Quasigroups and Related Systems **8** (2001), 97 – 104

The abstract groups (3, 3 | 3, p), their subgroup structure, and their significance for Paige loops

Petr Vojtěchovský

Abstract

For most (and possibly all) non-associative finite simple Moufang loops, three generators of order 3 can be chosen so that each two of them generate a group isomorphic to $(3,3\,|\,3,p)$. The subgroup structure of $(3,3\,|\,3,p)$ depends on the solvability of a certain quadratic congruence, and it is described here in terms of generators.

1. Introduction

Moufang loops and, more generally, diassociative loops are usually an abundant source of two-generated groups. In the end, this is what diassociativity is all about: every two elements generate an associative subloop, i.e. a group. (We refer the reader not familiar with the theory of loops to [5].) This short paper emerged as an offshoot of our larger-scale program to fully describe the subloop structure of all non-associative finite simple Moufang loops, sometimes called *Paige loops*.

Let $M^*(q)$ denote the Paige loop constructed over $F = GF(q)$ as in [4]. That is, $M^*(q)$ consists of vector matrices

$$M = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix},$$

where $a,\ b \in F$, $\alpha,\ \beta \in F^3$, $\det M = ab - \alpha \cdot \beta = 1$, and where M is identified with $-M$. The multiplication in $M^*(q)$ coincides with the Zorn

2000 Mathematics Subject Classification: 20D30, 20N10
Keywords: non-associative finite simple Moufang loop, Paige loop, the abstract group $(3,\,3\mid 3,\,p)$, loop generator, quadratic congruence

matrix multiplication

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}\begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac+\alpha\cdot\delta & a\gamma+d\alpha-\beta\times\delta \\ c\beta+b\delta+\alpha\times\gamma & \beta\cdot\gamma+bd \end{pmatrix},$$

where $\alpha\cdot\beta$ (resp. $\alpha\times\beta$) is the standard dot product (resp. cross product).

We have shown in [6, Theorem 1.1] that every $M^*(q)$ is three-generated, and when $q\neq 9$ is odd or $q=2$ then the generators can be chosen as

$$g_1 = \begin{pmatrix} 1 & e_1 \\ 0 & 1 \end{pmatrix},\quad g_2 = \begin{pmatrix} 1 & e_2 \\ 0 & 1 \end{pmatrix},\quad g_3 = \begin{pmatrix} 0 & ue_3 \\ -u^{-1}e_3 & 1 \end{pmatrix}, \tag{1}$$

where u is a primitive element of F (cf. [6, Proposition 4.1]). In particular, note that g_1, g_2 and g_3 generate $M^*(p)$ for every prime p. We find it more convenient to use another set of generators.

Proposition 1. *Let $q\neq 9$ be an odd prime power or $q=2$. Then $M^*(q)$ is generated by three elements of order three.*

Proof. Let us introduce

$$\begin{aligned} g_4 = g_3g_1 &= \begin{pmatrix} 0 & (0,0,u) \\ (0,u,-u^{-1}) & 1 \end{pmatrix}, \\ g_5 = g_3g_2 &= \begin{pmatrix} 0 & (0,0,u) \\ (-u,0,-u^{-1}) & 1 \end{pmatrix}. \end{aligned}$$

It follows from (1) that $M^*(q)$ is generated by g_3, g_4, and g_5. One easily verifies that these elements are of order 3. □

The groups $\langle g_3, g_4\rangle$, $\langle g_3, g_5\rangle$ and $\langle g_4, g_5\rangle$ play therefore a prominent role in the lattice of subloops of $M^*(q)$. As we prove in Section 3, each of them is isomorphic to the group $(3, 3 \mid 3, p)$, defined below.

2. The abstract groups (3, 3 | 3, p)

The two-generated abstract groups $(l, m \mid n, k)$ defined by presentations

$$(l, m \mid n, k) = \langle x, y \mid x^l = y^m = (xy)^n = (x^{-1}y)^k\rangle \tag{2}$$

were first studied by Edington [3], for some small values of l, m, n and k. The notation we use was devised by Coxeter [1] and Moser [2], and has a deeper meaning that we will not discuss here. From now on, we will always refer to presentation (2) when speaking about $(l,\, m \mid n,\, k)$.

The starting point for our discussion is Theorem 2, due to Edington [3, Theorem IV and pp. 208–210]. (Notice that there is a typo concerning the order of $(3,\, 3 \mid 3,\, n)$, and a misprint claiming that $(3,\, 3 \mid 3,\, 3)$ is isomorphic to A_4.). For the convenience of the reader, we give a short, contemporary proof.

Theorem 2 (Edington). *The group $G = (3,\, 3 \mid 3,\, n)$ exists for every $n \geqslant 1$, is of order $3n^2$, and is non-abelian when $n > 1$. It contains a normal subgroup $H = \langle x^2y,\, xy^2\rangle \cong C_n \times C_n$. In particular, $G \cong C_3$ when $n = 1$, $G \cong A_4$ when $n = 2$, and G is the unique non-abelian group of order 27 and exponent 3 when $n = 3$.*

Proof. Verify that $(3,\, 3 \mid 3,\, 1)$ is isomorphic to C_3. Let $n > 1$. Since $x(x^2y)x^{-1} = yx^{-1} = y(x^2y)y^{-1} \in H$, and $x^{-1}(xy^2)x = y^2x = y^{-1}(xy^2)y \in H$, the subgroup H is normal in G. It is an abelian group of order at most n^2 since $x^2y \cdot xy^2 = x(xy)^2y = x(xy)^{-1}y = xy^2 \cdot x^2y$. Clearly, $G/H \cong C_3$ (enumeration of cosets works fine), and hence $|G| = 3|H| \leqslant 3n^2$.

Let $N = \langle a\rangle \times \langle b\rangle \cong C_n \times C_n$, and $K = \langle f\rangle \leqslant \mathrm{Aut}(N)$, where f is defined by $f(a) = a^{-1}b$, $f(b) = a^{-1}$. Let E be the semidirect product of N and K via the natural action of K on N. We claim that E is non-abelian, and isomorphic to $(3,\, 3 \mid 3,\, n)$ with generators $x = (1,\, f)$ and $y = (a,\, f)$. We have $(a,\, f)^2 = (af(a),\, f^2) = (b,\, f^2)$, $(b,\, f^2)(1,\, f) = (b,\, \mathrm{id})$, and $(1,\, f)(b,\, f^2) = (a^{-1},\, \mathrm{id})$. Thus E is non-abelian, and generated by $(1,\, f)$, $(a,\, f)$. A routine computation shows that $(1,\, f)^3 = (a,\, f)^3 = ((1,\, f)(a,\, f))^3 = ((1,\, f)^{-1}(a,\, f))^n = 1$.

The group E proves that $|G| = 3|H| = 3n^2$. In particular, $H \cong C_n \times C_n$. □

We would like to give a detailed description of the lattice of subgroups of $(3,\, 3 \mid 3,\, p)$ in terms of generators x and y. From a group-theoretical point of view, the groups are rather boring, nevertheless, the lattice can be nicely visualized. The cases $p = 2$ and $p = 3$ cause troubles, and *we exclude them from our discussion for the time being.*

Lemma 3. *Let G and H be defined as before. Then H is the Sylow p-subgroup of G, and contains $p+1$ subgroups $H(i) = \langle h(i)\rangle$, for $0 \leqslant i < p$, or $p = \infty$, all isomorphic to C_p. We can take*

$$h(i) = x^2y(xy^2)^i, \ \textit{for}\ \ 0 \leqslant i < p \ \ \textit{and}\ \ h(\infty) = xy^2.$$

There are p^2 Sylow 3-subgroups $G(k, l) = \langle g(k, l)\rangle$, for $0 \leqslant k,\ l < p$, all isomorphic to C_3. We can take

$$g(k, l) = (x^2y)^{-k}(xy^2)^{-l}x(x^2y)^k(xy^2)^l.$$

Proof. The subgroup structure of H is obvious. Every element of $G \setminus H$ has order 3, so there are p^2 Sylow 3-subgroups of order 3 in G. The subgroup H acts transitively on the set of Sylow 3-subgroups. (By Sylow Theorems, G acts transitively on the copies of C_3. As $|G| = 3p^2$, the stabilizer of each C_3 under this action is isomorphic to C_3. Since p and 3 are relatively prime, no element of H can be found in any stabilizer.) This shows that our list of Sylow 3-subgroups is without repetitions, thus complete. □

For certain values of p (see below), there are no other subgroups in G. For the remaining values of p, there are additional subgroups of order $3p$.

If $K \leqslant G$ has order $3p$, it contains a unique normal subgroup of order p, say $L \leqslant H$. Since L is normalized by both K and H, it is normal in G. Then G/L is a non-abelian group of order $3p$, and has therefore p subgroups of order 3. Using the correspondence of lattices, we find p subgroups of order $3p$ containing L (the group K is one of them).

Lemma 4. *The group $H(i)$ is normal in G if and only if*

$$i^2 + i + 1 \equiv 0 \pmod{p}. \tag{3}$$

If $p \equiv 1 \pmod 3$, there are two solutions to (3). For other values of p, there is no solution.

Proof. We have

$$\begin{aligned} x^{-1}h(i)x &= x^{-1}x^2y(xy^2)^ix = xy^2y^2(xy^2)^ix \\ &= (xy^2)(y^2x)^{i+1} = (x^2y)^{-(i+1)}(xy^2). \end{aligned}$$

Thus $x^{-1}h(i)x$ belongs to $H(i)$ if and only if $(x^2y)^{-(i+1)i}(xy^2)^i = (x^2y)(xy^2)^i$, i.e. if and only if i satisfies (3). Similarly,

$$\begin{aligned} y^{-1}h(i)y &= y^{-1}x^2y(xy^2)^iy = (y^2x)(xy^2)y^2(xy^2)^iy \\ &= (y^2x)(xy^2)(y^2x)^i = (x^2y)^{-(i+1)}(xy^2). \end{aligned}$$

Then $y^{-1}h(i)y$ belongs to $H(i)$ if and only if i satisfies (3).

The quadratic congruence (3) has either two solutions or none. Pick $a \in GF(p)^*$, $a \neq 1$. Then $a^2 + a + 1 = 0$ if and only if $a^3 = 1$, since $a^3 - 1 = (a - 1)(a^2 + a + 1)$. This simple argument shows that (3) has a solution if and only if 3 divides $p - 1 = |GF(p)^*|$. □

Theorem 5 (The Lattice of Subgroups of $(3, 3 \mid 3, p)$). *For a prime $p > 3$, let $G = (3, 3 \mid 3, p)$, $H = \langle x^2y, xy^2\rangle$, $h(i) = x^2y(xy^2)^i$ for $0 \leqslant i < p$, $h(\infty) = xy^2$, $H(i) = \langle h(i)\rangle$, $g(k, l) = (x^2y)^{-k}(xy^2)^{-l}x(x^2y)^k(xy^2)^l$ for $0 \leqslant k, l < p$, and $G(k, l) = \langle g(k, l)\rangle$.*

Then $H(\infty) \cong C_p$, $H(i) \cong C_p$, $G(k, l) \cong C_3$ are the minimal subgroups of G, and $H(i) \vee H(j) = H \cong C_p \times C_p$ for every $i \neq j$. When 3 does not divide $p - 1$, there are no other subgroups in G. Otherwise, there are additional $2p$ non-abelian maximal subgroups of order $3p$; p for each $1 < i < p$ satisfying $i^3 \equiv 1 \pmod p$. These subgroups can be listed as $K(i, l) = H(i) \vee G(0, l)$, for $0 \leqslant l < p$. Then $H(i) \vee G(k', l') = K(i, l)$ if and only if $l' - l \equiv ik' \pmod p$; otherwise $H(i) \vee G(k', l') = G$. Finally, let $(k, l) \neq (k', l')$. Then $G(k, l) \vee G(k', l') = H(i) \vee G(k, l)$ if and only if there is $1 < i < p$ satisfying $i^3 \equiv 1 \pmod p$ such that $l' - l \equiv (k' - k)i \pmod p$; otherwise $G(k, l) \vee G(k', l') = G$.

The group $(3, 3 \mid 3, 2)$ is isomorphic to A_4, the alternating group on 4 points, and $(3, 3 \mid 3, 3)$ is the unique non-abelian group of order 27 and exponent 3.

Proof. Check that $h(i)^{-1}g(k, l)h(i) = g(k + 1, l + i)$, and conclude that $H(i) \vee G(k, l) = H(i) \vee G(k', l')$ if and only if $l' - l \equiv i(k' - k) \pmod p$. This also implies that, for some $1 < i < p$, $H(i) \vee G(k', l')$ equals $K(i, l)$ if and only if $l' - l \equiv ik' \pmod p$ and $i^3 \equiv 1 \pmod p$.

Finally, if $S = G(k, l) \vee G(k', l') \neq G$, it contains a unique $H(i) \trianglelefteq G$. Moreover, we have $S = H(i) \vee G(k, l) = H(i) \vee G(k', l')$ solely on the grounds of cardinality, and everything follows. □

We illustrate Theorem 5 with $p = 7$. The congruence (3) has two solutions, $i = 2$ and $i = 4$. The subgroup lattice of $(3, 3 \mid 3, 7)$ is depicted in the 3D Figure 1. The 49 subgroups $G(k, l)$ are represented by a parallelogram that is thought to be in a horizontal position. All lines connecting the subgroups $G(k, l)$ with $K(2, 0)$ and $K(4, 0)$ are drawn. The lines connecting the subgroups $G(k, l)$ with $K(2, j)$, $K(4, j)$, for $1 \leqslant j < p$, are omitted for the sake of transparency. The best way to add these missing lines is by the means of affine geometry of $GF(p) \times GF(p)$. To determine which groups $G(k, l)$ are connected to the group $K(i, j)$, start at $G(0, j)$ and follow the line with slope i, drawn modulo the parallelogram.

The group A_4 fits the description of Theorem 5, too, as can be seen from its lattice of subgroups in Figure 2. So does the group $(3, 3 \mid 3, 3)$.

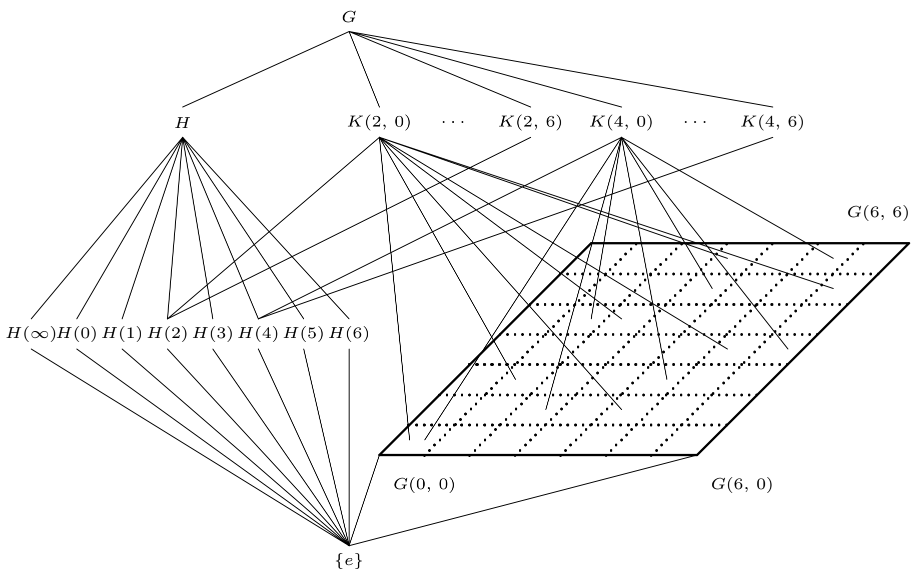

Figure 1: The lattice of subgroups of (3, 3 | 3, 7)

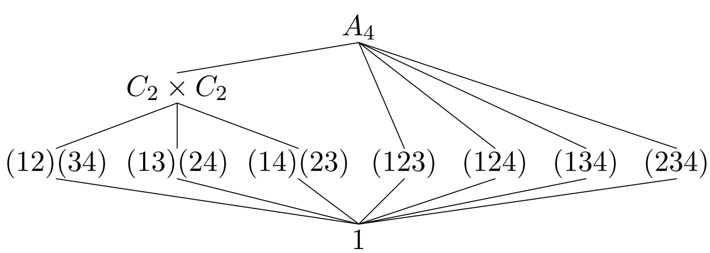

Figure 2: The subgroup structure of A_4

3. Three subgroups

We promised to show that each of the subgroups $\langle g_3,\, g_4\rangle$, $\langle g_3,\, g_5\rangle$, $\langle g_4,\, g_5\rangle$ of $M^*(q)$ is isomorphic to $(3,\, 3 \mid 3,\, p)$.

Proposition 3.1. *Let g_3, g_4, g_5 be defined as above, $q = p^r$. Then the three subgroups $\langle g_3,\, g_4\rangle$, $\langle g_3,\, g_5\rangle$, $\langle g_4,\, g_5\rangle$ of $M^*(p^r)$ are isomorphic to $(3,\, 3 \mid 3,\, p)$, if $q \neq 9$ is odd or $q = 2$.*

Proof. We prove that $G_1 = \langle g_3,\, g_4\rangle \cong (3,\, 3 \mid 3,\, p)$; the argument for the other two groups is similar. We have $g_3^3 = g_4^3 = (g_3g_4)^3 = (g_4g_3)^3 = (g_3^{-1}g_4)^p = (g_3^2g_4)^p = e$. Thus $G_1 \leqslant (3,\, 3 \mid 3,\, p)$. Also, $H_1 = \langle g_3^2g_4,\, g_3g_4^2\rangle \cong C_p \times C_p$. When $p \neq 3$, we conclude that $|G_1| = 3p^2$, since G_1 contains an element of order 3. When $p = 3$, we check that $g_3 \notin H_1$, and reach the same conclusion. $\square$

We finish this paper with a now obvious observation, that in order to describe all subloops of $M^*(q)$, one only has to study the interplay of the isomorphic subgroups $\langle g_3,\, g_4\rangle$, $\langle g_3,\, g_5\rangle$, and $\langle g_4,\, g_5\rangle$.

References

[1] **H. S. M. Coxeter**: *The abstract groups $G^{m,n,p}$*, Trans. Amer. Math. Soc., **45** (1939), 73 – 150.

[2] **H. S. M. Coxeter and W. O. J. Moser**: *Generators and relations for discrete groups*, fourth edition, A Series of Modern Surveys in Mathematics, vol. **14**, Springer-Verlag (1980).

[3] **W. E. Edington**: *Abstract group definitions and applications*, Trans. Amer. Math. Soc., **25** (1923), 193 – 210.

[4] **L. Paige**: *A class of simple Moufang loops*, Proc. Amer. Math. Soc. **7** (1956), 471 – 482.

[5] **H. O. Pflugfelder**: *Quasigroups and Loops: Introduction*, Sigma series in pure mathematics, vol. **7**, Heldermann Verlag Berlin 1990.

[6] **P. Vojtěchovský**: *Generators for finite simple Moufang loops*, submitted, available at `http://www.vojtechovsky.com`

[7] **P. Vojtěchovský**: *Generators of nonassociative simple Moufang loops over finite prime fields*, J. Algebra **241** (2001), 186 – 192.

Department of Mathematics
Iowa State University
Ames, IA 50011
U.S.A.
petr@iastate.edu

Received May 7, 2001