Relative multiplication groups and Moufang p-loops

Aleš Drápal

(Joint work with Petr Vojtěchovský)

Charles University in Prague
Czech Republic

June 29, 2023, Będlewo, Wielkopolska
Conference Loops'23

What will be the talk about

Definition of a relative multiplication loop

Q a loop, S a subloop, $\mathrm{Mlt}_Q(S) = \langle L_s, R_t;\ s, t \in S \rangle$.

A theorem that will be proved

Let Q be a finite Moufang loop and $S \le Q$ a p-subloop.
Then $\mathrm{Mlt}_Q(S)$ is a p-group.

Applications of the theorem

(A) A new proof that a Moufang loop of order p^k is centrally nilpotent.
(B) A characterization of $S \trianglelefteq Q$, Q Moufang, such that $\bmod S$ is an abelian congruence.

If time allows

Description of finite Moufang loops Q such that there exists $S \trianglelefteq Q$ abelian, Q/S cyclic, $3 \nmid |Q|$.

Ingredients of the proof that are of general form

Group theory - the Schur-Zassenhaus Theorem

Let G be a finite group with an abelian normal subgroup A. If A and G/A are of coprime orders, then A possesses a complement in G.

The notion of nucleus

Q a loop, $N_\lambda(Q) = \{a \in Q;\ a \cdot xy = ax \cdot y \text{ for all } x, y \in Q\}$ is the *left nucleus*. Shifting a yields the *middle nucleus* $N_\mu(Q)$ and the right nucleus $N_\rho(Q)$. In Moufang loops $\mathrm{Nuc}(Q) = N_\lambda(Q) = N_\mu(Q) = N_\rho(Q)$.

Left companions and pseudoautomorphisms

Let φ permute loop Q. Call φ a *pseudoautomorphism* if $\exists\ c \in Q$, $\forall x, y \in Q\ c\varphi(xy) = c\varphi(x) \cdot \varphi(y)$. Pairs (c, φ) form a group $\mathrm{LPs}(Q)$ with operations $(c, \varphi)(d, \psi) = (c\varphi(d), \varphi\psi)$ and $(c, \varphi)^{-1} = (\varphi^{-1}(c^{-1}), \varphi^{-1})$.
If $(c, \varphi) \in \mathrm{LPs}(Q)$ and $d \in Q$, then

$$(d, \varphi) \in \mathrm{LPs}(Q) \iff d = nc \text{ for some } n \in N_\lambda(Q).$$

Ideas and notions needed for the proof of theorem

Homomorphism $\mathrm{Mlt}_Q(S) \to \mathrm{Mlt}(S)$.

Assume $S \le Q$. All $\psi \in \mathrm{Mlt}_Q(S)$ act upon S. Hence $\psi \to \psi \restriction S$ is a homomorphism $\mathrm{Mlt}_Q(S) \to \mathrm{Mlt}(S)$.
Denote the kernel $\mathrm{Fix}_Q(S) = \{\psi \in \mathrm{Mlt}_Q(S);\ \psi(s) = s \text{ for each } s \in S\}$.

Standard generators of $\mathrm{Inn}_Q(S)$

$\mathrm{Inn}(Q) = \{\varphi \in \mathrm{Mlt}(Q);\ \varphi(1) = 1\}$, the *inner mapping group*.
$\mathrm{Inn}_Q(S) = \mathrm{Mlt}_Q(S) \cap \mathrm{Inn}(Q)$, the *relative inner mapping group*.
Standard generators of $\mathrm{Inn}(Q)$ are $L_{xy}^{-1} L_x L_y$, $R_{yx}^{-1} R_x R_y$, $R_x^{-1} L_x$.
Standard generators of $\mathrm{Inn}_Q(S)$ are $L_{st}^{-1} L_s L_t$, $R_{ts}^{-1} R_s R_t$, $R_s^{-1} L_s$.

Each element of $\mathrm{Inn}_Q(S)$ has a companion in S

Let Q be Moufang. Then $L_x^{-1} = L_{x^{-1}}$, $R_x^{-1} = R_{x^{-1}}$, $L_{xy}^{-1} L_x L_y = [R_x^{-1}, L_y]$, $R_{yx}^{-1} R_x R_y = [L_x^{-1}, R_y]$ and (x^{-3}, T_x), $([x^{-1}, y], [L_x, R_y]) \in \mathrm{LPs}(Q)$.
For each standard generator φ of $\mathrm{Inn}_Q(S)$ there thus exists $c \in S$ such that $(c, \varphi) \in \mathrm{LPs}(Q)$. If $c, d \in S$ and $\varphi \in \mathrm{Inn}_Q(S)$, then $c\varphi(d) \in S$.

The main part of the proof

- The subloop S is assumed to be centrally nilpotent. Hence $\mathrm{Mlt}(S)$ is a p-group. (A classical result of Bruck.) Thus
$$\mathrm{Mlt}_Q(S) \text{ is a } p\text{-group} \iff \mathrm{Fix}_Q(S) \text{ is a } p\text{-group.}$$
- For a pseudoautomorphism φ denote by $C(\varphi)$ the set of all $c \in Q$ such that $(c, \varphi) \in \mathrm{LPs}(Q)$. We know that $C(\varphi)$ is a coset of $\mathrm{Nuc}(Q)$ and that $C(\varphi) \cap S \neq \emptyset$ if $\varphi \in \mathrm{Inn}_Q(S)$. Thus
$$C(\varphi) \subseteq S\,\mathrm{Nuc}(Q) \text{ for each } \varphi \in \mathrm{Inn}_Q(S).$$
- Assume $\varphi, \psi \in \mathrm{Fix}_Q(S)$, $C(\varphi) = c\,\mathrm{Nuc}(Q)$, $C(\psi) = d\,\mathrm{Nuc}(Q)$, where $c, d \in S$. Since $\varphi(d) = d$, $(c, \varphi)(d, \psi) = (cd, \varphi\psi)$. Hence
$$C(\varphi\psi) = C(\varphi)C(\psi) \text{ for all } \varphi, \psi \in \mathrm{Fix}_Q(S).$$
- The image of this homomorphism is a subloop (and a subgroup) of $S\,\mathrm{Nuc}(Q)/\,\mathrm{Nuc}(Q) \cong S/S \cap \mathrm{Nuc}(Q)$, which is necesarilly a p-group. The kernel is equal to $A = \mathrm{Fix}_Q(S) \cap \mathrm{Aut}(Q)$. Thus
$$\mathrm{Mlt}_Q(S) \text{ is a } p\text{-group} \iff A \text{ is a } p\text{-group.}$$
- If $\alpha \in A$ and $s \in S$, then $\alpha L_s \alpha^{-1} = L_{\alpha(s)} = L_s$ since $\alpha \in \mathrm{Fix}_Q(S)$. Similarly $\alpha R_s \alpha^{-1} = R_s$. Hence $A \leq Z(\mathrm{Mlt}_Q(S))$.

Final steps of the proof

- Express A as $B \times D$, where B is p-group and $p \nmid |D|$. This is possible since A is abelian.
- Since $D \leq Z(\mathrm{Mlt}_Q(S))$, $D \trianglelefteq \mathrm{Mlt}_Q(S)$. Since $\mathrm{Mlt}_Q(S)/A$ is a p-group, $\mathrm{Mlt}_Q(S)/D$ is also a p-group.
- By Schur-Zassenhaus theorem there exists $C \leq \mathrm{Mlt}_Q(S)$ such that $\mathrm{Mlt}_Q(S) = CD$, $C \cap D = 1$ and C is a p-group.
- Since $D \leq Z(\mathrm{Mlt}_Q(S))$, the subgroup C is normal in $\mathrm{Mlt}_Q(S)$.
- Both C and D are normal in $\mathrm{Mlt}_Q(S)$. Hence $\mathrm{Mlt}_Q(S) = C \times D$.
- C contains all elements of order p^k since $p \nmid |D|$.
- C contains all L_s and R_t, where $s, t \in S$. These are the generators of $\mathrm{Mlt}_Q(S)$. Hence $C = \mathrm{Mlt}_Q(S)$ and $\mathrm{Mlt}_Q(S)$ is a p-group.

Why a new proof of central nilpotency is needed

The existing proof comes in two parts

Standard sources for the fact that finite Moufang loops of order p^k are centrally nilpotent are:

[GII] G. Glauberman: *On loops of odd order. II.* J. Algebra **8** (1968), 393–414.

[GW] G. Glauberman and C. R. B. Wright: *Nilpotence of finite Moufang 2-loops* J. Algebra **8** (1968), 415–417.

The existing proof depends on many previous results

To extract the proof of central nilpotency from [GII] requires to go through most of the material on B-loops in

[GI] G. Glauberman: *On loops of odd order*, J. Algebra **1** (1964), 374–396.

The proof in [GW] depends upon a less well known part of group theory (Engel elements).

Further comments

Teaching aspects

It is quite annoying that a basic result on Moufang loops is not easily accessible.

Alternative approach

J. I. Hall in *Central automorphisms, Z*-theorems, and loop structure*, Quasigroups Related Systems **19** (2011), 69–108, gives a proof based on Fisher's $\mathbb{Z}^*$-theorem.
In a personal communication Hall recently expressed an opinion that the dependence on Fisher's $\mathbb{Z}^*$-theorem may be removed from his proof.

Outline of the proof

- $|Q| = p^k$ the least counterexample, S the largest subloop of order p^ℓ that is centrally nilpotent. Thus $\ell < k$. $\mathrm{Mlt}_Q(S)$ is a p-group.
- Extend $\mathrm{Mlt}_Q(S)$ to the largest P such that $P \leq \mathrm{Mlt}(Q)$, P is a p-group and P acts upon S.
- Since P cannot be a Sylow subgroup, $\exists\ \widehat{P} \leq \mathrm{Mlt}(Q)$ such that $P \lhd \widehat{P}$ and $|\widehat{P}/P| = p$.
- Denote by $\widehat{S}$ the orbit of $\widehat{P}$ containing S. A structural proof of one page shows that $\widehat{S}$ is a subloop, $S \trianglelefteq \widehat{S}$ and $|\widehat{S}/S| = p$.
- Thus $Q = \widehat{S}$ and $\widehat{P}$ is a Sylow subgroup.
- We have $S \trianglelefteq Q$ and Q/S is of order p. This might seem easy to handle. Nevertheless, I was able to finish the proof only by using computational arguments involving pseudoautomorphisms. The extent is a page and half.
- The arguments give $[L_x, R_y] \in P$ for all $x, y \in Q$. That suffices to conclude.

What does it mean that $\operatorname{mod} X$ is abelian if $X \trianglelefteq Q$ and Q is a Moufang loop

Equivalent conditions—a theorem of D & Vojěchovský

- X is a normal abelian subgroup of a Moufang loop Q.
- $xu \cdot y = x \cdot uy$ whenever $x, y \in X$ and $u \in Q$.
- If $\varphi \in \mathrm{Inn}(Q)$, then $\varphi \restriction X \in \mathrm{Aut}(X)$.

Moral of the story

The congruence theory is not needed to express the notion of $X \trianglelefteq Q$ yielding an abelian congruence. This fact may be expressed in classical terms too. Perhaps a name for this situation that does not refer to congruences might be found. What about *innerly abelian*?

Structure of finite Moufang loops Q such that $3 \nmid |Q|$, $X \trianglelefteq Q$ is abelian, and Q/X is cyclic

The formula on $C \times X$. Applicable when $X \cap C = 1$, C cyclic

$$(b^i, x) \cdot (b^j, y) = \Big(b^{i+j}, g^j(x) + y + \sum_{k \in I(i+j,-j)} g^k(\beta(x,y)) \Big)$$

The meaning of inputs

$$I(i,j) = \begin{cases} \emptyset, & \text{if } i = j, \\ \{i, i+1, \ldots, j-1\}, & \text{if } i < j, \\ \{j, j+1, \ldots, i-1\}, & \text{if } j < i. \end{cases}$$

$g = f^{-3}$, where $\beta(x,y) = f^{-1}(f(x) + f(y)) - x - y$ is biadditive $X \times X \to X$. Furthermore, β is alternating, symmetric (thus $\beta(2x, y) = 0$) and fulfils $\beta(\beta(x,y), z) = 0$ and $\beta(f(x), f(y)) = f(\beta(f^3(x), y))$.

The general case ($X \cap C \neq 1$)

The same formula, but writing $b^i x$ in place (b^i, x). This is because such a situation is always a homomorphic image of a semidirect product.