax_1y_1 + b(x_2y_1 + \beta(x)y_2) - ax_1y_1 - b(x_2y_1 + \beta(x)y_2) + c(z_3y_1 + (\gamma(z+x) - \gamma(x))y_2)
$$

\n
$$
- b(x_2y_1 + \beta(x)y_2) + c(z_3y_1 + (\gamma(z+x) - \gamma(x))y_2)
$$

\n
$$
= c(z_3y_1 + (\gamma(z+x) - \gamma(x))y_2 - x_1x_2y_1^2 - x_1y_1y_2\beta(x)) \in D(R^+).
$$

Therefore, $D(R^+)$ is an ideal of R.

 \Box

Lemma 8. Let R be a local nearring whose additive group of R^+ is isomorphic to G₁. If $x = ax_1 + bx_2 + cx_3$, $y = ay_1 + by_2 + cy_3 \in R$, then the mappings $\beta: R \to \mathbb{Z}_{p^2}$ and $\gamma: R \to \mathbb{Z}_p$ from (*) can be one of the following:

- 1) $\beta(x) = x_1^i$ and $\gamma(x) = 0$ $(0 < i < p)$;
- 2) $\beta(x) = 1$ and $\gamma(x) = 0$;
- 3) $\beta(x) = x_1^2$ and $\gamma(x) = x_1 x_2$.

Proof. 1) Since zero-symmetric local nearrings of order p^2 are classified in [12], it follows that all non-isomorphic factor-nearrings with derived subgroup $N = R/D(R^+)$ are described. That is, you can apply the multiplication formula from the specified work, pre-adapting it for the left local nearrings. It is clear that $N^+ = \langle a \rangle + \langle b \rangle$. Namely, let $x = ax_1 + bx_2$ and $y = ay_1 + by_2$ be elements of N; then

$$
xy = ax_1y_1 + b(x_2y_1 + \rho(x_1)y_2).
$$

Moreover, in [12, Theorem 1.6] and [12, Corollary 1.11] it was shown that there are, up to isomorphism, $p-1$ local nearrings (which are not nearfields) with the additive group of order p^2 and exponent p. These local nearrings are completely determined by maps $\rho: \mathbb{Z}_p \to \mathbb{Z}_p$ such that (i) $\rho(x) = 0$ if and only if $x = 0$ and (ii) ρ is a group endomorphism of $(\mathbb{Z}_p - \{0\},\cdot)$ [10]. So ρ takes one of $p-1$ values for zero-symmetric nearrings.

On the other hand, by the formula (∗) we have:

$$
xy = ax_1y_1 + b(x_2y_1 + \beta(x)y_2).
$$

Equating the coefficients for generators, we obtain: $\beta(x)y_2 = \rho(x_1)y_2$. Hence $\beta(x) =$ $\rho(x_1)$. So there exist $p-1$ different zero-symmetric nearrings.

2) It is obvious that the multiplication (*) with the functions $\beta(x) = 1$ and $\gamma(x) = 0$ is the constant nearring multiplication.

3) We will show further that for $\beta(x) = x_1^2$ and $\gamma(x) = x_1x_2$ the multiplication $(*),$ i.e.

$$
x * y = ax_1y_1 + b(x_2y_1 + x_1^2y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1x_2y_2 + x_1^3y_3),
$$

is a nearring multiplication. By Lemma 6 (3) and (4), the functions $\beta(x)$ and $\gamma(x)$ need to satisfy the following conditions: $\beta(xy) = \beta(x)\beta(y)$ and $\gamma(xy) = \beta(y)\gamma(x) +$ $x_1\beta(x)\gamma(y)$. We check that $\beta(xy) = (x_1y_1)^2 = x_1^2y_1^2 = \beta(x)\beta(y)$ and $\gamma(xy) =$ $x_1y_1(x_2y_1+x_1y_2) = x_1x_2y_1^2 + x_1^2y_1y_2 = \beta(y)\gamma(x) + x_1\beta(x)\gamma(y)$. Therefore, $\beta(x)$ and $\gamma(x)$ satisfy conditions (3) and (4) of Lemma 6.

It is easy to see that the element a is a multiplicative identity for $(R, *)$ and $x * b = bx_1^2 + cx_1x_2$ for each $x \in R$. We show that with respect to the operations " + " and " * " the system $(R, +, *)$ is a nearring with identity element a. Clearly, it suffices to check that if $z = az_1 + bz_2 + cz_3$ is an arbitrary element of R, then $x * (y + z) = x * y + x * z$ and $(x * y) * b = x * (y * b)$.

Indeed, we have

$$
x * z = ax_1z_1 + b(x_2z_1 + x_1^2z_2) + c(-x_1x_2\binom{z_1}{2} + x_3z_1 + x_1x_2z_2 + x_1^3z_3)
$$

and

$$
b(x_2y_1+x_1^2y_2)+a(x_1z_1)=a(x_1z_1)+b(x_2y_1+x_1^2y_2)-c(x_1z_1(x_2y_1+x_1^2y_2))
$$

by Lemma 3. We get

$$
x * y + x * z = a(x_1y_1 + x_1z_1) + b(x_2y_1 + x_1^2y_2 + x_2z_1 + x_1^2z_2)
$$

+
$$
c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1x_2y_2 + x_1^3y_3
$$

$$
- x_1x_2\binom{z_1}{2} + x_3z_1 + x_1x_2z_2 + x_1^3z_3 - x_1z_1(x_2y_1 + x_1^2y_2))
$$

=
$$
ax_1(y_1 + z_1) + b(x_2(y_1 + z_1) + x_1^2(y_2 + z_2))
$$

+
$$
c(-x_1x_2\binom{(y_1 + z_1)}{2} + x_3(y_1 + z_1) + x_1x_2(y_2 + z_2) + x_1^3(y_3 + z_3 - z_1y_2)).
$$

On the other hand, $y + z = (ay_1 + by_2 + cy_3) + (az_1 + bz_2 + cz_3) = a(y_1 + z_1) + b(z_2 + cz_3)$ $b(y_2 + z_2) + c(y_3 + z_3 - z_1y_2)$ because $by_2 + az_1 = az_1 + by_2 - cz_1y_2$ by Lemma 3. Therefore,

$$
x * (y + z) = ax_1(y_1 + z_1) + b(x_2(y_1 + z_1) + x_1^2(y_2 + z_2))
$$

+
$$
c(-x_1x_2\binom{(y_1+z_1)}{2} + x_3(y_1+z_1) + x_1x_2(y_2+z_2) + x_1^3(y_3+z_3-z_1y_2)).
$$

Therefore, $x * (y + z) = x * y + x * z$, as desired.

Next, $y * b = by_1^2 + cy_1y_2$ and so $x * (y * b) = b(x_1^2y_1^2) + c(x_1x_2y_1^2 + x_1^3y_1y_2) =$ $b(x_1y_1)^2 + c(x_1x_2(x_2y_1 + x_1^2y_2).$

On the other hand, $(x * y) * b = (ax_1y_1 + b(x_2y_1 + x_1^2y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 +$ $x_1x_2y_2 + x_1^3y_3$ * $b = b(x_1y_1)^2 + c(x_1x_2(x_2y_1 + x_1^2y_2) = x * (y * b)$. Thus, the system $(R, +, *)$ is a nearring with identity element a, and so multiplication "*" is a nearring multiplication, as desired.

 \Box

So, we have examples of $p + 1$ nearring multiplications and we formulate the following result.

Theorem 2. There exist at least $p+1$ non-isomorphic local nearrings on each nonmetacyclic non-abelian groups of order p^3 .

Proof. The nearrings $R = (R, +, \cdot)$ with functions $\beta(x) = x_1^i$ and $\gamma(x) = 0$ (0 < $i < p$) are non-isomorphic zero-symmetric local nearrings according to the above and paper [12]. It is easy to check that the local nearrings $R = (R, +, \cdot)$ with functions $\beta(x) = 1$ and $\gamma(x) = 0$ are non-zero-symmetric. It is obvious that $R = (R, +, \cdot)$ with functions $\beta(x) = x_1^2$ and $\gamma(x) = x_1 x_2$ are zero-symmetric and non-isomorphic to the nearrings considered above. Therefore, there exist at least $p + 1$ non-isomorphic local nearrings on each non-metacyclic non-abelian groups of order p^3 . \Box

Example 1. Let $G \cong (C_5 \times C_5) \rtimes C_5$. If $x = ax_1+bx_2+cx_3$ and $y = ay_1+by_2+cy_3 \in C_5$ G and $(G, +, \cdot)$ is a local nearring, then by Lemma 8 " \cdot " is one of the following multiplications:

(1) $x \cdot y = ax_1y_1 + b(x_2y_1 + y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1y_3);$

LOWER BOUNDS FOR THE NUMBER OF LOCAL NEARRINGS 187

- (2) $x \cdot y = ax_1y_1 + b(x_2y_1 + x_1^3(x)y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1x_2y_2 + x_1^4y_3);$
- (3) $x \cdot y = ax_1y_1 + b(x_2y_1 + x_1y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1^2y_3);$
- (4) $x \cdot y = ax_1y_1 + b(x_2y_1 + x_1^2y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1^3y_3);$
- (5) $x \cdot y = ax_1y_1 + b(x_2y_1 + x_1^3(x)y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1^4y_3);$
- (6) $x \cdot y = ax_1y_1 + b(x_2y_1 + x_1^4y_2) + c(-x_1x_2\binom{y_1}{2} + x_3y_1 + x_1^5y_3).$

A computer program verified that for $p = 5$, the nearring obtained in Lemma 8 (3) is indeed a local nearring (see Example 1 (2)) deposited on GitHub:

https://github.com/raemarina/Examples/blob/main/LNR_125-3.txt From the packages SONATA and LocalNR [19] we have the following number of non-isomorphic local nearrings:

5. Local nearrings whose additive groups are isomorphic to G_2

Let R be a local nearring whose additive group of R^+ is isomorphic to G_2 . Then $R^+ = \langle a \rangle + \langle b \rangle$ for some elements a and b of R satisfying the relations $a p^2 = 0$, $bp = 0$ and $-b + a + b = a(1 + p)$. In particular, each element $x \in R$ is uniquely written in the form $x = ax_1 + bx_2$ with coefficients $0 \le x_1 < p^2$ and $0 \le x_2 < p$.

By [8, Theorem 7.1], for $p = 3$ there exist three zero-symmetric nearrings with identity on G_2 , and for $p > 3$ one. At the same time, by [8, Theorem 4.2] there exists one non-zero-symmetric nearring with identity on G_2 . On the other hand, in [14], it was shown that for each group G_2 there exists a zero-symmetric local nearring. With the SONATA nearring library, it is easy to make sure that all nearrings with identity on G_2 of order 27 are local. The formula for multiplying elements of local nearrings on Miller–Moreno metacyclic groups is defined in [20]. Since G_2 is a Miller–Moreno metacyclic group, using [20, Corollary 2], for arbitrary elements $x = ax_1 + bx_2$ and $y = ay_1 + by_2$ of G_2 and putting $\alpha(x) = 0$ and $\beta(x) = 1$, we obtain the following multiplication formula:

$$
x \cdot y = a(x_1y_1 - x_1x_2\binom{y_1}{2}p) + b(x_2y_1 + y_2). (*)
$$

It is easy to see that $R = (G_2, +, \cdot)$ is a non-zero-symmetric local nearring.

The multiplication formula for arbitrary elements of a zero-symmetric local nearring on G_2 is given when proving [20, Theorem 2], namely:

$$
x \cdot y = a(x_1y_1 - x_1x_2\binom{y_1}{2}p) + b(x_2y_1 + \beta(x)y_2), \quad (***)
$$

where $\beta(x) = \begin{cases} 1, & \text{if } x_1 \not\equiv 0 \pmod{p}; \\ 0, & \text{if } x_1 = 0 \pmod{p}; \end{cases}$ 0, if $x_1 \equiv 0 \pmod{p}$.

So, from the results presented in this section, we have:

- 1) $n(G_2) = 4$ for $p = 3$;
- 2) $n(G_2) = 2$ for $p > 3$. Moreover, the multiplication formulas in such nearrings are determined by formulas $(**)$ or $(***)$.

6. Local nearrings whose additive groups are isomorphic to G_3

Let R be a local nearring, which is not a nearfield, whose additive group of R^+ is isomorphic to G_3 . Then $R^+ = \langle a \rangle + \langle b \rangle$ for some elements a and b of R satisfying the relations $ap^2 = 0$, $bp = 0$ and $b + a = a + b$. In particular, each element $x \in R$ is uniquely written in the form $x = ax_1 + bx_2$ with coefficients $0 \le x_1 < p^2$ and $0 \le x_2 < p$.

We can assume, without loss of generality, that a is an identity of R, i.e., $ax =$ $xa = x$ for each $x \in R$. Furthermore, 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^2 and p, respectively, so that some mappings $\alpha: R \to \mathbb{Z}_{p^2}$ and $\beta: R \to \mathbb{Z}_p$ are determined.

Lemma 9. Let R be a local nearring, which is not a nearfield, whose additive group of R^+ is isomorphic to G_3 . If a coincides with identity element of R, $x = ax_1 + bx_2$, $y = ay_1 + by_2 \in R$, $xb = a\alpha(x) + b\beta(x)$, then

$$
xy = a(x_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2).
$$
 (* ***)

Moreover, for the mappings $\alpha: R \to \mathbb{Z}_{p^2}$ and $\beta: R \to \mathbb{Z}_p$ the following statements hold:

- (0) $\alpha(0) = \beta(0) = 0$ if and only if R is zero-symmetric;
- (1) $\alpha(a) = 0$ and $\beta(a) = 1$;
- (2) $\alpha(x) \equiv 0 \pmod{p}$;
- (3) $\alpha(xy) \equiv x_1 \alpha(y) + \alpha(x)\beta(y) \pmod{p}$;
- (4) $\beta(xy) \equiv x_2 \alpha(y) + \beta(x)\beta(y) \pmod{p}$.

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

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

We also have $(ax_1 + bx_2)y_1 = ax_1y_1 + bx_2y_1$ and $(ax(x) + b\beta(x))y_2 = a\alpha(x)y_2 + b\beta(x)y_1$ $b\beta(x)y_2$. Thus $xy = a(x_1y_1 + \alpha(x)y_2) + b(x_2y_1 + \beta(x)y_2)$ and so statement (2) holds.

By Corollary 1, $L = \langle ap \rangle + \langle b \rangle$. Since $xL \subseteq L$ for each $x \in R$ by Lemma 2, we have $xb = a\alpha(x) + b\beta(x) \in L$, whence $\alpha(x) \equiv 0 \pmod{p}$ for each $x \in R$.

Finally, the associativity of multiplication in R implies that

$$
(xy)b = x(yb) = a\alpha(xy) + b\beta(xy).
$$

Furthermore, substituting $yb = a\alpha(y) + b\beta(y)$ instead of y into formula (***), we also have

$$
x(yb) = a(x_1\alpha(y) + \alpha(x)\beta(y)) + b(x_2\alpha(y) + \beta(x)\beta(y)).
$$

Comparing the coefficients under a and b in two expressions obtained for $x(yb)$, we derive statements (3) and (4) of the lemma. \Box

Lemma 10. $\langle ap \rangle$ is an ideal of R.

Proof. Let $x = ax_1 + bx_2$, $y = ay_1 + by_2 \in R$, $z = apz_1 \in \langle ap \rangle$. Check whether $\langle ap \rangle$ is an ideal of R, i.e. $(z + x)y - xy \in \langle ap \rangle$. Using the formula $(** * *)$, we have

$$
(z+x)y - xy = (apz1 + ax1 + bx2)(ay1 + by2) – (ax1 + bx2)(ay1 + by2)= (a(pz1 + x1) + bx2)(ay1 + by2) – (ax1 + bx2)(ay1 + by2)= a((pz1 + x1)y1 + \alpha(z + x)y2) + b(x2y1 + \beta(z + x)y2)- (a(z1y1 + \alpha(x)y2) + b(x2y1 + \beta(x)y2))= a(pz1y1 + (\alpha(z + x) - \alpha(x))y2) + b(\beta(z + x) - \beta(x))y2= a(pz1y1 + (\alpha(z + x) - \alpha(x))y2) \in \langle ap \rangle,
$$

since $\beta(z+x) - \beta(x) = 0$.

Therefore, $\langle ap \rangle$ is an ideal of R.

Lemma 11. Let R be a local nearring, which is not a nearfield, whose additive group of R^+ is isomorphic to G_3 . If $x = ax_1 + bx_2$, $y = ay_1 + by_2 \in R$, then the mappings $\alpha: R \to \mathbb{Z}_{p^2}$ and $\beta: R \to \mathbb{Z}_p$ from $(***)$ can be one of the following:

- (1) $\alpha(x) = 0$ and $\beta(x) = x_1^i \pmod{p}$ $(0 < i < p)$;
- (2) $\alpha(x) = 0$ and $\beta(x) = 1$;
- (3) $\alpha(x) = px_2$ and $\beta(x) \equiv x_1 \pmod{p}$.

Proof. 1) Since zero-symmetric local nearrings of order p^2 are classified in [12], it follows that all non-isomorphic factor-nearrings with a derived subgroup $N = R/\langle ap \rangle$ are described. That is, you can apply the multiplication formula from the specified work, pre-adapting it for the left local nearrings. It is clear that $N^+ = \langle \overline{a} \rangle + \langle \overline{b} \rangle$. Namely, let $\bar{x} = \bar{a}x_1 + \bar{b}x_2$ and $\bar{y} = \bar{a}y_1 + \bar{b}y_2$ be elements of N; then

$$
\overline{xy} = \overline{a}x_1y_1 + \overline{b}(x_2y_1 + \rho(x_1)y_2).
$$

Moreover, by [12, Theorem 1.6], ρ takes one of $p-1$ values for zero-symmetric nearrings.

On the other hand, by the formula $(****)$ we have $\overline{xy} = \overline{a}x_1y_1+\overline{b}(x_2y_1+\beta(x)y_2)$.

 \Box

Equating the coefficients for generators, we obtain $\beta(x)y_2 = \rho(x_1)y_2$. Hence $\beta(x) = \rho(x_1)$. So there exist $p-1$ different zero-symmetric nearrings.

2) It is obvious that the multiplication (****) with the functions $\alpha(x) = 0$ and $\beta(x) = 1$ is the constant nearring multiplication.

3) By direct checking of conditions (3) and (4) of Lemma 9 for $\alpha(x) = px_2$ and $\beta(x) \equiv x_1 \pmod{p}$ and by using the multiplication (****), we prove the lemma. \Box

So, we have examples of $p + 1$ nearring multiplications and we formulate the following result.

Theorem 3. There exist at least $p + 1$ non-isomorphic local nearrings on each metacyclic abelian groups of order p^3 .

Proof. Nearrings $R = (R, +, \cdot)$ with functions $\alpha(x) = 0$ and $\beta(x) = x_1^i \pmod{p}$ $(0 \lt i \lt p)$ are non-isomorphic zero-symmetric local nearrings according to the above and paper [12]. It is easy to check that the local nearring $R = (R, +, \cdot)$ with functions $\alpha(x) = 0$ and $\beta(x) = 1$ is non-zero-symmetric.

Consider $R = (R, +, \cdot)$ with functions $\alpha(x) = px_2$ and $\beta(x) \equiv x_1 \pmod{p}$. In this case, we have $|\{xb = apx_2 + bx_1|x \in R\}| = p^2$ and R is zero-symmetric. For example, in the above case with $\alpha(x) = 0$ and $\beta(x) = x_1 \pmod{p}$ we get $\vert \{xb =$ $bx_1|x \in R| = p$, and so R is non-isomorphic to the nearrings considered above. Therefore, there exist at least $p+1$ non-isomorphic local nearrings on each metacyclic abelian group of order p^3 . \Box

From the packages SONATA and LocalNR we have the following number of non-isomorphic local nearrings:

Acknowledgement

The authors would like to thank the Institute of Mathematics of the Polish Academy of Sciences for hosting after evacuation from Ukraine. The authors are grateful IIE-SRF for the support of their fellowship at the University of Warsaw.

The authors thank the referees for recommending various improvements in the exposition of the paper.

References

[1] E. AICHINGER, F. BINDER, JU. ECKER, P. MAYR, C. NÖBAUER, SONATA – System of nearrings and their applications, GAP package, Version 2.8, 2015, available at (http://www.algebra.uni-linz.ac.at/Sonata/)

- [2] B. Amberg, P. Hubert, Ya. Sysak, Local near-rings with dihedral multiplicative group, J. Algebra. 273 (2004), 700–717.
- [3] $T.H. H. B$ BOYKETT, C. NOBAUER, A class of groups which cannot be the additive groups of near-rings with identity, Contributions to general algebra 10, Proceedings of the Klagenfurt Conference, Klagenfurt, 1998, 89–99.
- [4] J. R. CLAY, Research in near-ring theory using a digital computer, BIT. 10(1970), 249–265.
- [5] J. R. CLAY, JR. MALONE, The near-rings with identities on certain finite groups, Math. Scand. 19(1966), 146–150.
- [6] M. JR. HALL, The Theory of Groups, MacMillan Company, New York, 1959.
- [7] J. E. Krimmel, A condition on near-rings with identity, Monatsh. Math. 77(1973), 52–54.
- [8] R. R. LAXTON, R. LOCKHART, The near-rings hosted by a class of groups, Proc. Edinb. Math. Soc. 23(1980), 69-86.
- [9] S. LIGH, Near rings with identities on certain groups, Monatsh. Math. 75(1971), 38–43.
- [10] C. J. Maxson, Review on the paper [12], available at (http://mathscinet.imath.kiev.ua/mathscinet/article?mr=0236229)
- [11] C. J. MAXSON, On local near-rings, Math. Z. 106(1968), 197-205.
- [12] C. J. MAXSON, Local near-rings of cardinality p^2 , Canad. Math. Bull. 11(1968), 555– 561.
- [13] C. J. Maxson, On the construction of finite local near-rings (I): on non-cyclic abelian p-groups, Quart. J. Math. Oxford 21(1970), 449–457.
- [14] C. J. MAXSON, On the construction of finite local near-rings (II): on non-abelian pgroups, Quart. J. Math. Oxford 22(1971), 65–72.
- [15] I. Yu. Raievska, Local nearrings on Miller-Moreno p-group, Bulletin of Taras Shevchenko National University of Kyiv; Series: Mathematics and Mechanics 25(2011), 43–45, in Ukrainian.
- [16] I. Yu. Raievska, M. Yu. Raievska, Local nearrings with restrictions on the multiplicative groups and the subgroups of non-invertible elements, Sci. Journ. Dragomanov Ped. Univ. Ser. 1. Phys.–Math. Sci. (Kiev) 14(2013), 134–145, in Ukrainian.
- [17] I. Yu. Raievska, M. Yu. Raievska, Local nearrings on elementary Abelian groups of order p^3 , Scientific Bulletin of Uzhhorod University; Series: Mathematics and Informatics 1(2021), 85–93, in Ukrainian.
- [18] I. Yu. Raievska, M. Yu. Raievska, Ya. P. Sysak, Local nearrings on nonmetacyclic Miller-Moreno groups, Bulletin of Taras Shevchenko National University of Kyiv; Series: Physics and Mathematics 3(2012), 39–46, in Ukrainian.
- [19] I. Raievska, M. Raievska M., Y. Sysak, LocalNR, Package of local nearrings, Version 1.0.3, GAP package, 2021, available at (https://gap-packages.github.io/LocalNR)
- [20] I. Yu. Raievska, Ya. P. Sysak, Finite local nearrings on metacyclic Miller–Moreno p-groups, Algebra Discrete Math. 13(2012), 111–127.
- [21] The GAP Group, GAP Groups, Algorithms, and Programming, Version 4.11.0, 2020, available at (https://www.gap-system.org)
- [22] H. ZASSENHAUS, Uber endliche Fastkörper, Abh. Math. Sem., Univ. Hamburg. 11(1935/36), 187–220.