LOCAL NEAR-RINGS OF CARDINALITY p^2

Carlton J. Maxson*

(received February 9, 1968)

The main result of this paper is the determination of all non-isomorphic local near-rings $\langle N, +, \cdot\rangle$ with $\langle N, +\rangle \tilde{=} \langle C(p) \times C(p), +\rangle$ which are not near-fields. Together with the fundamental paper [6] by Zassenhaus on near-fields and the corollary to Theorem 1 of [2], this paper gives a complete description of all local near-rings of order p^2.

We recall that a unitary near-ring N is called local if the subset L of elements in N without left inverses is an (N, N)-subgroup and $N \neq J(N)$. ($J(N)$ denotes the radical of N given in [1].) In [3] it was proved that $N \neq J(N)$ whenever L is an ideal of N. (For previous results concerning local near-rings we refer the reader to [3].)

In this paper "local near-ring" will mean a finite local near-ring which is not a near field. Furthermore, it will be assumed that local near-rings N of order $|N| = p^2$ have additive groups isomorphic to $\langle C(p) \times C(p), +\rangle$ where $C(p) = \{0, 1, 2, \ldots, p-1\}$.

In the first section we show that the local near-rings under consideration give rise to maps $\rho : C(p) \to C(p)$ satisfying

(i) $\rho(x) = 0 \quad \langle = \rangle \quad x = 0$,

(ii) ρ is a group endomorphism of $\langle C(p)-\{0\}, \cdot\rangle$

and conversely, every such map ρ determines a local near-ring with additive group isomorphic to $\langle C(p) \times C(p), +\rangle$. We then establish that the number of non-isomorphic local near-rings of order p^2 is $p - 1$.

In §2 the apparently more general problem of determining all local near-rings N with $|L| = p$ is considered. However we show that such near-rings must have cardinality p^2 and hence have been determined.

*This work was supported by the Research Foundation of the State University of New York.

1. Local near-rings of order p^2. In this section $N \equiv \langle N, +, \cdot \rangle$ denotes a local near-ring of order $|N| = p^2$ and L denotes the set of elements in N which do not have left inverses in N. Since $L \equiv \langle L, +, \cdot \rangle$ is a proper ideal of N and N is not a near-field, $(0) \subset L \subset N$ implies that $\neq \quad \neq$ $\langle L, + \rangle$ is a cyclic subgroup of $\langle N, + \rangle$ of order $|L| = p$.

LEMMA 1.1. $\forall\, x \in L$, $Lx = (0)$.

Proof. Assume $Lx \neq (0)$ for $x \neq 0 \in L$. Then $Lx = L$ and so there exists $k \in L$ such that $kx = -x$ or $(1 + k)x = 0$. Since $1 \notin L$, $1 + k \notin L$ which means that there is some $\bar{k} \in N$ such that $\bar{k}(1 + k) = 1$. But then $x = \bar{k}(1 + k)x = 0$.

If e denotes the multiplicative identity of N then the order of e is p (see [2]); i.e., e is an element of maximal order in N. Let (e) denote the cyclic subgroup of $\langle N, + \rangle$ generated by e. It is clear that $(e) \cap \langle L, + \rangle = (0)$ and since $|(e)| = |L| = p$ we have

LEMMA 1.2. If (e) denotes the cyclic group of N generated by the multiplicative identity e then $\langle N, + \rangle = (e) \oplus \langle L, + \rangle$.

Let ℓ be a generator of $\langle L, + \rangle$. With respect to the basis $\{e, \ell\}$ each element $x \in N$ has the unique representation $x = x_1 e + x_2 \ell$ where $x_i \in C(p) = \{0, 1, 2, \ldots, p-1\}$, $i = 1, 2$. Thus we take $\langle N, + \rangle = \langle C(p) \times C(p), + \rangle$ where the addition $+$ on $C(p) \times C(p)$ is pointwise. Hence $e = \langle 1, 0 \rangle$, $\ell = \langle 0, 1 \rangle$ and $L = \{\langle 0, x \rangle \mid x \in C(p)\}$.

As in [4] every element $x = \langle x_1, x_2 \rangle \in N$ is associated with a matrix

$$M(x) = \begin{bmatrix} x_1 & x_2 \\ \rho_{21}(x) & \rho_{22}(x) \end{bmatrix}$$

where $\rho_{2i} : C(p) \times C(p) \to C(p)$ is a mapping with $\rho_{2i}(0, 0) = 0$, $i = 1, 2$, $\rho_{21}(1, 0) = 0$ and $\rho_{22}(1, 0) = 1$. Moreover the multiplication $\cdot$ in N is given by

$$\langle x_1, x_2 \rangle \cdot \langle y_1, y_2 \rangle = \langle x_1, x_2 \rangle \cdot M(y) = \langle x_1 y_1 + x_2 \rho_{21}(y),\ x_1 y_2 + x_2 \rho_{22}(y) \rangle.$$

https://doi.org/10.4153/CMB-1968-066-2 Published online by Cambridge University Press

Let $y = \langle y_1, y_2 \rangle \in N$. Since L is an (N, N)-subgroup, $\langle 0, 1 \rangle \cdot \langle y_1, y_2 \rangle = \langle \rho_{21}(y), \rho_{22}(y) \rangle \in L$ which implies that $\rho_{21}(y) = 0$, $y \in N$. Using some rather technical lemmas we next show that $\rho_{22} \equiv \rho$ can be considered as a map with domain $C(p)$.

LEMMA 1.3. $\langle 0, 1 \rangle \cdot \langle 1, 1 \rangle = \langle 0, 1 \rangle$.

Proof. Let $\rho(1, 1) = k$ where $k \in C(p)$. Then $\langle 0, 1 \rangle \cdot \langle 1, 1 \rangle = \langle 0, k \rangle$ and so for all $y \in C(p)$, $\langle y - ky, y \rangle \cdot \langle 1, 1 \rangle = \langle y - ky, y \rangle$. If $u = \langle y - ky, y \rangle \notin L$ then there exists $w \in N$ such that $wu = \langle 1, 0 \rangle$. This in turn gives $\langle 1, 1 \rangle = w \cdot u \cdot \langle 1, 1 \rangle = w \cdot u = \langle 1, 0 \rangle$. This contradiction shows that $u \in L$ and hence $y = ky$. But since $k \in C(p)$, $k = 1$ which is the desired result.

LEMMA 1.4. For all $b \in C(p)$, $\langle 0, 1 \rangle \cdot \langle 1, b \rangle = \langle 0, 1 \rangle$.

Proof. The result is clear if $b = 0$ or $b = 1$. We note further that $\langle 1, 1 \rangle^m = \langle 1, m' \rangle$ where $m' \in C(p)$, $m' \equiv m \bmod p$. For if $m = 2$ then $\langle 1, 1 \rangle \cdot \langle 1, 1 \rangle = \langle 1, 0 \rangle \cdot \langle 1, 1 \rangle + \langle 0, 1 \rangle \cdot \langle 1, 1 \rangle = \langle 1, 1 \rangle + \langle 0, 1 \rangle = \langle 1, 2 \rangle$ and $\langle 1, 1 \rangle^n = \langle 1, n-1 \rangle \cdot \langle 1, 1 \rangle = \langle 1, 0 \rangle \cdot \langle 1, 1 \rangle + (n-1)\langle 0, 1 \rangle \cdot \langle 1, 1 \rangle = \langle 1, n \rangle$. Then using associativity, $\langle 0, 1 \rangle \cdot \langle 1, b \rangle = \langle 0, 1 \rangle \langle 1, 1 \rangle^b = \langle 0, 1 \rangle$.

If $r \in N$ and $r \notin L$ then for every non-zero $x \in N$, $xr \neq 0$; otherwise since $r \notin L$, r is a unit and this implies $x = x \cdot 1 = xrr^{-1} = 0 \cdot r^{-1} = 0$. Hence for all $a (\neq 0) \in C(p)$, we have $\langle 0, 1 \rangle \cdot \langle a, 0 \rangle = \langle 0, k \rangle$, $k \neq 0$ in $C(p)$. Thus for all $b \in C(p)$, $\langle 0, 1 \rangle \cdot \langle a, b \rangle = \langle 0, 1 \rangle \cdot (\langle 1, bk^{-1} \rangle \cdot \langle a, 0 \rangle) = \langle 0, 1 \rangle \langle a, 0 \rangle = \langle 0, k \rangle$. This proves:

LEMMA 1.5. If $a (\neq 0) \in C(p)$ then $\langle 0, 1 \rangle \cdot \langle a, 0 \rangle = \langle 0, k \rangle$ where $k \neq 0$ in $C(p)$ and for all $b \in C(p)$, $\langle 0, 1 \rangle \cdot \langle a, b \rangle = \langle 0, k \rangle$.

From Lemma 1.1 which shows $\langle 0, 1 \rangle \cdot \langle 0, b \rangle = \langle 0, 0 \rangle$ for all $b \in N$ (i.e., $\rho(0, b) = 0$) and the preceding lemma we see that $\rho : \langle x_1, x_2 \rangle \in C(p) \times C(p) \mapsto y \in C(p)$ depends only on the first component and can therefore be considered as a map $\rho : C(p) \to C(p)$. Moreover the map $\rho : C(p) \to C(p)$ associated with the near-ring N is independent of the choice ℓ of generator of L. For if k also generates L then a map $\sigma : C(p) \to C(p)$ is determined using the basis $\{e, k\}$ of $\langle N, + \rangle$. With respect to the basis $\{e, \ell\}$, $k = a\ell$ for some $a \in C(p)$ and for every $x \in C(p)$, $\langle 0, a \rangle \cdot \langle x, 0 \rangle = \langle 0, a\rho(x) \rangle$. With respect to the basis $\{e, k\}$ this same product in N is $\langle 0, \sigma(x) \rangle$. Hence $\sigma(x)k = a\rho(x)\ell$ and since $k = a\ell \neq 0$ in $C(p)$ we have $\sigma(x) = \rho(x)$ for all $x \in C(p)$.

The associativity of the multiplication in N is equivalent to $M(x) \cdot M(y) = M(x \cdot y)$ (see [4]) where $x = \langle x_1, x_2 \rangle$, $\langle y_1, y_2 \rangle$, $z = \langle z_1, z_2 \rangle$

https://doi.org/10.4153/CMB-1968-066-2 Published online by Cambridge University Press

in N which in turn implies $\rho(x_1)\cdot\rho(y_1) = \rho(x_1y_1)$ in $C(p)$. Moreover $x_1 \neq 0$ in $C(p)$ implies $x = \langle x_1, x_2\rangle$ has a left inverse in N and thus there exists $y = \langle y_1, y_2\rangle$ with $y_1x_1 \equiv 1 \bmod p$ and $y_1x_2 + y_2\rho(x_1) \equiv 0 \bmod p$. Hence $\rho(x_1) \neq 0$ for $x_1 \neq 0$. We have established:

THEOREM 1.6. Every local near-ring with cardinality p^2 determines a map $\rho : C(p) \to C(p)$ which satisfies

(S) (i) $\rho(x) = 0 \iff x = 0$, $x \in C(p)$,

(ii) ρ is a group endomorphism of $\langle C(p) - \{0\}, \cdot\rangle$.

Conversely suppose we are given a map $\rho : C(p) \to C(p)$ which satisfies conditions (S) of the above theorem. Using ρ we define a multiplication $*$ on $\langle N, +\rangle \equiv \langle C(p) \times C(p), +\rangle$ as follows:

$$(\#\#) \qquad \langle x_1, x_2\rangle * \langle y_1, y_2\rangle = \langle x_1, x_2\rangle \begin{bmatrix} y_1 & y_2 \\ 0 & \rho(y_1) \end{bmatrix}.$$

It is easily verified that $*$ is associative and right distributive over $+$. Moreover $\langle 0, 0\rangle$ is a two-sided zero and $\langle 1, 0\rangle$ a two-sided identity for $*$.

We also note that for each $y = \langle y_1, y_2\rangle \in N$ the system

$$x_1y_1 \equiv 1 \bmod p$$

$$x_1y_2 + x_2\rho(y_1) \equiv 0 \bmod p$$

has a unique solution mod p if and only if

$$\begin{bmatrix} y_1 & 0 \\ y_2 & \rho(y_1) \end{bmatrix} = \begin{bmatrix} y_1 & y_2 \\ 0 & \rho(y_1) \end{bmatrix} \neq 0 \bmod p.$$

https://doi.org/10.4153/CMB-1968-066-2 Published online by Cambridge University Press

That is, if and only if $y_1 \neq 0$ in $C(p)$. Hence if L denotes the set of elements without left inverses in N then $y = \langle y_1, y_2 \rangle \in L$ if and only if $y_1 = 0$. It is clear that L is an (N, N)-subgroup and for $x, y \in N$, $k \in L$, an easy computation shows $x * (y + k) - x * y \in L$. This proves:

THEOREM 1.7. If $\rho : C(p) \to C(p)$ satisfies conditions (S) of Theorem 1.6 then $N \equiv \langle C(p) \times C(p), +, * \rangle$ is a local near-ring where $+$ is point-wise addition and $*$ is given by $(\#)$.

COROLLARY 1.8. The near-ring given in the above theorem is a ring $\iff \rho \in \mathrm{End}\ (\langle C(p), + \rangle)$.

Proof. Let $x, y, z \in N$, $x = \langle x_1, x_2 \rangle$, $y = \langle y_1, y_2 \rangle$ and $z = \langle z_1, z_2 \rangle$. Then $x * (y + z) = x * y + x * z \iff \langle x_1, x_2 \rangle * (y_1 + z_1, y_2 + z_2 \rangle = \langle x_1, x_2 \rangle * \langle y_1, y_2 \rangle + \langle x_1, x_2 \rangle * \langle z_1, z_2 \rangle$; i.e., $\iff \langle x_1(y_1 + z_1), x_1(y_2 + z_2) + x_2\rho(y_1 + z_1) \rangle = \langle x_1 y_1, x_1 y_2 + x_2 \rho(y_1) \rangle + \langle x_1 z_1, x_1 z_2 + x_2 \rho(z_1) \rangle$. But this is true if and only if $\rho(y_1) + \rho(z_1) = \rho(y_1 + z_1)$.

Theorems 1.6 and 1.7 show that every local near-ring of order p^2 determines a function $\rho : C(p) \to C(p)$ satisfying certain conditions (S) and conversely every such function determines a local near-ring of order p^2. We next show there exists a bijection between the set of functions satisfying (S) and the set of isomorphic classes of local near-rings of order p^2.

LEMMA 1.9. Every map $\rho : C(p) \to C(p)$ satisfying conditions (S) determines a set of isomorphic local near-rings.

Proof. Let N_1 and N_2 be local near-rings of order p^2 with multiplications $*_1$ and $*_2$ respectively, given by ρ. Let e_i denote the identity of N_i and ℓ_i a generator of L_i in N_i, $i = 1, 2$. The map $\emptyset : N_1 \to N_2$ given by $\emptyset(e_1) = e_2$ and $\emptyset(\ell_1) = \ell_2$ is a group isomorphism. It remains to show that $\emptyset$ is a near-ring homomorphism. To this end let $x = x_1 e_1 + x_2 \ell_1$ and $y = y_1 e_1 + y_2 \ell_2$ in N_1. Then $x *_1 y = x_1 y_1 e_1 + (x_1 y_2 + x_2 \rho(y_1)) \ell_1$ and $\emptyset(x *_1 y) = x_1 y_1 e_2 + (x_1 y_2 + x_2 \rho(y_1)) \ell_2 = \emptyset(x) *_2 \emptyset(y)$.

Let $N_1 \equiv \langle N_1, +, *_1 \rangle$, $N_2 \equiv \langle N_2, +, *_2 \rangle$ and $\emptyset : N_1 \to N_2$ be a near-ring isomorphism. Suppose further that $*_i$ determines ρ_i, $i = 1, 2$. As observed above, ρ_2 is independent of the choice of generator of L_2 and so without loss of generality we use $\{e_2, \emptyset(\ell_1)\}$ as a basis of

https://doi.org/10.4153/CMB-1968-066-2 Published online by Cambridge University Press

$\langle N_2, +\rangle$ where $\{e_1, \ell_1\}$ is a basis of $\langle N_1, +\rangle$. Hence $\emptyset(\langle 1, 0\rangle) = \langle 1, 0\rangle \in N_2$ and $\emptyset(\langle 0, 1\rangle) = \langle 0, 1\rangle \in N_2$. Thus for every $x \in C(p)$, $\langle 0, \rho_1(x)\rangle = \emptyset(\langle 0, \rho_1(x)\rangle) = \emptyset(\langle 0, 1\rangle *_1 \langle x, 0\rangle) = \emptyset(\langle 0, 1\rangle) *_2 \emptyset(\langle x, 0\rangle) = \langle 0, 1\rangle *_2 \langle x, 0\rangle = \langle 0, \rho_2(x)\rangle$; i.e., $\rho_1 = \rho_2$. Together with Lemma 1.9 this establishes:

THEOREM 1.10. *If $N_i = \langle N_i, +, *_i\rangle$ are local near rings of order p^2 where $*_i$ determines ρ_i, $i = 1, 2$ then $N_1 \cong N_2 \iff \rho_1 = \rho_2$.*

Thus, to determine the number of non-isomorphic local near-rings $\langle N, +, \cdot\rangle$ with $\langle N, +\rangle \cong \langle C(p) \times C(p), +\rangle$, which are not near-fields, it suffices to find the number of maps $\rho : C(p) \to C(p)$ satisfying conditions (S). This is precisely the cardinality of End $(\langle C(p) - \{0\}, \cdot\rangle)$ which is well-known to be $p - 1$ ([5]).

COROLLARY 1.11. *Up to isomorphism there are $p - 1$ local near-rings $N \equiv \langle N, +, \cdot\rangle$ with additive group isomorphic to $\langle C(p) \times C(p), +\rangle$ which are not near-fields.*

In particular, local near-rings N of cardinality $|N| = 4$ which are not near-fields are local rings. For $p \geq 3$ the maps $\rho : C(p) \to C(p)$ given by

$$\rho(x) = \begin{cases} 0 & x = 0, \\ 1 & \text{otherwise,} \end{cases}$$

determine local near-rings of orders p^2 which are not rings.

2. Finite local near-rings with $|L| = p$. Let y be an arbitrary element of a near-ring N. It is easily verified that the left annihilator of y, $A_\ell(y) = \{x \in N \mid xy = 0\}$, is a left ideal of N.

Let N denote a finite local near-ring (not a near-field) and let $y \in L$, $y \neq 0$. The map $\theta_y : N \to Ny$ given by $\theta_y(x) = xy$, $x \in N$ is an N-epimorphism of ${}_N N$ and $\operatorname{Ker} \theta_y = A_\ell(y)$. Hence $N/A_\ell(y) \cong Ny$ and consequently $|N| = |A_\ell(y)| \cdot |Ny|$. But $y \in L$ implies $Ny \subseteq L$ and since $A_\ell(y) \neq N$ we have $A_\ell(y) \subseteq L$. This proves:

THEOREM 2.1. *If N is a finite local near-ring which is not a near-field then $|N| \leq |L|^2$.*

https://doi.org/10.4153/CMB-1968-066-2 Published online by Cambridge University Press

COROLLARY 2.2. $|L| = p \iff |N| = p^2$.

Proof. If $|N| = p^2$ then $|L| = p$ since we are assuming $|L| > 1$. Conversely if $|L| = p$ then $|N| \leq p^2$ implies $|N| = p^2$ since we know $|N| = p^n$ for some positive integer n.

Hence our results of § 1 determine all local near-rings N with $|L| = p$ which are not near-fields.

COROLLARY 2.3. If N is a finite local near-ring with $|L| = p$ then $\langle N, + \rangle$ is an abelian group.

REFERENCES

1. James C. Beidleman, A radical for near-ring modules. Mich. Math. J., 12 (1965) 377-383.

2. James R. Clay and Joseph J. Malone, Jr., The near-rings with identities on certain finite groups. Math. Scand. 19 (1966) 146-150.

3. Carlton J. Maxson, On local near-rings. Math. Z., 106 (1968) 197-205.

4. Carlton J. Maxson, On the construction of finite local near-rings (I): On non-cyclic abelian p-groups (to appear).

5. Hans J. Zassenhaus, The theory of groups, 2nd ed. (Chelsea, New York, 1958).

6. Hans J. Zassenhaus, Über endliche Fastkörper. Abh. Math. Sem., Univ. Hamburg, Vol. II (1936) 187-220.

State University College,
Fredonia,
New York 14063