Europ. J. Combinatorics (1984) 5, 193–196

3-Abelian Groups and Commutative Moufang Loops

LUCIEN BÉNÉTEAU

It has been recently shown there exist only two non-abelian commutative Moufang loops of order $81 = 3^4$, and that the number v_s of pairwise non-isomorphic exponent 3 commutative Moufang loops (resp. distributive symmetric quasigroups) whose 3-order is s satisfies $v_4 = 2 = v_5$ and $v_6 = 4$. The object of this note is to establish a connection between these results and some theorems of classification of 3-abelian groups [i.e. the groups whose law satisfies the identical relation $x^3y^3 = (xy)^3$]. We use techniques introduced by Bruck so as to obtain group-theoretical descriptions of the considered quasigroups.

A commutative Moufang loop (CML) is a loop satisfying the two identities:

$$xy \cdot zx = (x \cdot yz)x, \; xy = yx,$$

or equivalently, the single identity $x^2(yz) = (xy)(xz)$. Such a loop is said to be non-abelian when it is not an abelian group, namely when the associativity is not obeyed. Let x, y, z be elements of such a loop E. The *associator* of x, y, z, denoted by (x, y, z), is defined by $xy \cdot z = (x \cdot yz) \cdot (x, y, z)$. The (associative) *centre* of E is the set $Z(E)$ of the zs satisfying $(x, y, z) = 1$ for any x and y. When $x^3 = 1$ for any x in E, one says that E is an exponent 3 CML; in such a loop the binary law $x \circ y = (xy)^{-1}$ defines a structure of *distributive symmetric quasigroup* (DSQ), namely $(\circ)$ is self-distributive $[x \circ (y \circ z) = (x \circ y) \circ (x \circ z)]$ and any equality of the form $x \circ y = z$ is invariant under permutation of x, y, z. Any DSQ$(E, \circ)$ arises in this way from an exponent 3 CML which is essentially unique, and that one may recover by setting $xy = u \circ (x \circ y)$ where u is any fixed element of E.

We refer the reader to [1, 2, 4, 7, 9, 12, 16] for a detailed discussion of CMLs and for their connection with the DSQs in the exponent 3 case. Any non-abelian finite CML (resp. exponent 3 CML) has an order of the form $3^s m$ (resp. 3^s) where $s \geq 4$ (see [1, 4, 6]). There are (up to isomorphism) only two non-abelian CMLs of order $3^4 = 81$ [2] [13], and only five non-abelian exponent 3 CMLs of order $\leq 3^6 = 729$ (see [3] and [5]). More precisely the number v_s of pairwise non-isomorphic exponent 3 CMLs (resp. DSQs) of order 3^s has been determined for $s < 7$, namely:

$v_s = 1$ for $s \leq 3$; $v_4 = 2$ (Marshall Hall Jr [11]),

$v_5 = 2$ (the author and Kepka independently [2, 13, 4]),

$v_6 = 4$ (the author [4] and [5]; see [3] for the initial formulation of the result in terms of Hall triple systems):

These statements are to be compared with some group-theoretical facts. Let us say that a group G is 3-*abelian* when $(xy)^3 = x^3y^3$ identically. One may readily verify that, in such a group G, any cube x^3 lies in the centre $Z(G)$ (see [8] for a more general statement), and therefore *if G has finite order $3^s m$ where m is prime to 3, then G is a direct product of a (3-abelian) subgroup of order 3^s by an abelian subgroup of order m* [observe that if $a3^s + bm = 1$, any x may be written $x = yz$ where $y = x^{bm}$ belongs to $H = \{y' | O(y') \text{ is a } 3\text{-power}\}$ and $z = x^{a3^s}$ belongs to $A = \{z' | O(z') \text{ divides } m\} \subset Z(G)$]. If G is nonabelian then $s \geq 3$. Lastly there are up to isomorphism exactly two non-abelian groups of order $3^3 = 27$, and only five non-abelian exponent 3 groups of order $\leq 3^5 = 243$. One may readily

0195-6698/84/030193+04 $02.00/0

check that the number u_s of pairwise non-isomorphic exponent 3 groups of order 3^s is 1 for $s \leqslant 2$ and satisfies: $u_3 = 2 = u_4$ and $u_5 = 4$. The fact that $v_{s+1} = u_s$, for $s \leqslant 5$, is not a fortuitous coincidence. The following statement is mainly due to Bruck [6]. Designate by $\mathbb{Z}_3 = \{-1, 0, 1\}$ the 3-element field.

THEOREM. *If G is a 3-abelian group $\neq \{1\}$, (a) the binary law $x * y = x^{-1} y x^2$ turns the underlying set G into a CML (denoted by G_*). (b) the set-product $\mathbb{Z}_3 \times G = \{(p, x) \mid p \in \mathbb{Z}_3, x \in G\}$, equipped with the law:*

$$(p, x) \tilde{*} (q, y) = (p + q, z_{q-p}(x, y))$$

where $z_{-1}(x, y) = yx$, $z_0(x, y) = x^{-1} y x^2$ and $z_1(x, y) = xy$ becomes a CML $\tilde{G}_*$ which contains $\{0\} \times G \simeq G_*$ as a maximal subloop of index 3. If G is non-abelian the associative centre of $\tilde{G}_*$ consists of the elements of the form $(0, z)$ where z ranges in $Z(G)$. If G is abelian then $\tilde{G}_* \simeq \mathbb{Z}_3 \times G$. (c) When G is of exponent 3^t, so are the loops G_* and $\tilde{G}_*$.

PROOF. We have already remarked that in a 3-abelian group G the mapping $x \mapsto x^3$ is an endomorphism from G into its centre. It then follows from [6, chapter II, theorems 8D, 8H] that G_* and $\tilde{G}_*$ are CMLs. A direct verification yields the centre. G_* may be identified with an index 3 normal subloop of $\tilde{G}_*$ since

$$\{1\} \mapsto G_* \overset{i}{\mapsto} \tilde{G}_* = (\mathbb{Z}_3 \times G, \tilde{*}) \overset{f}{\mapsto} (\mathbb{Z}_3, +) \mapsto \{0\}$$

is an exact sequence with $i(x) = (0, x)$ and $f((p, x)) = p$. If $y = x^n$ in the group G, then $x^{-1}\, y\, x^2 = x^{n+1} = xy = yx$, so that the nth power of x in G_* is x^n. Also for any p in $\mathbb{Z}_3$

$$(p, x) \tilde{*} (np, x^n) = ((n+1)p, x^{n+1});$$

one may thus show by induction on n that the nth power of (p, x) with respect to $\tilde{*}$ is (np, x^n). Now, since the identity element of G_* (resp. $\tilde{G}_*$) is obviously 1_G (resp. $(0, 1_G) =$ e), if x is an element of order $3^t \geqslant 3$ in the group G, then x is an element of order 3^t in the loop G_* and (p, x) is also an element of order 3^t in the loop $\tilde{G}_*$.

COROLLARY. *If G is an exponent 3 group,* (a) *the law $x \circ y = xy^2x$ turns the set G into a DSQ, denoted by $G_\circ$.* (b) *$\tilde{G}_* = (\mathbb{Z}_3 \times G, \tilde{*})$ is an exponent 3 CML,* (c) *The same set $\mathbb{Z}_3 \times G$ may be provided with a structure of DSQ by setting:*

$$(p, x) \tilde{\circ} (q, y) = (-p - q, t_{q-p}(x, y)),$$

where $t_{-1}(x, y) = x^2 y^2$, $t_0(x, y) = xy^2x$ and $t_1(x, y) = y^2 x^2$; we shall denote by $\tilde{G}_\circ$ the so-constructed DSQ.

PROOF. The inverse of $x * y = x^{-1} y x^2$ in the loop G_* is the same as the inverse with respect to the group multiplication, namely $(x^{-1} y x^2)^{-1} = x^{-2} y^{-1} x$ which may be written xy^2x in case G has exponent 3. Similarly the inverse of any element (r, z) of $\tilde{G}_*$ is $(-r, z^{-1})$. Now $(z_i(x, y))^{-1} = t_i(x, y)$. So $(\circ)$ and $\tilde{\circ})$ are the canonical laws of DSQ associated with the exponent 3 CML G_* and $\tilde{G}_*$.

In the light of the two preceding statements, we may give group-theoretical descriptions of the small quasigroups whose classification was precedingly recalled.

PROPOSITION. *If U and V designate the two non-abelian groups of order 27, then $\tilde{U}_*$ and $\tilde{V}_*$ are the two non-abelian CMLs of order 81.*

PROOF. One of the two considered groups, say U, is of exponent 3, and the other one is of exponent 9. Therefore the corresponding loops $\tilde{U}_*$ and $\tilde{V}_*$ are also of exponent 3 and 9 respectively, so that they are not isomorphic. It remains to observe that both $\tilde{U}_*$ and $\tilde{V}_*$ are non-associative. This derives from the fact that the initial groups are non-commutative.

The correspondence: $\Phi_*(G) = \tilde{G}_*$ (resp. $\Phi_\circ(G) = \tilde{G}_\circ$) associates an exponent 3 CML $\tilde{G}$ (resp. a DSQ $\tilde{G}_\circ$) of order 3^{s+1} to any exponent 3 group G of order 3^s.

THEOREM. *Φ_* (resp. $\Phi_\circ$) is one-to-one from the class of the exponent 3 groups of order $\leqslant 3^5$ onto the class of the exponent 3 CMLs (resp. the DSQs) of order 3^s with $1 \leqslant s \leqslant 6$.*

PROOF. Apart from the 6 elementary abelian 3-groups of order $\leqslant 3^5$ (with $\{0\}$ included), there are only five exponent 3 groups of order $\leqslant 3^5$: only one of order 3^3, say U; only one of order 3^4 (the direct product $U \times \mathbb{Z}_3$ necessarily); and exactly three of order 3^5 (again one reducible group $U \times \mathbb{Z}_3 \times \mathbb{Z}_3$ and two non reducible groups Π_3 and Π_4 which may be given the following presentations: Π_3 is the exponent 3 group on three generators e_1, e_2, e_3 subject to the only relation $(e_1, e_2) = 1$ (with $(x, y) = x^{-1}y^{-1}xy$ as usual), and Π_4 is the exponent 3 group on four generators e_1, e_2, e_3, e_4 subject to $(e_1, e_2) = (e_3, e_4)$ and $(e_i, e_j) = 1$ for any i, j such that $\{1, 2\} \neq \{i, j\} \neq \{3, 4\}$. One only need to prove that the three exponent 3 CMLs corresponding to $U \times \mathbb{Z}_3^2$, Π_3 and Π_4 are pairwise non-isomorphic. This may be accomplished by remarking that the orders of the centers of the considered CMLs are 27, 9 and 3, respectively, (the same as the orders of the centres of the initial groups). This completes the proof.

THEOREM. *There is only one exponent 3 group W on 3 generators of order 3^6, and $\tilde{W}_*$ is the unique exponent 3 CML on 4 generators of order 3^7.*

PROOF. The Burnside group $\mathbb{B}_3$ of exponent 3 on 3 generators e_1, e_2, e_3 is known to have order 3^7, and $(\mathbb{B}_3', \mathbb{B}_3) = \langle ((e_1, e_2), e_3) \rangle$ has order 3. In view of [4, p. 126] any exponent 3 group W of order 3^s with $s < 7$ is centrally nilpotent of class at most 2. If $s = 6$ and if moreover W can be generated by three elements, then $W = \mathbb{B}_3/(\mathbb{B}_3', \mathbb{B}_3)$ necessarily. Besides W needs to be irreducible and of central nilpotency class 2, so that $Z(W) = D(W) = \Phi(W)$ is a subgroup of index 3^3. Therefore the associative centre of the corresponding exponent 3 CML $\tilde{W}_*$ has index 3^4 [it is $\{0\} \times Z(W)$]. Again we have $Z(\tilde{W}_*) = D(\tilde{W}_*) = \Phi(\tilde{W}_*)$ because the so-constructed CML needs to have central nilpotency class 2 and to be irreducible. Consequently $\tilde{W}_*$ needs to be the unique 4-dimensional exponent 3 CML (the unicity follows from [3, 4]), and we are done.

As far as we are concerned v_s has not been yet determined for $s \geqslant 7$. But, despite the preceding statements, *it seems reasonable to conjecture that $v_{s+1} > u_s$ for any $s \geqslant 7$*. At the very least it seems that the exponent 3 CMLs of order 3^8 are more numerous than the exponent 3 groups of order 3^7: for instance there are four exponent 3 CMLs of order 3^8 on 4 generators while there is only one exponent 3 group of order 3^7 on 3 generators.... At any rate it must be recorded that Bruck's process $G \to \tilde{G}$ for obtaining exponent 3 CMLs from exponent 3 groups is not canonical: any CML of the form $\tilde{G}$ is centrally nilpotent of class bounded by 3 (as is the initial 3-abelian group; see [6, chapter II, Theorem 1A]) while Bruck himself established the existence of finite exponent 3 CMLs whose class is arbitrarily large [7]. It is also worth mentioning that an exponent 3 CML of class 4 whose order is minimum (3^{22}) was recently constructed by El Khouri [10].

I would like to thank the referees for suggestions improving the presentation of the present paper.

References

1. L. Bénéteau, Boucles de Moufang commutatives, d'exposant 3 et quasigroupes de Steiner distributifs, *C.R. Acad. Sc. Paris* **281** (1975), 75-76.
2. L. Bénéteau, Topics about Moufang Loops and Hall triple Systems, '*Simon Stevin*', **54**(2) (1980), 107-122.
3. L. Bénéteau, Une classe particulière de matroïdes parfaits Proc. Colloque franco-canadien de Combinatoire, Juin 1979, "Combinatorics 79", *Ann. Discrete Math.* **8** (1980), MS 921, 229-232.
4. L. Bénéteau, Contribution à l'étude des boucles de Moufang commutatives et des espaces apparentés (Algèbre, Combinatoire, Géométrie), Thèse d'Etat, Univ. de Provence, Marseille, France, 1981.
5. L. Bénéteau, Hall triple systems and related topics, Proceedings of the International Conference on Combinatorial Geometries and their Applications, (A. Barlotti, P. V. Ceccherini, G. Lallini, eds) *Ann. Discrete Math.* **18** (1983), 55-60.
6. R. H. Bruck, Contribution to the theory of loops, *Trans. Amer. Math. Soc.* **60** (1946), 245–354.
7. R. H. Bruck, *A Survey of Binary Systems*, Springer, Berlin, 1958; 2nd printing 1968.
8. R. H. Bruck, Some theorems on Moufang loops, *Math. Z.* **73** (1960), 59–78.
9. M. Deza, Finite commutative Moufang loops, related matroids, and association schemes, *Proc. West Coast Conf. on Combinatorics, Graph Theory and Computing, Humbolt St. Univ., Arcata, California*, 1979, pp. 3–15.
10. M. El Khouri, Ordre minimum des boucles de Moufang commutatives de classe 4, thèse de Spécialité, Univ. Paris VII, 1981.
11. M. Hall Jr, Automorphisms of Steiner triple systems, *IBM J. Res. Develop.* **4** (1960) 460–471.
12. M. Hall Jr, Group theory and block designs, *Proc. Internat. Conf. Theory of Groups, Australia Nat. Univ. Canberra*, Gordon and Breach, New York, 1967, pp. 115–144.
13. T. Kepka, Distributive Steiner quasigroups of order 3^5, *Comment. Math. Univers. Carolinae* **19**(2) (1978), 389-401.
14. T. Kepka and P. Nemec, Commutative Moufang loops and distributive groupoïds of small order, *Czechoslovak Math. J.* **106**(31) (1981), 633–669.
15. F. Levi and B. L. van der Waerden, Uber eine besondere Klasse von Gruppen, *Abh. Math. Sem. Hamsische Univ.* **9** (1933), 154–158.
16. Yu. I. Manin, *Cubic forms*; *Algebra, Geometry, Arithmetric*, North-Holland, Amsterdam, 1974.

Received 28 July 1983 and in revised form 20 October 1983

Lucien Bénéteau
Université Paul Satatier, U.E.R. Mathématiques,
118, route de Narbonne, 31062 Toulouse Cedex, France.