ON THE NILPOTENCE OF MOUFANG LOOPS

ISHAN JOSHI

Abstract. We establish an analogue of Fitting's Theorem for finite Moufang loops. If L is a finite Moufang loop and $H, K \lhd L$ are normal nilpotent subloops of nilpotency classes h and k, then their product HK is again a normal nilpotent subloop of L, with nilpotency class at most $h+k$. The proof proceeds through a detailed analysis of normality, Sylow decomposition, and an embedding of finite Moufang loops into groups.

1. Introduction

Moufang loops form a central class of nonassociative algebraic structures. Although they do not satisfy associativity in general, the Moufang identities are strong enough to guarantee power-associativity, the existence of inverses, and a well-behaved theory of inner mappings. As a result, many tools from group theory admit meaningful analogues in the Moufang setting.

One of the most important structural results in finite group theory is Fitting's Theorem, which asserts that the product of two normal nilpotent subgroups is again nilpotent. The goal of this paper is to establish a corresponding result for finite Moufang loops. Specifically, we prove that the product of normal nilpotent subloops is again nilpotent, with explicit control over the nilpotency class.

The paper is organized as follows. In Section 2 we recall the necessary background on Moufang loops, commutators, and nilpotency. Section 3 establishes that the product of two normal subloops is again normal. Section 4 develops a Sylow decomposition for finite nilpotent Moufang loops. In Section 5 we review the embedding of finite Moufang loops into groups, which serves as a bridge between loop-theoretic and group-theoretic arguments. These ingredients are combined in the second half of the paper to prove the main theorem.

2. Preliminaries

Definition 2.1 (Moufang loop)**.** A *loop* is a set L equipped with a binary operation $(x, y) \mapsto xy$ such that there exists an identity element $e \in L$, every element has a two-sided inverse, and left and right division are uniquely solvable. A loop L is a *Moufang loop* if it satisfies the identity

$$x(y(xz)) = ((xy)x)z \qquad (x, y, z \in L).$$

Every Moufang loop is power-associative.

Definition 2.2 (Commutators and associators)**.** For $a, b, c \in L$, define

$$[a, b] = (ab)(ba)^{-1}, \qquad (a, b, c) = (a(bc))((ab)c)^{-1}.$$

Date: December 21, 2025.

Definition 2.3 (Lower central series)**.** Let L be a Moufang loop. Define $\gamma_1(L) = L$ and recursively

$$\gamma_{i+1}(L) = \langle [x, y] : x \in \gamma_i(L),\, y \in L\rangle.$$

The loop L is *nilpotent of class* k if $\gamma_{k+1}(L) = \{e\}$.

Definition 2.4 (Normal subloop)**.** A subloop $H \le L$ is *normal*, written $H \triangleleft L$, if it is invariant under all inner mappings of L.

3. Normality of the Product HK

Lemma 3.1. *If H and K are normal subloops of a Moufang loop L, then HK is a normal subloop of L.*

Proof. Let $a \in HK$, so $a = hk$ for some $h \in H$ and $k \in K$. Since H is normal, for all $x, y \in L$ we have

$$(xy)H = x(yH) = x(Hy).$$

Right-multiplying by K yields

$$((xy)H)K = (x(yH))K.$$

Because K is normal, we may reassociate to obtain

$$(xy)(HK) = x((yH)K) = x(y(HK)).$$

A symmetric argument shows $y(HK) = (HK)y$, and therefore HK satisfies the normality condition. □

4. Sylow Decomposition of Nilpotent Moufang Loops

Lemma 4.1. *Let L be a finite nilpotent Moufang loop. Then L decomposes as a direct product of its normal Sylow p-subloops.*

Proof. Let L_p denote a Sylow p-subloop of L.

Step 1: Normality. We prove by induction on the nilpotency class of L that L_p is normal. If L is abelian, the claim is immediate. Assume L has class $n + 1$ and let $z \in Z(L)$. Then $\langle z\rangle$ is central and normal, and $L/\langle z\rangle$ has nilpotency class n. By induction, the image of L_p in the quotient is normal. Pulling back under the quotient map preserves normality, so L_p is normal in L.

Step 2: Trivial intersections. If $p \ne q$, then $L_p \cap L_q = \{e\}$. Indeed, the order of the intersection divides both $|L_p|$ and $|L_q|$, hence must be 1.

Step 3: Product decomposition. Let $p_1, \dots, p_n$ be the primes dividing $|L|$. Define

$$\Phi : L_{p_1} \times \cdots \times L_{p_n} \to L, \qquad (x_1, \dots, x_n) \mapsto x_1 \cdots x_n.$$

Using induction on n and the fact that distinct Sylow subloops centralize one another, one verifies that Φ is a homomorphism. Trivial intersections imply injectivity, and cardinality considerations imply surjectivity. Thus L is the internal direct product of its Sylow subloops. □

5. Embedding of Moufang Loops into Groups

The study of finite Moufang loops is greatly facilitated by their realization inside groups. This approach originates in work of Paige and allows one to transfer group-theoretic techniques to the nonassociative setting.

Theorem 5.1 (Paige embedding)**.** *For any finite Moufang loop L, there exists an injective homomorphism $\varphi : L \to G$ into a finite group G that preserves the loop operation.*

Proof. For each $x \in L$, let λ_x denote left multiplication by x. Let F be the free group generated by the set $\{\lambda_x : x \in L\}$. Introduce an abelian group C generated by symbols $c(x, y)$ subject to the relations

$$c(x, y)c(xy, z) = c(y, z)c(x, yz), \qquad c(x, e) = c(e, x) = e.$$

Impose the relations

$$\lambda_x \lambda_y = c(x, y)\lambda_{xy}$$

and the Moufang consistency conditions

$$c(xy, zx) = c(x, (yz)x).$$

Let R be the normal closure of these relations and define

$$U(L) = F/\langle R\rangle.$$

The map $\varphi : L \to U(L)$ given by $\varphi(x) = \lambda_x\langle R\rangle$ is injective and respects multiplication. □

6. Preservation of Normal Sylow Subloops under the Embedding

The Paige embedding allows us to translate loop-theoretic statements about normality and nilpotency into the group-theoretic setting. In this section we record the compatibility of Sylow subloops with the embedding constructed above.

Lemma 6.1. *Let L be a finite Moufang loop and let $\varphi : L \hookrightarrow G$ be the embedding from Theorem 5.1. If $P \leq L$ is a Sylow p-subloop, then $\varphi(P)$ is a Sylow p-subgroup of $\varphi(L)$. If $P \lhd L$, then $\varphi(P) \lhd \varphi(L)$.*

Proof. Since φ is injective, we have $|\varphi(P)| = |P| = p^k$. Moreover $|\varphi(L)| = |L|$, so p^k is the largest power of p dividing $|\varphi(L)|$. Hence $\varphi(P)$ is a Sylow p-subgroup of $\varphi(L)$.

If $P \lhd L$, then for every $x \in L$ we have $xPx^{-1} = P$. Applying φ and using homomorphicity yields

$$\varphi(x)\varphi(P)\varphi(x)^{-1} = \varphi(P),$$

so $\varphi(P)$ is normal in $\varphi(L)$. □

Remark 6.2. Although Moufang loops are not associative, normality is defined via invariance under inner mappings. The embedding intertwines these inner mappings with conjugation in the group, ensuring that normal subloops correspond exactly to normal subgroups inside $\varphi(L)$.

7. A Fitting-Type Theorem for Finite Moufang Loops

We now prove the main structural result of the paper.

Theorem 7.1. *Let L be a finite Moufang loop, and let $H, K \triangleleft L$ be normal nilpotent subloops of nilpotency classes h and k, respectively. Then the product HK is a normal nilpotent subloop of L of class at most $h+k$.*

Proof. Normality of HK was established in Section 3, so it suffices to prove nilpotency and the class bound.

Let $\varphi : L \hookrightarrow G$ be the embedding from Theorem 5.1. By Lemma 6.1, $\varphi(H)$ and $\varphi(K)$ are normal nilpotent subgroups of $\varphi(L)$ of classes at most h and k, respectively. Moreover,

$$\varphi(HK) = \varphi(H)\varphi(K).$$

In group theory one has the standard commutator inclusion

$$\gamma_{r+s}(\varphi(H)\varphi(K)) \subseteq \gamma_r(\varphi(H))\,\gamma_s(\varphi(K)) \qquad (r, s \geq 1).$$

Since $\gamma_{h+1}(\varphi(H)) = \gamma_{k+1}(\varphi(K)) = \{1\}$, it follows that

$$\gamma_{h+k+1}(\varphi(H)\varphi(K)) = \{1\}.$$

Hence $\varphi(H)\varphi(K)$ is nilpotent of class at most $h+k$.

Injectivity of φ implies that the lower central series of HK terminates at the same level, so HK is nilpotent of class at most $h+k$. □

[Fitting subloop] Every finite Moufang loop L possesses a unique largest normal nilpotent subloop, obtained as the product of all normal nilpotent subloops of L.

Proof. Since L is finite, the product of all normal nilpotent subloops stabilizes after finitely many factors. Repeated application of Theorem 7.1 shows that this product is itself nilpotent and normal. □

8. Cryptographic Applications: Two-Sided Moufang Key-Exchange

The structural results established above show that Moufang loops admit large, well-controlled nilpotent subloops and support power-associative exponentiation. These features allow the construction of cryptographic protocols analogous to classical group-based schemes. In this section we describe a one-round Diffie–Hellman–type key exchange operating entirely inside a finite Moufang loop.

8.1. Algebraic preliminaries.

Definition 8.1 (Paige loop)**.** For a prime power q, the *Paige simple Moufang loop* $P(q)$ consists of the unit-norm 2×2 Zorn matrices over $\mathbb{F}_q$. Its order is

$$|P(q)| = \frac{q^3(q^4-1)}{\gcd(q-1,2)} \sim q^7.$$

Definition 8.2 (Left–right translations)**.** Let L be a Moufang loop and let $g, h \in L$ commute. For $(a, b) \in \mathbb{Z}^2$ define

$$\Phi_{a,b}(x) = g^a x h^b.$$

Lemma 8.3. *For all* $(a_1, b_1), (a_2, b_2) \in \mathbb{Z}^2$*,*

$$\Phi_{a_1,b_1} \circ \Phi_{a_2,b_2} = \Phi_{a_1+a_2,b_1+b_2} = \Phi_{a_2,b_2} \circ \Phi_{a_1,b_1}.$$

Proof. Since g and h commute and powers are well-defined,

$$\Phi_{a_1,b_1}(\Phi_{a_2,b_2}(x)) = g^{a_1}(g^{a_2}xh^{b_2})h^{b_1} = g^{a_1+a_2}xh^{b_2+b_1}.$$

□

8.2. **Protocol description.**

Definition 8.4 (Public parameters)**.** A parameter set is a tuple (L, g, h, u) where

- L is a finite Moufang loop;
- $g, h \in L$ commute and have orders divisible by a large prime;
- $u \notin \langle g \rangle \cup \langle h \rangle$.

Definition 8.5 (TS–MKX)**.** Let (L, g, h, u) be public parameters.

Alice chooses (a, b) and publishes

$$A = g^a u h^b.$$

Bob chooses (c, d) and publishes

$$B = g^c u h^d.$$

Alice computes $K_A = g^a B h^b$, and Bob computes $K_B = g^c A h^d$.

Proposition 8.6 (Correctness)**.** *The two computed keys coincide:*

$$K_A = K_B = g^{a+c} u h^{b+d}.$$

Proof. By Lemma 8.3,

$$K_A = \Phi_{a,b}(B) = \Phi_{a,b}(\Phi_{c,d}(u)) = \Phi_{a+c,b+d}(u) = K_B.$$

□

8.3. **Generic security analysis.**

We analyze security in a generic-loop model analogous to the generic-group model.

Definition 8.7 (Protocol oracle)**.** The adversary receives opaque encodings of loop elements. It may query an oracle

$$\mathsf{TRAN}(X, \alpha, \beta) = \phi(g^\alpha \phi^{-1}(X) h^\beta)$$

and test equality of encodings.

Lemma 8.8 (Collision bound)**.** *If an adversary makes at most q oracle queries, the probability of a collision between distinct symbolic triples is at most $q^2/(2R)$, where R is the largest prime dividing* $\mathrm{ord}(g)$ *or* $\mathrm{ord}(h)$*.*

Proof. Each oracle call adds fixed increments to the (g, h)-exponents. Two distinct computation paths collide only if their exponent differences are simultaneously divisible by both orders. At least one large prime divisor must divide both differences, which occurs with probability at most $1/R$. A union bound over $\binom{q}{2}$ pairs yields the stated bound. □

Theorem 8.9 (Generic lower bound)**.** *For any adversary making at most q oracle queries,*

$$(\mathcal{A}) \leq \frac{q^2}{R}.$$

Proof. Conditioned on the absence of collisions, all encodings correspond to distinct symbolic triples and reveal no information about the secret exponents. Thus the adversary's advantage arises only from collision events, which are bounded by Lemma 8.8. □

Remark 8.10. This matches the square-root barrier familiar from Pollard–rho attacks in groups, showing that TS–MKX is generically secure under comparable assumptions.

9. Conclusion

We have established a Fitting-type theorem for finite Moufang loops, showing that the product of normal nilpotent subloops is again nilpotent with an explicit class bound. This result strengthens the structural parallel between groups and Moufang loops and provides a useful reduction tool in the study of finite loops.

As an application, we demonstrated that these structural features support nontrivial cryptographic constructions. The Two-Sided Moufang Key-Exchange protocol generalizes the Diffie–Hellman paradigm to a nonassociative setting while retaining one-round efficiency and provable generic security. This connection suggests further interactions between loop theory, computational hardness assumptions, and cryptographic design.

References

[1] R. H. Bruck, *A Survey of Binary Systems*, Springer, 1958.
[2] L. J. Paige, "A class of simple Moufang loops," *Proc. Amer. Math. Soc.* **7** (1956), 471–482.
[3] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory* **22** (1976), 644–654.
[4] J. M. Pollard, "Monte Carlo methods for index computation (mod p)," *Math. Comp.* **32** (1978), 918–924.
[5] V. Shoup, "Lower bounds for discrete logarithms and related problems," in *Advances in Cryptology—EUROCRYPT '97*, LNCS 1233, Springer, 1997.