УДК 512.6

I. Yu. Raievska, M. Yu. Raievska

FINITE NEARRINGS WITH IDENTITY ON MILLER-MORENO GROUPS

I. Yu. Raievska, M. Yu. Raievska. *Finite nearrings with identity on Miller-Moreno groups*, Mat. Stud. **42** (2014), 15–20.

In this paper all possible types of Miller-Moreno groups which can be the additive groups of nearrings with identity are described.

И. Ю. Раевская, М. Ю. Раевская. *Конечные почти-кольца с единицей на группах Миллера-Морено* // Мат. Студії. – 2014. – Т.42, №1. – С.15–20.

В статье описаны все возможные типы групп Миллера-Морено, которые могут быть аддитивными группами почти-колец с единицей.

1. Introduction. Nearrings are a generalization of rings in the sense that their addition need not be commutative and only left or right distributive law is assumed. In this paper the term "nearring" means a left nearring with identity. For terminology and basic facts about nearrings, see [1]–[4].

Clearly every associative ring is a nearring and each group is the additive group of a nearring, but not necessarily of a nearring with identity. The question what group can be the additive group of a nearring with identity is far from solution.

J. R. Clay and J. J. Malone ([5]) shown that on each cyclic group there is a unique nearring with identity which is in fact a commutative ring with identity. Furthermore, it was proved in [5], [6] and [7], respectively, that there does not exist a nearring with identity whose additive group is the symmetric group S_n with $n \geq 3$, the alternating group A_n with $n \geq 4$ or a finite non-abelian group with exactly one non-trivial proper normal subgroup. For groups whose lattice of normal subgroups is linearly ordered, the latter results were generalized by J. E. Krimmel in [8].

Further, J. R. Clay ([9]) proved that there exists no nearring on the quaternion group and found all nearrings with identity on the dihedral group of order 8. J. R. Clay and C. J. Maxson ([10]) showed that the generalized quaternion groups cannot be the additive groups of nearrings with identity. The dihedral groups D_n of order $2n$ as additive groups of a nearring with identity were investigated by M. J. Johnson ([11]). He proved that D_n is such a group if and only if $n = 2p$ for a prime number p and in the case, where p is odd, there exists, up to an isomorphism, a unique nearring with identity on D_n. T. H. H. Boykett and C. Nöbauer ([12]) classyfied all non-abelian groups of order less than 32 that can be the additive groups of a nearring with identity and found the number of non-isomorphic nearrings with identity on such groups (see also [14]).

2010 *Mathematics Subject Classification:* 16Y30.
Keywords: nearring with identity; additive group; Miller-Moreno group.

It is easily seen that every finite abelian group is the additive group of a ring and so a nearring with identity. Therefore the next natural step is to consider nearrings with identity whose additive group is minimal non-abelian or, in a different terminology, a Miller-Moreno group ([13]).

2. Preliminaries. We recall first some definitions.

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

1) $(R, +)$ is a (not necessarily abelian) 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, $z \in R$.

The group $(R, +)$ is said to be the additive group of R and denoted by R^+. Note that from Definition 1 it does not follow that $0 \cdot x = 0$ for each $x \in R$. A nearring R with the latter property is called zero-symmetric. If $(R, \cdot)$ is a monoid with identity i, then R is a nearring with identity i. In this case the group of all invertible elements of $(R, \cdot)$ is called the multiplicative group of R and denoted by R^*.

Recall that a finite group is called a Miller-Moreno group if it is non-abelian and all its proper subgroups are abelian. The structure of these groups is completely described by the well-known theorem of Redei (see, [13]).

Theorem 1. *Finite Miller-Moreno groups are groups of the following types:*

1) *the quaternion group Q_8;*
2) *the group $G = \langle a \rangle \rtimes \langle b \rangle$ of order p^{m+n} with $a^{p^m} = b^{p^n} = 1$ and $b^{-1}ab = a^{1+p^{m-1}}$, where p is prime, $m \geq 2$ and $n \geq 1$;*
3) *the group $G = (\langle a \rangle \times \langle c \rangle) \rtimes \langle b \rangle$ of order p^{m+n+1} with $a^{p^m} = b^{p^n} = c^p = 1$, $b^{-1}ab = ac$ and $b^{-1}cb = c$, where $m \geq n \geq 1$ and $m + n > 2$ for $p = 2$;*
4) *the group $G = P \rtimes \langle b \rangle$ of order $p^r q^s$ with an elementary abelian subgroup P of order p^r in which the element b induces an irreducible automorphism of prime order q and, in addition, $b^{q^s} = 1$ and $\langle b^q \rangle = Z(G)$, where p and q are different prime numbers and r, s are natural numbers.*

Recall that the exponent of a finite group is the least common multiple of orders of its elements. In particular, the exponent of a finite p-group is the maximal order of its elements.

The next 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.*

It is easily seen that any Miller-Moreno group of type 4) from Theorem 1 has no element whose order coincides with its exponent. This and Lemma 1 imply the following assertion.

Lemma 2. *There does not exist a nearring with identity whose additive group is isomorphic to a group of type 4) from Theorem 1.*

In what follows we use the following notation:

1) $G(p^m, p^n)$ denotes an additively written group of type 2) from Theorem 1 with generators a and b of orders p^m and p^n, respectively, so that $-b+a+b = a(1+p^{m-1})$;
2) $G(p^m, p^n, p)$ denotes an additively written group of type 3) from Theorem 1 with generators a, b and c of orders p^m, p^n and p, respectively, so that $-b+a+b = a+c$ and $-b+c+b = c$.

Lemmas 3 and 4 can be easily obtained by simple calculations.

Lemma 3. *In the group $G(p^m, p^n)$, for any natural numbers r, s and t, the equalities $bs + ar = ar(1 - sp^{m-1}) + bs$ and $(ar + bs)t = ar(t - s\binom{t}{2}p^{m-1}) + bst$ hold.*

Lemma 4. *The exponent of $G(p^m, p^n)$ is equal to p^m for $m > n$ and to p^n for $m \le n$. Moreover, if x is an element of maximal order in $G(p^m, p^n)$, then there exist generators a, b of this group such that either $x = a$ or $x = b$ and the relations $ap^m = bp^n = 0$ and $-b+a+b = a(1+p^{m-1})$ hold.*

Definition 2. 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^+.

Let the additive group of a nearring R with identity is isomorphic to a group $G(p^m, p^n)$. It follows from Lemma 4 that $R^+ = \langle a \rangle + \langle b \rangle$ with elements a, b one of which coincides with identity element of R and the relations $ap^m = bp^n = 0$ and $a+b = b+a(1+p^{m-1})$ are valid. Moreover, each element $x \in R$ is uniquely written in the form $x = ax_1 + bx_2$ with coefficients $0 \le x_1 < p^m$ and $0 \le x_2 < p^n$.

Consider the case when a coincides with identity element of R, so that $xa = ax = x$ for each $x \in R$. Then R^+ is of exponent p^m by Lemma 4 and so $m \ge n$. Furthermore, for each $x \in R$ there exist integers $\alpha(x)$ and $\beta(x)$ such that $xb = a\alpha(x) + b\beta(x)$. It is clear that modulo p^m and p^n, respectively, these integers are uniquely determined by x and so some mappings $\alpha\colon R \to \mathbb{Z}_{p^m}$ and $\beta\colon R \to \mathbb{Z}_{p^n}$ are determined.

Lemma 5. *Let $x = ax_1 + bx_2$ and $y = ay_1 + by_2$ be elements of R. If a coincides with identity element of R, then $m \ge n+1$ and*

$$xy = a\Big[(x_1y_1 + \alpha(x)y_2) - \Big(x_1x_2\binom{y_1}{2} + \alpha(x)x_2y_1y_2 + \alpha(x)\beta(x)\binom{y_2}{2}\Big)p^{m-1}\Big] + b(x_2y_1 + \beta(x)y_2).$$

Moreover, for the mappings $\alpha\colon R \to \mathbb{Z}_{p^m}$ and $\beta\colon R \to \mathbb{Z}_{p^n}$ 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) $\alpha(x) \equiv 0 (\mathrm{mod}\, p^{m-n})$, *except the case* $p = 2 = m$ *and* $n = 1$;

(3) $x_1(\beta(x) - 1) \equiv x_2\alpha(x) (\mathrm{mod}\, p)$;

(4) $\alpha(xy) = x_1\alpha(y) + \alpha(x)\beta(y) - [x_1x_2\binom{\alpha(y)}{2} + \alpha(x)x_2\alpha(y)\beta(y) + \alpha(x)\beta(x)\binom{\beta(y)}{2}]p^{m-1}$;

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

Proof. By the left distributive law, we have

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

Furthermore, Lemma 3 implies that

$$(ax_1+bx_2)y_1 = ax_1\Big(y_1 - x_2\binom{y_1}{2}p^{m-1}\Big) + bx_2y_1,$$

$$(a\alpha(x)+b\beta(x))y_2 = a\alpha(x)\Big(y_2 - \beta(x)\binom{y_2}{2}p^{m-1}\Big) + b\beta(x)y_2,$$

$$bx_2y_1 + a\alpha(x)\Big(y_2 - \beta(x)\binom{y_2}{2}p^{m-1}\Big) = a\alpha(x)\Big(y_2 - \beta(x)\binom{y_2}{2}p^{m-1}\Big)(1 - x_2y_1p^{m-1}) + bx_2y_1.$$

Thus

$$xy = a\Big[(x_1y_1+\alpha(x)y_2) - \Big(x_1x_2\binom{y_1}{2} + \alpha(x)x_2y_1y_2 + \\ +\alpha(x)\beta(x)\binom{y_2}{2}\Big)p^{m-1}\Big] + b(x_2y_1+\beta(x)y_2), \tag{1}$$

as desired.

As $0\cdot a = a\cdot 0 = 0$, the nearring R is zero-symmetric if and only if $0 = 0\cdot b = a\alpha(0)+b\beta(0)$ whence $\alpha(0) = \beta(0) = 0$. Similarly, from the equality $b = ab = a\alpha(a) + b\beta(a)$ it follows that $\alpha(a) = 0$ and $\beta(a) = 1$. Since $(xb)p^n = x(bp^n) = 0$ and $xb = a\alpha(x) + b\beta(x)$, we have $0 = (a\alpha(x) + b\beta(x))p^n = a\alpha(x)(p^n - \beta(x)\binom{p^n}{2}p^{m-1})$ by Lemma 3 and hence $\alpha(x) \equiv 0(\mathrm{mod}\, p^{m-n})$, except the case $p = 2 = m$ and $n = 1$ in which the group R^+ is dihedral of order 8. Next, if $y = a(1-p^{m-1}) + b$, then

$$xy = a[\alpha(x) + x_1 - (x_1 + \alpha(x)x_2)p^{m-1}] + b(x_2(1-p^{m-1}) + \beta(x))$$

by formula (1). On the other hand, $y = b + a$ and so

$$xy = xb + x = a(\alpha(x) + x_1 - x_1\beta(x)p^{m-1}) + b(x_2 + \beta(x))$$

by Lemma 3. Comparing both results for xy, we obtain

$$(x_1 + \alpha(x)x_2)p^{m-1} \equiv x_1\beta(x)p^{m-1}(\mathrm{mod}\, p^m)$$

and $x_2(1-p^{m-1}) + \beta(x) \equiv x_2 + \beta(x)(\mathrm{mod}\, p^n)$. Thus $m \geq n+1$ and $x_1(\beta(x)-1) \equiv x_2\alpha(x)(\mathrm{mod}\, p)$ and so statement (3) holds.

Finally, the associativity of multiplication in R implies that $x(yb) = (xy)b = a\alpha(xy) + b\beta(xy)$. Furthermore, substituting $yb = a\alpha(y) + b\beta(y)$ instead of y in formula (1), we also have

$$x(yb) = a\Big[(x_1\alpha(y) + \alpha(x)\beta(y)) - \Big(x_1x_2\binom{\alpha(y)}{2} + \alpha(x)x_2\alpha(y)\beta(y) + \tag{2}$$

$$+\alpha(x)\beta(x)\binom{\beta(y)}{2}\Big)p^{m-1}\Big] + b(x_2\alpha(y) + \beta(x)\beta(y)). \tag{3}$$

Comparing the coefficients under a and b in two expressions obtained for $x(yb)$, we derive statements (4) and (5) of the lemma. □

As a conclusion we summarize the results obtained in [15] and [16].

Theorem 2. *A Miller-Moreno group G is the additive group of a local nearring R if and only if it is a p-group for some prime p and one of the following statements hold:*

1) *the group G is isomorphic to one of the groups $G(p^m, p^n)$ with $p^{m+n} > 8$ and $m > n$ and the cyclic subgroup of order p^m generated by i is normal in G;*
2) *$p = 2$, the group G is isomorphic to one of the groups $G(2^m, 2^n)$ with $m \leq n$ and the cyclic subgroup of order 2^n generated by i is not normal in G;*
3) *the group G is isomorphic to one of the groups $G(p^m, p^n, p)$ and the cyclic subgroup generated by i is not normal in G.*

3. The main theorem. In this section we describe all possible types of Miller-Moreno groups which are the additive groups of nearrings with identity.

Theorem 3. *Let G be a Miller-Moreno group. The group G is the additive group of a nearring R with identity if and only if G is either one of the groups from Theorem 2 or the group $G(4, 2)$.*

Proof. Let there exist a nearring R with identity i whose additive group is G. Since G cannot be isomorphic to Q_8 by a result of J. R. Clay ([9]), it follows from Theorem 1 and Lemma 2 that G is isomorphic to one of the groups $G(p^m, p^n)$ or $G(p^m, p^n, p)$ for a suitable prime p and natural numbers m, n. The smallest of these groups is the dihedral group $G(4, 2)$ on which there exists a nearring R with identity by another result of J. R. Clay mentioned in the introduction. Next, the groups $G(p^m, p^n)$ with $p^{m+n} > 8$ and $m > n$, $G(2^m, 2^n)$ with $m \leq n$ and $G(p^m, p^n, p)$ with $m + n > 2$ for $p = 2$ are groups from Theorem 2. Therefore it remains to consider only the case where G is isomorphic to $G(p^m, p^n)$ with $m \leq n$ and $p > 2$.

Since i is an element of maximal order of G by Lemma 1, it follows from Lemma 4 that there exist generators a of order p^m and b of order p^n of this group such that $-b + a + b = a(1 + p^{m-1})$ and either $a = i$ or $b = i$. If $a = i$, then $m = n$ which is impossible by Lemma 5. We show that the case $b = i$ is also impossible.

Suppose the contrary, so that for each $x \in R$ we have $xb = x$. Since x is uniquely written in the form $x = ax_1 + bx_2$ with coefficients $0 \leq x_1 < p^m$ and $0 \leq x_2 < p^n$, there exist coefficients $\alpha(x)$ and $\beta(x)$ such that $xa = a\alpha(x) + b\beta(x)$. Moreover, it follows from [16], Lemma 8, that they satisfy the following conditions:

(1) $\alpha(b) \equiv 1 (\mathrm{mod}\, p^m)$ and $\beta(b) \equiv 0 (\mathrm{mod}\, p^n)$;

(2) $\alpha(x)(1 - x_2) \equiv 0 (\mathrm{mod}\, p)$;

(3) $\alpha(xy) \equiv \alpha(x)\alpha(y) + x_1\beta(y) - x_1x_2\binom{\beta(y)}{2}p^{m-1} (\mathrm{mod}\, p^m)$.

Put $x = y = -b$, so that $x_1 = y_1 = 0$ and $x_2 = y_2 = -1$. Then $2\alpha(-b) \equiv 0 (\mathrm{mod}\, p)$ by statement (2) which implies $\alpha(-b) \equiv 0 (\mathrm{mod}\, p)$. On the other hand, $b = (-b)^2$ and

$$\alpha((-b)^2) \equiv \alpha(-b)^2 (\mathrm{mod}\, p^m)$$

by statement (3). Therefore $\alpha(b) = \alpha((-b)^2) \equiv 0 (\mathrm{mod}\, p)$. Since $\alpha(b) \equiv 1 (\mathrm{mod}\, p^m)$ by statement (1), we have a contradiction. Thus the case $b = i$ is impossible, as desired. □

The following assertion is a direct consequence of Theorem 3.

Corollary 1. *There does not exist a nearring with identity whose additive group is isomorphic to the group $G(p^m, p^n)$ with $p > 2$ and $2 \leq m \leq n$.*

REFERENCES

1. Pilz G. Near-rings. The theory and its applications. – North Holland, Amsterdam, 1977.
2. Meldrum J.D.P. Near-rings and their links with groups. – London: Pitman Publishing Limited, 1985. – 273 p.
3. Clay J.R. Nearrings. Geneses and applications. – New York: Clarendon Press, Oxford University Press, 1992.
4. Ferrero C.C., Ferrero G. Nearrings. Some developments linked to semigroups and groups. – Kluwer Academic Publishers, Dordrecht, 2002. – 609 p.
5. Clay J.R., Malone Jr. *The near-rings with identities on certain finite groups*// Math. Scand. – 1966. – V.19. – P. 146–150.
6. Clay J.R., Doi D. *Near-rings with identity on alternating groups*// Math. Scand. – 1968. – V.23. – P. 54–56.
7. Ligh S. *Near rings with identities on certain groups*// Monatsh. Math. – 1971. – V.75. – P. 38–43.
8. Krimmel J.E. *A condition on near-rings with identity*// Monatsh. Math. – 1973. – V.77. – P. 52–54.
9. Clay J.R. *Research in near-ring theory using a digital computer*// BIT. – 1970. – V.10. – P. 249–265.
10. Clay J.R., Maxson C.J. *The near-rings with identities on generalized quaternion groups*// Ist. Lombardo Accad. Sci. Lett. Rend. A. – 1970. – V.104. – P. 525–530.
11. Johnson M.J. *Near-rings with identities on dihedral groups*// Proceedings of the Edinburgh Mathematical Society. – 1973. – V.18. – P. 219–228.
12. Boykett T.H.H., Nöbauer C. *A class of groups which cannot be the additive groups of near-rings with identity*// Contributions to general algebra. Klagenfurt: Heyn. – 1998. – V.10. – P. 89–99.
13. Redei L. *Das "schiefe Produkt" in der Gruppentheorie mit Anwendung auf die endlichen nichtkommutativen Gruppen mit lauter kommutativen echten Untergruppen und die Ordnungszahlen, zu denen nur kommutative Gruppen gehören*// Comment. Math. Helv. – 1947. – V.20. – P. 225–264.
14. Aichinger E., Binder F., Ecker J., Mayr P., Nöbauer C. SONATA – system of near-rings and their applications, GAP package, Version 2.6; 2012. (http:// www.algebra.uni-linz.ac.at/Sonata/)
15. Raievska I.Yu., Raievska M.Yu., Sysak Ya.P. *Local nearrings on nonmetacyclic Miller-Moreno groups*// Bulletin of Taras Shevchenko National University of Kyiv. Series: Physics and Mathematics. – 2012. – V.3. – P. 39–46. (in Ukrainian)
16. Raievska I.Yu., Sysak Ya.P. *Finite local nearrings on metacyclic Miller-Moreno p-groups*// Algebra and Discrete Mathematics. – 2012. – V.13, №1. – P. 111–127.

Institute of Mathematics of NAS of Ukraine
raemarina@rambler.ru.

Received 6.08.2014