pE Loops

By LEONG FOOK (Minden)

Abstract. Some properties of finite pE loops, a class of Moufang loops, are investigated. It is proved that : (i) Moufang loops of order p^4 are pE loops. (ii) Moufang loops of order p^5 are pE loops for $p>3$. If G is a pE loop, then: (iii) G_a, the association subloop of G, is of exponent p; G_a is an elementary abelian p-group if $p\neq 3$. (iv) G satisfies Lagranges Theorem and G has Sylow p-subloops for each p dividing the order of G. (v) $\mathbf{R}=\langle R(x, y), L(x, y)|x, y\in G\rangle$, the subgroup of multiplicative group of G is an elementary abelian p-group if $p\neq 3$. (vi) $G_a\subset Z$ for $p>3$.

Definitions & Notations: A loop G is a Moufang loop if $xy\cdot zx=(x\cdot yz)x$ for all $x, y, z\in G$.

G_a, the associator subloop of G, is generated by all the associators (x, y, z) where $xy\cdot z=(x\cdot yz)(x, y, z)$. G_c, the commutator subloop of G, is generated by all the commutators $[x, y]$ where $xy=yx\cdot[x, y]$. Let the center and nucleus of G be denoted by Z and N. It is known that both are normal in G; N and Z are groups; Z is abelian and $Z\subset N$. A Moufang loop is a pE loop if $\dfrac{G}{N}$ is commutative of exponent p, p a prime.

Fundamental Lemma. *Let G be a Moufang loop. Then G satisfies all or none of the following identities:*

(i) $[(x, y, z), x]=1$; (ii) $(x, y, [y, z])=1$; (iii) $(x, y, z)^{-1}=(x^{-1}, y, z)$; (iv) $(x, y, z)^{-1}=(x^{-1}, y^{-1}, z^{-1})$; (v) $(x, y, z)=(x, zy, z)$; (vi) $(x, y, z)=(x, z, y^{-1})$; (vii) $(x, y, z)=(x, xy, z)$. *When these identities hold, then the associator (x, y, z) lies in the centre of the subloop generated by x, y, z; and the following identities hold for all integers n:*

$$(x, y, z) = (y, z, x) = (y, x, z)^{-1}$$

$$(x^n, y, z) = (x, y, z)^n$$

$$[xy, z] = [x, z]\big[[x, z], y\big][y, z](x, y, z)^3.$$

PROOF. [1, p. 125, Lemma 5.5.]

Remark. A Moufang loop satisfying all the identities of the Fundamental Lemma is called an F loop.

Properties of G_a: If G is a Moufang loop, then $G_a\lhd G$, i.e. G_a is normal in G. Also $G_a\subset C_G(N)=\{g|gn=ng\ \forall n\in N\}$.

PROOF. [9, p. 33—34.]

Remark. A loop G is a $2E$ loop if and only if G is an extra loop, [5, p. 190, Theorem 1]. Commutative Moufang loops are $3E$ loops. There exists nonassociative $5E$ loops, [11, p. 408]. Many other pE loops can be constructed by holomorphy theory of loops [10, p. 141]. G/N is commutative implies $G_c \subset N$. Thus $(x, y, [y, z])=1$ for all $x, y, z \in G$. So pE loops are F lopps. The Fundamental lemma will be applied on pE loops repeatedly without mention. All definitions and notations follow those in [1], unless otherwise stated. All loops are assumed finite.

Theorem 1. *A Moufang loop G of order p^4 is a pE loop; G is a group if $p>3$.*

PROOF. By [6, p. 397, Theorem 4] and [6, p. 415, Theorem], G is nilpotent. Thus Z is nontrivial. If $|Z|>p$, then $G=\langle Z, x, y\rangle$ for some $x, y \in G$. As a Moufang loop is diassociative, G is a group. But a group is a pE loop. If $|Z|=p$, then $|G/Z|=p^3$. By [8, p. 33, Lemma 1], G/Z is a group. If G/Z is generated by two elements, then G is a group by diassociativity. If G/Z is generated by three elements, then G/Z is an elementary abelian p-group by [4, p. 145]. As $Z \subset N$, G/N is an elementary abelian p-group.

For the second statement of Theorem 1, see [8, p. 33].

Lemma 1. *Let x, y, z be elements of an F loop G. Then*

(i) *$zR(x, y)=z(z, x, y)$ where $R(x, y)=R(x)R(y)R(xy)^{-1}$ is an inner mapping of the multiplicative group of G.*

(ii) *$(xy)\Theta=x\Theta\, y\Theta(x\Theta, y\Theta, c^{-1})$ where Θ is a pseudoautomorphism of G with companion c.*

PROOF. By [3, p. 49, Lemma 1].

Theorem 2. *A nonassociative Moufang loop G of order p^5 is a pE loop for $p \geqq 5$.*

PROOF. If $p^2 \mid |N|$, then $|G/N| \leqq p^3$. As G is diassociative, G/N must be generated by three elements. By [4, p. 145], $G/N=C_p \times C_p \times C_p$ where C_p is a cyclic group of order p. As G is nilpotent, $Z \neq 1$. As $Z \subset N$, we can assume $Z=N=C_p$. So, $|G/Z|=p^4$. By Theorem 1, G/Z is a group or $G_a \subset Z$. As G is nonassociative, $G_a \neq 1$. Thus $G_a=Z=N=C_p$. So $(x, y, z)^p=1$ for all $x, y, z \in G$. Therefore $(x^p, y, z)=1$ or $x^p \in N$ for all $x \in G$. If $G'=C_p$, then $G_a=G'=N$. So G/N is commutative of exponent p. Suppose $G' \neq C_p$. By [1, p. 98, Theorem 2.2], $G' \subset \varphi(G)$, the Frattini subloop of G. As G is diassociative but nonassociative, $|\varphi(G)| \leqq p^2$. So $|G'| \leqq p^2$. Assume $|G'|=p^2$. Then G_2 from the decending central series of G is equal to Z. $(G_2=1 \Leftrightarrow G' \subset Z.)$ $|G'|=p^2$ implies that $G=\langle x, y, z\rangle$ for some $x, y, z \in G$. Let $u, v, w \in G$. As $[w, [x, y]] \in Z$, $(u, v, [w, [x, y]])=1$. By Lemma 1,

$$uvR(w, [x, y]) = uv(uv, w, [x, y])$$

$$= u(u, w, [x, y]) \cdot v(v, w, [x, y]) = uv \cdot (u, w, [x, y])(v, w, [x, y])$$

since $G_a \subset Z$.

Thus $(uv, w, [x, y])=(u, w, [x, y])(v, w, [x, y])$. By repeating the expansion for associators on the R.H.S. we see that $(uv, w, [x, y])$ is a product of associators of the form $(e, d, [x, y])$ where e, d are elements of the set $\{x, y, z\}$. By Fundamental Lemma $(e, d, [x, y])=1$. Thus $[x, y]\in N$. Similarly $[y, z]$ and $[z, x]$ are in N. This implies $G_c \subset N$. So $G' \subset N$. This is a contradiction.

Theorem 3. *Let G be a pE loop. Then:*

(i) *G_a is an elementary abelian p-group if $p\neq 3$.*

(ii) *G_a is a loop of exponent 3 if $p=3$.*

(iii) *G satisfies Lagranges Theorem (*i.e. *the order of a subloop divides $|G|$).*

(iv) *G contains p-Sylow subloops.*

PROOF. (i) G/N is commutative of exponent p implies $G_c \subset N$ and $x^p \in N$ for all $x \in G$. Let $b \in G_a$. Then $a^p \in N$. By the Fundamental lemma, $b^3 \in N$. As $(p, 3)=1$, $b\in N$. Thus $G_a \subset N$. By the properties of G_a, $G_a \subset Z(N)$, the centre of N. Thus G_a is an abelian group. Now $x^p \in N$ implies that $(x^p, y, z)=(x, y, z)^p=1$ for all $y, z\in G$. So G_a is an elementary abelian p-group.

(ii) G/N is commutative of exponent 3 implies $G_c \subset N$ and $x^3 \in N$ for all $x\in G$. Thus $(x, y, z)^3=(x^3, y, z)=1$, $y, z \in G$. Let $a=(x, y, z)$ and $b=(u, v, w)$. Since $[a, b]\in G_c \subset N$, $[[a, b], a]=1$ by the Properties of G_a. By [1, p. 122, Lemma 5.1], $(ab)^3=a^3b^3(a, b)^{-3}=(a^3, b)^{-1}=1$. Thus G_a is of exponent 3.

(iii) Consider $1 \lhd G_a \lhd G$. G/G_a is a group and G_a is a nilpotent p-loop. Hence both G/G_a and G_a satisfy Lagranges Theorem. By [2, p. 269, Theorem 6A], G satisfies Lagranges Theorem.

(iv) By (i) and (ii), G_a is nilpotent. By [Theorem 2, p. 34, 7] G contains p-Sylow subloops.

Theorem 4. $\mathbf{R}=\langle R(x, y),\ L(x, y)|x, y\in G\rangle$ *is an elementary abelian p-group for $p\neq 3$.*

PROOF. As $G_c \subset N$, $R(x, y)$ is an automorphism (its companion $[x, y]\in N$). Let $z\in G$.

$$\begin{aligned}
\therefore zR^p(x, y) &= z(z, x, y)\,R^{p-1}(x, y) = \\
&= z(z, x, y)^2 R^{p-2}(x, y) \quad \text{by Fundamental lemma} \\
&\ \ \vdots \\
&= z(z, x, y)^p \\
&= z \quad \text{by Theorem 3.}
\end{aligned}$$

$$\therefore R^p(x, y) = I.$$

Now $bR(x, y)\,R(u, v)=[b(b, x, y)]\,R(u, v)=b(b, u, v)\cdot(b, x, y)$ since $G_a \subset N$.

$$\begin{aligned}
bR(u, v)\,R(x, y) &= [b(b, u, v)]\,R(x, y) = b(b, x, y)\cdot(b, u, v) \\
&= b(b, u, v)\cdot(b, x, y) \quad \text{since} \quad G_a \subset Z(N) \\
&\qquad \text{by Propreties of } G_a.
\end{aligned}$$

$$\therefore R(x, y)\,R(u, v) = R(u, v)\,R(x, y).$$

By [1, p. 124, Lemma 5.4], $R(x, y)=L(x^{-1}, y^{-1})$. Thus $\mathbf{R}$ is an elementary abelian p-group.

Remark. For $p=3$, it can be shown that $R(x, y)$ is of order 3. However, it is not known if $\mathbf{R}$ is of exponent 3.

Theorem 5. *Let G be a pE loop. Then* $G_a \subset Z$ *for* $p \neq 2, 3$.

PROOF. Let $u, v, x, y \in G$.

$$\begin{aligned}(uv)R(x, y) &= (uv)(uv, x, y) \quad \text{by Lemma 1}\\ &= u(u, x, y)\cdot v(v, x, y) \quad \text{by Lemma 1 and} \quad G_c \subset N.\\ &= uv(u, x, y)[(u, x, y), v](v, x, y) \qquad G_a \subset N.\\ (uv, x, y) &= (u, x, y)[(u, x, y), v](v, x, y)\\ (uv, x, y) &= (vu[u, v], x, y)\\ &= (vu, x, y) \quad \text{as} \quad G_c \subset N.\\ &= (v, x, y)[(v, x, y), u](u, x, y)\end{aligned}$$

$[(u, x, y), v]=[(v, x, y), u]$ by Properties of G_a and $G_c \subset N$. Thus $[(u, x, y), v]$ is symmetric in u, v. By Fundamental lemma, $[(u, x, y), v]$ is skew-symmetric in u, x, y and in x, y, z. Hence $[(u, x, y), v]$ is skew-symmetric in w, x. Therefore $[(u, x, y), v]= =[(u, x, y), v]^{-1}$. So $[(u, x, y), v]^2=1$. $[[(u, x, y), v], (u, x, y)]=1$ by Properties of G_a. By [1, p. 122, Lemma 5.1], $[(u, x, y), v]^p=[(u, x, y)^p, v]=1$. Therefore $[(u, x, y), v]=1$ for all $u, v, x, y \in G$.

References

[1] R. H. BRUCK, A Survey of Binary System, *Springer-Verlag, Berlin* (1971).
[2] R. H. BRUCK, Contribution to the Theory of Loops, *Trans. Amer. Math. Soc.* **60** (1946), 245—253.
[3] R. H. BRUCK & LEONG FOOK, Schur's Splitting Theorems for Moufang Loops, *Nanta Mathematica, Vol. II,* (1978), p. 44—54.
[4] BURNSIDE, Theory of Groups of Finite Order.
[5] F. FENYVES, Extra Loops with Identities of Bol—Moufang Type, *Publ. Math. (Debrecen)* **16** (1969), 187—192.
[6] G. GLAUBERMAN, On Loops of order II, *Journal of Algebra* **8** (1968), 393—414.
[7] LEONG FOOK, *E* Loops, *Bulletin of S.E.A. Math. Soc.* **4** (1980).
[8] LEONG FOOK, Moufang Loops of Order p^4, *Nanta Mathematica, Vol. VII,* (1974), p. 33—34.
[9] LEONG FOOK, The Devil and the Angel of Loops, *Proceeding Amer. Math. Soc.* **54** (1976), 32—34.
[10] LEONG FOOK, Holomorphy Theory of Loops, *Publ. Math. (Debrecen)* **27** (1980), 139—141.
[11] C. R. B. WRIGHT, Nilpotency Conditions for Finite Loops, *Illinois J. Math.* **9** (1965), 399—409.

(Received January 25, 1985)