F loop of order p^6

By FOOK LEONG (Penang)

Abstract. It is known that a Moufang loop G of order p^4 is a pE loop, p a prime (G is in fact a group for $p>3$, see [4]). This paper proves that a Moufang loop of order p^5 is a pE loop for $p>3$; an F loop of order p^5 is a pE loop; an F loop of order p^6 is a pE loop for $p\neq 3$.

Definitions. Let G be a loop. The associator subloop G_a and the commutator subloop G_c are defined as follow: $G_a=\langle (x,y,z)\mid x,y,z\in G\rangle$ where $xy\cdot z=(x\cdot yz)(x,y,z)$. $G_c=\langle [x,y]\mid x,y\in G\rangle$ where $xy=(yx)[x,y]$. An F loop is a Moufang loop such that if H is a subloop generated by any three elements x,y,z, then $\langle (x,y,z)\rangle\subset Z(H)$, the centre of H. (It can be shown easily that $H_a=\langle (x,y,z)\rangle$.) A pE loop G is a Moufang loop such that G/N is commutative of exponent p, where N is the nucleus of G. All other definitions and notations follow those in [1], except otherwise stated.

Remark. An F loop satisfies all the equivalent identities of Lemma 5.5, [1, p. 125]. As this lemma is repeatedly needed, we shall quote it as Lemma F. Clearly a pE loop is an F loop. A Moufang loop of order a prime power is nilpotent, [3, p. 397] and [3, p. 415].

Lemma 1. *Let x,y,z be elements of an F loop G. Then:* (a) $zR(x,y)=z(z,x,y)$. (b) $(xy)\alpha=x\alpha y\alpha(x\alpha,y\alpha,c^{-1})$ *where α is a pseudoautomorphism of G with companion c.*

PROOF. (a) $zR(x,y)=zL(x^{-1},y^{-1})=z(z,y^{-1},x^{-1})^{-1}$ by [1, p. 124, L. 5.4]. $=z(z,x,y)$ by Lemma F. (b) $(xy)\alpha\cdot c=x\alpha\cdot y\alpha c$ by definition of α. $(xy)\alpha=(x\alpha\cdot y\alpha c)c^{-1}=(x\alpha x\alpha\cdot c)(x\alpha,y\alpha,c)^{-1}\cdot c^{-1}=x\alpha y\alpha(x\alpha,y\alpha,c^{-1})$ by Lemma F.

Lemma 2. *Let $G=\langle x,y,z\rangle$ be an F loop such that $[[u,v],w]$ is in N for all u,v,w in $\{x,y,z\}$. Then $G_c\subset N$.*

PROOF. By Lemma F (5.23) $[[u,v],w]\in N$ for all u,v,w in $\{x,y,z\}$ implies that $[[f,g],h]\in N$ for all f,g,h in G. By Lemma 1,

$$fgR(h,[u,v])=fg(fg,h,[u,v])=f(f,h,[u,v])\cdot g(g,h,[u,v]) \qquad :*$$

since the companion $c=[h,[u,v]]\in N$, $:*=fg\cdot(f,h,[u,v])(g,h,[u,v])$ as $G_a\subset Z(G)$. Therefore $(fg,h,[u,v])=(f,h,[u,v])(g,h,[u,v])$. By repeating the expansion for associators on the R.H.S., we see that $(fg,h,[x,y])$ is a product of associators of the form $(e, d, [x, y])$ where e, d are from $\{x, y, z\}$. By Lemma F, $(e, d, [x, y]) = 1$. Thus $[u, v]$ is in N for all u, v in $\{x, y, z\}$. By Lemma F, $\{g, h]$ is in N for all g, h in G. So $G_c \subset N$.

Theorem 1. *Let G be a nonassociative F loop of order p^5. Then G is a pE loop.*

PROOF. If $|N| \geqq p^3$, then $G = \langle N, x, y\rangle$ for some $x, y \in G$. As a Moufang loop is diassociative, G would be a group. Suppose $|N| = p^2$. As G is nonassociative, G/N must be generated by three elements and $G/N = C_p \times C_p \times C_p$. So G is a pE loop.

Suppose $|N| = |Z| = p$. If $|G'| = p$, then $G' = Z = N$ since it is a minimal normal subloop of a nilpotent loop. As G is nonassociative, $G_a \neq 1$. Thus $G_a = G' = C_p$ and $(x, y, z)^p = 1$ for all $x, y, z \in G$. By Lemma F, $(x^p, y, z) = 1$. So $x^p \in N$ for all $x \in G$. $G/N = G/G'$ is obviously commutative.

If $|G'| \geqq p^3$, then $G = \langle G', x, y\rangle$ for some $x, y \in G$. By [1, p. 98, Theorem 2.2,]. $G' \subset \varphi(G)$ where $\varphi(G)$ is the Frattini subloop of G. Thus $G = \langle x, y\rangle$ would be a group by diassociativity of G.

Suppose $|G'| = p^2$. Then there exist $x, y, z \in G$ such that $G = \langle G', x, y, z\rangle = \langle x, y, z\rangle$. Let $G_2 = \langle x^{-1}, x\theta \mid x \in G', \theta \in I(G)$, the group of inner mappings of $G\rangle$ be the third term of the lower central series of G. As G is nilpotent, $|G_2| \leqq p$. So $G_2 \subset Z = N$. By Lemma 2, $G_c \subset N$. As G is an F loop generated by three elements, $G_a \subset Z \subset N$. Thus $G' = \langle G_a, G_c\rangle \subset N$, a contradiction.

Corollary. *A Moufang loop of order p^5 is a pE loop for $p \geqq 5$. As G is nilpotent, $|Z| \neq 1$. Thus $|G/Z| \leqq p^4$. By* [4, p. 33], *G/Z is a group. So $G_a \subset Z$ and G satisfies Lemma F. Therefore G is an F loop. By Theorem* 1, *G is a pE loop.*

Theorem 2. *Let G be an F loop of order p^6. Then*

(a) *$x^p \in N$ for all $x \in G$,*

(b) *G is a pE loop for $p \neq 3$.*

PROOF. (a) Suppose $\exists x \in G$ such that $x^p \notin N$. Then $(x^p, y, z) \neq 1$ for some $y, z \in G$. Let $H = \langle x, y, z\rangle$. Then $|H_a| = |\langle (x, y, z)\rangle| \geqq p^2$ as $(x^p, y, z) = (x, y, z)^p \neq 1$. As H is an F loop, $H_a \subset Z(H)$. If $H \neq G$, then $|H/Z(H)| \leqq p^3$. Clearly H is nonassociative. So $H/Z(H)$ must be generated by three elements and is an elementary abelian p-group. Thus $x^p \in Z(H)$ and $(x^p, y, z) = 1$, a contradiction. Hence $H = G = \langle x, y, z\rangle$. As $(x^p, y, z) \neq 1$, y^p and z^p are not in N by Lemma F. Since $|G_a| \geqq p^2$ and $G_a \subset Z \subset N$, $|G/N| \leqq p^4$ and G/N is a group with three generators xN, yN, zN all of whose orders are not less than p^2. By [2, p. 145], such a group does not exist. Thus $x^p \in N$ for all $x \in G$.

(b) For $p = 2$, G/N is of exponent 2 by (a). But a Moufang loop of exponent 2 is commutative. We assume $p > 3$. Suppose G is generated by at least four elements. As $G' \subset \varphi(G)$, $|\langle G', x, y\rangle| \leqq p^4$ for any $x, y \in G$. By [4, p. 33], $(G', x, y) = 1$. So, $G' \subset N$ and G/N is commutative. Suppose $G = \langle x, y, z\rangle$, $x, y, z \in G$. Assume $G_2 \not\subset Z$. Then $|G_2| \geqq p^2$. As $G' \subset \varphi(G)$ and G is nilpotent, $|G'| = p^3$. Clearly $Z \subset G'$. Now $G' = ZG_2$. But $G_2 = \langle x^{-1} \cdot x\theta \mid x \in G', \theta \in I(G)$ which is the group of inner mappings of $G\rangle = \langle g^{-1} \cdot g\theta \mid g \in G_2, \theta \in I(G)\rangle = G_3$ as $G' = ZG_2$. Since G is nilpotent, this is a contradiction. Thus $G_2 \subset Z \subset N$. By Lemma 2, $G_c \subset N$. Therefore G/N is commutative.

Remark. This proof fails for $p=3$ because an F loop of order 3^4 is not necessarily associative.

References

[1] R. H. Bruck, A Survey of Binary System, *Springer Verlag*, (1971).
[2] W. Burnside, Theory of Groups of Finite Order, 2nd Edition, *Dover Publication*.
[3] G. Glauberman, On Loops of Odd Order II, *J. of Algebra* **8**, (1968).
[4] F. Leong, Moufang Loops of Order p^4, *Nanta Mathematica*, **7**.

(Received March 15, 1983.)