PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 139, Number 1, January 2011, Pages 93–98
S 0002-9939(2010)10501-4
Article electronically published on July 21, 2010

A SIMPLIFIED PROOF OF MOUFANG'S THEOREM

ALEŠ DRÁPAL

(Communicated by Jonathan I. Hall)

Abstract. Moufang's theorem states that if Q is a Moufang loop with elements x, y and z such that $x \cdot yz = xy \cdot z$, then these three elements generate a subgroup of Q. The paper contains a new proof of this theorem that is shorter and more transparent than the standardly used proof of Bruck.

A loop is a binary structure with a unit such that the equations

$$ax = b \qquad \text{and} \qquad ya = b$$

have unique solutions $x = a\backslash b$ and $y = b/a$. The inverses $x\backslash 1$ and $1/x$ may differ, but if they agree, we denote them by x^{-1}.

A loop is called *Moufang* if it satisfies the three equivalent identities

$$x(y \cdot xz) = (xy \cdot x)z, \quad (zx \cdot y)x = z(x \cdot yx) \text{ and } xy \cdot zx = x(yz \cdot x).$$

At the very foundations of Moufang loop theory there is a theorem that states that if x, y and z associate, then they generate a subgroup. This statement is called *Moufang's theorem*. The standardly used proof of Bruck is a bit of an obstacle to anybody who wishes to learn more about Moufang loops. The problem is not really the length, but rather the technicality, which makes it hard to identify the principles that are behind the proof.

The purpose of this note is to show that Moufang's theorem can be proved straightforwardly with clearly separated ingredients. Facts needed for the proof can be classified as (1) general properties of autotopisms in Moufang loops, (2) relationships between inner mappings that allow a circular shift of an associative triple and (3) a combinatorial observation that in a nonempty word over letters a, b and c, either one of the terminal symbols is in $\{b, c\}$ or both terminal symbols are equal to a. All these ingredients are present in a varying degree of explicitness in Bruck's proof. The proof presented here only organizes them in a different way. Technically, Lemma 4 and the proof of Proposition 1 are new. Everything else, the proofs included, is well known and appears just for the sake of completeness.

Following a suggestion of the referee, the equivalence of the three Moufang identities is proved at the end of the paper (Proposition 2), as a kind of appendix.

Permutations $R_x : y \mapsto yx$ and $L_x : y \mapsto xy$ of a loop Q are known as the *right* and *left translations* of x, respectively. A loop Q is called *left alternative* if $x \cdot xy = xx \cdot y$ for all $x, y \in Q$. *Right alternative* loops satisfy $yx \cdot x = y \cdot xx$, and

Received by the editors December 31, 2009 and, in revised form, March 12, 2010.
2010 *Mathematics Subject Classification.* Primary 20N05; Secondary 08A05.
Key words and phrases. Moufang loops, Moufang's theorem.
The author was supported by the Grant Agency of Czech Republic, grant 201/09/0296.

flexible loops fulfil the law $x \cdot yx = xy \cdot x$. A loop Q satisfies the *inverse property* if $1/x = x\backslash 1 = x^{-1}$, $x^{-1} \cdot xy = y$ and $yx \cdot x^{-1} = y$ for all $x, y \in Q$. An inverse property loop (i.e., an *IP loop*) fulfils not only $(x^{-1})^{-1} = x$ but also $(xy)^{-1} = y^{-1}x^{-1}$. The latter identity follows from

$$x = xy \cdot y^{-1} \quad \Leftrightarrow \quad (xy)^{-1}x = y^{-1} \quad \Leftrightarrow \quad (xy)^{-1} = y^{-1}x^{-1}.$$

Note that inverse property loops satisfy $R_x^{-1} = R_{x^{-1}}$ and $L_{x^{-1}} = L_x^{-1}$.

Lemma 1. *Each Moufang loop is both left and right alternative. It is also flexible and satisfies the inverse property.*

Proof. The alternativity and flexibility follow immediately from the three equivalent Moufang identities by putting $y = 1$. Setting $y = x\backslash 1$ in the first of them and $y = 1/x$ in the second yields $x((x\backslash 1) \cdot xz) = xz$ and $(zx \cdot (1/x))x = zx$. Thus $(x\backslash 1) \cdot xz = z$ and $zx \cdot (1/x) = z$ for all $x, z \in Q$. By setting $z = 1$ we get $(x\backslash 1)x = 1$, and so $1/x = x\backslash 1$. □

A triple (α, β, γ) of permutations of Q is said to be an *autotopism* if $\alpha(x)\beta(y) = \gamma(xy)$ for all $x, y \in Q$. Suppose that $\alpha(1) = 1$. It is then clear that $\beta = \gamma = R_b\alpha$, where $b = \beta(1)$, and that $\alpha(x) \cdot \alpha(y)b = \alpha(xy)b$ for all $x, y \in Q$. In such a situation it is usually said that α is a *left pseudoautomorphism with companion* b, but we shall not use that terminology here. Autotopisms are closed under compositions and inverses, and so they form a group.

Lemma 2. *Let (α, β, γ) be an autotopism of an inverse property loop Q. Suppose that $\alpha(1) = 1$ and that $\alpha(x) = x$ for some $x \in Q$. Then $\alpha(x^{-1}) = x^{-1}$ as well.*

Proof. Put $b = \beta(1)$. The identity $\alpha(x)\beta(x^{-1}) = \gamma(1)$ gives $x \cdot \alpha(x^{-1})b = b$, from which we derive $\alpha(x^{-1})b = x^{-1}b$. □

Lemma 3. *Let Q be a Moufang loop with an autotopism (α, β, γ) such that $\alpha(1) = 1$. If $x, y \in Q$ are such that $\alpha(x) = x$ and $\alpha(y) = y$, then $\alpha(xyx) = xyx$.*

Proof. Put $b = \beta(1)$. We have $\alpha(xy \cdot x) = (\alpha(xy) \cdot \alpha(x)b)b^{-1} = (((x \cdot yb)b^{-1})xb)b^{-1} = (x \cdot yb)(b^{-1} \cdot xb \cdot b^{-1}) = (x \cdot yb)(b^{-1}x) = x(yb \cdot b^{-1})x = xyx$. Note that we have used a Moufang identity twice. □

Let Q be a Moufang loop. We say that $X \subseteq Q$ *generates* Q if there is no proper subloop of Q that contains X. Clearly, X generates Q if and only if each $u \in Q$ can be expressed as a term over X that uses multiplication and inverses. Because of the inverse property, each element of Q is then equal to a multiplicative term over $X^{\pm} = \{x, x^{-1};\ x \in X\}$. We shall give notation to some of these terms. Let us define $s = \ell(u_1, \ldots, u_k)$ so that $s = 1$ if $k = 0$, and $s = u_1\ell(u_2, \ldots, u_k)$ if $k \geq 1$. Similarly, $r(u_1, \ldots, u_k)$ equals 1 if $k = 0$ and is equal to $r(u_1, \ldots, u_{k-1})u_k$ if $k \geq 1$.

Lemma 4. *Let Q be a Moufang loop generated by a set X such that $\ell(x_1, \ldots, x_k) = r(x_1, \ldots, x_k)$ for all finite sequences $x_1, \ldots, x_k$ over $X^{\pm}$. Then Q is a group.*

Proof. First we shall prove, by induction on n, that

$$\ell(u_1, \ldots, u_n) \cdot \ell(v_1, \ldots, v_m) = \ell(u_1, \ldots, u_n, v_1, \ldots, v_m)$$

for all $u_1, \ldots, u_n \in X^{\pm}$ and $v_1, \ldots, v_m \in X^{\pm}$. The case $n \leq 1$ is clearly true. Assume $n \geq 2$, and put $x = u_1$, $s = \ell(u_2, \ldots, u_n)$ and $t = \ell(v_1, \ldots, v_m)$.

Express $xs \cdot t$ as $xs \cdot (tx^{-1} \cdot x) = x(s \cdot tx^{-1})x$. Now, $tx^{-1} = r(v_1, \dots, v_m)x^{-1} = r(v_1, \dots, v_m, x^{-1}) = \ell(v_1, \dots, v_m, x^{-1})$, and so, by the induction assumption,

$$\begin{aligned} xs \cdot t &= x(s \cdot tx^{-1})x = x(s\ell(v_1, \dots, v_m, x^{-1}))x \\ &= x\ell(u_2, \dots, u_n, v_1, \dots, v_m, x^{-1})x = x(r(u_2, \dots, u_n, v_1, \dots, v_m)x^{-1})x \\ &= x\ell(u_2, \dots, u_n, v_1, \dots, v_m) = \ell(u_1, u_2, \dots, u_n, v_1, \dots, v_m). \end{aligned}$$

Set $a = \ell(u_1, \dots, u_n)$, $b = \ell(v_1, \dots, v_m)$ and $c = \ell(w_1, \dots, w_p)$. The proved equality makes clear that both $a \cdot bc$ and $ab \cdot c$ are equal to

$$\ell(u_1, \dots, u_n, v_1, \dots, v_m, w_1, \dots, w_p).$$

Hence $S = \{\ell(u_1, \dots, u_n);\ u_1, \dots, u_n \in X^{\pm}\}$ is a subsemigroup of Q that is generated by $X^{\pm}$. The semigroup S is a group since all generating elements possess inverses. Therefore $S = Q$. □

Lemma 5. *Let x and y be elements of a Moufang loop Q. Then $L_{xy}^{-1}L_xL_y = [R_x^{-1}, L_y]$ and $R_{yx}^{-1}R_xR_y = [L_x^{-1}, R_y]$.*

Proof. First observe that $L_{xy}^{-1}L_xL_y = [R_x^{-1}, L_y]$ is equivalent to $L_xR_xL_y = L_{xy}R_x$, which is an expression of the Moufang law $x(yz \cdot x) = xy \cdot zx$. The other identity of the statement can be obtained by a mirror argument. □

Lemma 6. *Let Q be a Moufang loop. Suppose that $\alpha = [R_x, L_y]^{\pm 1}$ where $x, y \in Q$ or that $\alpha = L_{x_1}^{\varepsilon_1} \dots L_{x_n}^{\varepsilon_n}$ where $x_1, \dots, x_n \in Q$ and $\varepsilon_1, \dots, \varepsilon_n \in \{-1, 1\}$. Then there exist β and γ such that (α, β, γ) is an autotopism of Q.*

Proof. We have $R_x = R_{x^{-1}}^{-1}$, and hence by Lemma 5 it suffices to prove the statement only for the case $\alpha = L_{x_1}^{\varepsilon_1} \dots L_{x_n}^{\varepsilon_n}$. The Moufang identity $xy \cdot zx = x(yz \cdot x)$ states that (L_x, R_x, L_xR_x) is an autotopism for every $x \in Q$. The sought autotopism (α, β, γ) can thus be obtained as the composition of autotopisms $(L_{x_i}, R_{x_i}, L_{x_i}R_{x_i})^{\varepsilon_i}$, $1 \le i \le n$. □

Lemma 7. *Let x_1, x_2, x_3 be elements of a Moufang loop Q. If $x_1 \cdot x_2x_3 = x_1x_2 \cdot x_3$, then*

$$x_{\sigma(1)}^{\varepsilon_1} \cdot x_{\sigma(2)}^{\varepsilon_2}x_{\sigma(3)}^{\varepsilon_3} = x_{\sigma(1)}^{\varepsilon_1}x_{\sigma(2)}^{\varepsilon_2} \cdot x_{\sigma(3)}^{\varepsilon_3}$$

for all permutations $\sigma \in S_3$ and all $\varepsilon_i \in \{-1, 1\}$, $i \in \{1, 2, 3\}$. Furthermore, $x_1 \cdot x_2x_3$ is equal to $x_1x_2 \cdot x_3$ whenever $x_i = x_j$, $1 \le i < j \le 3$.

Proof. The latter claim follows from Lemma 1. Let us assume that Q is generated by $x = x_1$, $y = x_2$ and $z = x_3$ and that $x \cdot yz = xy \cdot z$. By Lemmas 5 and 6 any of the mappings $L_{xy}^{-1}L_xL_y$, $R_{yz}^{-1}R_zR_y$ and $[R_x, L_z]$ can be put into the position of α in Lemma 2. Therefore $x \cdot yz^{-1} = xy \cdot z^{-1}$, $x^{-1} \cdot yz = x^{-1}y \cdot z$ and $x \cdot y^{-1}z = xy^{-1} \cdot z$, respectively. We see that if the equality of the lemma holds for a given σ and ε_i, $1 \le i \le 3$, then it holds for the permutation σ with any $\varepsilon_i' \in \{-1, 1\}$. Hence it suffices to show that the equality is true for any two permutations σ that generate S_3, irrespective of the signs ε_i. The identity $L_{xy}^{-1}L_xL_y = [R_x^{-1}, L_y]$ of Lemma 5 means that $x \cdot yz = xy \cdot z$ implies $y \cdot zx^{-1} = yz \cdot x^{-1}$. That provides a cyclic shift. The inverse property yields $z^{-1}y^{-1} \cdot x^{-1} = z^{-1} \cdot y^{-1}x^{-1}$, and that gives us a transposition. □

The referee has remarked that if the proof is explained in terms of the signed symmetric group of all $(\sigma;\varepsilon_1,\varepsilon_2,\varepsilon_3)$ instead of using only the symmetric group S_3, then it suffices to verify just one sign change.

Proposition 1. *Let Q be a Moufang loop generated by $X=\{x,y,z\}$. If $x\cdot yz = xy\cdot z$, then $u_0\cdot\ell(u_1,\dots,u_k)u_{k+1} = u_0\ell(u_1,\dots,u_k)\cdot u_{k+1}$ and $\ell(u_0,\dots,u_{k+1}) = r(u_0,\dots,u_{k+1})$ for any sequence $u_0,\dots,u_{k+1}$ of elements of $X^{\pm}$, $k\geq 1$.*

Proof. There are two equalities to be proved. We shall proceed by a common induction on k. The case $k=1$ follows from the assumption and from Lemma 7. In the induction step we shall first consider the equality

$$u_0\cdot\ell(u_1,\dots,u_k)u_{k+1} = u_0\ell(u_1,\dots,u_k)\cdot u_{k+1}.$$

The case $u_0 = u_{k+1}^{\pm 1}$ follows from Lemma 7. We can thus assume that, say, $u_0 = x$ and $u_{k+1} = y$.

Put $s=\ell(u_2,\dots,u_k)$. We wish to prove that $x(u_1s\cdot y) = (x\cdot u_1s)y$. If $u_1 = x^{-1}$, then this is equivalent to $x^{-1}s\cdot y = x^{-1}\cdot sy$, and that holds by the induction assumption. By exchanging x and x^{-1} we get $x^{-1}(xs\cdot y) = (x^{-1}\cdot xs)y$. Thus $x(xs\cdot y) = (x\cdot xs)y$, by Lemma 7. We have solved the case $u_1 = x^{\pm 1}$. The situation is left-right symmetric since $\ell(u_1,\dots,u_k) = r(u_1,\dots,u_k)$ by the induction assumption. The case $u_k = y^{\pm 1}$ can thus be obtained by mirror reasoning.

By the induction assumption, $xs\cdot y = x\cdot sy$. Therefore $xy\cdot s = x\cdot ys$ by Lemma 7, and $(x\cdot ys)y = (xy\cdot s)y = x(ys\cdot y)$ by the second Moufang law. This gives us the case $u_1 = y$. By Lemma 7, $(x\cdot ys)y^{-1} = x(ys\cdot y^{-1})$, and so $(x\cdot y^{-1}s)y = x(y^{-1}s\cdot y)$. We have settled the case $u_1 = y^{\pm 1}$. The mirror argument provides for $u_k = x^{\pm 1}$.

In the remaining cases there must be $u_1 = z^{\pm 1}$ and $u_k = z^{\pm 1}$. It will suffice to consider the case $u_1 = u_k = z$ and the case $u_1 = z$ and $u_k = z^{-1}$. Put $w = \ell(u_2,\dots,u_{k-1})$.

In the former case we need to show that $x(zwz)\cdot y = x\cdot(zwz)y$, i.e. that $[L_x,R_y](zwz) = zwz$. The induction assumption yields $[L_x,R_y](w) = w$. We have $[L_x,R_y](1) = 1$, and so $[L_x,R_y](zwz) = zwz$ by Lemmas 3 and 6.

For the latter case we need to show that $x(zwz^{-1})\cdot y = x\cdot(zwz^{-1})y$, i.e. that $\alpha(z^{-1}) = z^{-1}$ where $\alpha = L_w^{-1}L_z^{-1}[R_y,L_x]L_zL_w$. By the induction assumption, $x(zw\cdot y) = (x\cdot zw)y$. Hence $\alpha(1) = 1$. The already-proved equality $x(zwz)\cdot y = x\cdot(zwz)y$ can be expressed as $\alpha(z) = z$. By Lemma 6 there exist β and γ such that (α,β,γ) is an autotopism of Q. The sought equality thus follows from $\alpha(1) = 1$ and $\alpha(z) = z$ by Lemma 2.

To finish the induction step observe that $\ell(u_0,\dots,u_{k+1}) = u_0\ell(u_1,\dots,u_{k+1}) = u_0r(u_1,\dots,u_{k+1}) = u_0\cdot r(u_1,\dots,u_k)u_{k+1}$ is equal to $u_0\ell(u_1,\dots,u_k)\cdot u_{k+1} = \ell(u_0,u_1,\dots u_k)u_{k+1} = r(u_0,\dots,u_k)u_{k+1} = r(u_0,\dots,u_{k+1})$. □

Moufang's Theorem. *Let x, y and z be elements of a Moufang loop Q. If $x\cdot yz = xy\cdot z$, then x, y and z generate a subgroup of Q.*

Proof. This is a direct consequence of Lemma 4 and Proposition 1. □

The original proof of Ruth Moufang went by a complicated direct induction and fills about eight pages of her classical paper [8]. When Richard Bruck was writing his seminal paper [3] he obviously tried to concentrate there all the important facts about loops that were known at that time. One can conjecture that he was unsatisfied with the only available proof of the Moufang's theorem and that he

hoped to obtain a better proof. A reference to [8] is one of the very few instances where [3] is not self-contained. This conjecture is corroborated by Bruck's paper [4] in which he provided a short proof of Moufang's theorem in the case of commutative Moufang loops. He finally succeeded in obtaining in [5] a proof that utilizes the concept of pseudoautomorphisms in an efficient way. That proof was more or less faithfully reproduced in all three existing loop theory textbooks [6, 1, 9].

Let us now turn to the equivalence of the three loop identities that bear the name of Ruth Moufang. She did not know that they are equivalent when writing [8]; that was established by Geritt Bol [2]. Bruck developed another proof when composing [3], and that is the standard proof that got into the textbooks [6, 1, 9]. Recently, a shorter and more direct proof was discovered [7]:

Lemma 8. *Let Q be an IP loop. Denote the mapping $x \to x^{-1}$ by I and suppose that α, β and γ are permutations of Q. If any of the triples (α, β, γ), $(I\gamma I, \alpha, I\beta I)$ and $(\beta, I\gamma I, I\alpha I)$ is an autotopism of Q, then all three triples are autotopisms.*

Proof. If (α, β, γ) is an autotopism, then $\alpha(x) \cdot \beta(y) = \gamma(xy)$ for all $x, y \in Q$. Thus $\alpha(x) \cdot \beta((yx)^{-1}) = \gamma(y^{-1})$, $\alpha(x) = \gamma(y^{-1}) \cdot \beta((yx)^{-1})^{-1}$ and $\gamma(y^{-1})^{-1} \cdot \alpha(x) = \beta((yx)^{-1})^{-1}$. We see that $(I\gamma I, \alpha, I\beta I)$ is an autotopism. Let us call it the I-shift of (α, β, γ). Since I^2 is the identity, the two additional I-shifts are $(\beta, I\gamma I, I\alpha I)$ and (α, β, γ). The three triples of the lemma are equivalent because starting from any of them the other two can be obtained by applying the I-shifts. □

Lemma 9. *Let Q be an IP loop with an element x. Then (L_x, R_x, R_xL_x) is an autotopism of Q if and only if (R_xL_x, L_x^{-1}, L_x) is an autotopism. Similarly, (L_x, R_x, L_xR_x) is an autotopism if and only if (R_x^{-1}, L_xR_x, R_x) is an autotopism.*

Proof. We have $IL_xI = R_x^{-1}$ and $IR_xI = L_x^{-1}$ in every IP loop Q. The statement thus follows from Lemma 8 since $(IR_xL_xI, L_x, IR_xI)^{-1} = (L_x^{-1}R_x^{-1}, L_x, L_x^{-1})^{-1} = (R_xL_x, L_x^{-1}, L_x)$ and $(R_x, IL_xR_xI, IL_xI)^{-1} = (R_x^{-1}, L_xR_x, R_x)$. □

Proposition 2. *If a loop satisfies any of the identities*

$$(1)\ x(y \cdot xz) = (xy \cdot x)z, \quad (2)\ (zx \cdot y)x = z(x \cdot yx) \ \text{ and } \ (3)\ xy \cdot zx = x(yz \cdot x),$$

then it satisfies all of them.

Proof. By plugging $z = 1$ in (3) we get the flexible law. Hence (3) is equivalent to (4) $xy \cdot zx = (x \cdot yz)x$. Replacing z by $x\backslash z$ in (1) yields (1′) $x \cdot yz = (xy \cdot x)(x\backslash z)$. Similarly, (2) is equivalent to (2′) $zy \cdot x = (z/x)(x \cdot yx)$. These identities can be expressed by saying that the triple (1′) (R_xL_x, L_x^{-1}, L_x), (2′) (R_x^{-1}, L_xR_x, R_x), (3) (L_x, R_x, L_xR_x) along with (4) (L_x, R_x, R_xL_x) is an autotopism for each $x \in Q$, respectively. By Lemma 9 it remains to show that each of the identities (1), (2) and (3) implies the inverse property (cf. Lemma 1).

We are thus required to demonstrate that for all $a \in Q$ there exist $b, c \in Q$ such that $b \cdot ax = x$ and $xa \cdot c = x$ for every $x \in Q$. (Then $b = a\backslash 1 = 1/a$ as $a\backslash 1 = b(a \cdot (a\backslash 1))$ and $ba = 1$. Similarly $c = a\backslash 1 = 1/a$.) Now, (1) yields $x((x\backslash 1) \cdot xz) = xz$ and $xy = (xy \cdot x)(x\backslash 1)$, while for (3) and (4) we get, by cancelling x, that $y = y(1/x) \cdot x$ and $z = x \cdot (x\backslash 1)z$. To finish, it suffices to observe that (2) mirrors (1). □

Acknowledgment

The referee suggested expanding the proof at several spots, arguing that an elementary proof deserves an elementary exposition. I thank the referee for all suggestions and for the careful reading.

References

[1] V. D. Belousov, *Osnovy teorii kvazigrupp i lup*, Nauka, Moskva, 1967. MR0218483 (36:1569)
[2] G. Bol, Gewebe und gruppen, *Math. Ann.* **114** (1937), 414–431. MR1513147
[3] R. H. Bruck, Contributions to the theory of loops, *Trans. Amer. Math. Soc.* **60** (1946), 245–354. MR0017288 (8:134b)
[4] R. H. Bruck, On a theorem of R. Moufang, *Proc. Amer. Math. Soc.* **2** (1951), 144–145. MR0041839 (13:9b)
[5] R. H. Bruck, Pseudo-automorphisms and Moufang loops, *Proc. Amer. Math. Soc.* **3** (1952), 66–72. MR0047635 (13:905f)
[6] R. H. Bruck, *A survey of binary systems.* Springer Verlag, Berlin-Göttingen-Heidelberg, 1958. MR0093552 (20:76)
[7] A. Drápal and P. Jedlička, On loop identities that can be obtained by a nuclear identification, *Europ. J. Comb.* (in press). http://dx.doi.org/10.1016/j.ejc.2010.01.007.
[8] R. Moufang, Zur Struktur von Alternativkörpern, *Math. Ann.* **110** (1935), 416–430. MR1512948
[9] H. O. Pflugfelder, *Quasigroups and loops. Introduction.* Heldermann Verlag, Berlin, 1990. MR1125767 (93g:20132)

Department of Mathematics, Charles University, Sokolovská 83, 186 75 Praha 8, Czech Republic

E-mail address: drapal@karlin.mff.cuni.cz