Czechoslovak Mathematical Journal

Tomáš Kepka; Petr Němec

Commutative Moufang loops and distributive groupoids of small orders

Czechoslovak Mathematical Journal, Vol. 31 (1981), No. 4, 633–669

Persistent URL: http://dml.cz/dmlcz/101778

Czechoslovak Mathematical Journal, 31 (106) 1981, Praha

COMMUTATIVE MOUFANG LOOPS AND DISTRIBUTIVE GROUPOIDS OF SMALL ORDERS

Tomáš Kepka and Petr Němec, Praha

(Received July 22, 1980)

In this paper, the question of describing the commutative Moufang loops of orders $\leqq 728$ is treated. This work was motivated by that of O. Chein [4] dealing with (non-commutative) Moufang loops of small orders. Here we restrict ourselves to the commutative case only which enables us to construct all non-associative commutative Moufang loops of order lesser than 3^6. The principal tool is the investigation of commutative Moufang loops nilpotent of class at most two and their trilinear constructions. As a by-product, we obtain also a full constructive description of all commutative Moufang 3-loops generated by three elements. Further, this approach leads also to the description of the lattice of varieties of commutative Moufang loops nilpotent of class at most two.

As is well known, the theory of commutative Moufang loops is very closely related to that of distributive groupoids and quasigroups. As the theory of distributive groupoids is now being intensively investigated (see e.g. the detailed treatment of the topic in [7], where much further information can be found), we include also the description of non-medial commutative distributive groupoids of orders 81 and 82 (every such groupoid of order $\leqq 80$ is medial) and of distributive quasigroups of order $\leqq 15$. In this connection, it is also interesting to note that whereas there are only 2 isomorphism classes of non-medial commutative distributive groupoids of order 81, in the medial case there are at least 2^{79} of them.

The paper is divided into 14 sections. The first three of them have an auxiliary character. Section 1 contains the basic results concerning commutative Moufang loops. For further information as well as for detailed proofs, the reader is referred to [3]. In Section 2, several auxiliary assertions on finite abelian groups are presented. Although these results seem to be well-known, the authors were not able to find them explicitly in the literature and hence their proofs are also included. Section 3 contains several easy facts concerning triadditive mappings of abelian groups.

In Section 4, a trilinear construction of commutative Moufang loops nilpotent of class at most two is investigated. This construction had been implicitly employed already in the first examples of non-associative commutative Moufang loops (see

[1] and [2]). It was explicitly formulated in [11] and used also in [10]. Sections 5, 6 and 7 are devoted to the construction of particular types of non-associative commutative Moufang loops.

Section 8 deals with finitely generated commutative Moufang loops nilpotent of class at most two. It is shown (Theorem 8.6) that such a loop (if it does not contain elements of infinite order) can be constructed from an abelian group by means of trilinear construction described in Section 4. This result leads to the explicit description of all non-associative commutative Moufang loops of order $\leqq 728$ (Corollary 9.3) and of all non-associative commutative Moufang 3-loops with three generators (Theorem 9.5). As a corollary, we obtain the description of all finite non-associative commutative Moufang loops generated by three elements (Corollary 9.6).

T. Evans [5] has shown that there are only countably many varieties of nilpotent commutative Moufang loops. In Section 10, we give a full description of the lattice of varieties of commutative Moufang loops nilpotent of class at most two (Theorem 10.6).

The remaining sections are devoted to distributive groupoids and distributive quasigroups. Section 11 contains the necessary general results concerning distributive groupoids (for further material, see [7]). In Theorem 12.4, it is shown that there are (up to isomorphism) only 6 non-medial distributive quasigroups of order $\leqq 81$ (they are all of order 81) and among them only two commutative ones which are (Proposition 14.4) the only non-medial commutative distributive groupoids of order $\leqq 81$. Theorem 13.9 gives the description of all 45 distributive quasigroups of order $\leqq 15$. Finally, in Theorem 14.7 all 6 non-medial commutative distributive groupoids of order 82 are constructed.

1. PRELIMINARIES

Throughout the paper, m, n are non-negative integers, p is a prime, $G(n) = \{0, 1, \ldots, n-1\}$ denotes the additive group of integers modulo n, $F(p) = \{0, 1, \ldots, p-1\}$ is the field of integers modulo p and Z is the ring as well as the additive group of integers. If G is an abelian group and $x \in G$ then Zx denotes the subgroup generated by x.

In the following, let G be a commutative Moufang loop, i.e. a loop satisfying the identity $xx \,.\, yz = xy \,.\, xz$. For all $a, b, c \in G$, denote by $(a, b, c) = (a, b, c)_G$ the associator of a, b, c, i.e. $(a, b, c) = (ab \,.\, c)(a. \, bc)^{-1}$. Further, we denote by $C(G)$ the centre of G, i.e. the set of all elements $a \in G$ such that $(a, x, y) = 1$ for all $x, y \in G$, by $A(G)$ the associator subloop of G (i.e. the subloop generated by all associators), by $J(G)$ the intersection of all maximal subloops (if there is no maximal subloop then $J(G) = G$), by $\mathrm{Soc}\,(G)$ the subloop generated by all minimal subloops (if there is no such subloop then $\mathrm{Soc}\,(G) = \{1\}$) and we put $B(G) = \{x \in G \mid x^3 = 1\}$,

$D(G) = \{x^3 \mid x \in G\}$. G is said to be nilpotent of class at most n if $A_n(G) = 1$, where $A_i(G)$ are defined inductively by $A_0(G) = G$ and $A_i(G)$ is the subloop generated by all associators (a, x, y) with $a \in A_{i-1}(G)$, $x, y \in G$. Thus G is nilpotent of class at most two iff $A(G) \subseteq C(G)$. Further, G is nilpotent of class n iff $G/C(G)$ is nilpotent of class $n - 1$. In the rest of this section, we present for the convenience of the reader several more or less standard results concerning commutative Moufang loops which will be needed in the sequel. For further information as well as for detailed proofs, the reader is referred to [3].

1.1. Proposition. (i) *$A(G)$, $B(G)$, $C(G)$, $D(G)$, $\mathrm{Soc}(G)$ and $J(G)$ are normal subloops of G.*

(ii) *$A(G) \subseteq B(G) \subseteq \mathrm{Soc}(G)$ and $D(G) \subseteq C(G)$.*

(iii) *A subloop H of G is normal iff $(a, x, y) \in H$ for all $a \in H$ and $x, y \in G$.*

(iv) *If $a, b, c \in G$ and $a \,.\, bc = ab \,.\, c$ then the subloop generated by $\{a, b, c\}$ is a group.*

Proof. See [3, Lemma VII.5.7, Lemma VII.3.3, Theorem VII.4.2]. □

For a set M, $|M|$ denotes the cardinal number corresponding to M. Further, we put $q(G) = \min(|M|)$, M running through all generator sets of G.

1.2. Proposition. *Suppose that $q(G) = n$. Then:*

(i) *G is nilpotent of class at most* $\max(1, n - 1)$.

(ii) *Every subloop of G is finitely generated.*

(iii) *Every proper subloop of G is contained in a maximal subloop and every maximal subloop is normal.*

(iv) *$A(G) \subseteq J(G)$.*

(v) *If $H \subseteq J(G)$ is a normal subloop of G and f denotes the natural homomorphism of G onto G/H then a subset M of G generates G iff $f(M)$ generates G/H.*

(vi) *$q(G) = q(G/H)$ for every normal subloop H of G such that $H \subseteq J(G)$.*

(vii) *$q(G) = q(G/A(G)) = q(G/J(G))$.*

Proof. For (i) and (ii), see [3, Theorem VIII.10.1] and [5]. The first part of (iii) follows from (ii) by the trivial application of Zorn Lemma and the other may be proved by induction on the nilpotency class of G. The rest is easy. □

If $a \in G$, denote by $o(a)$ the order of a, i.e. $o(a) = |H|$, where H is the subgroup generated by a. The loop G is said to be a p-loop if $o(x)$ is a power of p for every $x \in G$. By 1.1(ii), $A(G)$ and $G/C(G)$ are 3-loops. Further, if G is a p-loop and $p \neq 3$ then G is a group.

1.3. Proposition. *If every element of G has a finite order then G is isomorphic to the direct product of a 3-loop and p-groups for some primes p.*

Proof. By 1.1(ii), every element from G of order not divisible by 3 is contained

in $C(G)$ and hence these elements form a subgroup H of $C(G)$. On the other hand, $H \cap K = \{1\}$ and G is generated by $H \cup K$, where K is the subloop of all elements from G having a 3-power order. The rest is clear. □

1.4. Lemma. *Let G be a 3-loop such that $q(G) = n$. Then:*

(i) $B(G) = \mathrm{Soc}(G)$ *and* $D(G) \subseteq J(G)$.
(ii) $|G| = 3^m$ *for some* $m \geqq n$, $q(G/D(G)) = n$ *and* $|G/J(G)| = 3^n$.
(iii) $J(G)$ *is the subloop generated by* $A(G) \cup D(G)$.
(iv) *If* $A(G) \subseteq D(G)$ *then* $D(G) = J(G)$.
(v) *If* $G = B(G)$ *then* $D(G) = \{1\}$ *and* $A(G) = J(G)$.

Proof. It follows easily from 1.2 and [3, Theorem VIII.11.3]. □

1.5. Lemma. *Suppose that G is nilpotent. Then:*

(i) $H \cap C(G) \neq \{1\}$ *for every non-trivial normal subloop* H.
(ii) G *is subdirectly irreducible iff* $C(G)$ *is so.*

Proof. The assertion (i) can be proved by an easy induction on the nilpotency class of G and (ii) follows immediately from (i). □

1.6. Lemma. (i) *If G is not associative then* $q(G/C(G)) \geqq 3$, $|G/C(G)| \geqq 27$ *and* $|G| \geqq 81$.
(ii) *If G is not nilpotent of class at most two then* $|G| \geqq 729$.

Proof. (i) If $q(G/C(G)) \leqq 2$ then G is generated by $C(G) \cup \{a, b\}$ for some $a, b \in G$ and so G is a group, a contradiction. Thus $q(G/C(G)) \geqq 3$ and $|G/C(G)| \geqq 27$ by 1.4. If G is finite then, by 1.5(i), $|C(G)| \geqq 2$ and hence $|G| \geqq 54$. If $A(G) \subseteq C(G)$ then $|C(G)| \geqq |A(G)| \geqq 3$ and $|G| \geqq 81$. In the opposite case, $G/C(G)$ is not associative, hence $|G/C(G)| \geqq 54$ and $|G| \geqq 108$.
(ii) By 1.2(i) and 1.4, $q(G) \geqq 4$ and $|G/A(G)| \geqq 81$. Suppose that G is finite and $|A(G)| \leqq 8$. Then $|A(G)| = 3$ and $A(G) \subseteq C(G)$ by 1.5(i), a contradiction. Thus $|A(G)| \geqq 9$ and $|G| \geqq 729$. □

1.7. Lemma. *If G is directly irreducible then* $C(G) \cap B(G) \subseteq J(G)$.

Proof. Let $x \in C(G) \cap B(G)$ and $x \notin J(G)$. Denote by H the subgroup generated by x. Then $|H| = 3$ and $H \cap K = \{1\}$ for some maximal subloop K of G. Thus G is isomorphic to $H \times K$. □

Let k be an integer and f a transformation of G. We shall say that f is k-central if $x^k f(x) \in C(G)$ for every $x \in G$.

1.8. Lemma. *Let k be an integer and $k = 3i + j$, $j \in \{0, 1, 2\}$. Then:*

(i) *The transformation $x \to x^k$ of G is a $(-j)$-central endomorphism of G.*
(ii) *If f is a k-central transformation of G then f is j-central.*

Proof. Use 1.1(ii). □

We denote by ι_G the identical mapping of G. Further, we put $\varepsilon_G(x) = x^{-1}$, $\nu_G(x) = x^2$ for every $x \in G$. Thus ε_G, ν_G are endomorphisms of G. Moreover, if ν_G is an automorphism, we denote by μ_G the inverse automorphism. Finally, if f is a transformation of G, we define $\bar{f}$ by $\bar{f}(x) = x f(x^{-1}) = x f \varepsilon(x)$.

1.9. Lemma. (i) *If f is an i-central endomorphism and g is a j-central endomorphism then fg is a $(-ij)$-central endomorphism and $f + g$ is an $(i + j)$-central endomorphism, where $(f + g)(x) = f(x)\, g(x)$ for all $x \in G$.*

(ii) *If f is an i-central automorphism then f^{-1} is an i-central automorphism.*

(iii) *ι_G is a 2-central automorphism, ε_G is a 1-central automorphism and ν_G is a 1-central endomorphism of G.*

(iv) *If ν_G is an automorphism then μ_G is a 1-central automorphism of G.*

(v) *If f is a 1-central endomorphism of G then $\bar{f}$ is a 1-central endomorphism of G.*

Proof. (i) Let $a, b \in G$, $x = f(a)^{-1} a^{-i}$, $y = g(a)^{-1} a^{-j}$, $u = f(b)^{-1} b^{-i}$, $v = g(b)^{-1} b^{-j}$. Then $x, y, u, v \in C(G)$ and we can write $(f(a)\, g(a) \,.\, f(b)\, g(b))\,(xyuv) = a^{-i}a^{-j} \,.\, b^{-i}b^{-j} = a^{-i}b^{-i} \,.\, a^{-j}b^{-j} = (f(a)f(b) \,.\, g(a)\, g(b))\,(xyuv)$. Hence $f + g$ is an endomorphism. Further, $a^{i+j}(f + g)(a) \,.\, xy = 1$, however $xy \in C(G)$ and so $f + g$ is $(i + j)$-central. Finally, $g(a)^i f\, g(a) \in C(G)$ and $a^{-ji}\, g(a^i)^{-1} \in C(G)$, so that $a^{-ji} f\, g(a) \in C(G)$.

(ii) By 1.8(ii), we can assume that $i \in \{0, 1, 2\}$. If $i = 0$ then G is a group and there is nothing to prove. If $i = 1$ then $a f(a) \in C(G)$ and so $f^{-1}(a)\, a \in C(G)$. Finally, if $i = 2$ then $a^{-3}a^2 f(a) \in C(G)$, hence $a^{-1} f(a)$, $a f^{-1}(a^{-1})$, $a^{-1} f^{-1}(a)$ and $a^2 f^{-1}(a)$ belong to $C(G)$.

The rest easily follows. □

1.10. Lemma. *Let f be a 1-central endomorphism of G and put $f(x) = x f(x)$ for every $x \in G$. Then:*

(i) *$\hat{f}$ is a 0-central endomorphism of G and $A(G) \subseteq \operatorname{Ker} \hat{f}$.*

(ii) *$f(x) = x^{-1}$ for every $x \in A(G)$.*

Proof. By 1.9(i). □

A 1-central automorphism f of G is said to be *complete* if $\bar{f}$ is an automorphism.

1.11. Lemma. (i) *$\bar{\varepsilon}_G = \nu_G$ and $\bar{\nu}_G = \varepsilon_G$.*

(ii) *If ν_G is an automorphism then $\bar{\mu}_G = \mu_G$ and ε_G, ν_G, μ_G are complete.*

Proof. Evident. □

1.12. Lemma. *Suppose that G is finite and let f be a 1-central automorphism of G. Then:*

(i) *f is complete iff $x \neq f(x)$ for every $1 \neq x \in G$.*

(ii) *If G is subdirectly irreducible and not associative then f is complete.*
(iii) *If $D(G) \subseteq A(G)$, G is directly irreducible and not associative then f is complete.*

Proof. (i) is clear.

(ii) and (iii). By 1.3, G is a 3-loop. Suppose on the contrary that f is not complete. Then $f(x) = x$ for some $1 \neq x \in G$, hence $x f(x) = x^2 \in C(G)$ and $x \in C(G)$. Without loss of generality, we can assume that $x \in B(C(G))$. If (ii) holds then $B(C(G)) \subseteq A(G)$, hence $f(x) = x^{-1}$ by 1.10(ii) and $x = 1$, a contradiction. If (iii) holds then $x \in J(G)$ by 1.7, however $J(G) = A(G)$ by 1.4(iii) and hence $x \in A(G)$, a contradiction. □

An automorphism f of G is said to be simple if no non-trivial proper subloop of G is invariant under f. Obviously, if f is a complete 1-central automorphism then f is simple iff $\bar{f}$ is. Two automorphisms f and g of G are said to be equivalent if $fh = hg$ for some automorphism h of G, i.e. if f and g are conjugated in the automorphism group of G.

1.13. Lemma. (i) *Every automorphism equivalent to a 1-central automorphism is 1-central.*

(ii) *Every automorphism equivalent to a simple automorphism is simple.*

(iii) *Let f, g be two complete 1-central automorphisms. Then f and g are equivalent iff $\bar{f}$ and $\bar{g}$ are equivalent.*

(iv) *Let k be an integer such that $f(x) = x^k$ is an automorphism of G. Then f is the only automorphism equivalent to f.*

Proof. Obvious. □

1.14. Lemma. *Let G be nilpotent of class at most two and let $M = \{a_1, \ldots, a_n\}$, $n \geq 3$, be a generator set of G. Then $A(G)$ is generated by $N = \{(a_i, a_j, a_k) \mid 1 \leq i < j < k \leq n\}$.*

Proof. Let H be the subloop generated by N. Then $H \subseteq A(G) \subseteq C(G)$ and H is a normal subloop of G. Denote by f the natural homomorphism of G onto G/H. Then $K = \{f(a_1), \ldots, f(a_n)\}$ generates G/H and by 1.1(iv) $x \,.\, yz = xy \,.\, z$ for all $x, y, z \in K$. By [3, Theorem VII.4.1], G/H is a group and hence $A(G) \subseteq H$. □

1.15. Corollary. (i) *If G is generated by $\{a, b, c\}$ then $A(G)$ is generated by (a, b, c).*
(ii) *If $q(G) \leq 3$ then $q(A(G)) \leq 1$ and either G is a group or $|A(G)| = 3$.* □

1.16. Lemma. *Let G be a non-associative 3-loop and $q(G) = 3$. Then G is directly irreducible.*

Proof. Suppose on the contrary that $G = H \times K$, $|K| > 1$ and H is not a group.

Since $|A(G)| = 3$, $A(H) = A(G) \subseteq H$ and K is a group. Then $H/C(H) \cong G(3)^3$ and K has a factor isomorphic to $G(3)$, K being a 3-group. Thus G has a factor isomorphic to $G(3)^4$, a contradiction with $q(G) = 3$. □

2. SOME TECHNICAL RESULTS ON FINITE ABELIAN GROUPS

Let $G = G(+)$ be a finite abelian p-group. A subset $M = \{x_1, \ldots, x_n\}$ of G is said to be independent if for all integers $\lambda_1, \ldots, \lambda_n$, $\lambda_1 x_1 + \ldots + \lambda_n x_n = 0$ implies $\lambda_1 x_1 = \ldots = \lambda_n x_n = 0$, i.e. if the subgroup generated by M is the direct sum of the cyclic subgroups $Zx_1, \ldots, Zx_n$. Further, M is said to be a basis of G if $0 \notin M$ and M is an independent generator set of G. Obviously, G has at least one basis (the empty set if G is trivial) and the number of elements of each basis is equal to $q(G)$.

In the sequel, we shall assume that G is non-zero and $N = \{a_1, \ldots, a_n\}$ is a basis of G such that $o(a_n) \leqq o(a_{n-1}) \leqq \ldots \leqq o(a_1)$. For each $0 \neq a \in G$, denote by $e(a)$ the exponent of a, $\bar{a} = p^{e(a)-1}a$ and by $h(a)$ the p-height of a. Further, we choose and fix an element $\hat{a} \in G$ with $a = p^{h(a)}\hat{a}$. Evidently, $0 \neq \bar{a} \in \mathrm{Soc}(G)$, $h(\hat{a}) = 0$, $e(\hat{a}) = e(a) + h(a)$ and $\bar{\hat{a}} = \bar{a}$. Finally, we put $\bar{0} = \hat{0} = 0$ and $\bar{S} = \{\bar{x} \mid x \in S\}$, $\hat{S} = \{\hat{x} \mid x \in S\}$ for every subset S of G.

2.1. Lemma. *A subset S of G is independent iff $\bar{S}$ is.*

Proof. If S is independent then clearly $\bar{S}$ is independent. Conversely, suppose that $\bar{S}$ is independent and proceed by induction on $m = |S|$. For $m \leqq 1$ there is nothing to prove. If $m \geqq 2$, $S = \{x_1, \ldots, x_m\}$ and $x \in Zx_1 \cap (Zx_2 + \ldots + Zx_m)$ then $\bar{x} \in Z\bar{x}_1 \cap \mathrm{Soc}(Zx_2 + \ldots + Zx_m) = Z\bar{x}_1 \cap (Z\bar{x}_2 + \ldots + Z\bar{x}_m)$, since $\{x_2, \ldots, x_m\}$ is independent with respect to the induction hypothesis. Thus $\bar{x} = 0$ and $x = 0$. □

2.2. Corollary. *A subset S of G is independent iff $\hat{S}$ is.* □

2.3. Lemma. *Let $S = \{x_1, \ldots, x_n\}$ be a generator set of G such that $e(x_1) \leqq \leqq e(a_1), \ldots, e(x_n) \leqq e(a_n)$. Then S is a basis of G.*

Proof. Put $H = Zx_1 \times \ldots \times Zx_n$ and define $f : H \to G$ by $f(\langle y_1, \ldots, y_n \rangle) = y_1 + \ldots + y_n$. Then f is a surjective homomorphism and $|G| \leqq |H|$, however $|H| = p^l \leqq p^k = |G|$, where $l = e(x_1) + \ldots + e(x_n)$ and $k = e(a_1) + \ldots + e(a_n)$, consequently $|G| = |H|$, hence f is injective and S is independent. Finally, it is easy to see that $0 \notin S$. □

2.4. Lemma. *The following conditions are equivalent for $0 \neq a \in G$:*

(i) *Za is a direct summand of G.*
(ii) *$h(a - b) = 0$ for every $b \in G$ with $e(b) < e(a)$.*
(iii) *There is $1 \leqq i \leqq n$ such that $\{a_1, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_n\}$ is a basis of G.*

Proof. (i) $\Rightarrow$ (ii). There is a subgroup H of G such that $G = Za \oplus H$. If $e(b) < e(a)$ then $b = \lambda a + h$ for some $\lambda \in Z$, $h \in H$, and p divides λ. If $a - b \in pG$ then $a - h \in pG$, hence $a = p\alpha a$ for some $\alpha \in Z$, a contradiction.

(ii) $\Rightarrow$ (iii) Let $a = \lambda_1 a_1 + \ldots + \lambda_n a_n$. Obviously, if $e(a) < e(a_i)$ then λ_i is divisible by p. It suffices to show that there is i such that $e(a) = e(a_i)$ and λ_i is not divisible by p, since then the set $S = \{a_1, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_n\}$ generates G and S is a basis by 2.3. Suppose on the contrary that such i does not exist. Let j be the least with $e(a_j) \leqq e(a)$ (if such j does not exist then $a - 0 = a \in pG$, a contradiction) and k be the greatest with $e(a_k) = e(a_j)$. Put $m = j$ if $e(a_j) < e(a)$ and $m = k + 1$ otherwise. Then, for $b = \lambda_m a_m + \ldots + \lambda_n a_n$ ($b = 0$ if $m > n$), $e(b) < e(a)$ and $a - b \in pG$, a contradiction.

(iii) $\Rightarrow$ (i). This is trivial. □

2.5. Lemma. *Let $S = \{x_1, \ldots, x_n\}$ be an independent subset of G such that $0 \notin S$ and, for each i, $h(y) \leqq h(x_i)$ for all $0 \neq y \in Zx_i + \ldots + Zx_n$. Then $\hat{S}$ is a basis of G.*

Proof. Let f denote the natural homomorphism of G onto $V = G/pG$. Obviously, V is a vector space over $F(p)$ and $\dim V = n$. Let $\lambda_1 \hat{x}_1 + \ldots + \lambda_n \hat{x}_n = pz$. Denote $\beta_i = h(x_i)$ and $u = p^{\beta_1 + 1} z = \lambda_1 x_1 + \lambda_2 p^{\beta_1 - \beta_2} x_2 + \ldots + \lambda_n p^{\beta_1 - \beta_n} x_n$. If $u \neq 0$ then $h(x_1) + 1 \leqq h(u)$, a contradiction. Hence $u = 0$ and p divides λ_1. Similarly we can show that p divides $\lambda_2, \ldots, \lambda_n$. Now it is easy to see that $f(\hat{S})$ is independent in V and $|f(\hat{S})| = n$. Thus $f(\hat{S})$ is a basis of V and $\hat{S}$ generates G by 1.2(v). Finally, $0 \notin \hat{S}$ and $\hat{S}$ is independent by 2.2. □

2.6. Lemma. *Let $0 \neq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_m \subseteq K_{m+1} = \operatorname{Soc}(G)$ and $H \neq 0$ be subgroups of $\operatorname{Soc}(G)$. Then there is a basis $S = \{x_1, \ldots, x_n\}$ of $\operatorname{Soc}(G)$ with the following two properties:*

(i) *For every $1 \leqq i \leqq m + 1$ there is $1 \leqq j_i \leqq n$ such that $\{x_1, \ldots, x_{j_i}\}$ is a basis of K_i.*

(ii) *There is a subset of S which is a basis of H.*

Proof. $\operatorname{Soc}(G)$ is a vector space over $F(p)$ and $\dim \operatorname{Soc}(G) = n$. For $k = 1, \ldots, m + 1$ put $L_k = K_k \cap H$. A basis Y_k of K_k is said to be admissible if it has properties (i) and (ii) with $m + 1$ replaced by k and H by L_k. We are going to show by induction on k that K_k has at least one admissible basis. For $k = 1$, the assertion is obvious. Let $k \geqq 1$ and let $\{z_1, \ldots, z_j\}$ be an admissible basis of K_k. We can assume that $k \leqq m$ and $K_k \neq K_{k+1}$. We have $L_{k+1} = L_k \oplus P$, $P \cap K_k = 0$ and $K_{k+1} = K_k \oplus R$, where $P \subseteq R$. There are $z_{j+1}, \ldots, z_q$ such that $T = \{z_{j+1}, \ldots, z_q\}$ is a basis of R and a subset of T is a basis of P. Obviously, $\{z_1, \ldots, z_q\}$ is an admissible basis of K_{k+1}. □

2.7. Proposition. *Let $H \neq 0$ be a subgroup of G such that at least one of the following conditions is satisfied:*

(i) *H is a direct summand of G.*

(ii) $pG \subseteq H$.

(iii) $H \subseteq \mathrm{Soc}(G)$.

Then there are a basis $\{b_1, \ldots, b_n\}$ of G and integers $\lambda_1, \ldots, \lambda_n$ such that $\{\lambda_1 b_1, \ldots, \lambda_n b_n\}$ is an independent generator set of H.

Proof. (i) is trivial.

(ii) We shall proceed by induction on n. The assertion is obvious for $n = 1$. Now let $n \geqq 2$. If there is $0 \neq a \in H$ such that $G = Za \oplus R$ then $H = Za \oplus (R \cap H)$, $pR \subseteq R \cap H$, $q(R) = n - 1$ and we can use the induction hypothesis. In the opposite case, suppose first that $\mathrm{Soc}(G) \subseteq pG$. By induction on $e(a)$ we shall show that each $a \in H$ belongs to pG. If $e(a) = 1$ then $a \in \mathrm{Soc}(G) \subseteq pG$. Now let $e(a) \geqq 2$. By 2.4, $a - b \in pG$ for some $b \in G$ with $e(b) < e(a)$. Since $pG \subseteq H$, we have $b \in H$. Thus $b \in pG$ by the induction hypothesis and $a \in pG$. Hence $H = pG$ and $\{pa_1, \ldots, pa_n\}$ is an independent generator set of H. Finally, let $x \in \mathrm{Soc}(G) \setminus pG$. With respect to 2.4, Za is a direct summand of G for e ery $0 \neq a \in H \cap Zx$. Hence $H \cap Zx = 0$ and there is a subgroup L of G such that $H \subseteq L$ and L is maximal with respect to $L \cap Zx = 0$. Clearly $pL \subseteq H$ and it suffices to show that $Zx + L = G$. Suppose on the contrary that $a \notin Zx + L$ and put $P = L + Za$. If $b \in L$, $\lambda \in Z$ are such that $c = b + \lambda a \in Zx$ then $\lambda a \in K + L$, hence p divides λ and $\lambda a \in pG \subseteq H \subseteq L$. Thus $c \in L \cap Zx = 0$ and $P \cap Zx = 0$, a contradiction.

(iii) Let $m = \max h(x)$, $0 \neq x \in \mathrm{Soc}(G)$, $K_i = \mathrm{Soc}(G) \cap p^{m+1-i}G$, $i = 1, \ldots, m+1$, and let $S = \{x_1, \ldots, x_n\}$ be a basis of $\mathrm{Soc}(G)$ having properties (i), (ii) from 2.6. For each i, if $y \in Zx_i + \ldots + Zx_n$ and $h(y) > h(x_i)$ then $x_i \in K_j \setminus K_{j-1}$ for some $j \geqq 2$, $y \in K_{j-1}$ and $K_{j-1} \cap (Zx_i + \ldots + Zx_n) = 0$. Thus S satisfies the hypothesis of 2.5, hence $\hat{S}$ is a basis of G and we are through. □

3. TERNARY RINGS

Let $G = G(+)$ be an abelian group. A mapping T of $G^3 = G \times G \times G$ into G is said to be triadditive if the mappings $T(-, u, v)$, $T(u, -, v)$, $T(u, v, -)$ are endomorphisms of G. Some obvious observations concerning triadditive mappings are formulated in the following five lemmas.

3.1. Lemma. *Let T be a triadditive mapping of G^3 into G. Then:*

(i) $T(\lambda x, y, z) = T(x, \lambda y, z) = T(x, y, \lambda z) = \lambda\, T(x, y, z)$ *for all* $x, y, z \in G$ *and every integer* λ.

(ii) $T(0, x, y) = T(x, 0, y) = T(x, y, 0) = 0$ *for all* $x, y \in G$. □

3.2. Lemma. *Let M be a generator set of G and T, S triadditive mappings of G^3 into G. Then $T = S$ iff $T \mid M^3 = S \mid M^3$.* □

3.3. Lemma. *Let M be a generator set of G and t a mapping of M^3 into G. Then t can be extended to a triadditive mapping iff $\Sigma\lambda_i\, t(a_i, b, c) = \Sigma\lambda_i\, t(b, a_i, c) = \Sigma\lambda_i\, t(b, c, a_i) = 0$ whenever $b, c, a_1, \ldots, a_n \in M$ and $\lambda_1, \ldots, \lambda_n$ are integers with $\Sigma\lambda_i a_i = 0$.* □

3.4. Lemma. *Let M be an independent generator set of G and t be a mapping of M^3 into G. Then t can be extended to a triadditive mapping iff for all $a, b, c \in M$ the number $o(t(a, b, c))$ divides the numbers $o(a), o(b), o(c)$.* □

3.5. Lemma. *Suppose that G is a 3-group and M is a basis of G. Then every mapping of M^3 into $B(G) = \mathrm{Soc}\,(G)$ can be extended to a triadditive mapping.* □

Consider the following five conditions for a triadditive mapping T of G^3 into G:

(1) $T(x, y, z) = -T(y, x, z)$ for all $x, y, z \in G$.
(2) $3\,T(x, y, z) = 0$ for all $x, y, z \in G$.
(3) $T(x, x, y) = 0$ for all $x, y \in G$.
(4) $T(T(x, y, z), u, v) = T(u, T(x, y, z), v) = T(u, v, T(x, y, z)) = 0$ for all $x, y, z, u, v \in G$.
(5) $T(x, y, z) + T(y, z, x) + T(z, x, y) = 0$ for all $x, y, z \in G$.

Further, put $\overline{T}(x, y, z) = T(x, y, z) + T(y, z, x) + T(z, x, y)$.

3.6. Lemma. *Let T be a triadditive mapping of G^3 into G. Then:*

(i) *$\overline{T}$ is a triadditive mapping.*
(ii) *$\overline{T}(x, y, z) = \overline{T}(y, z, x) = \overline{T}(z, x, y)$ for all $x, y, z \in G$.*
(iii) *If T satisfies (1) then $\overline{T}$ satisfies (1), $\overline{T}(x, x, y) = T(x, x, y)$ and $2\,T(x, x, y) = 0$ for all $x, y \in G$.*
(iv) *If T satisfies (2) then $\overline{T}$ satisfies (2) and (5).*
(v) *If T satisfies (1) and (2) then T satisfies (3).*
(vi) *If T satisfies (3) then T satisfies (1).*
(vii) *If T satisfies (3) then $\overline{T}(x, x, y) = \overline{T}(x, y, x) = \overline{T}(y, x, x) = 0$.*

Proof. Evident. □

3.7. Lemma. *Let T be a triadditive mapping of G^3 into G and M a generator set of G. Then:*

(i) *T satisfies (5) iff $\overline{T}(a, b, c) = 0$ for all $a, b, c \in M$.*
(ii) *T satisfies (1) iff $T(a, b, c) = -T(b, a, c)$ for all $a, b, c \in M$.*
(iii) *T satisfies (2) iff $T(M^3) \subseteq B(G)$.*
(iv) *If T satisfies (2) and $T(M^3) \subseteq D(G)$ then T satisfies (4).*

Proof. Evident (for (i) and (ii) use 3.2). □

3.8. Lemma. *Let T be a triadditive mapping of G^3 into G and M a generator set of G. Then:*

(i) *$T = 0$ provided G is cyclic and T satisfies (3).*

(ii) *T satisfies (5) provided T satisfies (3) and $\overline{T}(a, b, c) = 0$ for any three pairwise different elements $a, b, c \in M$.*

(iii) *T satisfies (5) provided T satisfies (3) and $q(G) \leqq 2$.*

Proof. Use 3.6 and 3.7. □

3.9. Proposition. *Let M be a basis of a 3-group G and t a mapping of M^3 into $B(G)$ such that $t(a, b, c) = -t(b, a, c)$ for all $a, b, c \in M$. Then t can be extended to a triadditive mapping T of G^3 into G such that T satisfies (1) and (2). Moreover, T satisfies (4) provided $t(M^3) \subseteq D(G)$ and T satisfies (5) provided $t(a, b, c) + t(b, c, a) + t(c, a, b) = 0$ for any three pairwise different elements $a, b, c \in M$.*

Proof. Apply 3.5, 3.7 and 3.8. □

By a ternary ring we mean an algebra $G(+, T)$, where $G(+)$ is an abelian group and T is a triadditive mapping of G^3 into G. We put $\mathrm{An}(T) = \{a \in G \mid T(a, x, y) = T(x, a, y) = T(x, y, a) = 0 \text{ for all } x, y \in G\}$. Clearly, $\mathrm{An}(T)$ is an ideal of the ternary ring.

Let $G(+, T)$ and $H(+, S)$ be ternary rings. A mapping f of G into H is said to be a weak homomorphism if $f(x + y + T(x, y, x - y)) = f(x) + f(y) + S(f(x), f(y), f(x) - f(y))$ for all $x, y \in G$. Obviously, every homomorphism of ternary rings is a weak homomorphism.

3.10. Lemma. *Let $f : G(+, T) \to H(+, S)$ be a weak homomorphism of ternary rings. Then:*

(i) *$f(0) = 0$ and $f(2x) = 2f(x)$ for every $x \in G$.*

(ii) *If T and S satisfy (3) then $f(\lambda x) = \lambda f(x)$ for every $x \in G$ and every integer λ.*

Moreover, if $f(\mathrm{Im}\ T) \subseteq \mathrm{An}(S)$ and both T and S satisfy (4) then:

(iii) *$f(x + y + T(x, y, x - y)) = f(x + y) + f(T(x, y, x - y))$ for all $x, y \in G$.*

(iv) *$f(x + y) - f(x) - f(y) \in \mathrm{An}(S)$ for all $x, y \in G$.*

(v) *$S(f(x + y), u, v) = S(f(x) + f(y), u, v)$ for all $x, y \in G$, $u, v \in H$.*

(vi) *f is a homomorphism of ternary rings iff $f(T(x, y, z)) = S(f(x), f(y), f(z))$ for all $x, y, z \in G$.*

Proof. Only (ii) is not immediate. For $\lambda \geqq 1$, the proof is straitghtforward by induction on λ and we also have $f((\lambda - 1)x) = (\lambda - 1)f(x) = f(\lambda x - x) = \lambda f(x) + f(-x) + \lambda((\lambda - 1)S_1 + S_2)$, where $S_1 = S(f(x), f(-x), f(x))$, $S_2 = S(f(x), f(-x), f(x) - f(-x))$. Thus $\lambda((\lambda - 1)S_1 + S_2) = -f(x) - f(-x)$ and taking $\lambda = 1, 2, 3$, we get $S_2 = 2S_1 + 2S_2 = 6S_1 + 3S_2$. Thus $S_2 = 0$ and $f(-x) = -f(x)$. The rest is clear. □

4. TERNARY CONSTRUCTIONS OF COMMUTATIVE MOUFANG LOOPS

Throughout this section, let $G(+, T)$ be a ternary ring satisfying (1), (2) and (4). We put $x \circ y = x + y + T(x, y, x - y)$ for all $x, y \in G$.

4.1. Proposition. (i) *$G(\circ)$ is a commutative Moufang loop nilpotent of class at most two.*

(ii) *$G(\circ)$ is a group iff T satisfies* (5).

(iii) *$G(+)$ and $G(\circ)$ have the same neutral element.*

(iv) *$\lambda a = a + \ldots + a = a \circ \ldots \circ a = a^{\lambda}$ for every $a \in G$ and every integer λ.*

(v) *Every element from G has the same order in $G(+)$ and in $G(\circ)$.*

(vi) *For all $a, b, c \in G$, $(a, b, c) = \overline{T}(a, b, c)$.*

(vii) *$A(G(\circ))$ is just the subgroup of $G(+)$ generated by* Im $\overline{T}$.

(viii) *$C(G(\circ)) =$* An $(\overline{T})$ *and $A(G(\circ)) \subseteq$* An $(T) \subseteq C(G(\circ))$.

(ix) *$B(G(\circ)) = B(G(+))$ and $D(G(\circ)) = D(G(+)) \subseteq$* An (T).

Proof. The proof needs just a tedious checking. □

4.2. Lemma. (i) *If $H \subseteq$* An (T) *then H is a subgroup iff it is a subloop. In this case, $H(\circ)$ is a normal subloop and the corresponding congruences of $G(+)$ and $G(\circ)$ coincide.*

(ii) *If* Im $T \subseteq H$ *then H is a subgroup iff it is a subloop. In this case, $H(\circ)$ is a normal and $G(\circ)/H = G(+)/H$.*

(iii) *If M is a generator set of $G(+)$ and N is a subset of* An (T) *such that* Im T *is contained in the subgroup generated by N then $M \cup N$ is a generator set of $G(\circ)$.*

(iv) *If $G(\circ)$ is finitely generated and* Im $T \subseteq A(G(\circ))$ *then every generator set of $G(+)$ generates $G(\circ)$.*

Proof. (i) This is clear, since $x \circ h = x + h$ for all $x \in G$, $h \in H$.

(ii) If H is a subloop and $a, b \in H$ then $c = b \circ (T(a, b, a - b))^{-1} = b - T(a, b, a - b) \in H$ and $a + b = a \circ c \in H$. Now suppose that H is a subgroup and denote by r the corresponding congruence of $G(+)$. Then clearly H is a subloop, r is a congruence of $G(\circ)$ and $(x + y)\, r\, (x \circ y)$ for all $x, y \in G$.

(iii) This is an easy consequence of (i) and (ii).

(iv) Use (ii) and 1.2(iv). □

4.3. Proposition. *The loop $G(\circ)$ is finitely generated iff the ternary ring $G(+, T)$ is finitely generated.*

Proof. First, let M be a finite generator set of $G(+, T)$ and $N = T(M^3)$. Denote by K the subgroup generated by N. Since $N \subseteq$ An (T), K is an ideal of $G(+, T)$ and it is easy to check that Im $T \subseteq K$. With respect to 4.2(iii), this implies that $G(\circ)$

is generated by $M \cup N$. Conversely, let M be a finite generator set of $G(\circ)$ and H be the subring generated by M. Then H is a subloop of $G(\circ)$ and so $H = G$. □

In the remaining part of this section, we shall assume that $G(+)$ is a non-zero 3-group and $n = q(G(+))$. A basis $\{a_1, \ldots, a_n\}$ of $G(+)$ is said to be T-admissible (T-special) if there are integers $\lambda_1, \ldots, \lambda_n$ such that $\{\lambda_1 a_1, \ldots, \lambda_n a_n\}$ is a generator set of An (T) $(A(G(\circ)))$. Such a basis always exists by 2.7.

4.4. Lemma. *Every T-admissible basis of $G(+)$ is a generator set of $G(\circ)$. In particular, $q(G(\circ)) \leqq n = q(G(+))$.*

Proof. If S is a T-admissible basis of $G(+)$, denote by H the subloop generated by S. By 4.1(iv), Im $T \subseteq$ An $(T) \subseteq H$ and 4.2(ii) yields the result. □

4.5. Lemma. *Suppose that T satisfies (5) and let $M = \{a_1, \ldots, a_n\}$ be a T-admissible basis of $G(+)$. Then $G(\circ)$ is an abelian group, M is a basis of $G(\circ)$ and there is an isomorphism f of $G(+)$ onto $G(\circ)$ such that $f(x) = x$ for every $x \in M \cup$ An (T) and $f(T(u, v, w)) = T(u, v, w) = T(f(u), f(v), f(w))$ for all $u, v, w \in G$.*

Proof. By 4.1(ii), $G(\circ)$ is an abelian group and by 4.4, M generates $G(\circ)$. With respect to 4.1(iv), the cyclic subgroups of $G(+)$ and $G(\circ)$ coincide and $g : H \to G(\circ)$, $h : H \to G(+)$, where $H = Za_1 \times \ldots \times Za_n$, defined by $g(\langle x_1, \ldots, x_n \rangle) = x_1 \circ \ldots \circ x_n$ and $h(\langle x_1, \ldots, x_n \rangle) = x_1 + \ldots + x_n$, are surjective homomorphisms. However, M is a basis of $G(+)$, hence $|H| = |G|$ and $g, h, f = gh^{-1}$ are isomorphisms. Obviously, $f(x) = x$ for every $x \in M$. Since M is T-admissible and $x \circ y = x + y$ for all $x, y \in$ An (T), $f(z) = z$ for every $z \in M \cup$ An (T). Finally, denote by L the set of all $x \in G$ with $x - f(x) \in$ An (T). Then $M \subseteq L$ and $x + y - f(x + y) = x - f(x) + y - f(y) - T(f(x), f(y), f(x) - f(y)) \in$ An (T) for all $x, y \in L$. Thus $L = G$ and $T(f(u), f(v), f(w)) = T(u, v, w) = f(T(u, v, w))$ for all $u, v, w \in G$. □

4.6. Lemma. *Let S be a triadditive mapping of G^3 into G such that S satisfies (1), (2), $T - S$ satisfies (5) and* Im $T \cup$ Im $S \subseteq$ An $(T) \cap$ An (S). *Then there is a weak isomorphism f of $G(+, S)$ onto $G(+, T)$ and consequently $G(\circ)$ is isomorphic to $G(*)$, where $G(*)$ is the commutative Moufang loop corresponding to $G(+, S)$.*

Proof. Obviously, $T - S$ satisfies (1), (2), (4) and (5). By 4.5, there are a generator set M of $G(+)$ and a permutation f of G such that $f(x) = x$ for every $x \in$ Im $T \cup$ Im $S \cup M$ and $f(u + v) = f(u) + f(v) + T(f(u), f(v), f(u) - f(v)) - S(f(u), f(v), f(u) - f(v))$ for all $u, v \in G$. Proceeding similarly as in the proof of 4.5, we can show that $f(T(x, y, z)) = T(x, y, z) = T(f(x), f(y), f(z))$ and $f(S(x, y, z)) = S(x, y, z) = S(f(x), f(y), f(z))$ for all $x, y, z \in G$. Finally, we have $f(u + v + S(u, v, u - v)) = f(u + v) + f(S(u, v, u - v)) = f(u) + f(v) + T(u, v, u - v) - S(u, v, u - v) + S(u, v, u - v) = f(u) + f(v) + T(f(u), f(v), f(u) - f(v))$. □

4.7. Lemma. *If* $\operatorname{Im} T \subseteq A(G(\circ)) \cap D(G(+))$ *then a subset* M *of* G *generates* $G(+)$ *iff it generates* $G(\circ)$.

Proof. By 4.2(ii), $G(\circ)/A(G(\circ)) = G(+)/A(G(\circ))$ and $G(\circ)/D(G(+)) = G(+)/D(G(+))$. Now it suffices to use 1.4(i) and 1.2(iv). □

4.8. Lemma. (i) $q(G(\circ)) = q(G(+)/A(G(\circ)))$.
(ii) *If* $A(G(\circ)) \subseteq D(G(\circ))$ *then* $q(G(\circ)) = q(G(+))$.

Proof. (i) Put $H = G/r$, where r is the congruence of both $G(+)$ and $G(\circ)$ corresponding to $A(G(\circ))$ and let $f : G \to H$ be the natural projection. Define $S : H^3 \to H$ by $S(f(x), f(y), f(z)) = f(T(x, y, z))$ for all $x, y, z \in G$. It is easy to check that S is a triadditive mapping satisfying (1), (2), (4) and (5) and $x \circ y = x + y + S(x, y, x - y)$ for all $x, y \in H$. Now, by 4.5 and 1.2(vii), $q(H(+)) = q(H(\circ)) = q(G(\circ))$.
(ii) By 1.2(iv) and 1.4(i) for $G(+)$, $q(G(+)/A(G(\circ))) = q(G(+))$. □

4.9. Proposition. *Let* $M = \{a_1, \ldots, a_n\}$ *be a* T*-admissible basis of* $G(+)$. *Then there is a triadditive mapping* S *of* G^3 *into* G *such that the following conditions hold*:

(i) S *satisfies* (1), (2) *and* (4), $T - S$ *satisfies* (1), (2), (4), (5) *and* $\operatorname{Im} T \cup \operatorname{Im} S \subseteq \subseteq \operatorname{An}(T) \subseteq \operatorname{An}(S)$.

(ii) $G(\circ)$ *is isomorphic to* $G(*)$, *where* $G(*)$ *is the commutative Moufang loop corresponding to* $G(+, S)$.

(iii) *If* $S(a_i, a_j, a_k) \neq 0$ *then* $S(a_i, a_j, a_k) = \bar{S}(a_i, a_j, a_k)$ *and either* $i < j < k$ *or* $j < i < k$.

(iv) $\operatorname{Im} S \subseteq A(G(G(*))$ *and* $A(G(*))$ *is just the subgroup generated by* $\operatorname{Im} S$.

(v) *Every generator set of* $G(+)$ *generates* $G(*)$.

Proof. Define a mapping $r : M^{3^*} \to B(G(+))$ as follows: $r(a_i, a_j, a_k) = = -T(a_j, a_k, a_i) - T(a_k, a_i, a_j)$ provided either $i < j < k$ or $j < i < k$, and $r(a_i, a_j, a_k) = T(a_i, a_j, a_k)$ otherwise. According to 3.9, r can be extended to a triadditive mapping R of G^3 into G satisfying (1), (2) and (5). Since M is a T-admissible basis, $\operatorname{An}(T) \subseteq \operatorname{An}(R)$. Put $S = T - R$. Then S is a triadditive mapping satisfying (1), (2) and (4), $\operatorname{Im} T \subseteq \cup \operatorname{Im} S \subseteq \operatorname{An}(T) \subseteq \operatorname{An}(S)$ and $R = T - S$. By 4.6, $G(\circ)$ is isomorphic to $G(*)$. The rest follows easily from 4.1 and 4.2(iv). □

4.10. Lemma. *Suppose that* T *does not satisfy* (5), $q(G(\circ)) = 3$ *and* $q(G(+)) \geqq 4$. *Then* $q(G(+)) = 4$ *and there is a* T*-special basis* $\{a, b, c, d\}$ *of* $G(+)$ *such that* $o(a) = 3$ *and* $A(G(\circ)) = Za$.

Proof. Let $\{a_1, \ldots, a_n\}$ be a T-special basis. Then $n \geqq 4$ and there are integers $\lambda_1, \ldots, \lambda_n$ such that $\{\lambda_1 a_1, \ldots, \lambda_n a_n\}$ generates $A(G(\circ))$. If $A(G(\circ)) \subseteq D(G(\circ))$ then $q(G(+)) = 3$ by 4.8(ii), a contradiction. Therefore $A(G(\circ)) \not\subseteq D(G(\circ))$ and we can

assume that $\lambda_1 a_1 \notin D(G(\circ))$. Then $\lambda_1 a_1 \neq 0$, λ_1 is not divisible by 3 and $a_1 \in A(G(\circ))$. By 1.15, $A(G(\circ)) = Za_1$. Further, $A(G(\circ))$ is a direct summand of $G(+)$ and $q(G(+)/A(G(\circ))) = 3$ by 4.8(i). Thus $q(G(+)) = 4$. □

4.11. Lemma. *Suppose that T does not satisfy* (5), Im $T \subseteq A(G(\circ))$ *and* $\{a, b, c, d\}$ *is a basis of* $G(+)$ *such that* $o(a) = 3$ *and* $A(G(\circ)) = Za$. *Then* $\{b, c, d\}$ *generates* $G(\circ)$ *and either* $a = \overline{T}(b, c, d)$ *or* $a = \overline{T}(c, b, d)$.

Proof. By 4.2(iv), $\{a, b, c, d\}$ generates $G(\circ)$. Since $a \in \mathrm{An}(T) \subseteq \mathrm{An}(\overline{T})$, by 3.9 $\overline{T}(b, c, d) = -\overline{T}(c, b, d) \neq 0$. However, Im $T \subseteq A(G(\circ))$, hence Im $\overline{T} \subseteq A(G(\circ))$ and either $a = (b, c, d)$ or $a = (c, b, d)$. □

5. THE LOOP $L(n, m, k, 1)$

Throughout this section, let $G(+) = G(3) \times G(3^n) \times G(3^m) \times G(3^k)$, where $1 \leqq n \leqq m \leqq k$. Put $a = \langle 1, 0, 0, 0\rangle$, $b = \langle 0, 1, 0, 0\rangle$, $c = \langle 0, 0, 1, 0\rangle$ and $d = \langle 0, 0, 0, 1\rangle$. Then $M = \{a, b, c, d\}$ is a basis of $G(+)$.

Define a mapping $t_1 : M^3 \to B(G(+))$ by $t_1(b, c, d) = a$, $t_1(c, b, d) = 2a$ and $t_1(x, y, z) = 0$ otherwise. By 3.9, t_1 can be extended to a triadditive mapping T_1 of G^3 into G satisfying (1) and (2). Clearly, Im $T_1 \subseteq Za$ and it is easy to see that T_1 satisfies (4). Hence $G(\circ)$ is a commutative Moufang loop nilpotent of class at most two, where $x \circ y = x + y + T_1(x, y, x - y)$ for all $x, y \in G$. We shall use the notation $G(\circ) = L(n, m, k, 1)$, $L(1) = L(1, 1, 1, 1)$ and $L(3) = L(1, 1, 2, 1)$.

5.1. Proposition. (i) $G(\circ)$ *is a commutative Moufang loop nilpotent of class* 2.

(ii) $A(G(\circ)) = \mathrm{Im}\ T_1 = \mathrm{Im}\ \overline{T}_1 = Za$ *and* $C(G(\circ)) = \mathrm{An}(T_1) = Za \oplus Z\,3b \oplus \oplus Z\,3c \oplus Z\,3d$.

(iii) $q(G(\circ)) = 3$, $\{b, c, d\}$ *is a generator set of* $G(\circ)$, $G(\circ)$ *is directly irreducible, and* $G(\circ)$ *is subdirectly irreducible iff* $n = m = k = 1$.

(iv) $G(\circ)$ *is given up to isomorphism (as a commutative Moufang loop) by three generators* x, y, z *and relations* $x^{3^n} = y^{3^m} = z^{3^k} = 1$.

Proof. The assertions (i) and (ii) easily follow from 4.1. By 4.11 and 1.1(iv), $\{a, c, d\}$ generates $G(\circ)$ and $q(G(\circ)) = 3$. By 1.16, $G(\circ)$ is directly irreducible and by 1.5(ii), $G(\circ)$ is subdirectly irreducible iff $n = m = k = 1$. Finally, let Q be a commutative Moufang loop given by three generators x, y, z and relations $x^{3^n} = y^{3^m} = z^{3^k} = 1$. By 1.15, $|A(Q)| \leqq 3$. On the other hand, clearly $|Q/A(Q)| \leqq 3^{n+m+k}$ and hence $|Q| \leqq 3^{n+m+k+1} = |G|$. By 4.11, $G(\circ)$ is a homomorphic image of Q and thus $G(\circ)$ is isomorphic to Q. □

5.2. Remark. Each $u \in G$ can be expressed as $u = \sum_{i \in M} u_i i$. One may easily check

that for all $x, y, z \in G$, $T(x, y, z) = (x_b y_c - x_c y_b) z_d a$. Hence $x \circ y = (x_a + y_a + (x_b y_c - x_c y_b)(x_d - y_d)) a + (x_b + y_b) b + (x_c + y_c) c + (x_d + y_d) d$.

5.3. Proposition. *Let S be a triadditive mapping of G^3 into G satisfying* (1), (2) *and* (4), *but not* (5). *Denote by $G(*)$ the corresponding commutative Moufang loop. If $q(G(*)) = 3$ then $G(*)$ is isomorphic to $G(\circ) = L(n, m, k, 1)$.*

Proof. According to 4.9, we can assume that $\operatorname{Im} S \subseteq A(G(*))$. Now the result immediately follows from 4.10, 4.11 and 5.1(iv). □

In the rest of this section, we shall assume that $n = m = k = 1$, i.e. $G(\circ) = L(1)$, and we put $\iota = \iota_G$, $\varepsilon = \varepsilon_{G(\circ)}$.

5.4. Lemma. *Let $\{a, b', c', d'\}$ be a basis of $G(+)$. Then there is an automorphism h of $L(1)$ such that $h(a) = a$, $h(d) = d'$ and either $h(b) = b'$, $h(c) = c'$ or $h(b) = c'$, $h(c) = b'$.*

Proof. By 4.11, $\{b', c', d'\}$ generates $G(\circ)$ and we can suppose $\overline{T}(b', c', d') = a$, the other case being similar. With respect to 5.1(iv), there is a homomorphism h of $G(\circ)$ onto $G(\circ)$ with $h(b) = b'$, $h(c) = c'$ and $h(d) = d$. Finally, $h(a) = h((b, c, d)) = (h(b), h(c), h(d)) = (b', c', d') = a$. □

5.5. Lemma. *Let f, g be 1-central automorphisms of $L(1)$. Then f and g are equivalent iff either $f = g$ or $f \neq \varepsilon \neq g$.*

Proof. Suppose that $f \neq \varepsilon \neq g$ and put $p(x) = x + f(x)$, $q(x) = x + g(x)$ for every $x \in G$. Then p and q map G into $C(G(\circ)) = A(G(\circ)) = Za$. Further, $p(x) \in \operatorname{An}(T)$, $T(x, f(x), x - f(x)) = T(x - p(x), f(x), x - f(x)) = -T(f(x), f(x), x - f(x)) = 0$ and $p(x) = x \circ f(x)$. Similarly $q(x) = x \circ g(x)$ and by 1.9(i), p and q are endomorphisms of $G(\circ)$. Moreover, since $f \neq \varepsilon \neq g$, $\operatorname{Im} p = A(G(\circ)) = \operatorname{Im} q$. Put $H = \operatorname{Ker} p$ and $K = \operatorname{Ker} q$. Since $\operatorname{Im} p = \operatorname{Im} q$ is a three-element group, $A(G(\circ)) \subseteq H \cap K$ and H, K are maximal subloops of $G(\circ)$, however $\operatorname{Im} T \subseteq H \cap K$ and so H, K are maximal subgroups of $G(+)$ as well. The group $G(+)$ is a vector space of dimension 4 over $F(3)$ and there are bases $\{a, b_1, c_1, d_1\}$, $\{a, b_2, c_2, d_2\}$ of $G(+)$ such that $\{a, b_1, c_1\}$ is a basis of $H(+)$ and $\{a, b_2, c_2\}$ a basis of $K(+)$. If $p(d_1) \neq q(d_2)$ then $p(d_1) = q(-d_2)$ (we have $p(d_1), q(d_2) \in \{a, 2a\}$) and hence we can assume that $p(d_1) = q(d_2)$. By 5.4, there is an automorphism h of $G(\circ)$ with $h(a) = a$, $h(b_1) = b_2$, $h(c_1) = c_2$ and $h(d_1) = d_2$. We have $h\,p(a) = 0 = q\,h(a)$, $h\,p(b_1) = 0 = q\,h(b_1)$, $h\,p(c_1) = 0 = q\,h(c_1)$ and $h\,p(d_1) = p(d_1) = q(d_2) = q\,h(d_1)$. Since $\{b_1, c_1, d_1\}$ generates $G(\circ)$, $hp = qh$. Finally, for each $x \in G$, $f(x) = p(x) - x = p(x) \circ (-x)$ (since $p(x) \in \operatorname{An}(T)$), $g(x) = q(x) \circ (-x)$ and $h f(x) = h\,p(x) \circ h(-x) = q\,h(x) \circ h(-x) = g\,h(x)$, so that f and g are equivalent. The converse implication is obvious. □

Define a transformation φ of G by $\varphi(x) = (x_b - x_a) a - x_b b - x_c c - x_d d$.

Using 5.2, it is easy to check that φ is a 1-central automorphism of $G(\circ)$. Moreover, $\bar{\varphi}(x) = x - \varphi(x) = (-x_a - x_b)\, a - x_b b - x_c c - x_d d$ for all $x \in G$ and $\bar{\varphi}$ is a 1-central automorphism.

5.6. Corollary. (i) *ε and φ are complete 1-central automorphisms of $L(1)$.*
(ii) *ε and φ are not equivalent.*
(iii) *Every 1-central automorphism of $L(1)$ is equivalent either to ε or to φ.* □

6. THE LOOPS $L(n, m, k, 2)$, $L(n, m, k, 3)$, $L(n, m, k, 4)$

Throughout this section, let $G(+) = G(3^n) \times G(3^m) \times G(3^k)$, where $1 \leqq n \leqq m \leqq k$. Put $a = \langle 1, 0, 0\rangle$, $b = \langle 0, 1, 0\rangle$, $c = \langle 0, 0, 1\rangle$. Then $M = \{a, b, c\}$ is a basis of $G(+)$.

If $n \geqq 2$, define a mapping t_2 from M^3 into $B(G(+))$ as follows: $t_2(a, b, c) = 3^{n-1}a$, $t_2(b, a, c) = 3^{n-1} \cdot 2a$ and $t_2(x, y, z) = 0$ otherwise.

If $m \geqq 2$, define $t_3 : M^3 \to B(G(+))$ by $t_3(a, b, c) = 3^{m-1}b$, $t_3(b, a, c) = 3^{m-1} \cdot 2b$ and $t_3(x, y, z) = 0$ otherwise.

Finally, if $k \geqq 2$, define $t_4 : M^3 \to B(G(+))$ by $t_4(a, b, c) = 3^{k-1}c$, $t_4(b, a, c) = 3^{k-1} \cdot 2c$ and $t_4(x, y, z) = 0$ otherwise.

According to 3.9, these mappings can be extended to triadditive mappings T_2, T_3, T_4 satisfying (1), (2) and (4). The corresponding commutative Moufang loops we denote by $L(n, m, k, 2)$, $L(n, m, k, 3)$ and $L(n, m, k, 4)$, respectively. We also put $L(2) = L(1, 1, 2, 4)$, $L(4) = L(1, 1, 3, 4)$ and $L(5) = L(1, 2, 2, 4)$.

6.1. Proposition. *Let $n \geqq 2$ and $G(\circ) = L(n, m, k, 2)$. Then:*
(i) *$G(\circ)$ is a commutative Moufang loop nilpotent of class 2.*
(ii) *$A(G(\circ)) = \operatorname{Im} T_2 = \operatorname{Im} \overline{T}_2 = Z\, 3^{n-1}a$ and $C(G(\circ)) = D(G(\circ)) = \operatorname{An}(T_2) = Z\, 3a \oplus Z\, 3b \oplus Z\, 3c$.*
(iii) *$q(G(\circ)) = 3$, $\{a, b, c\}$ generates $G(\circ)$, $G(\circ)$ is directly irreducible and $G(\circ)$ is not subdirectly irreducible.*
(iv) *$G(\circ)$ is given up to isomorphism by three generators x, y, z and relations $x^{3^n} = y^{3^m} = z^{3^k} = 1$, $(x, y, z) = x^{3^{n-1}}$.*

Proof. Similar to that of 5.1. □

6.2. Proposition. *Let $m \geqq 2$ and $G(\circ) = L(n, m, k, 3)$. Then:*
(i) *$G(\circ)$ is a commutative Moufang loop nilpotent of class 2.*
(ii) *$A(G(\circ)) = \operatorname{Im} T_3 = \operatorname{Im} \overline{T}_3 = Z\, 3^{m-1}b$ and $C(G(\circ)) = D(G(\circ)) = \operatorname{An}(T_3) = Z\, 3a \oplus Z\, 3b \oplus Z\, 3c$.*
(iii) *$q(G(\circ)) = 3$, $\{a, b, c\}$ generates $G(\circ)$, $G(\circ)$ is directly irreducible and $G(\circ)$ is not subdirectly irreducible.*

(iv) $G(\circ)$ *is given up to isomorphism by three generators* x, y, z *and relations* $x^{3^n} = y^{3^m} = z^{3^k} = 1$, $(x, y, z) = y^{3^{m-1}}$.

Proof. Similar to that of 6.1. □

6.3. Proposition. *Let* $k \geqq 2$ *and* $G(\circ) = L(n, m, k, 4)$. *Then*:

(i) $G(\circ)$ *is a commutative Moufang loop nilpotent of class* 2.

(ii) $A(G(\circ)) = \operatorname{Im} T_4 = \operatorname{Im} \overline{T}_4 = Z\, 3^{k-1}c$ *and* $C(G(\circ)) = D(G(\circ)) = \operatorname{An}(T_4) = Z\, 3a \oplus Z\, 3b \oplus Z\, 3c$.

(iii) $q(G(\circ)) = 3$, $\{a, b, c\}$ *generates* $G(\circ)$, $G(\circ)$ *is directly irreducible and* $G(\circ)$ *is subdirectly irreducible iff* $n = m = 1$.

(iv) $G(\circ)$ *is given up to isomorphism by three generators* x, y, z *and relations* $x^{3^n} = y^{3^m} = z^{3^k} = 1$, $(x, y, z) = z^{3^{k-1}}$.

Proof. Similar to that of 6.1. □

6.4. Remark. It is easy to see that for all $x, y, z \in G$, $T_2(x, y, z) = 3^{n-1}(x_a y_b - x_b y_a)\, z_c a$, $T_3(x, y, z) = 3^{m-1}(x_a y_b - x_b y_a)\, z_c b$ and $T_4(x, y, z) = 3^{k-1}(x_a y_b - x_b y_a)\, z_c c$.

6.5. Proposition. *Let* S *be a triadditive mapping of* G^3 *into* G *satisfying* (1), (2) *and* (4), *but not* (5). *Then the corresponding commutative Moufang loop* $G(*)$ *is isomorphic to at least one of the loops* $L(n, m, k, 2)$, $L(n, m, k, 3)$ *and* $L(n, m, k, 4)$.

Proof. We can assume that $\operatorname{Im} S \subseteq A(G(*))$ and $\{x, y, z\}$ is a basis of $G(+)$ such that $o(x) = 3^n$, $o(y) = 3^m$, $o(z) = 3^k$ and $\{\lambda x, \varrho y, \sigma z\}$ is an independent generator set of $A(G(*))$. However, $A(G(*))$ is cyclic and non-zero, hence exactly one of λx, ϱy, σz is non-zero and we can assume $\lambda x \neq 0$, $\varrho y = \sigma z = 0$, the other cases being similar. Then $A(G(*)) = Z\lambda x$, however, $A(G(*)) \subseteq B(G(+))$ and thus $A(G(*)) = Z\, 3^{n-1}x$. Since S does not satisfy (5), by 3.6(ii) and 3.8(ii) $\bar{S}(x, y, z) \neq 0$ and $n \geqq 2$ (otherwise $x \in A(G(*)) \subseteq \operatorname{An}(S) \subseteq \operatorname{An}(\bar{S})$). Hence we have in $G(*)$ $x^{3^n} = y^{3^m} = (-y)^{3^m} = z^{3^k} = 0$ and either $(x, y, z) = \bar{S}(x, y, z) = x^{3^{n-1}}$ or $(x, -y, z) = -\bar{S}(x, y, z) = x^{n-1}$. In both cases, $G(*)$ is a homomorphic image of and thus isomorphic to $L(n, m, k, 2)$. □

6.6. Lemma. *Let* $1 \leqq n \leqq m \leqq k$, $1 \leqq n' \leqq m' \leqq k'$ *and* $1 \leqq i, j \leqq 4$. *Then*:

(i) *If* $j \geqq 2$ *then* $L(n, m, k, 1)$ *is not isomorphic to* $L(n', m', k', j)$.

(ii) *If* $L(n, m, k, i)$ *is isomorphic to* $L(n', m', k', j)$ *then* $n = n'$, $m = m'$, $k = k'$.

(iii) $L(n, m, k, 2)$ *is isomorphic to* $L(n', m', k', 3)$ *iff* $n = m = n' = m'$ *and* $k = k'$.

(iv) $L(n, m, k, 2)$ *is isomorphic to* $L(n', m', k', 4)$ *iff* $n = m = k = n' = m' = k'$.

(v) $L(n, m, k, 3)$ *is isomorphic to* $L(n', m', k', 4)$ *iff* $n = n'$ *and* $m = k = m' = k'$.

Proof. Denote $G(\circ) = L(n, m, k, i)$, $H(\circ) = L(n', m', k', j)$ and f be an isomorphism of $G(\circ)$ onto $H(\circ)$.

(i) There is $0 \neq x \in A(H(\circ)) \cap D(H(\circ))$ and hence $f^{-1}(x) \in A(G(\circ)) \cap D(G(\circ)) = 0$, a contradiction.

(ii) If $i = j = 1$ then f induces an isomorphism of $G(\circ)/A(G(\circ))$ onto $H(\circ)/A(H(\circ))$, however $G(\circ)/A(G(\circ)) = G(+)/A(G(\circ))$ by 4.2(ii). If $i, j \geqq 2$ then $N = \{f(a), f(b), f(c)\}$ generates $H(\circ)$ and by 4.7 N generates $H(+)$. Since $o(f(a)) = n$, $o(f(b)) = m$, $o(f(c)) = k$ and $n + m + k = n' + m' + k'$, the sum $H(+) = Zf(a) + Zf(b) + Zf(c)$ is necessarily direct and N is a basis of $H(+)$.

(iii) If $i = 3$ and $j = 2$ then $0 \neq (f(a), f(b), f(c)) = 3^{m-1} f(b) \in A(H(\circ))$ and hence $m \leqq n' \leqq m' = m$. The converse implication follows easily from 6.2(iv).

(iv) and (v). Similar to (iii). □

In the rest of this section, we shall assume that $n = m = 1$, $k = 2$ and we put $G(\circ) = L(1, 1, 2, 4) = L(2)$, $T = T_4$. Define a transformation ψ of G by $\psi(x) = -x_a a - x_b + (3x_a - x_c) c$. It is easy to see that ψ is a 1-central automorphism of $G(\circ)$. Moreover, $\bar{\psi}(x) = -x_a a - x_b b + (-x_c - 3x_a) c$ for each $x \in G$, $\bar{\psi}$ is a 1-central automorphism and $\operatorname{Ker}(\iota + \psi) = Zb \oplus Zc$, where $(\iota + \psi)(x) = x \circ \psi(x)$.

6.7. Lemma. *Let f be a 1-central automorphism of $G(\circ) = L(2)$. Then f is equivalent to ψ iff $B(G(\circ)) \nsubseteq \operatorname{Ker}(\iota + f)$.*

Proof. First, let $h\psi = fh$ for some automorphism h of $G(\circ)$. Then $h(\operatorname{Ker}(\iota + \psi)) \subseteq \operatorname{Ker}(\iota + f)$ and so $h(Zb \oplus Zc) \subseteq \operatorname{Ker}(\iota + f) = H$. In particular, the subloop $H(\circ)$ contains an element d of order 9. If $B(G(\circ)) \subseteq H$ then $a, b \in H$, however, as one may easily check, $\{a, b, d\}$ is a generator set of $G(\circ)$, hence $H = G$, $f = \varepsilon$ and $\psi = \varepsilon$, a contradiction. Conversely, assume that there is $a' \in B(G(\circ)) \setminus H$. Then $f \neq \varepsilon$, $\operatorname{Im}(\iota + f) = C(G(\circ)) = Z\,3c$ and $H(\circ)$ is a maximal subloop of $G(\circ)$. Since $\operatorname{Im} T \subseteq H$, $H(+)$ is a maximal subgroup of $G(+)$ and hence $G(+) = Za' \oplus H(+)$. It is easy to see that there is a generator set $\{a', b', c'\}$ of $G(+)$ such that $o(a') = o(b') = 3$, $o(c') = 9$, $3c' = 3c$ and $H(+) = Zb' \oplus Zc'$. Clearly, $\{a', b', c'\}$ generates $G(\circ)$ and $\bar{T}(a', b', c') \neq 0$ by 3.9. We must distinguish the following cases:

(i) $a' \circ f(a') = 3c = 3c' = \bar{T}(a', b', c')$. By 6.3(iv), there is an automorphism h of $G(\circ)$ with $h(a) = a'$, $h(b) = b'$, $h(c) = c'$. Now $h(a \circ \psi(a)) = h(3c) = 3c' = 3c = a' \circ f(a') = h(a) \circ f\, h(a)$, $h(b \circ \psi(b)) = 0 = b' \circ f(b') = h(b) \circ f\, h(b)$, $h(c \circ \psi(c)) = 0 = h(c) \circ f\, h(c)$. Thus $h(\iota + \psi) = (\iota + f)\, h$ and $h\psi = fh$.

(ii) $a' \circ f(a') = 6c$ and $\bar{T}(a', b', c') = 3c$. Then $(-a') \circ f(-a') = 3c'$, $\bar{T}(-a', -b', c') = 3c'$ and we can proceed similarly as in (i).

(iii) $a' \circ f(a') = 3c$ and $\bar{T}(a', b', c') = 6c$. Then $\bar{T}(a', -b', c') = 3c'$.

(iv) $a' \circ f(a') = 6c = \bar{T}(a', b', c')$. Then $(-a') \circ f(-a') = 3c' = \bar{T}(-a', b', c')$. □

6.8. Proposition. (i) *ε, ν, μ and ψ are complete 1-central automorphisms of $L(2)$.*
(ii) *The automorphisms ε, ν, μ and ψ are pairwise non-equivalent.*
(iii) *Every 1-central automorphism of $L(2)$ is equivalent to exactly one of the automorphisms ε, ν, μ, ψ.*

Proof. Only (iii) is not immediate. If f is not equivalent to ψ then, by 6.7, $B(G(\circ)) \subseteq$ $\subseteq \operatorname{Ker}(\iota + f)$ and $f(a) = \varepsilon(a) = \nu(a) = \mu(a)$, $f(b) = \varepsilon(b) = \nu(b) = \mu(b)$. Since $c \circ f(c) \in Z\,3c$, $f(c) + c \in Z\,3c$. Thus either $f(c) = -c = \varepsilon(c)$ and $f = \varepsilon$, or $f(c) =$ $= 2c = \nu(c)$ and $f = \nu$ or $f(c) = 5c = \mu(c)$ and $f = \mu$. □

7. THE LOOP $L(6)$

In this section, let $G(+) = G(3) \times G(3) \times G(3) \times G(9)$. Put $a = \langle 1, 0, 0, 0\rangle$, $b = \langle 0, 1, 0, 0\rangle$, $c = \langle 0, 0, 1, 0\rangle$, $d = \langle 0, 0, 0, 1\rangle$ and $M = \{a, b, c, d\}$. Further, define $t : M^3 \to B(G(+))$ by $t(a, b, c) = 3d$, $t(b, a, c) = 6d$ and $t(x, y, z) = 0$ otherwise. Then t can be extended to a triadditive mapping T satisfying (1), (2), (4) and we denote by $L(6)$ the corresponding commutative Moufang loop.

7.1. Proposition. *Put $G(\circ) = L(6)$. Then:*
(i) *$G(\circ)$ is a commutative Moufang loop nilpotent of class 2.*
(ii) *$A(G(\circ)) = D(G(\circ)) = \operatorname{Im} T = \operatorname{Im} \overline{T} = Z\,3d$ and $C(G(\circ)) = \operatorname{An}(T) = Zd$.*
(iii) *$q(G(\circ)) = 4$, $\{a, b, c, d\}$ is a generator set of $G(\circ)$ and $G(\circ)$ is subdirectly irreducible.*
(iv) *$G(\circ)$ is given up to isomorphism by four generators x, y, z, u and relations $x^3 = y^3 = z^3 = u^9 = 1$, $(x, y, z) = u^3$, $(x, y, u) = (x, z, u) = (y, z, u) = 1$.*

Proof. Similar to that of 6.1. □

7.2. Lemma. *Let $H(+)$ be a 3-group, S a triadditive mapping of H^3 into H satisfying (1), (2) and (4), and $M = \{a, b, c, d\} \cup N$ a basis of $H(+)$ such that $\operatorname{Im} S \subseteq A(H(*)) = Zu$, $o(u) = 3$, $N \subseteq \operatorname{An}(\bar{S})$ and $u \in Z\,3a \oplus Z\,3b \oplus Z\,3c \oplus$ $\oplus Z\,3d \oplus \sum_{x \in N} Zx$. Then $C(H(*)) \nsubseteq A(H(*))$.*

Proof. Obviously, $\operatorname{Im} \bar{S} \subseteq Zu$ and there are $\alpha, \beta, \gamma, \delta \in F(3)$ such that $\bar{S}(a, b, c) =$ $= \bar{\alpha}u$, $\bar{S}(a, b, d) = \beta u$, $\bar{S}(a, c, d) = \gamma u$ and $\bar{S}(b, c, d) = \delta u$. Consider the following system of linear equations over $F(3)$: $\alpha x + \delta v = 0$, $-\alpha y + \gamma v = 0$, $\beta x - \delta u = 0$, $-\beta y - \gamma u = 0$, $\gamma x + \delta y = 0$, $\alpha u + \beta v = 0$. It is easy to check that this system has a non-trivial solution in $F(3)$, say $\pi, \varrho, \sigma, \tau$. Then, for $w = \pi a + \varrho b + \sigma c + \tau d$, $\bar{S}(w, x, y) = 0$ for all $x, y \in M$. Hence $w \in \operatorname{An}(\bar{S}) = C(H(*))$ and, obviously, $w \notin Zu$. □

7.3. Proposition. Let S be a triadditive mapping of G^3 into G satisfying (1), (2)

and (4), but not (5). If the corresponding commutative Moufang loop $G(*)$ is directly irreducible and $q(G(*)) = 4$ then $G(*)$ is isomorphic to $L(6)$.

Proof. By 4.9, we can suppose that Im $S \subseteq A(G(*))$. Since $q(G(*)) = 4$, $q(G(*)/J(G(*))) = 4$ and $|G(*)/J(G(*))| = 81$. Consequently $|J(G(*))| = 3$ and $A(G(*)) = J(G(*)) = D(G(*)) = Z\,3d$. By 7.2, $A(G(*)) \subsetneq C(G(*))$. Since $G(*)$ is directly irreducible, by 1.7 $C(G(*)) \cap B(G(*)) \subseteq J(G(*)) = A(G(*))$, hence there is $w \in C(G(*))$ with $o(w) = 9$, however, $|G(*/C(G(*))| \geqq 27$ and so $C(G(*)) = Zw$. Clearly, $\{a, b, c, w\}$ is a basis of $G(+)$, hence a generator set of $G(*)$, $w \in \mathrm{An}(\bar{S})$ and $\bar{S}(a, b, c) \neq 0$ (otherwise $G(*)$ would be a group by 3.9). Thus $\bar{S}(a, b, c) \in \{3d, 6d\} = \{3w, 6w\}$ and we can use 7.1(iv). □

7.4. Proposition. *Let $H(+) = G(3) \times G(3) \times G(3) \times G(3) \times G(3)$ and the S be a triadditive mapping of H^3 into H satisfying* (1), (2) *and* (4). *Then the corresponding commutative Moufang loop $H(*)$ is not directly irreducible.*

Proof. With respect to 4.9, $q(H(*)) \leqq 5$ and we can assume that Im $S \subseteq A(H(*))$. If $q(H(*)) = 5$ then by 1.2 $q(K(*)) = 5$, where $K(*) = H(*)/J(H(*))$, hence by 1.4 $|K| = 243 = |H|$, $A(H(*)) \subseteq J(H(*)) = 0$ and $H(*)$ is a group. If $q(H(*)) \leqq 3$ then, with respect to 4.10, $q(H(*)) \leqq 2$ and $H(*)$ is a group again. However, in this case $H(*)$ is clearly isomorphic to $H(+)$. Now suppose that $H(*)$ is not associative. Then $q(H(*)) = 4$, $|K| = 81$ and $|J(H(*))| = 3$. Consequently $|A(H(*))| = 3$ and there is a basis $\{a, b, c, d, e\}$ of $H(+)$ such that $Ze = A(H(*)) \subseteq C(H(*)) = \mathrm{An}(\bar{S})$. By 7.2, $C(H(*)) \nsubseteq A(H(*))$, however, $C(H(*)) \subseteq H(*) = B(H(*))$ and $A(H(*)) = J(H(*))$. Now it suffices to use 1.7. □

8. COMMUTATIVE MOUFANG LOOPS NILPOTENT OF CLASS AT MOST TWO

We denote by $\mathscr{M}$ the variety of commutative Moufang loops nilpotent of class at most two and by $\mathscr{G}$ the variety of abelian groups. Further, for $n \geqq 0$, let $\mathscr{M}_n$ be the subvariety of $\mathscr{M}$ determined by the identity $x^n \approx 1$ and $\mathscr{G}_n = \mathscr{G} \cap \mathscr{M}_n$. Thus $\mathscr{M}_0 = \mathscr{M}$, $\mathscr{G}_0 = \mathscr{G}$ and $\mathscr{M}_1 = \mathscr{G}_1$ is the trivial variety. Moreover, $\mathscr{G} \subseteq \mathscr{M}$ and $\mathscr{G}_n \subseteq \mathscr{M}_n$.

8.1. Lemma. *Let $Q \in \mathscr{M}_3$ be finitely generated and $q(Q) = n$. Then $|Q| \leqq 3^{n+m}$, where $m = \binom{n}{3}$.*

Proof. Since $Q/A(Q) \in \mathscr{G}_3$ and $q(Q/A(Q)) = n$, $|Q/A(Q)| = 3^n$. On the other hand, $A(Q) \in \mathscr{G}_3$ and $q(A(Q)) \leqq m$ by 1.14. Thus $|A(Q)| \leqq 3^m$ and $|Q| \leqq 3^{n+m}$. □

8.2. Lemma. *Let $Q \in \mathscr{M}$ be free. Then $A(Q) = B(Q)$ and $A(Q) \cap D(Q) = \{1\}$.*

Proof. Denote by f the natural homomorphism of Q onto $Q/A(Q)$. If $x \in B(Q)$ then

$x^3 = 1, f(x)^3 = 1$ and $f(x) = 1$, since $Q/A(Q)$ is a free abelian group. Thus $x \in A(Q)$. If, moreover, $x \in D(Q)$ then $x = y^3$ for some $y \in Q$, hence $f(y)^3 = 1$, $f(y) = 1$, $y \in A(Q)$ and $x = y^3 = 1$. □

Let $n \geqq 3$, $m = \binom{n}{3}$ and $E_n(+) = Z^n \times G(3)^m$. Further, put $a_{1,n} = \langle 1, 0, \ldots, 0\rangle, \ldots, a_{n,n} = \langle 0, \ldots, 0, 1, 0, \ldots, 0\rangle$, $a_{n+1,n} = b_{1,n} = \langle 0, \ldots, 0, 0, 1, 0, \ldots, 0\rangle, \ldots, a_{n+m,n} = b_{m,n} = \langle 0, \ldots, 0, 1\rangle$, $N_n = \{a_{1,n}, \ldots, a_{m+n,n}\}$ and $M_n = \{a_{1,n}, \ldots, a_{n,n}\}$. Obviously, N_n is a basis of $E_n(+)$. Denote by K_n the set of all ordered triples $\langle i, j, k\rangle$, where $1 \leqq i < j < k \leqq n$ and let $\leqq$ be the lexicographic ordering on K_n. There is a biunique mapping $p_n : K_n \to \{1, \ldots, m\}$ such that for $\alpha, \beta \in K_n$, $\alpha \leqq \beta$ implies $p_n(\alpha) \leqq p_n(\beta)$. Now, define a mapping $t_n : N_n^3 \to B(E_n(+))$ by $t_n(a_i, a_j, a_k) = b_{p_n(\alpha)}$ and $t_n(a_j, a_i, a_k) = 2b_{p_n(\alpha)}$ for $\alpha = \langle i, j, k\rangle \in K_n$ and $t_n(x, y, z) = 0$ otherwise. Clearly, t_n can be extended to a triadditive mapping T_n satisfying (1), (2) and (4). Put $x \circ y = x + y + T_n(x, y, x - y)$ for all $x, y \in E_n$. Then $E_n(\circ)$ is a commutative Moufang loop nilpotent of class at most two.

8.3. Lemma. (i) *$A(E_n(\circ)) = Zb_{1,n} \oplus \ldots \oplus Zb_{m,n}$ and $E_n(\circ)/A(E_n(\circ))$ is isomorphic to Z^n.*

(ii) *$D(E_n(\circ)) = Z\,3a_{1,n} \oplus \ldots \oplus Z\,3a_{n,n}$ and $|E_n(\circ)/D(E_n(\circ))| = 3^{n+m}$.*

(iii) *$C(E_n(\circ)) = \mathrm{An}(T_n) = D(E_n(\circ)) \oplus A(E(\circ))$.*

Proof. Easy. □

The following proposition was for the first time proved in [2]. Here we present a somewhat different proof.

8.4. Proposition. *The loop $E_n(\circ)$ is a free commutative Moufang loop nilpotent of class at most two and M_n is a free generator set of $E_n(\circ)$.*

Proof. It is easily seen that $M = M_n$ generates $E(\circ) = E_n(\circ)$. Let $Q \in \mathscr{M}$ be free of rank n and let $\{x_1, \ldots, x_n\}$ be a free generator set of Q. There is a surjective homomorphism f of Q onto $E(\circ)$ such that $f(x_1) = a_{1,n}, \ldots, f(x_n) = a_{n,n}$. We have $f(A(Q)) = A(E(\circ))$, $f(D(Q)) = D(E(\circ))$ and so f induces two surjective homomorphisms $g : Q/A(Q) \to E(\circ)/A(E(\circ))$ and $h : Q/D(Q) \to E(\circ)/D(E(\circ))$. Finally, denote by k and l the natural homomorphisms of Q onto $Q/A(Q)$ and $Q/D(Q)$, respectively. We are going to show that g and h are injective. The abelian group $Q/A(Q)$ is free of rank n. On the other hand, $E(\circ)/A(E(\circ))$ is isomorphic to Z^n and thus to $Q/A(Q)$. However, every surjective endomorphism of Z^n is an automorphism and hence g is injective. Further, $Q/D(Q)$ is free of rank n in $\mathscr{M}_3$ and $|Q/D(Q)| \leqq 3^{n+m}$ by 8.1. Since $|E(\circ)/D(E(\circ))| = 3^{n+m}$, h is injective. Now we can show that f is injective and hence an isomorphism: if $x, y \in Q$ and $f(x) = f(y)$ then $g\,k(x) = g\,k(y)$, $k(x) = k(y)$, $h\,l(x) = h\,l(y)$, $l(x) = l(y)$, $xy^{-1} \in A(Q) \cap D(Q)$ and $x = y$ by 8.2. □

8.5. Lemma. *Let $Q \in \mathcal{M}_3$, $q(Q) = n$ and let P be a normal subloop of Q such that $q(Q/P) = n$. Then $P \subseteq A(Q)$.*

Proof. Denote by L the subloop of Q generated by $A(Q) \cup P$. Then $L/P = A(Q/P)$ and Q/L is isomorphic to $(Q/P)/A(Q/P) = H$. Since $q(Q/P) = n$, $q(H) = n$ and $|H| = |Q/L| = 3^n$. However, by 1.4 $|Q/A(Q)| = 3^n$ and $A(Q) \subseteq L$. This implies $A(Q) = L$ and $P \subseteq A(Q)$. □

8.6. Theorem. *The following conditions are equivalent for a groupoid Q:*

(i) *Q is a finitely generated commutative Moufang loop nilpotent of class at most two without elements of infinite order.*

(ii) *Q is a finite commutative Moufang loop nilpotent of class at most two.*

(iii) *There exists a finite ternary ring $Q(+, S)$ satisfying (1), (2) and (4) such that $xy = x + y + S(x, y, x - y)$ for all $x, y \in Q$.*

Proof. The equivalence of (i) and (ii) is clear and (iii) implies (i) by 4.1.

(ii) $\Rightarrow$ (iii). With respect to 1.3 and 1.2(i), we can assume that Q is a 3-loop and $q(Q) = n \geqq 3$. Then there is a surjective homomorphism $f : E(\circ) \to Q$, where $E(\circ) = E_n(\circ)$. We are going to show that $P = \operatorname{Ker} f \subseteq C(E(\circ))$. Denote by L the subloop of $E(\circ)$ generated by $P \cup D(E(\circ))$ and by h the natural homomorphism of $E(\circ)$ onto $H(\circ) = E(\circ)/D(E(\circ))$. Then $h(L)$ is a normal subloop of $H(\circ)$ and $H(\circ)/h(L)$ is isomorphic to $Q/D(Q)$. However, $D(Q) \subseteq J(Q)$ by 1.4(i), hence $q(Q/D(Q)) = n$ and $q(H(\circ)/h(L)) = n$. Thus $h(L) \subseteq A(H(\circ))$ by 8.5 and $L \subseteq R$, where R is the subloop of $E(\circ)$ generated by $A(E(\circ)) \cup D(E(\circ))$. In particular, $P \subseteq R \subseteq C(E(\circ))$. Since $C(E(\circ)) = \operatorname{An}(T_n)$, P is an ideal of the ternary ring $E(+, T_n)$. Denote by r the congruence of $E(\circ)$ corresponding to P. Then obviously $x \, r \, y$ iff $x - y \in P$ and hence r is also a congruence of the ternary ring $E(+, T_n)$. □

9. COMMUTATIVE MOUFANG LOOPS OF SMALL ORDERS AND COMMUTATIVE MOUFANG LOOPS GENERATED BY THREE ELEMENTS

9.1. Proposition. *Let Q be a commutative Moufang loop such that Q is not associative and $|Q| \leqq 728$. Then there are an abelian group G and a non-associative commutative Moufang 3-loop P such that Q is isomorphic to the product $G \times P$ and either $|P| = 81$ or $|P| = 243$.*

Proof. Apply 1.3 and 1.8. □

9.2. Theorem. (i) *$L(1)$ and $L(2)$ are up to isomorphism the only non-associative commutative Moufang loops of order 81 and these two loops are not isomorphic.* (ii) *$L(3)$, $L(4)$, $L(5)$, $L(6)$, $G(3) \times L(1)$ and $G(3) \times L(2)$ are up to isomorphism the*

only non-associative commutative Moufang loops of order 243 *and these six loops are pairwise non-isomorphic.*

Proof. (i) Let Q be a non-associative commutative Moufang loop of order 81. By 1.6(ii) and 8.6, there are a group $Q(+)$ and a triadditive mapping S of Q^3 into Q such that S satisfies (1), (2) and (4), does not satisfy (5) and $xy = x + y + S(x, y, x - y)$ for all $x, y \in Q$. First, let $q(Q(+)) = 4$. Then $Q(+)$ is isomorphic to $G(3) \times G(3) \times G(3) \times G(3)$. If $q(Q) = 4$ then $q(Q/J(Q)) = 4$, $|Q/J(Q)| = 81$ and $A(Q) \subseteq J(Q) = \{1\}$, a contradiction. Thus $q(Q) = 3$ and Q is isomorphic to $L(1)$ by 5.3. If $q(Q(+)) \neq 4$ then $q(Q(+)) \leqq 3$ and $q(Q(+)) = 3$ by 3.8(iii). Hence $Q(+)$ is isomorhic to $G(3) \times G(3) \times G(9)$ and Q to $L(2)$ (apply 6.5).

(ii) If $|Q| = 243$ then $3 \leqq q(Q(+)) \leqq 5$ and the following cases can arise:

(a) $Q(+) \cong G(3) \times G(3) \times G(27)$. By 6.5, Q is isomorphic to $L(4)$.

(b) $Q(+) \cong G(3) \times G(9) \times G(9)$. By 6.5, Q is isomorphic to $L(5)$.

(c) $Q(+) \cong G(3) \times G(3) \times G(3) \times G(9)$. If $q(Q) = 3$ then Q is isomorphic to $L(3)$ by 5.3. If $q(Q) \neq 3$ then $q(Q) = 4$ and Q is isomorphic to $L(6)$ by 7.3, provided Q is directly irreducible. In the opposite case, $Q \cong G(3) \times P$, where P is a non-associative commutative Moufang loop of order 81. Since P must contain an element of order 9, P is isomorphic to $L(2)$.

(d) $Q(+) \cong G(3) \times G(3) \times G(3) \times G(3) \times G(3)$. By 7.4 and 8.1, $Q \cong G(3) \times P$, where P is a non-associative commutative Moufang loop of order 81. Since every non-zero element of P has order 3, P is isomorphic to $L(1)$. □

9.3. Corollary. $L(1)$, $L(2)$, $G(2) \times L(1)$, $G(2) \times L(2)$, $L(3)$, $L(4)$, $L(5)$, $L(6)$, $G(3) \times L(1)$, $G(3) \times L(2)$, $G(4) \times L(1)$, $G(4) \times L(2)$, $G(2) \times G(2) \times L(1)$, $G(2) \times G(2) \times L(2)$, $G(5) \times L(1)$, $G(5) \times L(2)$, $G(2) \times G(3) \times L(1)$, $G(2) \times G(3) \times L(2)$, $G(2) \times L(3)$, $G(2) \times L(4)$, $G(2) \times L(5)$, $G(2) \times L(6)$, $G(7) \times L(1)$, $G(7) \times L(2)$, $G(8) \times L(1)$, $G(8) \times L(2)$, $G(2) \times G(4) \times L(1)$, $G(2) \times G(4) \times L(2)$, $G(2) \times G(2) \times G(2) \times L(1)$, $G(2) \times G(2) \times G(2) \times L(2)$ are up to isomorphism the only non-associative commutative Moufang loops of order $\leqq 728$. Moreover, these 30 loops are pairwise non-isomorphic. □

9.4. Remark. In the following table, $l(n)$ denotes the number of isomorphism classes of commutative Moufang loops of order 3^n (groups are included):

n	1	2	3	4	5	6
$l(n)$	1	2	3	7	13	$\geqq 30$

9.5. Theorem. $L(n_1, m_1, k_1, 1)$, *where* $1 \leqq n_1 \leqq m_1 \leqq k_1$, $L(n_2, m_2, k_2, 2)$, where $2 \leqq n_2 \leqq m_2 \leqq k_2$, $L(n_3, m_3, k_3, 3)$, *where* $1 \leqq n_3 < m_3 \leqq k_3$ *and* $L(n_4, m_4, k_4, 4)$, *where* $1 \leqq n_4 \leqq m_4 < k_4$, *are up to isomorphism the only non-associative com-*

mutative Moufang 3-loops with three generators. Moreover, $L(n_i, m_i, k_i, i)$ is isomorphic to $L(n_j, m_j, k_j, j)$ iff $i = j$, $n_i = n_j$, $m_i = m_j$, $k_i = k_j$.

Proof. Let Q be a non-associative commutative Moufang 3-loop with $q(Q) \leqq 3$. Then $q(Q) = 3$, Q is finite and nilpotent of class 2. By 8.6, there are a group $Q(+)$ and a triadditive mapping S of Q^3 into Q satisfying (1), (2) and (4), but not (5), such that $xy = x + y + S(x, y, x - y)$ for all $x, y \in Q$. Obviously, $Q(+)$ is a 3-group and $q(Q(+)) \geqq 3$. If $q(Q(+)) = 3$ then 6.5 may be used. If $q(Q(+)) \geqq 4$ then the result follows from 4.10 and 5.3 and an application of 6.6 completes the proof. □

9.6. Corollary. *The following assertions are equivalent for a groupoid Q:*

(i) *Q is a finite non-associative commutative Moufang loop with $q(Q) = 3$.*
(ii) *There exist positive integers n, m, k, i, r, s, t such that r, s, t are not divisible by 3 and Q is isomorphic to $L(n, m, k, i) \times G(r) \times G(s) \times G(t)$.*

Proof. (i) ⇒ (ii). By 1.3, Q is isomorphic to $H \times K$, where H is a non-associative commutative Moufang 3-loop, K is an abelian group whose elements have orders not divisible by 3 and obviously $q(H), q(K) \leqq 3$.

(ii) ⇒ (i). If $\{a, b, c\}$ is a generator set of $L(n, m, k, i)$, $G(r) = Zx$, $G(s) = Zy$ and $G(t) = Zw$ then obviously $\{\langle a\, x\rangle, \langle b, y\rangle, \langle c, w\rangle\}$ is a generator set of $L(n, m, k, i) \times G(r) \times G(s) \times G(t)$. □

9.7. Theorem. *The following assertions are equivalent for a commutative Moufang loop Q:*

(i) *Q is not associative and every proper subloop as well as every proper factor-loop of Q is a group.*
(ii) *Q is subdirectly irreducible, not associative and $q(Q) \leqq 3$.*
(iii) *Q is subdirectly irreducible and $q(Q) = 3$.*
(iv) *Q is isomorphic either to $L(1)$ or to $L(1, 1, k, 4)$ for some $k \geqq 2$.*

Proof. (i) ⇒ (ii). Obviously, Q is subdirectly irreducible. If $q(Q) \geqq 4$ then for all $a, b, c \in Q$, the subloop generated by $\{a, b, c\}$ is a group and $(a, b, c) = 1$.

(ii) ⇒ (iii). This is trivial.

(iii) ⇒ (iv). Clearly, Q is not associative and $A(Q)$ is the least normal subloop. If $1 \neq x \in A(Q)$ and $a \in Q$ is arbitrary then $a^3 \in C(Q)$, hence there is $k \geqq 1$ with $x = a^{3k}$ and $a^{9k} = 1$. By 1.3, Q is a 3-loop and we can use 9.5, 5.1 and 6.3.

(iv) ⇒ (i). First, we make the following simple observation: If G is a commutative Moufang loop with $q(G) = 3$ and P is a maximal subloop of G such that $C(G) \subseteq P$ then P is a group (indeed, $G/C(G) \in \mathscr{G}_3$ and $q(G/C(G)) \leqq 3$, hence $q(P/C(P)) \leqq 2$ and P is a group). In our case, every proper subloop is contained in a maximal subloop by 1.2(iii) and $J(Q) = C(Q)$ by 5.1 and 6.3. Finally, let H be a non-trivial normal subloop. Obviously, $A(Q)$ is the least non-trivial subloop of $C(Q)$ and so, with respect to 1.5, $A(Q) \subseteq H$. □

10. THE LATTICE OF VARIETIES OF COMMUTATIVE MOUFANG LOOPS NILPOTENT OF CLASS AT MOST TWO

10.1. Lemma. *Let $Q \in \mathscr{M}_3$ be free and $q(Q) = n \geqq 3$. Then Q is isomorphic to a subdirect product of copies of $L(1)$.*

Proof. By 8.4, Q is isomorphic to $E_n(\circ)/D(E_n(\circ))$. Let $1 \leqq l \leqq m = \binom{n}{3}$ and let $1 \leqq i < j < k \leqq n$ be such that $l = p_n(\langle i, j, k\rangle)$. Denote by P_l the set of all $\langle \lambda_1, \ldots, \lambda_n, \varrho_1, \ldots, \varrho_m\rangle \in E_n$ such that $\lambda_i, \lambda_j, \lambda_k$ are divisible by 3 and $\varrho_l = 0$. Obviously $D(E_n(\circ)) \subseteq P_l$. On the other hand, it is easy to check that $P_l(\circ)$ is a normal subloop of $E_n(\circ)$ and $E_n(\circ)/P_l(\circ) \cong L(1)$. Finally, $\bigcap_{l=1}^{m} P_l = D(E_n(\circ))$. □

10.2. Lemma. *Let $k \geqq 2$. Then there is a subloop P of $L(1, 1, k, 4) \times L(1, 1, k, 4)$ such that $L(1)$ is a homomorphic image of P.*

Proof. Put $G(\circ) = L(1, 1, k, 4)$, $T = T_4$, $H(\circ) = G(\circ) \times G(\circ)$, $H(+) = G(+) \times$ $\times G(+)$ and $S = T \times T$. Further, let $\alpha = \langle a, -a\rangle$, $\beta = \langle b, b\rangle$, $\gamma = \langle c, c\rangle$, $\delta =$ $= \langle 3^{k-1}c, \ldots, 3^{k-1}c\rangle$ and let $P(+)$ be the subgroup of $H(+)$ generated by $\{\alpha, \beta, \gamma, \delta\}$. We have $S(P^3) = Z\delta \subseteq P$, and so $P(\circ)$ is a non-associative subloop of $H(\circ)$. Further, $(\alpha, \beta, \gamma) = \delta$ in $H(\circ)$ and so $P(\circ)$ is generated by $\{\alpha, \beta, \gamma\}$ and $q(P(\circ)) = 3$. Moreover, we have $A(P(\circ)) = Z\delta$. Put $L = Z\,3\gamma$. Then $L \subseteq C(P(\circ))$, L is a normal subloop of $P(\circ)$, $L = D(P(\circ))$ and $P(\circ)/L \in \mathscr{M}_3$. Since $L \cap A(P(\circ)) = 0$, $P(\circ)/L$ is not associative and by 9.5 $P(\circ)/L \cong L(1)$. □

10.3. Lemma. *Let $k \geqq 0$ and let $Q \in \mathscr{M}_{3^k}$ be free. Then $A(Q) \cap D(Q) = \{1\}$.*

Proof. There are a free loop $E \in \mathscr{M}$ and a homomorphism f of E onto Q such that $\operatorname{Ker} f = \{x^{3^k} \mid x \in E\}$. For $k = 0$, there is nothing to prove. Let $k \geqq 1$. Then $\operatorname{Ker} f \subseteq D(E)$. If $a \in A(Q) \cap D(Q)$ then $f(x) = a = f(y)$ for some $x \in A(E)$, $y \in D(E)$, hence $xy^{-1} \in \operatorname{Ker} f \subseteq D(E)$ and $x \in A(E) \cap D(E) = \{1\}$ by 8.2. Consequently $x = 1$ and $a = 1$. □

10.4. Lemma. *Let $\mathscr{V}$ be a subvariety of $\mathscr{M}$ such that $\mathscr{V} \not\subseteq \mathscr{G}$. Then $\mathscr{M}_3 \subseteq \mathscr{V}$.*

Proof. There is $Q \in \mathscr{V}$ such that Q is not associative, hence $a \,.\, bc \neq ab \,.\, c$ for some $a, b, c \in Q$. Denote by P the subloop generated by $\{a, b, c\}$. Then $P \in \mathscr{V}$ and $q(P) = 3$. Further, P has a subdirectly irreducible factor L such that L is not associative. Hence $q(L) = 3$ and by 9.7 L is isomorphic either to $L(1)$ or to $L(1, 1, k, 4)$ for some $k \geqq 2$. According to 10.2, $L(1) \in \mathscr{V}$ and by 10.1 every finitely generated free loop from $\mathscr{M}_3$ belongs to $\mathscr{V}$. Thus $\mathscr{M}_3 \subseteq \mathscr{V}$. □

10.5. Proposition. *Let $\mathscr{V}$ be a subvariety of $\mathscr{M}$. Then either $\mathscr{V} = \mathscr{G}_n$ for some $n \geqq 0$ or $\mathscr{V} = \mathscr{M}_m$ for some $m \geqq 0$ divisible by 3.*

Proof. We can assume that $\mathscr{V} \not\subseteq \mathscr{G}$, the case $\mathscr{V} \subseteq \mathscr{G}$ being clear. There is $m \geqq 0$

such that $\mathscr{V} \cap \mathscr{G} = \mathscr{G}_m$. Further, by 10.4, $G(3) \in \mathscr{G}_m$ and so 3 divides m. If $m = 0$ then $\mathscr{G} = \mathscr{G}_0 \subseteq \mathscr{V}$ and $\mathscr{V} = \mathscr{M}_0$ by 10.4 and 8.2. Now assume that $m \neq 0$. Then $m = 3^k l$, where $k \geqq 1$ and l is not divisible by 3. If $Q \in \mathscr{M}_{3^k}$ is a finitely generated free loop then by 10.3 Q is isomorphic to a subdirect product of $Q/A(Q)$ and $Q/D(Q)$. However, $Q/A(Q) \in \mathscr{G}_{3^k} \subseteq \mathscr{G}_m$ and $Q/D(Q) \in \mathscr{M}_3 \subseteq \mathscr{V}$ by 10.4, therefore $Q \in \mathscr{V}$ and $\mathscr{M}_{3^k} \subseteq \mathscr{V}$. If $Q \in \mathscr{M}_m$ is a finitely generated free loop then Q is isomorphic to a product $P \times L$, where $P \in \mathscr{M}_{3^k}$ and $L \in \mathscr{G}_l$, hence $Q \in \mathscr{V}$ and $\mathscr{M}_m \subseteq \mathscr{V}$. Conversely, if $Q \in \mathscr{V}$ is arbitrary and $x \in Q$ then the cyclic subgroup generated by x belongs to $\mathscr{G}_m$, consequently $x^m = 1$ and $Q \in \mathscr{M}_m$. □

Denote by $\mathscr{L}$ the set of all ordered pairs $\langle n, 0\rangle$ with $n \geqq 0$ and $\langle m, 1\rangle$ with $m \geqq 0$ divisible by 3. Define an ordering $\leqq$ on $\mathscr{L}$ by $\langle n, i\rangle \leqq \langle m, j\rangle$ iff $i \leqq j$ and n divides m. It is easy to see that $\mathscr{L} = (\mathscr{L}, \leqq)$ is a lattice. Now we can summarize our results:

10.6. Theorem. (i) *$\mathscr{G}_n$, for $n \geqq 0$, and $\mathscr{M}_m$, for $m \geqq 0$ divisible by 3, are the only subvarieties of $\mathscr{M}$.*

(ii) *$\mathscr{G}_n \subseteq \mathscr{G}_{n'}$ iff n divides n', $\mathscr{M}_m \subseteq \mathscr{M}_{m'}$ iff m divides m', $\mathscr{G}_n \subseteq \mathscr{M}_m$ iff n divides m. Moreover, $\mathscr{M}_m \not\subseteq \mathscr{G}_n$.*

(iii) *The lattice of subvarieties of the variety $\mathscr{M}$ of commutative Moufang loops nilpotent of class at most two is isomorphic to the lattice $\mathscr{L}$. The isomorphism is given by $\mathscr{G}_n \to \langle n, 0\rangle$, $\mathscr{M}_m \to \langle m, 1\rangle$.* □

11. DISTRIBUTIVE GROUPOIDS

A groupoid G is said to be distributive if it satisfies the identities $x \,.\, yz \doteq xy \,.\, xz$ and $yz \,.\, x \doteq yx \,.\, zx$. Obviously, G is distributive iff the translations L_a and R_a $(L_a(x) = ax,\ R_a(x) = xa)$ are endomorphisms of G for every $a \in G$. A groupoid G is said to be medial if it satisfies the identity $xy \,.\, uv \doteq xu \,.\, yv$.

A non-empty subset I of a groupoid G is said to be an ideal if $xa, ax \in I$ for all $a \in I$, $x \in G$. In this case, the relation $r = (I \times I) \cup \iota_G$ is a congruence of G and the corresponding factorgroupoid is denoted by G/I. This factorgroupoid contains a zero element, i.e. an element z such that $zx = z = xz$ for every x. The ideal I is said to be prime if $xy \in I$ implies either $x \in I$ or $y \in I$. Obviously, a proper ideal I is prime iff $G \setminus I$ is a subgroupoid of G.

For a groupoid G, let Id G denote the set of all idempotents of G.

11.1. Proposition. *Let G be a distributive groupoid. Then:*

(i) Id G *is an ideal of G and $a \,.\, bc$, $ab \,.\, c \in$ Id G for all $a, b, c \in G$.*

(ii) $G/\mathrm{Id}\ G$ *is a medial semigroup and G is isomorphic to a subdirect product of* Id G *and* $G/\mathrm{Id}\ G$.

(iii) G *is medial iff* Id G *is.*

Proof. See [6, Propositions 1.2, 1.3]. □

11.2. Lemma. *Let I be an ideal of a distributive groupoid G such that both I and G/I are medial. Then G is medial.*

Proof. With respect to 11.1, we can assume that G is idempotent. For each $a \in I$, the translations L_a and R_a of G are homomorphisms of G into I. Denote by s the intersection of all congruences of G corresponding to these homomorphisms. Then G/s is medial and $x\ s\ y$ iff $ax = ay$, $xa = ya$ for all $a \in I$. Further, let f and g denote the natural homomorphisms of G onto G/s and G/I, respectively. The groupoid $H = G/s \times G/I$ is medial and $h : G \to H$ defined by $h(x) = \langle f(x), g(x) \rangle$ is a homomorphism. If $x, y \in G$ and $h(x) = h(y)$ then $g(x) = g(y)$ implies either $x = y$ or $x, y \in I$, however, in the latter case $x = xx = xy = yy = y$, since $f(x) = f(y)$. □

11.3. Proposition. *Let G be a subdirectly irreducible commutative distributive idempotent groupoid. Then at least one of the following assertions holds:*

(i) *G is a cancellation groupoid.*

(ii) *G contains a zero element 0 such that $H = G \setminus \{0\}$ is a subgroupoid of G and H is a cancellation groupoid. In this case, G is medial iff H is.*

Proof. See [8, Proposition 5.1]. □

11.4. Lemma. *Every proper ideal of a commutative distributive idempotent groupoid is contained in a proper prime ideal.*

Proof. Let I be a proper ideal of G and f the natural homomorphism of G onto G/I. Then G/I is not a cancellation groupoid and by 11.3 there exists a homomorphism g of G/I onto a groupoid H such that H contains a zero element 0 and $H \setminus \{0\}$ is a subgroupoid of H. Then $J = \{x \in G \mid g f(x) = 0\}$ is a proper prime ideal containing I. □

11.5. Lemma. *Let G be a finite commutative distributive groupoid without proper ideals. Then G is a quasigroup.*

Proof. Apply 11.1 and 11.3. □

11.6. Remark. For $n \geqq 1$, let $a(n)$ ($b(n)$, $c(n)$, $d(n)$, $e(n)$) denote the number of isomorphism classes of distributive groupoids (distributive idempotent groupoids, commutative distributive groupoids, commutative distributive idempotent groupoids, distributive semigroups) of order n. We have the following table:

n	$a(n)$	$b(n)$	$c(n)$	$d(n)$	$e(n)$
1	1	1	1	1	1
2	4	3	2	1	4
3	19	13	7	3	14

12. NON-MEDIAL DISTRIBUTIVE QUASIGROUPS OF ORDER 81

12.1. Proposition. *The following conditions are equivalent for a groupoid* Q:

(i) Q *is a distributive quasigroup.*

(ii) *There exist a commutative Moufang loop* $Q(+)$ *and a complete* 1*-central automorphism* f *of* $Q(+)$ *such that* $xy = f(x) + \bar{f}(y) = f(x) + (y - f(y))$ *for all* $x, y \in Q$. *In this case,* Q *is medial iff* $Q(+)$ *is a group.*

Proof. See [11, § II.7 Théorème 1, § V.1 Proposition 4]. □

12.2. Proposition. *The following conditions are equivalent for a groupoid* Q:

(i) Q *is a commutative distributive quasigroup.*

(ii) *There exists a commutative Moufang loop* $Q(+)$ *such that* $v_{Q(+)}$ *is an automorphism of* $Q(+)$ *and* $xy = \mu(x + y)$ *for all* $x, y \in Q$.

Proof. This is an easy consequence of 12.1. □

12.3. Lemma. *Let* $Q(+)$, $P(+)$ *be commutative Moufang loops and* f, g *be complete* 1*-central automorphisms of* $Q(+)$, $P(+)$, *respectively. The following conditions are equivalent*:

(i) *The corresponding distributive quasigroups* Q *and* P *are isomorphic.*

(ii) *There is an isomorphism* h *of* $Q(+)$ *onto* $P(+)$ *such that* $hf = gh$.

Proof. (i) $\Rightarrow$ (ii). Let $k : Q \to P$ be an isomorphism of distributive quasigroups. There is $a \in P$ such that $a\,k(0) = 0$. Put $l(x) = ax$ for every $x \in P$ and $h = lk$. Then l is an automorphism of P and h is an isomorphism of Q onto P, hence $h(0) = 0$, $h(f(x) + \bar{f}(y)) = g\,h(x) + \bar{g}\,h(y)$ for all $x, y \in Q$ and the result easily follows.

(ii) $\Rightarrow$ (i). This is clear. □

We shall define six distributive quasigroups $D(1), \ldots, D(6)$ as follows: The underlying set of $D(1)$, $D(2)$ is that of $L(1) = G(\circ)$ and the multiplication is given by $xy = x^{-1} \circ y^{-1} = \varepsilon(x \circ y)$, $xy = \varphi(x) \circ (y \circ \varphi(y^{-1})) = \varphi(x) \circ \bar{\varphi}(y)$, respectively, where φ is the automorphism of $L(1)$ defined in Section 5. The underlying set of $D(3)$, $D(4)$, $D(5)$, $D(6)$ is that of $L(2) = G(\circ)$ and the multiplication is given by $xy = \mu(x \circ y)$, $xy = x^{-1} \circ y^2 = \varepsilon(x) \circ v(y)$, $xy = x^2 \circ y^{-1} = v(x) \circ \varepsilon(y)$ and $xy = \psi(x) \circ (y \circ \psi(y^{-1})) = \psi(x) \circ \bar{\psi}(y)$, respectively, where ψ is the automorphism of $L(2)$ defined in Section 6.

12.4. Theorem. (i) *Every non-medial distributive quasigroup contains at least* 81 *elements.*

(ii) $D(1)$, $D(2)$, $D(3)$, $D(4)$, $D(5)$ *and* $D(6)$ *are up to isomorphism the only non-medial distributive quasigroups of order* 81 *and these quasigroups are pairwise non-isomorphic.*

Proof. Apply 12.1, 12.3, 9.2(i), 5.6 and 6.8. □

12.5. Corollary. *$D(1)$ and $D(3)$ are up to isomorphism the only non-medial commutative distributive quasigroups of order* 81. □

12.6. Remark. It seems that the number of isomorphism classes of distributive quasigroups of order 81 exceeds 100.

Let G_i, $i \in I$, be all pairwise non-isomorphic abelian groups of odd order. For each $i \in I$, v_{G_i} is an automorphism of G_i and we can define $x \circ y = \mu_{G_i}(x + y)$ for all $x, y \in G_i$. For the sake of completeness we include also the following two obvious results:

12.7. Proposition. *$G_i(\circ)$, $i \in I$, are up to isomorphism the only finite commutative medial idempotent quasigroups. Moreover, these quasigroups are pairwise non-isomorphic.*

Proof. By 12.2 and 12.3, taking into account that for a finite group G, v_G is a permutation iff $|G|$ is odd. □

12.8. Corollary. $G_i(\circ)$ with $|G_i| \leqq 80$ are up to isomorphism the only commutative distributive quasigroups of order $\leqq 80$. Moreover, these quasigroups are pairwise non-isomorphic. □

13. DISTRIBUTIVE QUASIGROUPS OF ORDER AT MOST 15

13.1. Lemma. *Let $m > n > 0$ and $f(x) = nx$ for all $x \in G(m)$. Then f is a complete automorphism of $G(m)$ iff $(m, n) = (m, n - 1) = 1$. Moreover, if f, g are equivalent automorphisms of $G(m)$ then $f = g$.*

Proof. Straightforward. □

13.2. Lemma. *The group $G(2) \times G(4)$ has no complete automorphism.*

Proof. Obviously, $g(\langle 0, 2\rangle) = \langle 0, 2\rangle$ for every automorphism g of $G(2) \times G(4)$ and by 1.12(i) g is not complete. □

In the following lemma, let $G(+) = G(2) \times G(6)$ and define an endomorphism τ of $G(+)$ by $\tau(\langle 1, 0\rangle) = \langle 0, 3\rangle$, $\tau(\langle 0, 1\rangle) = \langle 1, 5\rangle$.

13.3. Lemma. *τ is up to equivalence the only complete automorphism of $G(+) = G(2) \times G(6)$.*

Proof. It is easy to check that τ is a complete automorphism of $G(+)$. If f is a complete automorphism of $G(+)$ then $f(x) \neq x$ and $o(f(x)) = o(x)$ for all $x \in G$. Hence $f(\langle 1, 0\rangle) \in \{\langle 1, 3\rangle, \langle 0, 3\rangle\}$ and $f(\langle 0, 1\rangle) \in \{\langle 0, 5\rangle, \langle 1, 1\rangle, \langle 1, 5\rangle, \langle 1, 2\rangle, \langle 1, 4\rangle\}$. If $f(\langle 0, 1\rangle) = \langle 0, 5\rangle$ then $f \mid G(6)$ is a complete automorphism of $G(6)$,

a contradiction with 13.1. If $f(\langle 0, 1\rangle) = \langle 1, 1\rangle$ or $\langle 1, 4\rangle$ then $f(\langle 0, 2\rangle) = \langle 0, 2\rangle$, a contradiction. If $f(\langle 0, 1\rangle) = \langle 1, 5\rangle$ then $f(\langle 0, 3\rangle) = \langle 1, 3\rangle$, hence $f(\langle 1, 0\rangle) = \langle 0, 3\rangle$ and $f = \tau$. Finally, let $f(\langle 0, 1\rangle) = \langle 1, 2\rangle$. If $f(\langle 1, 0\rangle) = \langle 0, 3\rangle$ then $f(\langle 1, 3\rangle) = \langle 1, 3\rangle$, a contradiction. Thus $f(\langle 1, 0\rangle) = \langle 1, 3\rangle$. Now define $h : G \to G$ by $h(\langle 1, 0\rangle) = \langle 1, 0\rangle$, $h(\langle 0. 1\rangle) = \langle 1, 1\rangle$. It is easy to check that h is an automorphism of $G(+)$ and $hf = \tau h$. □

13.4. Lemma. *Let F be a finite field, $|F| = p^n$. For all $a, x \in F$ put $\pi_a(x) = ax$. Then:*

(i) *If $a \neq 0, 1$ then π_a is a complete automorphism of $F(+)$. In this case, π_a is simple iff a generates F as a ring.*

(ii) *If $a, b \neq 0, 1$ and $b = a^{p^m}$ for some $m \geqq 0$ then π_a and π_b are equivalent.*

(iii) *If $a, b \neq 0, 1$ are such that π_a is simple then π_a is equivalent to π_b iff $b = a^{p^m}$ for some $0 \leqq m \leqq n - 1$.*

(iv) *If f is a simple complete automorphism of $F(+)$ then there is $a \in F$ such that $a \neq 0, 1$, a is a generator of F as a ring and f is equivalent to π_a.*

Proof. The assertions (i) and (ii) are easy.

(iii) Suppose that $h\pi_a = \pi_b h$ for some automorphism h of $F(+)$ and put $k = \pi_{h(1)^{-1}} h$. Then $k\,\pi_a(x) = k(ax) = h(1)^{-1}\, h(ax) = h(1)^{-1}\, b\, h(x) = b\, h(1)^{-1} .$ $. h(x) = b\, k(x) = \pi_b\, k(x)$ and $k(a) = k(a \,.\, 1) = b\, k(1) = b$. Hence $k(ax) = k(a) .$ $. k(x)$. Denote by S the set of all $z \in F$ with $k(zx) = k(z)\, k(x)$ for every $x \in F$. Then $a \in S$, S is a subring of F, hence $S = F$ and k is an automorphism of the field F. Thus $b = k(a) = a^{p^m}$ for some $0 \leqq m \leqq n - 1$.

(iv) Let R be the subring of the endomorphism ring of $F(+)$ generated by f. Then R is commutative and the group $F(+)$ can be viewed as an R-module. Since f is simple, this R-module is simple. In particular, there is a maximal ideal I of R and a module isomorphism of R/I onto $F(+)$ inducing on $F(+)$ the structure of a field. Denote this field by $F(+, \circ)$. Obviously, there is $a \in F(+, \circ)$ such that $f(x) = a \circ x$ for every $x \in F$. Further, there is an isomorphism h of the field $F(+, \circ)$ onto the field F. Now $hf = \pi_{h(a)} h$ and f is equivalent to $\pi_{h(a)}$. □

13.5. Lemma. *Let $F(4) = \{0, 1, a, a^2\}$ be a four-element field. Then $x \to ax$ is up to equivalence the only complete automorphism of $F(4)(+)$.*

Proof. Let f be a complete automorphism of $F(4)(+)$. Suppose that $f(K) \subseteq K$ for a subgroup $K(+)$. Then $f \mid K$ is a complete automorphism of $K(+)$ and by 13.1 either $K = 0$ or $K = F(4)$. Thus f is simple and we can use 13.4. □

13.6. Lemma. *Let $F(8) = \{0, 1, a, a^2, a^3, a^4, a^5, a^6\}$ be an eight-element field. Then $x \to ax$ and $x \to a^3x$ are up to equivalence the only complete automorphisms of $F(8)(+)$. Moreover, these automorphisms are not equivalent.*

Proof. Let f be a complete automorphism of $F(8)(+)$. Suppose that $f(K) \subseteq K$ for a subgroup $K(+) \neq 0, F(8)$. By 13.1, $|K| = 4$. If $x \notin K$ then $f(x) \notin K$, and so $x - f(x) \in K$, since $F(8)(+)/K$ is a two-element group. Thus $\bar{f}(x) = x - f(x) \in K$ for every $x \in F(8)$, a contradiction. Hence f is simple and the rest is clear from 13.4. □

13.7. Lemma. *Let $F(9) = \{0, 1, a, a^2, a^3, a^4, a^5, a^6, a^7\}$ be a nine-element field. Then $x \to ax$, $x \to a^2x$ and $x \to a^5x$ are up to equivalence the only simple complete automorphisms of $F(9)(+)$. Moreover, these automorphisms are pairwise non-equivalent.*

Proof. Apply 13.4. □

In the following lemma, let $G(+) = G(3) \times G(3)$ and define an automorphism σ of $G(+)$ by $\sigma(\langle x, y\rangle) = \langle 2x + y, 2y\rangle = \langle y - x, y\rangle$.

13.8. Lemma. *ε_G and σ are up to equivalence the only non-simple complete automorphisms of $G(+) = G(3) \times G(3)$. Moreover, these two automorphisms are not equivalent.*

Proof. Let f be a non-simple complete automorphism of $G(+)$. There is a subgroup $K(+)$ of $G(+)$ such that $|K| = 3$ and $f(K) \subseteq K$. Let $0 \neq a \in K$ and $b \in G$ be such that $\{a, b\}$ is a basis of $G(+)$. Since $f(a) \in K$ and $f(a) \neq 0$, $a, f(a) = 2a = -a$. Further, $f(b) = \lambda a + \varrho b$ for some $\lambda, \varrho \in \{0, 1, 2\}$. If $\varrho = 0$ then f is not an automorphism, a contradiction. If $\varrho = 1$ then $f(-\lambda a + b) = \lambda a + \lambda a + b = -\lambda a + b$, a contradiction. Therefore $\varrho = 2$. If $\lambda = 0$ then $f(b) = -b$ and so $f = \varepsilon_G$. Let $\lambda = 1$. There is an automorphism h of $G(+)$ with $h(a) = \langle 0, 1\rangle$ and $h(b) = \langle 1, 0\rangle$. Now $hf(a) = -h(a) = \langle -1, 0\rangle = \sigma h(a)$, $hf(b) = \langle 1, -1\rangle = \sigma h(b)$ and f, σ are equivalent. Finally, let $\lambda = 2$. There is an automorphism k of $G(+)$ with $k(a) = \langle -1, 0\rangle$, $k(b) = \langle 0, 1\rangle$. Then $kf = \sigma k$ and we are through. □

Now, we shall define 45 distributive quasigroups $M(1), \ldots, M(45)$ as follows (the operation will be denoted by $\circ$): $M(1) = G(1)$. The underlying set of $M(2)$ is that of $G(3)$ and $x \circ y = -x - y = 2x + 2y$. The underlying set of $M(3)$ is that of $F(4)$ and $x \circ y = ax + (1 - a)y$ (see 13.5). The underlying set of $M(4)$, $M(5)$, $M(6)$ is that of $G(5)$ and $x \circ y = 2x + 4y$, $x \circ y = 3x + 3y$, $x \circ y = 4x + 2y$, respectively. The underlying set of $M(7)$, $M(8)$, $M(9)$, $M(10)$, $M(11)$ is that of $G(7)$ and $x \circ y = 2x + 6y$, $x \circ y = 3x + 5y$, $x \circ y = 4x + 4y$, $x \circ y = 5x + 3y$, $x \circ y = 6x + 2y$, respectively. The underlying set of $M(12)$ and $M(13)$ is that of $F(8)$ and $x \circ y = ax + (1 - a)y$, $x \circ y = a^3x + (1 - a^3)y$, respectively (see 13.6). The underlying set of $M(14)$, $M(15)$ and $M(16)$ is that of $G(9)$ and $x \circ y = 2x + 8y$, $x \circ y = 5x + 5y$, $x \circ y = 8x + 2y$, respectively. The underlying set of $M(17)$, $M(18)$ and $M(19)$ is that of $F(9)$ and $x \circ y = ax + (1 - a)y$, $x \circ y = a^2x + (1 - a^2)y$, $x \circ y = a^5x + (1 - a^5)y$, respectively (see 13.7). The underlying set of $M(20)$ and $M(21)$ is that of $G(3) \times G(3)$ and $x \circ y = -x - y = 2x + 2y$, $x \circ y = \sigma(x) +$

$+ y - \sigma(y)$, respectively (see 13.8; in fact, $M(20)$ is isomorphic to $M(2) \times M(2)$). The underlying set of $M(22)$, $M(23)$, $M(24)$, $M(25)$, $M(26)$, $M(27)$, $M(28)$, $M(29)$ and $M(30)$ is that of $G(11)$ and $x \circ y = 2x + 10y$, $x \circ y = 3x + 9y$, $x \circ y = 4x + 8y$, $x \circ y = 5x + 7y$, $x \circ y = 6x + 6y$, $x \circ y = 7x + 5y$, $x \circ y = 8x + 4y$, $x \circ y = 9x + 3y$, $x \circ y = 10x + 2y$, respectively. The underlying set of $M(31)$ is that of $G(2) \times G(6)$ and $x \circ y = \tau(x) + y - \tau(y)$ (see 13.3). The underlying set of $M(32)$, $M(33)$, $M(34)$, $M(35)$, $M(36)$, $M(37)$, $M(38)$, $M(39)$, $M(40)$, $M(41)$, $M(42)$ is that of $G(13)$ and $x \circ y = 2x + 12y$, $x \circ y = 3x + 11y$, $x \circ y = 4x + 10y$, $x \circ y = 5x + 9y$, $x \circ y = 6x + 8y$, $x \circ y = 7x + 7y$, $x \circ y = 8x + 6y$, $x \circ y = 9x + 5y$, $x \circ y = 10x + 4y$, $x \circ y = 11x + 3y$, $x \circ y = 12x + 2y$, respectively. Finally, the underlying set of $M(43)$, $M(44)$ and $M(45)$ is that of $G(15)$ and $x \circ y = 2x + 14y$, $x \circ y = 8x + 8y$ and $x \circ y = 14x + 2y$, respectively.

13.9. Theorem. *The quasigroups $M(1), \ldots, M(45)$ are up to isomorphism the only distributive quasigroups of order at most* 15. *Moreover, these quasigroups are pairwise non-isomorphic.*

Proof. Apply 12.1, 12.3, 13.1, 13.2, 13.3, 13.5, 13.6, 13.7 and 13.8. □

13.10. Corollary. *The quasigroups $M(1)$, $M(2)$, $M(5)$, $M(9)$, $M(15)$, $M(20)$, $M(26)$, $M(37)$ and $M(44)$ are up to isomorphism the only commutative distributive quasigroups of order at most* 15. □

13.11. Remark. In the following table, $q(n)$ and $p(n)$ denote the number of isomorphism classes of distributive quasigroups and commutative distributive quasigroups, respectively, of order n:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$q(n)$	1	0	1	1	3	0	5	2	8	0	9	1	11	0	3
$p(n)$	1	0	1	0	1	0	1	0	2	0	1	0	1	0	1

It seems that all these quasigroups are already known (see e.g. [11] for some of them), however, the authors were not able to find explicitly their description in the literature and hence they decided to include it in the present paper.

14. NON-MEDIAL COMMUTATIVE DISTRIBUTIVE GROUPOIDS OF ORDERS 81 AND 82

Let G be a groupoid and A, $B \subseteq G$ two disjoint subsets of G such that $A \cup B = G$, A is either empty or a subgroupoid of G and B is either empty or an ideal of G. Let f be an endomorphism of B ($f = \emptyset$ if $B = \emptyset$) and α an element not belonging to G. We define a groupoid $H = G(A, B, f, \alpha)$ as follows: $H = G \cup \{\alpha\}$, G is a sub-

groupoid of H, $\alpha\alpha = \alpha x = x\alpha = \alpha$ for every $x \in A$ and $\alpha y = y\alpha = f(y)$ for every $y \in B$.

14.1. Lemma. *If G is a commutative distributive idempotent groupoid then $G(A, B, f, \alpha)$ is a commutative distributive idempotent groupoid iff the following three conditions are satisfied:*

(a) $xf(y) = f(xy) = f^2(y)$ *for all* $x \in A$, $y \in B$.
(b) $f(y) = xy \,.\, f(y)$ *for all* $x \in A$, $y \in B$.
(c) $xf(y) = f(x) \,.\, xy$ *for all* $x, y \in B$.

Proof. Straightforward. □

14.2. Proposition. *Let H be a non-trivial groupoid, $\alpha \in H$ and $G = H \setminus \{\alpha\}$. The following conditions are equivalent:*

(i) *H is a commutative distributive idempotent groupoid and G is a subgroupoid of H.*
(ii) *G is a subgroupoid of H, G is a commutative distributive idempotent groupoid and there are two disjoint subsets A, B of G and a transformation f of B such that $G = A \cup B$, A is either empty or a subgroupoid of G, B is either empty or an ideal of G, f is an endomorphism of B satisfying conditions* (a), (b), (c) *from* 14.1 *and $H = G(A, B, f, \alpha)$.*

Proof. (i) $\Rightarrow$ (ii). Put $A = \{x \in G \mid \alpha x = \alpha\}$, $B = \{x \in G \mid \alpha x \neq \alpha\}$ and $f(x) = \alpha x$ for every $x \in B$. If $x \in A$, $y \in B$ then $\alpha \,.\, xy = x\alpha \,.\, xy = x \,.\, \alpha y \neq \alpha$. Further, $\alpha \neq f(xy) = \alpha \,.\, xy = \alpha x \,.\, \alpha y = \alpha \,.\, \alpha y$. Hence $\alpha y = f(y) \in B$ and $f(xy) = f^2(y)$. The rest is easy.

(ii) $\Rightarrow$ (i). Apply 14.1. □

14.3. Lemma. *Let Q be a finite commutative distributive quasigroup and f a transformation of Q. The following conditions are equivalent:*

(i) *f is an endomorphism of Q and $xf(y) = f(x) \,.\, xy$ for all $x, y \in Q$.*
(ii) *There is $a \in Q$ such that $f(x) = ax$ for every $x \in Q$.*

Proof. (i) $\Rightarrow$ (ii). For all $x, y \in Q$, let $L_x(y) = xy$. Since Q is a finite quasigroup, there is $n \geqq 1$ such that $L_x^{n+1} = \iota_Q$ for every $x \in Q$. Hence for all $x, y \in Q$, $f(y) = L_x^{n+1} f(y) = L_x^n(x f(y)) = L_x^n(f(x) \,.\, xy) = L_x^n f(x) \,.\, y = L_y L_x^n f(x)$ and $L_y^n f(y) = L_x^n f(x)$. Let $b \in Q$ be arbitrary and $a = L_b^n f(b)$. Then $f(a) = f(L_b^n f(b)) = L_{f(b)}^n f^2(b) = L_b^n f(b) = a$ and $af(x) = f(a) \,.\, ax = a \,.\, ax$ for every $x \in Q$. Thus $f(x) = ax$.

(ii) $\Rightarrow$ (i). This is clear. □

14.4. Proposition. *$D(1)$ and $D(3)$ are up to isomorphism the only non-medial commutative distributive groupoids of order at most* 81.

Proof. Let G be a non-medial commutative distributive groupoid of the least cardinality. Then obviously G is idempotent and subdirectly irreducible. If G is a quasigroup then, by 12.4 and 12.5, $|G| = 81$ and G is isomorphic either to $D(1)$ or to $D(3)$. In the opposite case, with respect to 11.3, G contains a zero element 0 such that $H = G \setminus \{0\}$ is a non-medial commutative distributive quasigroup, a contradiction. □

Now we shall define four groupoids $D(7)$, $D(8)$, $D(9)$ and $D(10)$ as follows: Choose and fix three elements α, β, γ such that $\alpha \notin D(1) \cup D(3)$, $\beta \in D(1)$, $\gamma \in D(3)$. We put $D(7) = D(1)(D(1), \emptyset, \emptyset, \alpha)$ (i.e. $D(7) = D(1) \cup \{\alpha\}$, $D(1)$ is a subgroupoid of $D(7)$ and α is a zero of $D(7)$), $D(8) = D(3)(D(3), \emptyset, \emptyset, \alpha)$, $D(9) = D(1)(\emptyset, D(1), L_\beta, \alpha)$ (i.e. $D(9) = D(1) \cup \{\alpha\}$, $D(1)$ is a subgroupoid of $D(9)$, $\alpha\alpha = \alpha$ and $x\alpha = \alpha x = \beta x$ for every $x \in D(1)$) and $D(10) = D(3)(\emptyset, D(3), L_\gamma, \alpha)$.

14.5. Proposition. *$D(7)$, $D(8)$, $D(9)$ and $D(10)$ are up to isomorphism the only non-medial commutative distributive idempotent groupoids of order 82. Moreover, these groupoids are pairwise non-isomorphic.*

Proof. Let G be a non-medial commutative distributive idempotent groupoid of order 82. If G contains no proper ideal then G is a quasigroup by 11.5. However, 82 is no tdivisible by 81 and so G is medial, a contradiction (in fact, there is no distributive quasigroup of order 82). Hence, let I be a proper ideal of G. With respect to 11.4, we can assume that I is prime. First, let the factorgroupoid G/I be not medial. Then $|G/I| \geqq 81$ and so $|I| \leqq 2$. If $|I| = 2$ then $|G/I| = 81$. However, G/I contains a zero and G/I is not medial, a contradiction with 14.4. Therefore $I = \{0\}$ for some $0 \in G$ and 0 is a zero of G. Put $K = G \setminus \{0\}$. Since I is prime, K is a subgroupoid of G and by 14.4 K is isomorphic to one of $D(1)$, $D(3)$. Now it is easy to see that G is isomorphic either to $D(7)$ or to $D(8)$. Further, assume that G/I is medial. By 11.2, I is not medial and so $|I| \geqq 81$. Hence $|I| = 81$ and $G \setminus I = \{a\}$ for some $a \in G$. By 14.4, I is isomorphic either to $D(1)$ or to $D(3)$. Suppose that $I = D(1)$, the other case being similar. Since $aI \subseteq I$ and I contains no proper ideal, by 14.2 there is an endomorphism f of I such that $xf(y) = f(x) \,.\, xy$ for all $x, y \in I$ and $G = I(\emptyset, I, f, a)$. By 14.3, there is $b \in I$ with $f(x) = bx$ for every $x \in I$. Further, $b = \beta c$ for some $c \in I$ and L_c is an automorphism of I. Define $g : D(9) \to G$ by $g(x) = cx$ for every $x \in I$ and $g(\alpha) = a$. It is easy to see that g is an isomorphism. Finally, $D(7)$, $D(8)$, $D(9)$ and $D(10)$ are non-medial commutative distributive idempotent groupoids by 14.2 and these groupoids are clearly pair-wise non-isomorphic, since $D(7)$, $D(8)$ contain zero elements, $D(9)$ and $D(10)$ do not, and α is the only element of $D(9)$, $D(10)$ with L_α surjective. □

Define two groupoids $D(11)$ and $D(12)$ as follows: $D(11) = D(1) \cup \{\alpha\}$, $D(1)$ is a subgroupoid of $D(11)$ and $\alpha\alpha = \beta$, $\alpha x = x\alpha = \beta x$ for every $x \in D(1)$. $D(12) = D(3) \cup \{\alpha\}$, $D(3)$ is a subgroupoid of $D(12)$ and $\alpha\alpha = \gamma$, $\alpha x = x\alpha = \gamma x$ for every $x \in D(3)$.

14.6. Proposition. *$D(11)$ and $D(12)$ are up to isomorphism the only non-medial non-idempotent commutative distributive groupoids of order 82. Moreover, these two groupoids are not isomorphic.*

Proof. Let G be a commutative distributive groupoid such that G is not medial, not idempotent and $|G| = 82$. According to 11.1, Id G is not medial, hence $|\mathrm{Id}\ G| = 81$ and $G \setminus \mathrm{Id}\ G = \{a\}$ for some $a \in G$. By 14.4, Id G is isomorphic either to $D(1)$ or to $D(3)$. Further, $b = aa \in \mathrm{Id}\ G$ and $ax = ax \,.\, ax = aa \,.\, x = bx$ for every $x \in \mathrm{Id}\ G$. Finally, there is an isomorphism f of $D(1)$ (or $D(3)$) onto Id G such that $f(\beta) = b$ (or $f(\gamma) = b$). The rest is clear. □

14.7. Theorem. (i) *Every non-medial commutative distributive groupoid contains at least 81 elements.*

(ii) *$D(1)$ and $D(3)$ are up to isomorphism the only non-medial commutative distributive groupoids of order 81. Moreover, these two groupoids are not isomorphic.*

(iii) *$D(7)$, $D(8)$, $D(9)$, $D(10)$, $D(11)$ and $D(12)$ are up to isomorphism the only non-medial commutative distributive groupoids of order 82. Moreover, these six groupoids are pairwise non-isomorphic.*

Proof. Apply 14.4, 14.5 and 14.6. □

14.8. Remark. Obviously, every semilattice (i.e. a commutative idempotent semigroup) is a medial commutative distributive idempotent groupoid. Denote by $s(n)$ the number of isomorphism classes of semilattices of order n. For a finite semilattice S, we can define two semilattices $\bar{S}$ and $\hat{S}$ of order $|S| + 1$ as follows: Choose an element α not belonging to S. The underlying sets of $\bar{S}$ and $\hat{S}$ are equal to $S \cup \{\alpha\}$, S is a subgroupoid of both $\bar{S}$ and $\hat{S}$ and $\alpha\alpha = \alpha$. Further, $\alpha x = x\alpha = \alpha$ for every $x \in S$ in $\bar{S}$ and $\alpha x = x\alpha = 0$ in $\hat{S}$, where 0 is the zero element of S (it exists, since S is finite). Using this construction, it is easy to show that $s(n) \geqq 2^{n-2}$ for $n \geqq 2$. In particular, we have $s(81) \geqq 2^{79} > 6 \,.\, 10^{23}$.

References

[1] *G. Bol:* Gewebe und Gruppen, Math. Ann. *114* (1937), 414—431.

[2] *R. H. Bruck:* Contributions to the theory of loops, Trans. Amer. Math. Soc. *60* (1946), 245—354.

[3] *R. H. Bruck:* "A Survey of Binary Systems", Springer Verlag, Berlin—Heidelberg—New York, 1966.

[4] *O. Chein:* "Moufang Loops of Small Orders", Mem. Amer. Math. Soc. 197, Providence R. I., 1978.

[5] *T. Evans:* Identities and relations in commutative Moufang loops, J. Algebra *31* (1974), 508—513.

[6] *J. Ježek* and *T. Kepka:* The lattice of varieties of commutative abelian distributive groupoids, Algebra Universalis *5* (1975), 225—237.
[7] *J. Ježek, T. Kepka* and *P. Němec:* Distributive groupoids (to appear).
[8] *T. Kepka:* Commutative distributive groupoids, Acta Univ. Carolinae Math. Phys. *19*, 2 (1978), 45—58.
[9] *T. Kepka* and *P. Němec:* Distributive groupoids and the finite basis property, J. Algebra *70* (1981), 229—237.
[10] *S. Klossek:* "Kommutative Spiegelungsräume", Mitteilungen Math. Sem. Giessen, Heft 117, Giessen, 1975.
[11] *J.-P. Soublin:* Etude algébrique de la notion de moyenne, J. Math. Pures Appl. *50* (1971), 53—264.

Authors' address: 186 00 Praha 8, Sokolovská 83, ČSSR (Matematicko-fyzikální fakulta UK).