Czechoslovak Mathematical Journal

Jung R. Cho; Tomáš Kepka

Finite simple zeropotent paramedial groupoids

Czechoslovak Mathematical Journal, Vol. 52 (2002), No. 1, 41–53

Persistent URL: http://dml.cz/dmlcz/127701

Czechoslovak Mathematical Journal, 52 (127) (2002), 41–53

FINITE SIMPLE ZEROPOTENT PARAMEDIAL GROUPOIDS

Jung R. Cho, Pusan, and Tomáš Kepka, Praha

(Received January 22, 1999)

Abstract. The study of paramedial groupoids (with emphasis on the structure of simple paramedial groupoids) was initiated in [1] and continued in [2], [3] and [5]. The aim of the present paper is to give a full description of finite simple zeropotent paramedial groupoids (i.e., of finite simple paramedial groupoids of type (II)—see [2]).

A reader is referred to [1], [2], [3] and [7] for notation and various prerequisites.

Keywords: groupoid, simple, paramedial

MSC 2000: 20N02

1. Introduction

Let $\mathcal{G}$ be a transitive permutation group on a non-empty finite set G^* and let $\mathcal{G}$ be generated by elements f and g, i.e. such that $\mathcal{G} = \langle f, g\rangle$. Let o be a symbol not in G^* and $G = G^* \cup \{o\}$. Now, define a multiplication on G as follows:

(a) $oo = o$;

(b) $ox = o = xo$ for every $x \in G^*$;

(c) $xy = o$ for all x, $y \in G^*$, $f(x) \neq g(y)$;

(d) $xy = f(x) = g(y)$ for all x, $y \in G^*$ such that $f(x) = g(y)$.

Then we denote the groupoid G defined in this way by $G = [\mathcal{G}, G^*, f, g, o]$.

1.1. Proposition.

(i) *G is a simple balanced groupoid.*

While working on this paper, the first author was supported by the Academic Research Fund, Ministry of Education, Korea, Project No. BSRI-97-1433, and the second author by the Grant Agency of the Czech Republic, Grant # 201/96/0312, and by the institutional grant MSM113200007.

(ii) *G is zeropotent if and only if $f(a) \neq g(a)$ for every $a \in G^*$.*
(iii) *If $f \neq g$ and $f^2 = g^2$, then G is zeropotent.*
(iv) *G is paramedial if and only if $f^2 = g^2$.*

P r o o f. (i) and (ii) See [7, Prop. 3.1].

(iii) The set $I = \{a \in G^*;\ f(a) \neq g(a)\}$ is non-empty. If $a \in I$, then $f^2(a) = g^2(a) \neq gf(a)$, so that $f(a) \in I$. Quite similarly, $g(a) \in I$ and we conclude that $I = G^*$.

(iv) Assume that G is paramedial and $a \in G^*$. Then there are b, c, $d \in G^*$ such that $f^2(a) = g^2(b)$, $f(a) = g(c)$ and $f(d) = g(b)$. Now, $o \neq f^2(a) = g^2(b) = ac \cdot db = bc \cdot da$, and so $bc \neq o$, $f(b) = g(c)$ and $a = b$. Thus $f^2(a) = g^2(a)$.

For the converse, assume $f^2 = g^2$ and let a, b, c, $d \in G$. Suppose first that $ac \cdot db \neq o$. Then none of a, b, c, d, ac and db is o and $f(a) = g(c) = ac$, $f(d) = g(b) = db$ and $f(ac) = g(db)$. Thus $g^2(a) = f^2(a) = fg(c) = f(ac) = g(bd) = g^2(b)$, and so $a = b$. Then obviously $ac \cdot db = bc \cdot da$. This argument also shows that if $ac \cdot db = o$, then $bc \cdot da = o$ as well, which completes the proof. □

Let $\mathcal{A}_{zppm}$ denote the class of all ordered quadruples (A, B, a, b), where A is a finite group, B a corefree subgroup of A and $A = \langle a, b\rangle$, $a \neq b$, $a^2 = b^2$. Now, define an equivalence relation $\approx$ on $\mathcal{A}_{zppm}$ by $(A_1, B_1, a_1, b_1) \approx (A_2, B_2, a_2, b_2)$ if and only if there is a (group) isomorphism $\lambda\colon A_1 \to A_2$ such that $\lambda(a_1) = a_2$, $\lambda(b_1) = b_2$ and the subgroups $\lambda(B_1)$, B_2 are conjugate in A_2.

For $(A, B, a, b) \in \mathcal{A}_{zppm}$, let A/B denote the set $\{xB;\ x \in A\}$ of all left cosets of B in A. For every $x \in A$, the equality $\pi(x)(yB) = xy(B)$ defines a permutation $\pi(x)$ of A/B. Thus $\pi(A)$ is a subgroup of the symmetric group on A/B and $\pi(A)$ is clearly transitive. Now, we put $\Phi\big((A, B, a, b)\big) = [\pi(A), A/B, \pi(a), \pi(b), o]$, $o \notin A/B$, the groupoid defined above.

Let G be a finite simple zeropotent paramedial groupoid (i.e., a finite simple paramedial groupoid of type (II)—see [2]) containing at least three elements. Now, G is balanced by [3, Theorem 2.1] and for every $a \in G^* = G\setminus\{o\}$ there exist uniquely determined elements b, $c \in G$ such that $f(a) = ab \neq o \neq ca = g(a)$. Furthermore, the mappings f, g are permutations of G^*, $f^2 = g^2$, $f \neq g$, and $\mathcal{G} = \langle f, g\rangle$ operates transitively on G^*. If $u \in G^*$ and $\mathcal{H} = \mathrm{Stab}_{\mathcal{G}}(u)$, then $\Psi(G) = (\mathcal{G}, \mathcal{H}, f, g) \in \mathcal{A}_{zppm}$.

1.2. Theorem. *There exists a one-to-one correspondence between isomorphism classes of finite simple zeropotent paramedial groupoids containing at least three elements and equivalence classes of quadruples from $\mathcal{A}_{zppm}$. This correspondence is given by Φ and Ψ.*

P r o o f. Combine 1.1 and [7, Theorem 4.1]. □

Throughout this section, let A be a finite non-commutative group generated by two elements a, b such that $a^2 = b^2$; obviously, $a \neq b$. We put $A_1 = \langle a \rangle$, $m = \mathrm{ord}(a) = \mathrm{card}(A_1)$, $c = a^{-1}b$, $C = \langle c \rangle$, $n = \mathrm{ord}(c)$, $D = \langle a^2 \rangle$, $E = A_1 \cap C$, $k = \mathrm{card}(E)$ and $F = Z(A) \cap C$, where $\mathrm{ord}(a)$ is the order of a, $\mathrm{card}(A)$ is the cardinality of A and $Z(A)$ is the centre of A.

2.1. Lemma.

(i) $A = \langle a, c \rangle$, $c = a^{-1}b = ab^{-1}$.

(ii) *For* $u \in C$, *we have* $a^{-1}ua = b^{-1}ub = aua^{-1} = bub^{-1} = u^{-1}$.

(iii) *For* $u \in C$ *we have* $u \in Z(A)$ *if and only if* $u^2 = 1$.

P r o o f. (i) and (ii) are trivial and (iii) follows by (ii). □

2.2. Lemma.

(i) $A' = \langle c^2 \rangle \subseteq C$, *where* A' *is the commutator subgroup of* A.

(ii) $A = A_1C$ *and every subgroup of* C *is normal in* A.

(iii) $D \subseteq Z(A) = DF$.

(iv) *If* n *is odd, then* $k = 1$ *and* $Z(A) = D \subseteq A_1$.

(v) *If* n *is even, then* $k = 2$ *and* F *is a unique minimal 2-subgroup of* C.

P r o o f. (i) We have $c^2 = a^{-1}bab^{-1} \in A'$, and so $K = \langle c^2 \rangle \subseteq A'$. On the other hand, $K \trianglelefteq A$ and A/K is abelian. Thus $K = A'$.

(ii) Easy.

(iii), (iv) and (v). Obviously, $D \subseteq Z(A)$. If $u \in C$, then $u \in Z(A)$ iff $a^{-1}ua = u = b^{-1}ub$, i.e., iff $u^2 = 1$. Further, if $u \in C$, $\alpha \in \mathbb{Z}$ and $a^\alpha u \in Z(A)$, then $a^\alpha u = a^{-1}a^\alpha ua = a^\alpha u^{-1}$, $u^2 = 1$, $u \in Z(A)$, $a^\alpha \in Z(A)$. Since $a^2 \in Z(A)$ and $a \notin Z(A)$, α is even and $a^\alpha \in D$. □

2.3. Lemma.

(i) $m \geqslant 2$ *is even and* $m = \mathrm{ord}(b)$.

(ii) $n \geqslant 3$.

(iii) $E = C \cap \langle b \rangle$ *and* $E \subseteq F$.

(iv) $k \mid m$ *and* $k \mid n$.

(v) *If either* n *is odd or* $4 \nmid m$, *then* $E = 1$ *and* $k = 1$.

(vi) $\mathrm{card}(A) = mn/k$ *is even.*

P r o o f. (i) If m is odd, then $a \in D \subseteq Z(A)$, which is not true. Hence m is even and $\mathrm{card}(D) = m/2$.

(ii) If $n \leqslant 2$, then $C \subseteq Z(A)$, which is again not true.

(iii), (iv) and (v) If $a^\alpha E = A_1 \cap C$, then, by 2.1(ii), $a^\alpha = a^{-1}a^\alpha a = b^{-1}a^\alpha b = a^{-\alpha}$. Thus $a^\alpha \in Z(A) \cap C = F$ and $a^{2\alpha} = 1$. Similarly, $C \cap \langle b\rangle \subseteq F$. In n is odd, then $F = 1$ by 2.2(iv), and so $E = 1 = C \cap \langle b\rangle$. Now, let n be even and $1 \neq a^\alpha \in E$. Since $E \subseteq Z(A)$, α is even and, since $a^{2\alpha} = 1$, n dividss 2α. Consequently, $m = 2\alpha$ and $4 \mid m$. Moreover, $b^\alpha = a^\alpha \in E$ and $E = \langle a^{m/2}\rangle = C \cap \langle b\rangle$.

(vi) We have $A = A_1C$. If n is odd, then $F = 1$ by 2.2(iv). Since $E \subseteq Z(A)$, α is even and, since $a^{2\alpha} = 1$, m divides 2α. Consequently, $m = 2\alpha$ and $4 \mid m$. □

For a prime $p \geqslant 2$, let S_p and T_p denote the Sylow p-subgroup of A_1 and C, respectively. Then $T_p \trianglelefteq A$ and we put $R_p = T_pS_p$.

2.4. Lemma. *Let $p \geqslant 3$. Then $S_p \subseteq Z(A)$, $S_p \cap T_p = 1$, $R_p \subseteq DC$, $S_p \times T_p = R_p \trianglelefteq A$ and R_p is a unique Sylow p-subgroup of A.*

P r o o f. Clearly, $S_p \subseteq D \subseteq Z(A)$ and $S_p \cap T_p = 1$ by 2.2(iv),(v). The rest is clear. □

2.5. Lemma. *R_2 is a Sylow 2-subgroup of A.*

P r o o f. We have $R_2 \subseteq K$ for a Sylow 2-subgroup K of A. Now, if $u = a^\alpha c^\beta \in K$, then there is $\gamma \geqslant 0$ such that $a^{\alpha 2^\gamma} \in A_1 \cap C = E$ (since $C \trianglelefteq A$), and hence $a^\alpha \in S_2$, $c^\beta \in K \cap C = T_2$ and $u \in R_2$. □

For a prime p, let $m = p^{r_p} \cdot m_p$, $p \nmid m_p$, $n = p^{s_p} \cdot n_p$, $p \nmid n_p$. Then $S_p = \langle a^{m_p}\rangle$ and $T_p = \langle c^{n_p}\rangle$. For a subgroup B of A, we denote by $\mathrm{Cen}_A(B)$ and $\mathrm{Nor}_A(B)$ the centralizer of B in A and the normalizer of B in A, respectively.

2.6. Lemma.

(i) *$\mathrm{Cen}_A(C) = DC = Z(A)C$ and $[A : \mathrm{Cen}_A(C)] = 2$.*

(ii) *If L is a subgroup of DC and $L \ntrianglelefteq A$, then $\mathrm{Nor}_A(L) = DC$ and L is conjugate to only one subgroup of A other than L.*

P r o o f. (i) Clearly, $DC \subseteq Z(A)C \subseteq \mathrm{Cen}_A(C)$ and $a \notin \mathrm{Cen}_A(C)$. Thus $2 \leqslant [A : \mathrm{Cen}_A(C)] \leqslant [A : Z(A)C] \leqslant [A : DC] = 2$.

(ii) Since $L \subseteq \mathrm{Cen}_A(C)$, we have $C \subseteq \mathrm{Cen}_A(L)$, and so $DC = \mathrm{Cen}_A(C) \subseteq \mathrm{Cen}_A(L)$. But $\mathrm{Cen}_A(L) \neq A$, and therefore $\mathrm{Cen}_A(L) = \mathrm{Nor}_A(L) = DC$. □

2.7. Lemma. *Let B be a corefree subgroup of A. Then*

(i) *B is cyclic, $B \cap C = 1 = B \cap D$ and B is isomorphic to a subgroup of A_1/E.*

(ii) *$\mathrm{card}(B) \leqslant m/k$ and $[A : B] \geqslant n$.*

(iii) *If $B \nsubseteq DC$, then $4 \nmid m$, $r_2 = 1$ and $B \cong \mathbb{Z}_2$.*

P r o o f. (i) and (ii) First, $B \cap C = 1 = B \cap Z(A)$, since all subgroups of C and $Z(A)$ are normal in A. Further, B is isomorphic to a subgroup of $A/C \cong A_1/E$ and, in particular, B is cyclic.

(iii) For every prime $p \geqslant 3$, the Sylow p-subgroup B_p of B is contained in $R_p \subseteq DC$, and hence $B_2 \nsubseteq DC$.

However, $B_2 = \langle u \rangle$ for some $u = a^\alpha c^\beta \notin DC$, where α is odd, $1 \leqslant \alpha < m$ and $0 \leqslant \beta < n$. Now, $u^2 = a^{2\alpha} a^{-\alpha} c^\beta a^\alpha c^\beta = a^{2\alpha} \in D \subseteq Z(A)$. Since B_2 is corefree, we have $u^2 = 1$, $m = 2\alpha$, $4 \nmid m$ and $B \cong \mathbb{Z}_2$. □

2.8. Lemma. *Suppose that $4 \nmid m$, n is odd and put $B_1 = \langle a^{m_2} \rangle = \langle a^{m/2} \rangle$. Then*

(i) *$B_1 = S_2 = R_2$ is a corefree two-element subgroup of A and $[A : B_1] = m/2$.*

(ii) *If B is a corefree subgroup of A such that $B \nsubseteq DC$, then B and B_1 are conjugate.*

P r o o f. (i) We note that $m_2 = m/2$ and the rest is clear by 2.3.

(ii) By 2.7(iii), $B \cong \mathbb{Z}_2$ and $B = \langle u \rangle$, $u = a^{m/2} \cdot c^\beta$, $0 \leqslant \beta < n$. Further, $c^{-1}uc = uc^2$, and hence $v^{-1}uv = a^{m/2}$, where $v = c^{(n-\beta)/2}$ for β odd and $v = c^{-\beta/2}$ for β even. □

2.9. Lemma. *Suppose that $4 \nmid m$, n is even and put $B_1 = \langle a^{m_2} \rangle = \langle a^{m/2} \rangle$ and $B_1^* = \langle a^{m/2} \cdot c^{n_2} \rangle$. Then*

(i) *$B_1 = S_2 \subseteq R_2$, $B_1^* \subseteq R_2$, $B_1 \cong B_1^* \cong \mathbb{Z}_2$, both B_1 and B_1^* are corefree and $[A : B_1] = [A : B_1^*] = mn/2$.*

(ii) *B_1 and B_1^* are not conjugate.*

(iii) *If B is a corefree subgroup of A such that $B \nsubseteq DC$, then B is conjugate either to B_1 or to B_1^*.*

P r o o f. (i) Clear.

(ii) For $0 \leqslant \alpha < n$ we have $c^{-\alpha} a^{m/2} c^\alpha = a^{m/2} \cdot c^{2\alpha}$ and $c^{2\alpha} \neq c^{n_2}$, since n is even and n_2 odd.

(iii) By 2.7(iii), $B \cong \mathbb{Z}_2$ and we can assume without loss of generality that $B \subseteq R_2$. Then $B = \langle u \rangle$, $u = a^{m/2} \cdot c^{\alpha n_2}$, $0 \leqslant \alpha < 2^{s_2}$. Again, $c^{-1}uc = uc^2$, and so u is conjugate to $a^{m/2}$ for α even and to $a^{m/2} \cdot c^{n_2}$ for α odd. □

Put $Q = DC$. Then $Q = Z(A)C = \mathrm{Cen}_A(C)$ is an abelian group, $[A : Q] = 2$ and $Q_p = R_p = S_p \times T_p$ is the Sylow p-subgroup of Q for every prime $p \geqslant 3$. Further, $Q_2 = S_2^* T_2$, where $S_2^* = \langle a^{2m_2} \rangle \subseteq Z(A)$. If $k = 1$, then $S_2^* \cap T_2 = 1$ and $Q_2 = S_2^* \times T_2$.

Now, suppose that $k = 2$. Then $r_2 \geqslant 2$, $s_2 \geqslant 1$, $a^{m/2} = c^{n/2}$, $S_2^* \cap T_2 = E \cong \mathbb{Z}_2$ and $\mathrm{card}(Q_2) = 2^{r_2+s_2-2}$. Further, let $1 \neq u = a^{2\alpha m_2} \cdot c^{\beta n_2} \in Q_2$, $0 \leqslant \alpha < 2^{r_2-1}$, $0 \leqslant \beta < 2^{s_2}$. Then $u^2 = 1$ iff either $a^{4\alpha m_2} = 1 = c^{2\beta n_2}$ or $a^{4\alpha m_2} = a^{m/2}$ and $c^{2\beta n_2} = c^{n/2}$. In the former case, $u = a^{m/2} = c^{n/2}$. In the latter case, $r_2 \geqslant 3$, $s_2 \geqslant 2$ and either $u = a^{m/4} \cdot c^{n/4}$ or $u = a^{3m/4} \cdot c^{n/4}$; these two elements are conjugate but different. The following lemma is clear.

2.10. Lemma. *Suppose that $k = 2$. Then Q_2 is cyclic if and only if either $8 \nmid m$ or $4 \nmid n$.*

3. Auxiliary results on groups (b)

This section is an immediate continuation of the preceding one.

For $l \geqslant 1$, let $\mathfrak{w}(l)$ denote the number of corefree subgroups B of A such that $\operatorname{card}(B) = l$. Further, let $\mathfrak{s}(l)$ denote the number of conjugacy classes of such subgroups.

3.1. Lemma. *Let $l \geqslant 3$ be odd. Then $\mathfrak{w}(l) \neq 0$ if and only if l divides both m and n. In that case, $\mathfrak{w}(l) = \underline{\varphi}(l)$ and $\mathfrak{s}(l) = \underline{\varphi}(l)/2$ ($\underline{\varphi}$ denotes the Euler function).*

Proof. Let B be a subgroup of A, $\operatorname{card}(B) = l$. Then B is corefree iff B is cyclic, $B \subseteq Q$ and no minimal subgroup of B is normal in A (see 2.7). In particular, B is corefree iff all Sylow subgroups of B are so. Henceforth, there is no loss of generality in assuming that $l = p^t$, $p \geqslant 3$ prime and $t \geqslant 1$.

Now, let $B \subseteq R_p$, B a corefree subgroup of order p^t. We have $B = \langle u \rangle$, $u = a^\alpha c^\beta$, $0 \leqslant \alpha < m$, $0 \leqslant \beta < n$, $a^\alpha \in S^p$, $c^\beta \in T_p$, $p^t = \operatorname{ord}(u) = \max(\operatorname{ord}(a^\alpha), \operatorname{ord}(c^\beta))$. Since B is corefree, we have $B \cap S_p = 1 = B \cap T_p$, and so $\operatorname{ord}(a^\alpha) = \operatorname{ord}(c^\beta)$ showing that p^t divides both m and n. Note that $S_p = \langle a^{m_p} \rangle$, $T_p = \langle c^{n_p} \rangle$ and $B \subseteq R_p^* = \langle a^{p^{r_p - t_p} \cdot m_p} \rangle \times \langle c^{p^{s_p - t_p} \cdot n_p} \rangle$, $t_p = \min(r_p, s_p)$. Now, R_p^* is the product of two cyclic groups of order p^{t_p}.

Conversely, if B is a cyclic subgroup of R_p^*, $\operatorname{card}(B) = p^t$ and if $B \cap S_p = 1 = B \cap T_p$, then B is corefree and it is easy to see that the number of such subgroups is just $p^t - p^{t-1} = \underline{\varphi}(p^t)$. Consequently, $\mathfrak{w}(l) = \underline{\varphi}(l)$ and $\mathfrak{s}(l) = \underline{\varphi}(l)/2$ (by 2.6(iii)). □

3.2. Lemma.

(i) *If $4 \nmid m$ and n is odd, then $\mathfrak{s}(2) = 1$.*
(ii) *If $4 \nmid m$ and n is even, then $\mathfrak{s}(2) = 2$.*
(iii) *If $4 \mid m$ and n is odd, then $\mathfrak{s}(2) = 0$.*
(iv) *If $4 \mid m$, n is even and $k = 1$, then $\mathfrak{s}(2) = 0$.*
(v) *If $4 \mid m$, $8 \nmid m$, n is even and $k = 2$, then $\mathfrak{s}(2) = 0$.*
(vi) *If $8 \mid m$, $4 \nmid n$, n is even and $k = 2$, then $\mathfrak{s}(2) = 0$.*
(vii) *If $8 \mid m$, $4 \mid n$ and $k = 2$, then $\mathfrak{s}(2) = 1$.*

Proof. See 2.9 and 2.10. □

3.3. Lemma. *Suppose that either $k = 1$ or $8 \nmid m$ or $4 \nmid n$. If B is a corefree subgroup of A with at least three elements, then $\operatorname{card}(B)$ is odd.*

P r o o f. By 2.7, $B \subseteq DC$, and so $B_2 \subseteq Q_2 = S_2^* T_2$ (see 2.10). Now, suppose that $B_2 \neq 1$ and let L be a (unique) minimal subgroup of B_2. If $k = 1$, then $Q_2 = S_2^* \times T_2$, the socle of Q_2 is contained in $Z(A)$, L is contained in the socle and $L \trianglelefteq A$, a contradiction.

If $k = 2$ and either $8 \nmid m$ or $4 \nmid n$, then Q_2 is cyclic by 2.10 and again $L = E = F \trianglelefteq A$, a contradiction. □

3.4. Lemma. *Suppose that $k = 2$, $8 \mid m$ and $4 \mid n$. If $t \geqslant 1$, then $\mathfrak{w}(2^t) \neq 0$ if and only if $t \leqslant t_2 = \min(r_2 - 1, s_2 - 1)$. In that case, $\mathfrak{w}(2^t) = 2^t = \underline{\varphi}(2^{t+1})$ and $\mathfrak{s}(2^t) = 2^{t-1} = \underline{\varphi}(2^t)$.*

P r o o f. Let $u \in Q_2 = S_2^* T_2$ be an element of order 2^t and such that $\langle u \rangle$ is corefree. Then $E = \langle a^{m/2} \rangle = \langle c^{n/2} \rangle \nsubseteq \langle u \rangle$, and hence $u = a_\alpha c_\beta$, where $a_\alpha = a^{q_\alpha}$, $q_\alpha = \alpha 2^{r_2 - t - 1} \cdot m_2$, $1 \leqslant \alpha$ odd, $c_\beta = c^{w_\beta}$, $w_\beta = \beta 2^{s_2 - t - 1} \cdot n_2$, $1 \leqslant \beta$ odd. We have $t \leqslant t_2$ and we can assume that α, $\beta < 2^{t+1}$. Now, $a_\alpha c_\beta = a_\gamma c_\delta$ iff either $\alpha = \gamma$ and $\beta = \delta$ or $|\alpha - \gamma| = 2^t = |\beta - \delta|$. Consequently, $\mathfrak{w}(2^t) = \big((2^t \cdot 2^t)/2\big)/2^{t-1} = 2^t$. □

3.5. Lemma. *Let $l \geqslant 4$ be even. Then $\mathfrak{w}(l) \neq 0$ if and only if $k = 2$, $8 \mid m$, $4 \mid n$ and $2l$ divides both m and n. In that case, $\mathfrak{w}(l) = \underline{\varphi}(2l)$ and $\mathfrak{s}(l) = \underline{\varphi}(2l)/2 = \underline{\varphi}(l)$.*

P r o o f. Using 3.3 and 3.4, we can proceed similarly as in the proof of 3.1. □

4. Auxiliary results on groups (c)

This section also continues the preceding two sections. We will assume that $\tilde{a}$, $\tilde{b} \in A$ are such that $A = \langle \tilde{a}, \tilde{b} \rangle$ and $\tilde{a}^2 = \tilde{b}^2$. We put $\tilde{A}_1 = \langle \tilde{a} \rangle$, $\tilde{c} = \tilde{a}^{-1}\tilde{b}$, $\tilde{C} = \langle \tilde{c} \rangle$, $\tilde{D} = \langle \tilde{a}^2 \rangle$, $\tilde{E} = \tilde{C} \cap \tilde{A}_1$, $\tilde{F} = \tilde{C} \cap Z(A)$, $\tilde{m} = \operatorname{ord}(\tilde{a})$, $\tilde{n} = \operatorname{ord}(\tilde{c})$, $\tilde{k} = \operatorname{ord}(\tilde{E})$, etc.

4.1. Lemma. *Let $2 = k$ and $\tilde{k} = 1$. Then $4 \mid m$, $m = \tilde{m}$, $n = 2\tilde{n}$ and $\tilde{n}$ is odd.*

P r o o f. Suppose that $8 \mid m$ and $4 \mid n$. Then $16 \mid \operatorname{card}(A)$ and $\mathfrak{s}(2) = 1$ by 3.2(vii). Now, using 3.2 again, we get that either $4 \nmid \tilde{m}$ and $2 \nmid \tilde{n}$ or $8 \nmid \tilde{m}$, $4 \nmid \tilde{n}$ and $\tilde{k} = 2$. In the first case, $4 \nmid \operatorname{card}(A)$, a contradiction.

Now, assume that either $8 \nmid m$ or $4 \nmid n$. By 2.3, $4 \mid m$ and $2 \mid n$ and we have $\mathfrak{s}(2) = 0$ by 3.2. Further, $D = Z(A) = \tilde{D} \times \tilde{F}$, $\operatorname{card}(D) = m/2$, $\operatorname{card}(\tilde{D}) = \tilde{m}/2$ and $\operatorname{card}(\tilde{F}) = 2$ for $\tilde{n}$ even and $\operatorname{card}(\tilde{F}) = 1$ for $\tilde{n}$ odd.

Let $\tilde{n}$ be even. Since D is cyclic, $\tilde{D}$ is a cyclic group of odd order, $\tilde{m}/2$ is odd and $4 \nmid \tilde{m}$, a contradiction with $\mathfrak{s}(2) = 0$ and 3.2(i), (ii). Thus $\tilde{n}$ is odd, $D = \tilde{D}$, $m = \tilde{m}$, $mn/2 = \operatorname{card}(A) = \tilde{m}\tilde{n}$, $\tilde{n} = n/2$. □

4.2. Lemma. *Either $n = \tilde{n}$ or $n = 2\tilde{n}$ or $n = \tilde{n}/2$.*

P r o o f. We have $\langle c^2 \rangle = A' = \langle \tilde{c}^2 \rangle$. □

4.3. Lemma. *If $k = \tilde{k}$, then $m = \tilde{m}$ and $n = \tilde{n}$.*

P r o o f. First, let $k = 1 = \tilde{k}$. Then $mn = \operatorname{card}(A) = \tilde{m}\tilde{n}$ and $D \times F = Z(A) = \tilde{D} \times \tilde{F}$, $\operatorname{card}(D) = m/2$ and $\operatorname{card}(\tilde{D}) = \tilde{m}/2$. If both n and $\tilde{n}$ are odd, then $F = 1 = \tilde{F}$, $m = \tilde{m}$ and $n = \tilde{n}$. If both n and $\tilde{n}$ are even, then $F \cong \mathbb{Z}_2 \cong \tilde{F}$ and $m = \tilde{m}$, $n = \tilde{n}$ again.

Now, suppose that n is odd and $\tilde{n}$ even (the other case being similar); then $m = 2\tilde{m}$ and $n = \tilde{n}/2$. Let $\tilde{a} = a^\alpha c^\beta$, $0 \leqslant \alpha < m$, $0 \leqslant \beta < n$. If α is odd, then $\tilde{a}^2 = a^{2\alpha}$ and $\tilde{m}/2 = \operatorname{ord}(\tilde{a}^2) = \operatorname{ord}(a^{2\alpha}) = \operatorname{ord}(a^2) = m/2$, $m = \tilde{m}$, a contradiction. Consequently, α is even and, similarly, $\tilde{b} = a^\gamma c^\delta$, where γ is even. However, then $\tilde{a}\tilde{b} = \tilde{b}\tilde{a}$, a contradiction.

Finally, let $k = 2 = \tilde{k}$. Then $F \subseteq D$, $\tilde{F} \subseteq \tilde{D}$, $m/2 = \tilde{m}/2$ and the rest is clear. □

4.4. Lemma.

(i) $m = \tilde{m}$.

(ii) *If $k = \tilde{k}$, then $n = \tilde{n}$.*

(iii) *If $n = \tilde{n}$, then $k = \tilde{k}$.*

(iv) *If $k \neq \tilde{k}$, then $4 \mid m$ and either $k = 2$, $n = 2\tilde{n}$ and $\tilde{n}$ is odd or $k = 1$, $n = \tilde{n}/2$ and n is odd.*

P r o o f. Combine 4.1, 4.2 and 4.3. □

4.5. Remark. Let $k = 2$, $4 \mid m$, $2 \mid n$, $n/2$ odd. Put $\tilde{a} = a$ and $\tilde{b} = ac^2$. Then $\tilde{b}^2 = ac^2ac^2 = a^2$ and $\tilde{c} = \tilde{a}^{-1}\tilde{b} = c^2$. If $K = \langle \tilde{a}, \tilde{b} \rangle = \langle a, c^2 \rangle$, then $c^{n/2} = a^{m/2} \in K$ implies $c \in K$ and $K = A$. Clearly, $\tilde{k} = 1$, $\tilde{m} = m$ and $\tilde{n} = n/2$.

4.6. Remark. The elements a, b are conjugate in A if and only if n is odd. If $n = 2\alpha - 1$, then $a^{-1}c^\alpha ac = c^{-\alpha+1} = c^\alpha$ and $b = ac = c^{-\alpha}ac^\alpha$. Conversely, if $au = uac$, $u = a^\alpha c^\beta$, then $a^{\alpha+1}c^\beta = a^\alpha c^\beta ac = a^{\alpha+1}c^{1-\beta}$, $c^{2\beta-1} = 1$ and n is odd.

5. A few constructions

5.1. Let $m \geqslant 2$ be even and let $n \geqslant 3$ be arbitrary. Put $A = A(m,n,1) = \mathbb{Z}_m \times \mathbb{Z}_n$, $\mathbb{Z}_i = \{0, 1, \dots, i-1\}$ being the ring of integers modulo i and define a multiplication on A by $(\alpha,\beta)(\gamma,\delta) = (\alpha+\gamma, (-1)^\gamma\beta + \delta)$. Then A becomes a group, $a^2 = b^2$, where $a = (1,0)$, $b = (1,1)$, $c = (0,1)$ and we have $A = \langle a, b \rangle$. Moreover, $\langle a \rangle \cap \langle c \rangle = 1_A$, $ab \neq ba$ and $\operatorname{card}(A) = mn$.

Suppose finally that $4 \mid m$, $2 \mid n$ and put $E = \{(0,0), (m \mid 2, n \mid 2)\}$. Then E is a normal subgroup of A and we denote by $A(m,n,2)$ the factor-group A/E; clearly, $\operatorname{card}(A/E) = mn/2$.

5.2. Proposition. *Let $m \geqslant 2$, $n \geqslant 3$, m even.*

(i) *The group* $A(m,n,1)$ *is given by two generators* u, v *and by the relations* $u^2 = v^2$ *and* $u^m = 1 = (u^{-1}v)^n$.

(ii) *If* A *is a group such that* $A = \langle a, b\rangle$, $a^2 = b^2$, $\mathrm{ord}(a) = m$, $\mathrm{ord}(a^{-1}b) = n$ *and* $\langle a\rangle \cap \langle a^{-1}b\rangle = 1$, *then there exists an isomorphism* $f\colon\ A(m,n,1) \to A$ *such that* $f\big((1,0)\big) = a$, $f\big((1,1)\big) = b$ *and* $f\big((0,1)\big) = a^{-1}b$.

P r o o f. See 5.1 and the preceding sections. □

5.3. Proposition. *Let* $m \geqslant 4$ *and* $n \geqslant 4$ *be such that* $4 \mid m$ *and* $2 \mid n$.

(i) *The group* $A(m,n,2)$ *is given by two generators* u, v *and by the relations* $u^2 = v^2$, $u^m = 1 = (u^{-1}v)^n$ *and* $u^{m/2} = (u^{-1}v)^{n/2}$.

(ii) *If* A *is a group such that* $A = \langle a, b\rangle$, $a^2 = b^2$, $\mathrm{ord}(a) = m$, $\mathrm{ord}(a^{-1}b) = n$ *and* $a^{m/2} = (a^{-1}b)^{n/2}$, *then there exists an isomorphism* $f\colon\ A(m,n,2) \to A$ *such that* $f\big((1,0)/E\big) = a$, $f\big((1,1)/E\big) = b$ *and* $f\big((0,1)/E\big) = a^{-1}b$.

P r o o f. See 5.1, 5.2 and the preceding sections. □

5.4. Proposition. *Let* $m, \tilde m \geqslant 2$, $n, \tilde n \geqslant 3$, m *and* $\tilde m$ *even. Then*

(i) $A(m,n,1) \cong A(\tilde m,\tilde n,1)$ *if and only if* $m = \tilde m$ *and* $n = \tilde n$.

(ii) *If* $4 \mid m$, $4 \mid \tilde m$, $2 \mid n$, $2 \mid \tilde n$, *then* $A(m,n,2) \cong A(\tilde m,\tilde n,2)$ *if and only if* $m = \tilde m$ *and* $n = \tilde n$.

(iii) *If* $4 \mid m$ *and* $2 \mid n$, *then* $A(m,n,2) \cong A(\tilde m,\tilde n,1)$ *if and only if* $m = \tilde m$, $n/2 = \tilde n$ *and* $\tilde n$ *is odd.*

(iv) *If* $4 \mid \tilde m$ *and* $2 \mid \tilde n$, *then* $A(m,n,1) \cong A(\tilde m,\tilde n,2)$ *if and only if* $m = \tilde m$, $2n = \tilde n$ *and* n *is odd.*

P r o o f. Use 4.4 and 4.5. □

5.5. Proposition. *Let* $m \geqslant 2$, $n \geqslant 3$, m *even, and let* A *be a group such that* $A = \langle a, b\rangle$, *where* $a^2 = b^2$, $\mathrm{ord}(a) = m$ *and* $\mathrm{ord}(a^{-1}b) = n$. *Further, let* $A = \langle \tilde a, \tilde b\rangle$, *where* $\tilde a^2 = \tilde b^2$, $\tilde m = \mathrm{ord}(\tilde a)$ *and* $\tilde n = \mathrm{ord}(\tilde a^{-1}\tilde b)$.

(i) *If either* $\langle a\rangle \cap \langle a^{-1}b\rangle = 1 = \langle \tilde a\rangle \cap \langle \tilde a^{-1}\tilde b\rangle$ *or* $\langle a\rangle \cap \langle a^{-1}b\rangle \neq 1 \neq \langle \tilde a\rangle \cap \langle \tilde a^{-1}\tilde b\rangle$, *then* $m = \tilde m$, $n = \tilde n$ *and there exists an automorphism* f *of* A *such that* $f(a) = \tilde a$ *and* $f(b) = \tilde b$.

(ii) *If* $\langle a\rangle \cap \langle a^{-1}b\rangle \neq 1 = \langle \tilde a\rangle \cap \langle \tilde a^{-1}\tilde b\rangle$, *then* $m = \tilde m$, $4 \mid m$, $n = 2\tilde n$, $\tilde n$ *is odd and there exists no automorphism* f *of* A *such that* $f(a) = \tilde a$, $f(b) = \tilde b$.

(iii) *If* $\langle a\rangle \cap \langle a^{-1}b\rangle = 1 \neq \langle \tilde a\rangle \cap \langle \tilde a^{-1}\tilde b\rangle$, *then* $m = \tilde m$, $4 \mid m$, $\tilde n = 2n$, n *is odd and there exists no automorphism* f *of* A *such that* $f(a) = \tilde a$, $f(b) = \tilde b$.

P r o o f. (i) By 4.4(i), (ii), we have $m = \tilde m$, and $n = \tilde n$. The result now follows from 5.2(ii) and 5.3(ii).

(ii) and (iii). See 4.1. □

5.6. (i) Let $m \geqslant 2$ be even and $A(m,3) = \mathbb{Z}_m(+) \times \mathbb{Z}_2(+)$. Then $A(m,3)$ is a non-cyclic abelian group of order $2m$, $A(m,3) = \langle a,b\rangle = \langle a,c\rangle$, where $a = (1,0)$, $b = (1,1)$, $c = (0,1)$, $2a = 2b$, $\operatorname{ord}(a) = m = \operatorname{ord}(b)$.

(ii) Let A be a non-cyclic abelian group (written multiplicatively) such that $A = \langle a,b\rangle$, $a^2 = b^2$, $m = \operatorname{ord}(a)$, $c = a^{-1}b$. Then $c^2 = 1$, $c \neq 1$, $A = \langle a,c\rangle$, $\langle a\rangle \cap \langle c\rangle = 1$, so that $A = \langle a\rangle \times \langle c\rangle$ and, since A is not cyclic, m is even. Further, there exists an isomorphism $f\colon A(m,3) \to A$ such that $f\bigl((1,0)\bigr) = a$, $f\bigl((1,1)\bigr) = b$ and $f\bigl((0,1)\bigr) = c$. Moreover, if $A = \langle \tilde a, \tilde b\rangle$, $\tilde a^2 = \tilde b^2$, then $g(a) = \tilde a$ and $g(b) = \tilde b$ for an automorphism g of A.

5.7. (i) Let $m \geqslant 3$ be odd and $A(m,3) = \mathbb{Z}_m(+) \times \mathbb{Z}_2(+)$. Then $A(m,3)$ is a cyclic group of order $2m$, $A(m,3) = \langle a,b\rangle = \langle a,c\rangle = \langle b\rangle$, where $a = (1,0)$, $b = (1,1)$, $c = (0,1)$, $2a = 2b$, $\operatorname{ord}(a) = m$ and $\operatorname{ord}(b) = 2m$.

(ii) Let A be a cyclic group (written multiplicatively) such that $A = \langle a,b\rangle$, $a^2 = b^2$, $A \neq \langle a\rangle$ and $\operatorname{ord}(a) = m \geqslant 2$, $c = a^{-1}b$. Then $c^2 = 1$, $c \neq 1$, $\langle a\rangle \cap \langle c\rangle = 1$, $A = \langle a\rangle \times \langle c\rangle$ and, since A is cyclic, m is odd. Further, $b^{m+1} = a$, $\operatorname{ord}(b) = 2m$, $A = \langle b\rangle$ and there exists an isomorphism $f\colon A(m,3) \to A$ such that $f\bigl((1,0)\bigr) = a$, $f\bigl((1,1)\bigr) = b$ and $f\bigl((0,1)\bigr) = c$. Moreover, if $A = \langle \tilde a, \tilde b\rangle$, then $\tilde a^2 = \tilde b^2$ and if $A \neq \langle \tilde a\rangle$, then $g(a) = \tilde a$ and $g(b) = \tilde b$ for an automorphism g of A. If $A \neq \langle \tilde b\rangle$, then $A = \langle \tilde a\rangle$ and there exists no automorphism g of A with $g(a) = \tilde a$ and $g(b) = \tilde b$.

Finally, suppose $A = \langle \tilde a\rangle = \langle \tilde b\rangle$. Then $\tilde b = \tilde a^i$ for some $i \geqslant 0$, $\tilde a^2 = \tilde a^{2i}$, $m \mid i-1$, $i = \alpha m+1$, $\alpha \geqslant 0$, and either α is even and $\tilde a = \tilde b$ or α is odd, $\tilde b = \tilde a^{m+1}$ and $\langle \tilde b\rangle \neq A$, a contradiction. Thus $\tilde a = \tilde b$ and there exists no automorphism g of A with $g(a) = \tilde a$, $g(b) = \tilde b$.

5.8. (i) Let $m \geqslant 4$ be such that $4 \mid m$ and $A(m,4) = \mathbb{Z}_m(+)$. Then $A(m,4) = \langle 1\rangle = \langle (m+2)/2\rangle$, $2 \cdot 1 \equiv 2 \cdot \bigl((m+2)/2\bigr) \pmod m$ and $1 \equiv (m+2)/2 \pmod m$.

(ii) Let A be a cyclic group (written multiplicatively) such that $A = \langle a\rangle = \langle b\rangle$, where $a \neq b$ and $a^2 = b^2$. Then $\operatorname{ord}(a) = \operatorname{ord}(b) = \operatorname{card}(A) = m$, $4 \mid m$, $b = a^{(m+2)/2}$, $a = b^{(m+2)/2}$ and there exists an automorphism $f\colon A(m,4) \to A$ such that $f(1) = a$ and $f\bigl((m+2)/2\bigr) = b$. Moreover, if $A = \langle \tilde a, \tilde b\rangle$, where $\tilde a \neq \tilde b$, $\tilde a^2 = \tilde b^2$, then $g(a) = \tilde a$ and $g(b) = \tilde b$ for an automorphism g of A (use 5.7(ii) to show that $A = \langle \tilde a\rangle = \langle \tilde b\rangle$).

5.9. $A(2,5) = \mathbb{Z}_2(+) = \langle 0,1\rangle = \langle 1,0\rangle$ and $2 \cdot 0 \equiv 0 \equiv 2 \cdot 1 \pmod 2$. There exists no automorphism f of $A(2,5)$ with $f(0) = 1$ and $f(1) = 0$.

6. The numbers of isomorphism classes of finite simple zeropotent paramedial groupoids

First, let us recall some results from elementary number theory. For a positive integer n, let $\underline{\delta}(n) = \operatorname{card}(\{m;\ 1 \leqslant m \leqslant n, m \mid n\})$ and $\underline{\varepsilon}(n) = \sum\limits_{1 \leqslant m \leqslant n, m \mid n} m$. Then

$\underline{\varepsilon}(n) = \sum_{m|n} \underline{\delta}(m)\underline{\varphi}(n/m)$ and $n = \sum_{m|n} \underline{\mu}(n/m)\underline{\varepsilon}(m)$, $\underline{\mu}$ being the Möbius function. If n_1, n_2 are relatively prime, then $\underline{\delta}(n_1 \cdot n_2) = \underline{\delta}(n_1)\underline{\delta}(n_2)$ and $\underline{\varepsilon}(n_1 \cdot n_2) = \underline{\varepsilon}(n_1)\underline{\varepsilon}(n_2)$. If $n = p^r$ is a power of a prime, then $\underline{\delta}(n) = r+1$ and $\underline{\varepsilon}(n) = 1+p+\ldots+p^r = (p^{r+1} - 1)/(p-1)$. If $n = p_1^{r_1} \ldots p_t^{r_t}$ is a prime decomposition of n, then $\underline{\delta}(n) = \prod_{i=1}^{t}(r_i+1)$ and $\underline{\varepsilon}(n) = \prod_{i=1}^{t}\sum_{j=0}^{r_i} p^j = \sum_{0\leqslant j_i \leqslant r_i} p_1^{j_1}\ldots p_t^{j_t} = \prod_{i=1}^{t}\big((p_i^{r_i+1}-1)/(p_i-1)\big)$.

For a non-negative integer n, let $\underline{\sigma}(n) = \sum_{m=0}^{n} 2^m(n-m) = 2^{n+1} - n - 2$.

6.1. Remark. Let $q = 2^r w + 1 \geqslant 3$ with $r \geqslant 0$, w odd. Then $\underline{\varepsilon}(w) = \sum_{l|q-1} l$ and $2^r\underline{\varepsilon}(w) = \sum_{l|q-1,(q-1)/l \text{ odd}} l$. Further, $\sum_{l|q-1} 1 = \underline{\delta}(q-1) = (r+1)\underline{\delta}(w)$ and $\underline{\delta}(w) = \sum_{l|q-1, l \text{ odd}} 1$.

For $q \geqslant 2$, let SIMZP(pm, q) denote the number of isomorphism classes of simple zeropotent paramedial groupoids of order q.

6.2. Theorem. *Let $q = 2^r w + 1 \geqslant 2$, $r \geqslant 0$, w odd. Then*

(i) SIMZP$(\mathrm{pm}, 2) = 1$ *and* SIMZP$(\mathrm{pm}, 3) = 2$.

(ii) *If q is even with $q \geqslant 4$ (i.e., $r = 0$, $w \geqslant 3$), then* SIMZP$(\mathrm{pm}, q) = \underline{\delta}(w) - 1 = \underline{\delta}(q-1) - 1$.

(iii) *If q is odd with $q \geqslant 3$ and $4 \nmid q-1$ (i.e., $r = 1$ or, equivalently, $q \equiv 3, 7 \pmod 8$), then* SIMZP$(\mathrm{pm}, q) = (\underline{\varepsilon}(w) + 5\underline{\delta}(w) - 2)/2 = (\underline{\varepsilon}((q-1)/2) + 5\underline{\delta}((q-1)/2) - 2)/2$.

(iv) *If q is odd with $q \geqslant 5$, $4 \mid q-1$ and $8 \nmid q-1$ (i.e., $r = 2$ or, equivalently, $q \equiv 5 \pmod 8$), then* SIMZP$(\mathrm{pm}, q) = (3\underline{\varepsilon}(w) + 7\underline{\delta}(w))/2 = (3\underline{\varepsilon}((q-1)/4) + 7\underline{\delta}((q-1)/4))/2$.

(v) *If q is odd with $q \geqslant 9$ and $8 \mid q-1$ (i.e., $r \geqslant 3$ or, equivalently, $q \equiv 1 \pmod 8$), then* SIMZP$(\mathrm{pm}, q) = ((2^{r+1} - 5)\underline{\varepsilon}(w) + (4r-1)\underline{\delta}(w)/2 = ((2^{r+1} - 5)\underline{\varepsilon}((q-1)/8)/(2^{r-2} - 2) + (4r-1)\underline{\delta}((q-1)/8)/(r-2))/2$.

(Notice that $2^{r+1} - 5 = 3$ and $4r - 1 = 7$ for $r = 2$ — cf. (iv).)

P r o o f. (i) One checks easily that SIMZP$(\mathrm{pm}, 2) = 1$ and SIMZP$(\mathrm{pm}, 3) = 2$.

(ii) Suppose that $q \geqslant 4$ is even, and so $r = 0$ and $w = q - 1 \geqslant 3$. We shall use 1.2.

Let $(A, B, a, b) \in \mathcal{A}_{zppm}$ be such that $[A : B] = w$. Then $\mathrm{card}(A) = lw$, $l = \mathrm{card}(B)$. If A is abelian, then $l = 1$ and this is a contradiction with $a^{-1}b \neq 1$ and $(a^{-1}b)^2 = 1$. Hence A is non-abelian and (keeping the notation from the preceding sections) we have either $k = 1$ and $mn = lw$ or $k = 2$ and $mn = 2lw$.

First, assume $k = 1$. Then l is even (since $2 \mid m$) and $l = 2$ by 3.5, i.e., $mn = 2w$, $w = (m/2) \cdot n$ and both $m/2$ and n are odd. We must have $n \geqslant 3$, and so we have just $\underline{\delta}(w) - 1$ possibilities for $m/2$ (use 3.2, 5.1, 5.2 and 5.5).

Next, let $k = 1$. Then $4 \mid m$, $2 \mid n$, hence $4 \mid l$ and $2l \mid m$, $2l \mid n$ by 3.5. From this, $2l \mid w$, a contradiction.

(iii) Suppose that $q \geqslant 5$ is odd, so that $r \geqslant 1$. Again, let $(A, B, a, b) \in \mathcal{A}_{zppm}$ be such that $[A : B] = q - 1 = 2^r w$. Put $l = \mathrm{card}(B)$, $\mathrm{card}(A) = l2^r w$.

(iii1) Let A be abelian. Then $l = 1$ and $\mathrm{card}(A) = 2^r w$. If A is not cyclic, then $r \geqslant 2$, $A \cong A(2^{r-1}w, 3)$ and, by 5.6, there is just 1 equivalence class for (A, B, a, b). If A is cyclic and either $A \neq \langle a \rangle$ or $A \neq \langle b \rangle$, then $r = 1$ and the number of the corresponding equivalence classes is 2 (see 5.7). Finally, if A is cyclic and $A = \langle a \rangle = \langle b \rangle$, then $r \geqslant 2$ and the number of the equivalence classes is 1 (see 5.8).

(iii2) Let $l = 1$ and let A be not abelian, $\mathrm{card}(A) = 2^r w$. If $k = 1$, then $2^{r-1}w = n \cdot m/2$, $n \geqslant 3$, and so the number of the corresponding equivalence classes is $\underline{\delta}(2^{r-1}w) - 1 = r\underline{\delta}(w) - 1$ (use 5.1, 5.2, 5.5 and other results from the preceding sections).

(iii3) Let $l \geqslant 3$ be odd. Then $\mathrm{card}(A) = 2^r lw$, lw odd. If $k = 1$, then $2^r lw = mn$, $m = 2\alpha l$, $n = \beta l$, $2^{r-1}w = \alpha\beta l$, $l \mid w$ and $2^{r-1}w \mid l = \alpha\beta$ (see 3.1). In this case, the number of the equivalence classes is $\underline{\delta}(2^{r-1}w/l)\underline{\varphi}(l)/2 = r\underline{\delta}(w/l)\underline{\varphi}(l)/2$ (see 3.1, 5.1, 5.2 and 5.5). Now, the sum over all $l \geqslant 3$ dividing w makes $(r/2)\sum_{l \mid w}\underline{\delta}(w/l)\underline{\varphi}(l) - (r/2)\underline{\delta}(w) = r\underline{\varepsilon}(w)/2 - r\underline{\delta}(w)/2$.

If $k = 2$, then $2^{r+1}lw = mn$, $m = 4\alpha l$, $n = 2\beta l$, $r \geqslant 2$, $2^{r-2}w = \alpha\beta l$ and $2^{r-2}w/l = \alpha\beta$ (see 3.1 and 2.3). Now, we get $\underline{\delta}(2^{r-2}w/l)\underline{\varphi}(l)/2 = (r-1)\underline{\delta}(w/l)\underline{\varphi}(l)/2$ equivalence classes and the sum is equal to $((r-1)/2)\sum_{l \mid w}\underline{\delta}\underline{\varphi}(l) = ((r-1)/2)\underline{\delta}(w) = (r-1)\underline{\varepsilon}(w)/2 - (r-1)\underline{\delta}(w)/2$ (5.1, 5.3 and 5.5).

(iii4) Let $l = 2$. Then $\mathrm{card}(A) = 2^{r+1}w$. If $k = 1$, then $2^{r+1}w = mn$, $m = 2\alpha$, α odd, $n \geqslant 3$, $2^r w = \alpha n$, $\alpha \mid w$, $n = 2^r w/\alpha$, n even (see 3.2). If $r = 1$, then we get $2\underline{\delta}(w) - 2$ equivalence classes (3.2, 5.1, 5.2 and 5.5). If $r \geqslant 2$, we get $2\underline{\delta}(w)$ classes.

If $k = 2$, then $2^{r+2}w = mn$, $m = 8\alpha$, $n = 4\beta$, $r \geqslant 3$, $2^{r-3}w = \alpha\beta$ and we get $\underline{\delta}(2^{r-3}w) = (r-2)\underline{\delta}(w)$ classes (3.2, 5.1, 5.3 and 5.5).

(iii5) Let $l \geqslant 4$ be even. Then $\mathrm{card}(A) = 2^r lw = 2^{r+s} \cdot uw$, where $l = 2^s u$, $s \geqslant 1$, u odd. By 3.5, $k = 2$, $8 \mid m$, $4 \mid n$, $2l = 2^{s+1}u$ divides both m and n, $m = 2^{s+1} \cdot u\alpha$, $n = 2^{s+1} \cdot u\beta$, $\mathrm{card}(A) = mn/2$. Consequently, $2^{r+s+1} \cdot uw = 2^{2s+2} \cdot u^2\alpha\beta$, $2^{r-s-1} \cdot w = u\alpha\beta$, $1 \leqslant s \leqslant r-1$, $u \mid w$, $\alpha\beta = 2^{r-s-1} \cdot w/u$. If $s = 1$, then α is even, $\alpha = 2\alpha_1$, $\alpha_1\beta = 2^{r-3} \cdot w/u$, $r \geqslant 3$ and we get just $\underline{\delta}(2^{r-3} \cdot w/u)\underline{\varphi}(2u) = (r-2)\underline{\delta}(w/u)\underline{\varphi}(u)$ equivalence classes (see 3.5, 5.1, 5.3 and 5.5). If $s \geqslant 2$, then $r \geqslant 3$ and the number of the equivalence classes is $\underline{\delta}(2^{r-s-1} \cdot w/u)\underline{\varphi}(2^s u) = (r-s)\underline{\delta}(w/u)2^{s-1}\underline{\varphi}(u)$. The sum is now $\sum_{s=1}^{r-1} 2^{s-1}(r-s)\underline{\varepsilon}(w) - \underline{\varepsilon}(w) = (\underline{\sigma}(r)\underline{\varepsilon}(w) - (r+2)\underline{\varepsilon}(w))/2 = (2^{r+1} - 2r - 4)\underline{\varepsilon}(w)/2$. □

Combining 6.1 and 6.2, we get the following results:

6.3. Corollary. *Let $q \geqslant 3$.*

(i) *If $q \equiv 0, 2 \pmod 4$, then* $\textsc{simzp}(\mathrm{pm}, q) = -1 + \sum_{l \mid q-1} 1$.

(ii) *If* $q \equiv 3$ *(mod 4), then* $\text{SIMZP}(\text{pm}, q) = -1 + \sum\limits_{l|q-1} 5/4 + \sum\limits_{l|q-1} l/6$.

(iii) *If* $q \equiv 1$ *(mod 4), then*

$$\text{SIMZP}(\text{pm}, q) = \sum_{l|q-1} 2 - \sum_{l|q-1,\, l \text{ odd}} 5/2 + \sum_{l|q-1,\, (q-1)/l \text{ odd}} l - \sum_{l|q-1,\, l \text{ odd}} 5l/2.$$

6.4. Remark.

(i) If $q \geqslant 4$ is such that $q-1$ is a prime, then $\text{SIMZP}(\text{pm}, q) = 1$.

(ii) If $q \geqslant 5$ is such that $q-1$ is a power of 2, then $\text{SIMZP}(\text{pm}, q) = q-4+2\log_2(q-1)$.

6.5. Remark. For q, let $\text{SIMZP}(\text{md}, q)$ denote the number of isomorphism classes of simple zeropotent medial groupoids of order q. By [4, Prop. 7.5.10], $\text{SIMZP}(\text{md}, 2) = 1$ and $\text{SIMZP}(\text{md}, q) = -1+\underline{\varepsilon}(q-1) = -1+\sum\limits_{l|q-1} l$ for $q \geqslant 3$. Now, we have the following table:

q	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{SIMZP}(\text{pm}, q)$	1	2	1	5	1	6	1	11	2	7	1	13	1	8	3
$\text{SIMZP}(\text{md}, q)$	1	2	3	6	5	11	7	14	12	17	11	25	13	23	23

References

[1] *J. R. Cho, J. Ježek and T. Kepka*: Paramedial groupoids. Czechoslovak Math. J. *49(124)* (1999), 277–290.

[2] *J. R. Cho, J. Ježek and T. Kepka*: Simple paramedial groupoids. Czechoslovak Math. J. *49(124)* (1999), 391–399.

[3] *R. El Bashir, J. Ježek and T. Kepka*: Simple zeropotent paramedial groupoids are balanced. Czechoslovak Math. J. *50(125)* (2000), 397–399.

[4] *J. Ježek and T. Kepka*: Medial groupoids. Rozpravy ČSAV, Řada mat. a přír. věd *93* (1983), 93.

[5] *J. Ježek and T. Kepka*: The equational theory of paramedial cancellation groupoids. Czechoslovak Math. J. *50(125)* (2000), 25–34.

[6] *J. Ježek and T. Kepka*: Linear equational theories and semimodule representations. Internat. J. Algebra Comput. *8* (1998), 599–615.

[7] *T. Kepka and P. Němec*: Simple balanced groupoids. Acta Univ. Palackianae Olomoucensis, Fac. rer. mat., Mathematica *35* (1996), 53–60.

Authors' addresses: J. R. Cho, Department of Mathematics, Pusan National University, Kumjung, Pusan 609-735, Republic of Korea, e-mail: `jungcho@hyowon.cc.pusan.ac.kr`; T. Kepka, Department of Algebra, Charles University, Sokolovská 83, 186 75 Praha 8, Czech Republic, e-mail: `kepka@karlin.mff.cuni.cz`.