

## Split extension in Moufang loops

By FOOK LEONG (Pulau Pinang) and ANDREW RAJAH (Pulau Pinang)

**Abstract.** In this paper, we prove the following:

1. Let  $G$  be a Moufang loop of order  $p^\alpha m$ ,  $(p, m) = 1$ ,  $(p - 1, p^\alpha m) = 1$  and  $p$  is a prime. Suppose  $G$  has an element of order  $p^\alpha$ . Then  $G = P \rtimes K$ , a split extension of a normal subloop  $K$  of order  $m$  with a subloop  $P$  order  $p^\alpha$ .
2. Let  $G$  be a Moufang loop of odd order  $p^2 m$ ,  $(p, m) = 1$ , and  $p$  is the smallest prime dividing  $|G|$ . Then a similar result holds as in (1) with  $\alpha = 2$ .

### I. Introduction

Let  $G$  be a group of order  $p^\alpha m$ ,  $(p, m) = 1$ ,  $(p - 1, p^\alpha m) = 1$  and suppose  $G$  has an element  $x$  of order  $p^\alpha$ . Then  $G = \langle x \rangle \rtimes K$ , a split extension of a normal subgroup  $K$  of order  $m$  with the subgroup  $\langle x \rangle$  [4]. To prove an analogous result on a Moufang loop  $G$ , we need a normal subloop  $K$  so that we can use induction on  $G/K$ . In other words,  $G$  has to be nonsimple. By LIEBECK [8], every simple nonassociative Moufang loop is isomorphic to one of the Paige's loop  $M^*(q)$ . Considering the orders of elements in each of the conjugate classes of  $M^*(q)$ , as examined by BANNAI and SONG [2], we find that a Moufang loop  $G$  with the given properties stated above cannot be simple. Then  $G$  has a normal subloop  $K$ , and so induction will be possible.

Let  $G$  be a group of order,  $p^2 m$ ,  $(p, m) = 1$ , and  $p$  is the smallest prime dividing  $|G|$ . Then  $G = P \rtimes K$ , a split extension of a normal subgroup  $K$  of order  $m$  with the subgroup  $P$  of order  $p^2$  [11]. We prove

---

*Mathematics Subject Classification:* 20N05.

*Key words and phrases:* Moufang loop, normal, extension, simple loop.

also an analogous result on a Moufang loop  $G$  by using repeatedly several theorems of GLAUBERMAN [5].

There exist nonassociative Moufang loops of order  $pq^3$  with  $q = 1 \pmod{p}$  [10]. Moufang loops of odd order  $p^2q^3$  can be similarly constructed. Hence our two splitting theorems are very useful in studying the structure of such finite Moufang loops.

## II. Definitions

1. A binary system  $\langle G, \cdot \rangle$ , in which specification of any two of the elements  $x, y, z$  in the equation  $x \cdot y = z$  uniquely determines the third element, is called a quasigroup. If it further contains an identity element, then it is called a loop. Clearly, a group is a loop. But there are loops which are not associative.

2. A loop  $\langle G, \cdot \rangle$  is a Moufang loop if  $xy \cdot zx = (x \cdot yz)x$  for all  $x, y, z$  in  $G$ . From now on,  $G$  is defined as a finite Moufang loop.

3. Define  $zR(x, y) = (zx \cdot y)(xy)^{-1}$ ,  
 $zL(x, y) = (yx)^{-1}(y \cdot xz)$  and  
 $zT(x) = x^{-1} \cdot zx$ .

$I(G) = \langle R(x, y), L(x, y), T(x) \mid x, y \in G \rangle$  is called the inner mapping group of  $G$ .

4. Let  $x$  and  $y$  be elements of  $G$ .  $x$  and  $y$  are conjugate if there exists  $\theta \in I(G)$  such that  $x\theta = y$ .

5. Let  $H$  be a subloop of  $G$  and  $\pi$  a set of primes.

(i)  $H$  is a normal subloop of  $G$ , ( $H \triangleleft G$ ), if  $H\theta = H$  for all  $\theta \in I(G)$  where  $H\theta = \{h\theta \mid h \in H\}$ .

(ii)  $H$  is a  $\pi$ -loop if the order of every element of  $H$  is a  $\pi$ -number. (A positive integer  $n$  is a  $\pi$ -number if every prime divisor of  $n$  lies in  $\pi$ ).

(iii)  $H$  is a Hall  $\pi$ -subloop of  $G$  if  $|H|$  is the largest  $\pi$ -number dividing  $|L|$ .

6.  $G_a$ , the associator subloop of  $G$ , is the subloop generated by all the associators  $(x, y, z)$  where  $(x, y, z) = (x \cdot yz)^{-1} \cdot (xy \cdot z)$ . Write  $G_a = (G, G, G)$  also.

7.  $G_c$ , the commutator subloop of  $G$ , is the subloop generated by all the commutators  $[x, y]$  where  $[x, y] = (yx)^{-1} \cdot (xy)$ .

8.  $N = N(L)$ , the nucleus of  $L$ , is the subloops generated by all  $n$  in  $L$  where  $(n, x, y) = (x, n, y) = (x, y, n) = 1$  for all  $x, y$  in  $L$ .

9.  $Z = Z(L)$ , the centre of  $L$ , is the subloop generated by all  $z$  in  $N$  such that  $[z, x] = 1$  for all  $x$  in  $L$ .

### III. Known results with Moufang loops

Let  $G$  be a finite Moufang loop.

**R<sub>1</sub>.** (a)  $x \in G \Rightarrow |x| \mid |G|$ . [1, p. 92, Thm. 1.2].

(b)  $G$  is disassociative. [1, p. 117, Moufang's Theorem].

(c)  $x \in G$  and  $\theta \in I(G) \Rightarrow x^n \theta = (x\theta)^n$  for any integer  $n$ . [1, p. 120, (4.1) and p. 117, Lemma 3.2].

**R<sub>2</sub>.**  $N$  and  $Z$  are normal subloops of  $G$ . [1, p. 114, Thm. 2.1 and p. 60, Lemma 1.1]. In fact  $N$  and  $Z$  are associative by their definitions.

**R<sub>3</sub>.** Let  $H$  be a normal subloop of  $G$  such that  $H \subset N$ . Then

(a)  $G/C_G(H) < \text{Aut } H$  where  $C_G(H) = \{g \mid g \in G, gh = hg\}$  for all  $h \in H$ .

(b)  $C_G(H) \cap H = Z(H)$ , the centre of  $H$ . If  $H = N$ , then  $G_a \subset C_G(N)$ . [7, p. 33, Thm. 3].

**R<sub>4</sub>.**  $G$  is a 2-loop if and only if  $|G| = 2^m$  for some positive integer  $m$ . [6, p. 415, Thm.].

**R<sub>5</sub>.** Suppose  $|G|$  is odd and  $K$  is a normal subloop of  $G$ .

(a) If  $K$  is minimal normal in  $G$ , then  $K$  is an elementary Abelian group and  $(K, K, G) = 1$ . [5, p. 402, Thm. 7].

(b) If  $(K, K, G) = 1$  and  $(|K|, |G/K|) = 1$ , then  $K \subset N$ . [5, p. 405, Thm. 10].

(c)  $G$  is solvable. [5, p. 413, Thm. 16].

(d)  $G$  contains a Hall  $\pi$ -subloop,  $\pi$  a set of primes. [5, p. 409, Thm. 12.]

(e) If  $H < G$  then  $|H| \mid |G|$ . [5, p. 359, Thm. 2].

**R<sub>6</sub>.** If  $H$  is a subloop of  $G$ ,  $x \in G$  and  $d$  is the smallest positive integer such that  $x^d \in H$ , then  $|\langle H, x \rangle| \geq |H|d$ . [3, p. 5, Lemma 0].

**R<sub>7</sub>.** There exist simple nonassociative Moufang loops  $M^*(p^n)$  with  $|M^*(p^n)| = p^{3n}(p^{4n} - 1)/d(p)$  where  $d(2) = 1$  and  $d(p) = 2$  if  $p$  is an odd prime. [9, p. 474, Thm. 4.1].

**R<sub>8</sub>.**  $G$  is a nonassociative simple Moufang loop  $\iff G$  is isomorphic with  $M^*(p^n)$  for some prime  $p$ . [8, p. 33, Theorem].

**R<sub>9</sub>.** The conjugacy classes of  $M^*(p^n)$  contain elements whose orders are 1,  $p$ , divisors of  $p^n - 1$  or divisors of  $p^n + 1$ . [2, p. 224, Thm. 2.1.1 and p. 227, Thm. 2.1.2].

#### IV. Moufang loops of order $p^\alpha m$

**Lemma 1.** *Let  $G$  be a simple nonassociative Moufang loop of order  $2^\alpha m$ ,  $(2, m) = 1$ . Then  $G$  has no element of order  $2^\alpha$ .*

PROOF. By  $R_7$  and  $R_8$ ,  $G$  is isomorphic to  $M^*(q)$  for some  $q$  where  $q = p^n$  and  $p$  is a prime. Let  $x$  be any 2-element of  $M^*(q)$ .

*Case 1:*  $p \geq 3$ . Let  $q - 1 = 2^{\beta_1} m_1$  and  $q + 1 = 2^{\beta_2} m_2$ , where  $m_1$  and  $m_2$  are odd. Suppose  $\beta = \max\{\beta_1, \beta_2\}$ . By  $R_9$ ,  $|x| \mid 2^\beta$ .

$$\begin{aligned} |M^*(q)| &= \frac{q^3(q^4 - 1)}{2} = \frac{q^3(q^2 + 1)}{2} (q - 1)(q + 1) \\ &= \frac{q^3(q^2 + 1)}{2} 2^{(\beta_1 + \beta_2)} m_1 m_2 = 2^\alpha m. \end{aligned}$$

Since  $q$  is odd,  $2 \mid (q^2 + 1)$ . So  $\beta_1 + \beta_2 \leq \alpha$ . Thus  $|x| \leq 2^\beta < 2^{\beta_1 + \beta_2} \leq 2^\alpha$  as  $\beta_1 > 0$  and  $\beta_2 > 0$ .

*Case 2:*  $p = 2$ . As  $q - 1$  and  $q + 1$  are odd,  $2 \nmid (q - 1)(q + 1)$ . So by  $R_9$ ,  $|x| = 2$ . Now  $|M^*(2^n)| = 2^{3n}(2^{4n} - 1) = 2^\alpha m$ . So  $2^\alpha = 2^{3n} \geq 2^3 > 2 = |x|$ . Thus  $G$  has no element of order  $2^\alpha$ .

**Lemma 2.** *Let  $G$  be a Moufang loop and  $M$  a normal subloop of  $G$ . Suppose  $H$  is a normal Hall  $\pi$ -subloop of  $M$ . Then  $H$  is normal in  $G$  in each of the following two cases:*

- (a)  $G$  is of odd order;

(b)  $|M| = 2^r m$  where  $m$  is odd,  $|H| = m$  and there exists an element of order  $2^r$  in  $M$ .

PROOF. Suppose  $H \not\triangleleft G$ . Then there exists  $\theta \in I(G)$  such that  $H\theta \neq H$ . Since any inner mapping  $\theta$  is a permutation of  $G$ ,  $H\theta - H \neq \emptyset$ .

Let  $h\theta \in H\theta - H$ . Since  $H \triangleleft M \triangleleft G$ ,  $H\theta \subset M\theta = M$ . Since  $H$  and  $\langle h\theta \rangle$  are both subloops of  $M$  with  $H \triangleleft M$ , clearly  $H\langle h\theta \rangle$  is a subloop of  $M$ . Now by  $R_1(c)$ ,  $(h\theta)^{|h|} = (h^{|h|})\theta = 1\theta = 1$ . So  $|h\theta| \mid |h|$ . By  $R_1(a)$ ,  $|h| \mid |H|$ .

So  $|h\theta| \mid |H|$ . Also  $|H\langle h\theta \rangle| = \frac{|H| \cdot |\langle h\theta \rangle|}{|H \cap \langle h\theta \rangle|}$ .

(a) Suppose  $G$  is of odd order. Since  $|h\theta| \mid |H|$ ,  $H\langle h\theta \rangle$  is a  $\pi$ -loop in  $M$  strictly containing the Hall  $\pi$ -subloop  $H$ . So  $|H\langle h\theta \rangle| \nmid |M|$ . This is a contradiction by  $R_5(e)$ .

So  $H \triangleleft G$  if  $G$  is of odd order.

(b) Suppose  $|M| = 2^r m$  where  $m$  is odd,  $|H| = m$  and there exists an element  $x$  of order  $2^r$  in  $M$ . Since  $|h\theta| \mid |H|$ ,  $|H\langle h\theta \rangle|$  is odd. Also  $|H\langle h\theta \rangle| > m$  as  $h\theta \notin H$ . Now by  $R_1(a)$ ,  $x^d \notin H\langle h\theta \rangle$  for each  $0 < d < 2^r$ . But  $x^{2^r} = 1 \in H\langle h\theta \rangle$ . Thus  $|\langle H\langle h\theta \rangle, x \rangle| \geq |H\langle h\theta \rangle| 2^r$  by  $R_6 > m 2^r = |M|$ .

This is a contradiction as  $\langle H\langle h\theta \rangle, x \rangle \subset M$ . Hence  $H \triangleleft G$  in this case also.

**Lemma 3.** Suppose  $G$  is a Moufang loop of order  $p^\alpha m$ ,  $(p, m) = 1$ ;  $K$  is a normal subloop of  $G$  such that  $|G/K| = p^\beta m_0$ ,  $m_0 \mid m$ . Suppose there exists an element  $x$  of order  $p^\alpha$  in  $G$ . Then  $xK$  is an element of order  $p^\beta$  in  $G/K$ .

PROOF.  $(xK)^{p^\alpha} = x^{p^\alpha} K = 1K \Rightarrow |xK| \mid p^\alpha \Rightarrow xK$  is a  $p$ -element in  $G/K \Rightarrow |xK| \mid p^\beta$  by  $R_1(a)$ . So  $|xK| = p^\gamma$ ,  $\gamma \leq \beta$ . Then  $(xK)^{p^\gamma} = x^{p^\gamma} K = 1K$  and  $x^{p^\gamma} \in K$ . Since  $|K| = p^{\alpha-\beta} m/m_0$  and  $x^{p^\gamma}$  is a  $p$ -element in  $K$ ,  $|x^{p^\gamma}| \mid p^{\alpha-\beta}$  by  $R_1(a)$ . Thus  $(x^{p^\gamma})^{p^{\alpha-\beta}} = 1$  or  $x^{p^{\alpha+\gamma-\beta}} = 1$ . So  $\alpha + \gamma - \beta \geq \alpha$ . Then  $\gamma \geq \beta$ . Hence  $\gamma = \beta$ . So  $|xK| = p^\beta$ .

**Lemma 4.** Let  $G$  be a Moufang loop of order  $2^\alpha m$ ,  $(2, m) = 1$ . Suppose  $G$  has an element  $x$  of order  $2^\alpha$ . Then  $G = \langle x \rangle \rtimes K$ , i.e.,  $G$  is a split extension of a cyclic group  $\langle x \rangle$  of order  $2^\alpha$  with a normal subloop  $K$  of order  $m$ .

PROOF. If  $G$  is a group, we are through by [4, p. 14, Problem 2.16]. So we assume that  $G$  is nonassociative. By Lemma 1, we know that  $G$  is

nonsimple. Let  $K$  be a maximal normal subloop of  $G$ . Let  $|G/K| = 2^\beta m_0$ ,  $0 \leq \beta \leq \alpha$ ,  $m_0 \mid m$ .

*Case 1:*  $1 < m_0 < m : |G/K| = 2^\beta m_0$ .

$1(a) : \beta = 0$ . Then  $|G/K| = m_0$  and  $|K| = 2^\alpha(m/m_0)$ . By Lemma 3,  $|xK| = 1$ . Hence  $x \in K$ . By induction, there exists a subloop  $K_0$  of order  $m/m_0$  normal in  $K$ . By Lemma 2,  $K_0 \triangleleft G$ . Now  $|G/K_0| = 2^\alpha m_0$  and  $xK_0$  is an element of order  $2^\alpha$  in  $G/K_0$  by Lemma 3. By induction, there exists a subloop  $K_1/K_0$  of order  $m_0$  normal in  $G/K_0$ . Then  $K_1 \triangleleft G$  and  $|K_1| = |K_0|m_0 = m$ . So  $G = \langle x \rangle \rtimes K_1$ .

$1(b) : \beta \geq 1$ . By Lemma 3,  $xK$  is an element of order  $2^\beta$  in  $G/K$ . By induction, there exists a subloop  $K_1/K$  of order  $m_0$  normal in  $G/K$ . Thus  $K_1 \triangleleft G$  and  $|K_1| = |K|m_0 > |K|$ , contradicting the maximality of  $K$ .

*Case 2:*  $m_0 = 1 : |G/K| = 2^\beta$ .

$2(a) : \beta = 0$ .  $|G/K| = 1 \Rightarrow G = K$ , a contradiction.

$2(b) : 0 < \beta < \alpha$ .  $|K| = 2^{\alpha-\beta}m$ . Since  $xK \in G/K$ ,  $(xK)^{2^\beta} = 1K$  and  $x^{2^\beta} \in K$ . Clearly  $|x^{2^\beta}| = 2^{\alpha-\beta}$ . By induction,  $K$  has a normal subloop  $K_0$  of order  $m$ . Thus  $K_0 \triangleleft G$  by Lemma 2(b). So  $G = \langle x \rangle \rtimes K_0$ .

$2(c) : \beta = \alpha$ .  $|K| = m$  and  $G = \langle x \rangle \rtimes K$ .

*Case 3:*  $m_0 = m : |G/K| = 2^\beta m$ .

$3(a) : \beta = 0$ .  $|G/K| = m$ . Suppose  $m$  is not a prime. Then  $G/K$  is solvable by  $R_5(c)$ . So it has proper normal subloop  $K_1/K$ . Then  $K_1 \triangleleft G$  and  $|K| < |K_1| < |G|$ . This contradicts that  $K$  is a maximal normal subloop of  $L$ . So  $m = p$ , an odd prime. Now  $|G| = 2^\alpha p$ . By  $R_1(a)$ , there exists  $w \in G$  such that  $|w| = p$  as otherwise,  $G$  would be a 2-loop, which is impossible by  $R_4$ . Now by  $R_6$ ,  $G = \langle x, w \rangle$  is a group by diassociativity, a contradiction.

$3(b) : 0 < \beta < \alpha$ . By Lemma 3,  $xK$  is an element of order  $2^\beta$  in  $G/K$ . By induction, there exists a subloop  $K_1/K$  of order  $m$  normal in  $G/K$ . Then  $K_1 \triangleleft G$  and  $|K_1| = m|K| > |K|$ , a contradiction.

$3(c) : \beta = \alpha$ . Then  $|K| = 1$ , a contradiction since  $K$  is a maximal normal subloop of  $G$ .

**Theorem 1.** *Let  $G$  be a finite Moufang loop of order  $p^\alpha m$ ,  $(p, m) = 1$ ,  $(p - 1, p^\alpha m) = 1$ . Suppose  $G$  has an element  $x$  of order  $p^\alpha$ . Then  $G = \langle x \rangle \rtimes K$ , i.e.,  $G$  is a split extension of a cyclic group  $\langle x \rangle$  of order  $p^\alpha$  and a normal subloop  $K$  of order  $m$ .*

PROOF. By Lemma 4, we can assume that  $p$  is an odd prime. Since  $(p - 1, p^\alpha m) = 1$ ,  $G$  is of odd order. By  $R_5(e)$ ,  $G$  is solvable. Let  $K$  be a minimal normal subloop of  $G$ . By  $R_5(a)$ ,  $K$  is an elementary abelian  $q$ -group (where  $q$  is a prime).

*Case 1:  $q = p$ .  $K < \langle x \rangle$ .* Otherwise,  $K\langle x \rangle$  is a  $p$ -subloop of  $G$  whose order is bigger than  $p^\alpha$ , contradicting  $R_5(e)$ . As  $\langle x \rangle$  is cyclic,  $K$  is cyclic. So  $K = C_p$  as it is an elementary abelian group.

*1(a) :  $K \not\leq \langle x \rangle$ .* Then  $\alpha \geq 2$ ,  $|G/K| = p^{\alpha-1}m$  and  $xK$  is an element of order  $p^{\alpha-1}$  by Lemma 3. By induction, there exists a subloop  $K_1/K$  of order  $m$  normal in  $G/K$ . Then  $K_1 \triangleleft G$  and  $|K_1| = pm$ . Now  $x^{p^{\alpha-1}}$  is an element of order  $p$  in  $K_1$ . By induction, there exists a subloop  $K_2$  of order  $m$  normal in  $K_1$ . Now  $K_2$  is a normal Hall subloop in  $K_1$  and  $K_1 \triangleleft G$  implies that  $K_2 \triangleleft G$  by Lemma 2(a). Thus  $G = \langle x \rangle \rtimes K_2$ .

*1(b) :  $K = \langle x \rangle = C_p$ .* Now  $(K, K, G) = 1$  by  $R_5(a)$  and  $(|K|, |G/K|) = 1 \Rightarrow K \subset N$ , the nucleus of  $G$ , by  $R_5(b)$ . By  $R_3(a)$ ,  $G/C_G(K) \leq \text{Aut } K$ . As the order of the group of automorphisms of  $C_p$  is  $p - 1$ ,  $\left| \frac{G}{C_G(K)} \right| \mid p - 1$ . As  $(p - 1, |G|) = (p - 1, p^\alpha m) = 1$ ,  $G = C_G(K)$ . Thus  $K \subset Z$ , the centre of  $G$ . By  $R_5(d)$ , there exists a Hall subloop  $H$  of order  $m$  in  $G$ . Then  $G = HZ$ .

Now  $G_a = (G, G, G) = (HZ, HZ, HZ) = (H, H, H) \subset H$ ; and

$$G_c = [G, G] = [HZ, HZ] = [H, H] \subset H.$$

Let  $h \in H$ ,  $x, y \in G$ .

Then  $hT(x) = x^{-1}hx = hh^{-1}x^{-1}hx = h[h, x]$  and

$$\begin{aligned} hL(x, y) &= hR(x^{-1}, y^{-1}), && \text{by [1, p. 124, Lemma 5.4, (5.13)]} \\ &= h(h, y, x)^{-1}, && \text{by [1, p. 124, Lemma 5.4, (5.16)].} \end{aligned}$$

Since  $G_a \subset H$  and  $G_c \subset H$ ,  $h\theta \in H$  for all  $\theta \in I(G)$ . Thus  $H \triangleleft G$  and  $G = \langle x \rangle \triangleleft H$ .

*Case 2:  $q \neq p$ .* Let  $|K| = q^\gamma$ . Then  $|G/K| = p^\alpha \frac{m}{q^\gamma}$  where  $q^\gamma \mid m$ .

$\mathcal{2}(a) : m > q^\gamma$ . By Lemma 3,  $xK$  is an element of order  $p^\alpha$  in  $G/K$ . By induction, there exists a normal subloop  $K_1/K$  of order  $m/q^\gamma$  in  $G/K$ . Therefore  $K_1 \triangleleft G$  and  $|K_1| = \frac{|K|m}{q^\gamma} = m$ . Thus  $G = \langle x \rangle \rtimes K_1$ .

$\mathcal{2}(b) : m = q^\gamma$ . Then  $G = \langle x \rangle \rtimes K$  as required.

**Corollary 1.** *Let  $G$  be a Moufang loop of order  $p^\alpha m$ ,  $(p, m) = 1$ ,  $(p-1, p^\alpha m) = 1$  and suppose  $G$  has an element of order  $p^\alpha$ . Then  $G$  is solvable.*

PROOF. *Case 1:  $p = 2$ .* Then by Theorem 1,  $G = C_{2^\alpha} \rtimes K$  with  $|K| = m$  which is odd. So  $G/K$  is isomorphic to  $C_{2^\alpha}$  which is solvable. By  $R_5(c)$ ,  $K$  is solvable. Thus  $G$  is solvable.

*Case 2:  $p \neq 2$ .* Then  $|G|$  is odd as  $(p-1, p^\alpha m) = 1$ . Thus  $G$  is solvable by  $R_5(c)$ .

## V. Moufang loops of odd order $p^2 m$

**Theorem 2.** *Let  $G$  be a Moufang loop of odd order  $p^2 m$ ,  $(p, m) = 1$ ,  $p$  the smallest prime dividing  $|G|$ . Then there exist subloops  $M$  and  $P$  in  $G$  with  $|P| = p^2$ ,  $|M| = m$ ,  $M \triangleleft G$  such that  $G = P \rtimes M$ .*

PROOF. If  $G$  is a group, we are through by [10, p. 141, 6.3.16]. By  $R_5(c)$ ,  $G$  is solvable. Let  $K$  be a minimal normal subloop of  $G$ . By  $R_5(a)$ ,  $K$  is elementary abelian. Let  $|K| = q^\alpha$ . Existence of  $P$  is guaranteed by  $R_5(d)$ .

*Case 1:  $q \neq p$ .* If  $|K| = m$ , then  $K = M$  and we are through. If  $|K| < m$ , then  $|G/K| = p^2 (m/q^\alpha)$ . By induction, there exists a normal subloop  $M/K$  in  $G/K$  with  $|M/K| = \frac{m}{q^\alpha}$ . Then  $M \triangleleft G$  and  $|M| = \frac{m}{q^\alpha} |K| = m$ .

*Case 2:  $q = p$ .* Then by  $R_5(e)$ ,  $\alpha = 1$  or  $2$ .

$\mathcal{2}(a) : \alpha = 1 : |K| = p$ . By  $R_5(d)$ , we can get an element  $xK$  of order  $p$  in  $G/K$ .  $|G/K| = pm$ . So by Theorem 1, there exists a normal subloop  $\widehat{M}/K$  of order  $m$  in  $G/K$ . Then  $\widehat{M} \triangleleft G$  and  $|\widehat{M}| = pm$ . Similarly by  $R_5(d)$  and by Theorem 1, there exists a subloop  $M$  of order  $m$  normal in  $\widehat{M}$ . By Lemma 2(a),  $M \triangleleft G$ .



2(b):  $\alpha = 2 : |K| = p^2$ . By  $R_5(a)$  and  $R_5(b)$ ,  $K \subset N$ . Since  $K$  is an elementary abelian group,  $K = C_p \times C_p$ .

Now by  $R_3(a)$ ,  $|G/C_G(K)| \mid |\text{Aut } K| = (p+1)p(p-1)^2$  using [10, p. 141, 6.3.15]. Since  $K \subset C_G(K)$ , and  $p$  is the smallest prime dividing  $|G|$ ,  $|G/C_G(K)| \mid (p+1)$ . As  $p$  is odd and 2 does not divide the order of  $G$ ,  $G = C_G(K)$ . Thus  $K \subset Z$ .

By  $R_5(d)$ , there exists a subloop  $M$  of order  $m$  in  $G$ . As  $G = KM = ZM$ , it can be shown in a similar way as before (see the proof of Theorem 1, Case 1(b)) that  $M \triangleleft G$ .

**Corollary 2.** *Let  $G$  be a Moufang loop of odd order  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$  where  $p_1 < p_2 < \dots < p_m$  and  $1 \leq \alpha_i \leq 2$ . Then there exists a subloop of order  $p_m^{\alpha_m}$  normal in  $G$ .*

PROOF. For  $\alpha_1 = 1$ ,  $R_5(d)$  guarantees the existence of an element of order  $p_1$  in  $G$ . So by Theorem 1 or Theorem 2, there exists  $M_1$ , a normal subloop in  $G$  with  $|M_1| = p_2^{\alpha_2} \dots p_m^{\alpha_m}$ . Again there exists a subloop  $M_2$  of order  $p_3^{\alpha_3} \dots p_m^{\alpha_m}$  normal in  $M_1$ . By Lemma 2(a),  $M_2 \triangleleft G$ . By this process, we get a subloop  $M_{m-1}$  of order  $p_m^{\alpha_m}$  normal in  $G$ .

## References

- [1] R. H. BRUCK, A Survey of Binary Systems, *Springer-Verlag, Berlin*, 1971.
- [2] EIICHI BANNAI and SUNG-YELL SONG, The Character Tables of Paige's Simple Moufang Loops and their Relationship to the Character Tables of  $\text{PSL}(2, q)$ , *Proc. London Math. Soc.* (3) **58** (1989), 209–236.
- [3] ORIN CHEIN, Moufang Loop of Small Order, *Memoirs Amer. Math. Soc.* 13, Issue 1, No. 197, 1978.
- [4] JOHN D. DIXON, Problems in Group Theory, *Blaisdell Publishing Company*, 1967.
- [5] G. GLAUBERMAN, On Loops of Odd Order II, *J. Algebra* **8** (1968), 393–414.
- [6] G. GLAUBERMAN and C. R. B. WRIGHT, Nilpotency of Finite Moufang 2-Loops, *J. Algebra* **8** (1968), 415–417.
- [7] LEONG FOOK, The Devil and Angel of Loops, *Proc. Amer. Math. Soc.* **54** (1976), 33–47.
- [8] M. W. LIEBECK, The Classification of Finite Simple Moufang Loops, *Math. Proc. Camb. Philos. Soc.* **102** (1987), 33–47.
- [9] L. J. PAIGE, A Class of Simple Moufang Loops, *Proc. Amer. Math. Soc.* **7** (1956), 471–482.
- [10] ANDREW RAJAH, Which Moufang Loops are Associate, Ph.D Thesis, *Universiti Sains Malaysia*, 1997.

[11] W. R. SCOTT, Group Theory, *Prentice-Hall, New Jersey*, 1964.

FOOK LEONG  
SCHOOL OF MATHEMATICAL SCIENCES  
UNIVERSITI SAINS MALAYSIA  
11800 USM, PULAU PINANG  
MALAYSIA

ANDREW RAJAH  
SCHOOL OF MATHEMATICAL SCIENCES  
UNIVERSITI SAINS MALAYSIA  
11800 USM, PULAU PINANG  
MALAYSIA

*(Received August 2, 1995; revised January 22, 1997)*