Math. Proc. Camb. Phil. Soc. (1976), **80**, 37
MPCPS 80–3
Printed in Great Britain

Finite distributive quasigroups

By J. D. H. SMITH

Department of Pure Mathematics and Mathematical Statistics, University of Cambridge

(*Received* 27 *June* 1975, *revised* 14 *October* 1975)

Abstract. The Bruck–Slaby theorem on nilpotence of commutative Moufang loops may be combined with a theorem of Belousov to give a quick elementary proof of a stronger version of Fischer's Theorem on the solubility of right multiplication groups of finite distributive quasigroups.

A *quasigroup* $(Q, .)$ is a set Q with binary multiplication, such that in the equation $x.y = z$ (also written $xy = z$) knowledge of any two of x, y, z specifies the third uniquely. The permutations $R(x)$: $Q \to Q$; $y \mapsto yx$ and $L(x)$: $Q \to Q$; $y \mapsto xy$ are known as *right* and *left multiplication* respectively. The *right multiplication group* $RMlt(Q, .)$ of $(Q, .)$ is the subgroup of the permutation group on Q generated by $\{R(x) | x \in Q\}$. The quasigroup $(Q, .)$ is said to be *right distributive* if it satisfies the law $(xy)z = (xz)(yz)$, and *left distributive* if $x(yz) = (xy)(xz)$ holds. If both these laws are satisfied, $(Q, .)$ is called a *distributive quasigroup*.

The deepest theorem about distributive quasigroups is the following result of Fischer:

Fischer's Theorem [(3), Satz 4·2]. *If* $(Q, .)$ *is a finite distributive quasigroup, then* $RMlt(Q, .)$ *is a soluble group.*

Fischer's proof of this theorem depends on a group-theoretic lemma:

Proposition 1. *Let* G *be a finite group generated by a conjugacy class* Q *of involutions, such that for all* x, y *in* Q, *the product* xy *has order* 3. *Then the derived group* G' *is nilpotent.*

Fischer in fact proves a generalization, in which the product xy has p-power order for a given odd prime p [(3), Satz 4·1]. His proof involves the Feit–Thompson theorem on solubility of groups of odd order and the Brauer–Suzuki theorem that there are no finite simple groups with generalized quaternion Sylow 2-subgroups. Glauberman [(4), note on page 390] has given an alternative proof of Fischer's Satz 4·1 avoiding the Feit–Thompson theorem, but still requiring the Brauer–Suzuki theorem and 20 pages of hard work. Fischer's application of Proposition 1 to prove the theorem requires Thompson's theorem about the nilpotency of Frobenius kernels as well as 30 pages of non-associative algebra. The purpose of this note is to point out, as appears not to have been done before, that Fischer's Theorem can be proved with no more than 30 pages of non-associative algebra, avoiding all the heavy group theory. Proposition 1 will then appear as a corollary to the theorem, not as a lemma for its proof, thus reversing the

https://doi.org/10.1017/S0305004100052634 Published online by Cambridge University Press

logical direction of Fischer's paper. This is remarkable for being the first case in which a substantial group-theoretic result has its simplest proof in non-associative algebra.

Let $(Q, .)$ be a distributive quasigroup. Each element x of Q is idempotent under $.$ (for $(xx)(xx) = x(xx) \Rightarrow xx = x$); fix a particular one e, say. Let $L = L(e)$, $R = R(e)$. Define an operation $+$ on Q by $x+y = xR^{-1}.yL^{-1}$. Then $(Q, +, e)$ is a *loop*, i.e. a quasigroup $(Q, +)$ with an element e such that for all x in Q, $x+e = x = e+x$. The loop $(Q, +, e)$ is said to be a *Moufang loop* if it satisfies the identity

$$(x+y)+(z+x) = (x+(y+z))+x.$$

There is a connexion between distributive quasigroups and Moufang loops due to Belousov:

BELOUSOV'S THEOREM [(1), *Teorema* 1]. *If $(Q, .)$ is a distributive quasigroup, then $(Q, +, e)$ is a commutative Moufang loop.*

In the context of Belousov's Theorem one can make the following observation:

PROPOSITION 2. *$RMlt(Q, +, e)$ is the derived group of $RMlt(Q, .)$.*

Proof. Let $G = RMlt(Q, .)$, $H = RMlt(Q, +, e)$. If a, b, c are elements of Q,

$$(ab)(cb) = (ac)b$$

by right distributivity. Thus

$$R(b)R(cb) = R(c)R(b). \qquad (*)$$

For x in Q, let $R_+(x)$ denote right multiplication by x in the loop $(Q, +, e)$. If $y \in Q$,

$$yR_+(x) = y+x = yR^{-1}.xL^{-1} \quad \text{so that} \quad R_+(x) = R^{-1}R(xL^{-1}).$$

Putting $b = xL^{-2}$, $c = e$ in (*),

$$R(xL^{-2})R(xL^{-1}) = RR(xL^{-2}).$$

Thus $\quad R_+(x) = R^{-1}R(xL^{-1}) = R^{-1}R(xL^{-2})^{-1}RR(xL^{-2}) = [R, R(xL^{-2})] \in G'.$

Since H is generated by all such $R_+(x)$, $H \leqslant G'$.

Conversely, any commutator $\gamma = \alpha^{-1}\beta^{-1}\alpha\beta$ in G can be written as a product of an equal number of terms $R(x_i)^{-1}$ and $R(y_i)$ with the x_i and y_i in Q, since both α and β are products of terms of this sort. Rearranging (*) with $b = x$, $c = y$ or $b = x$, $c = yR(x)^{-1}$ respectively gives

$$R(x)^{-1}R(y) = R(yx)R(x)^{-1}$$

or

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

so that the terms $R(x_i)^{-1}$ may be shifted past the terms $R(y_i)$ either to the right or to the left at the mere cost of changing the y_i. Thus γ may be rewritten as a product of terms $R(x_i)^{-1}R(z_i)$ for some z_i in Q. But

$$R(x)^{-1}R(z) = (R^{-1}R(x))^{-1}R^{-1}R(z) = R_+(ex)^{-1}R_+(ez) \in H,$$

so every commutator γ is in H, whence $G' \leqslant H$.

Commutative Moufang loops have been studied in detail by Bruck and Slaby. The *centre* of a commutative Moufang loop $(Q, +, e)$ is

$$Z(Q, +, e) = \{z \in Q \mid \forall x, y \in Q, \quad x+(y+z) = (x+y)+z\}.$$

https://doi.org/10.1017/S0305004100052634 Published online by Cambridge University Press

It is a normal subloop of $(Q, +, e)$, i.e. its cosets form a loop $Q/Z(Q)$. Inductively defining $Z_i(Q)$ by $Z_0(Q) = \{e\}$ and

$$Z_i(Q)/Z_{i-1}(Q) = Z(Q/Z_{i-1}(Q)),$$

a loop Q is said to be *nilpotent* if there is a positive integer c such that $Z_c(Q) = Q$. In thirty pages of complicated but 'bare hands' non-associative algebra, Bruck proved the following theorem formulated and partially proved by Slaby:

BRUCK–SLABY THEOREM. *A finite commutative Moufang loop $(Q, +, e)$ is the direct product of an abelian group A of order prime to 3 and a nilpotent commutative loop L of 3-power order.*

Bruck [(2), chapter VIII and pages 101–102] indeed proves rather more, but that is not needed here. The close connections between the Bruck–Slaby Theorem and Fischer's work are emphasized by the fact that Manin [(6), Teoremy 1·6, 1·7] [(7), Theorems 1·8, 1·9] and Glauberman [(5), Corollary to Theorem 4] both give essentially group-theoretic proofs of the Bruck–Slaby Theorem. Manin applies Proposition 1 (with an appropriately streamlined version of Fischer's proof). Glauberman's proof uses results from (4) and the Brauer–Suzuki theorem, but avoids the Feit–Thompson theorem.

Combining Belousov's Theorem with the Bruck–Slaby Theorem gives the following quick proof of Fischer's Theorem, in a slightly strengthened version. If $(Q, .)$ is a finite distributive quasigroup, then by Belousov's Theorem $(Q, +, e)$ is a commutative Moufang loop. By the Bruck–Slaby Theorem, $(Q, +, e)$ is the direct product of an abelian group A of order prime to 3 and a nilpotent commutative Moufang loop L of 3-power order. Thus

$$RMlt(Q, +, e) \cong RMlt(A) \times RMlt(L).$$

By Proposition 2, $RMlt(Q, +, e)$ is the derived group of $RMlt(Q, .)$. But by Cayley's Theorem on right regular representations $RMlt(A) \cong A$, and by a result of Bruck [(2), Lemma VI. 2.2] $RMlt(L)$ is of 3-power order. Putting all this together, one has the

THEOREM. *If $(Q, .)$ is a finite distributive quasigroup, then the derived group of the right multiplication group of $(Q, .)$ is the direct product of an abelian group of order prime to 3 with a group of 3-power order. In particular, the derived group is nilpotent.*

With this theorem proved, the group-theoretical Proposition 1 follows as a corollary of:

PROPOSITION 3. *Let G be a group generated by a finite conjugacy class Q of involutions such that for all x, y in Q the product xy has odd order. Define an operation $\circ$ on Q by $x \circ y = yxy$. Then $(Q, \circ)$ is a right distributive quasigroup and $RMlt(Q, \circ) \cong G/Z(G)$.*

Proof. Since Q is a conjugacy class of involutions, it is closed under $\circ$. Let x, y, z denote elements of Q. If $x \circ y = z \circ y$, clearly $x = z$. If $x \circ y = x \circ z$, $(xy)^2 = (xz)^2$. Let xy, xz have orders $2r+1, 2s+1$ respectively. Then

$$(xy)^{(2r+1)(2s+1)} = 1 = (xz)^{(2r+1)(2s+1)},$$

https://doi.org/10.1017/S0305004100052634 Published online by Cambridge University Press

whence $xy = xz$ and $y = z$. Thus $(Q, \circ)$ is a quasigroup. It is right distributive since

$$(x \circ z) \circ (y \circ z) = zyzzxzzyz = zyxyz = (x \circ y) \circ z.$$

Define a mapping ϕ from G to the permutation group on Q by $g\phi$: $y \mapsto g^{-1}yg$ for all y, g in G. ϕ is a group morphism, and $G\phi \cong G/Z(G)$. Any g in G can be expressed as a product $g = x_1 \dots x_n$ with x_i in Q, and then $g\phi = R_0(x_1) \dots R_0(x_n)$. Thus $G\phi = RMlt(Q, \circ)$, and the result follows.

COROLLARY. (Proposition 1). *If, in the situation of Proposition* 3, $(xy)^3 = 1$ *for* x, y *in* Q, *then* $(Q, \circ)$ *is distributive and* G' *is nilpotent.*

Proof. From $(xy)^3 = 1$, it follows that $x \circ y = yxy = xyx = y \circ x$, so that $(Q, \circ)$ is commutative, and hence left as well as right distributive. By the main theorem $(RMlt(Q, \circ))'$ is nilpotent. By Proposition 3, this means that $G/Z(G)$ is nilpotent, and so G' is also.

Unfortunately the method of proof of the Corollary does not extend to cover the more general case of Fischer's Satz 4.1 in which the product xy has p-power order other than 3, since the quasigroup $(Q, \circ)$ of Proposition 3 need not be distributive:

Example. Let $(V, +)$ be a vector space of dimension 3 over the field of odd prime order p, and let a be the automorphism of V with matrix

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

with respect to a given basis of V. Let t be the involution of V with matrix

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & -1 \end{bmatrix}$$

with respect to the same basis. Let G be the subgroup of the group of permutations of V generated by $\{a, t\} \cup RMlt(V, +)$. Let Q be the conjugacy class of G containing t. To show that G is generated by Q, it suffices to exhibit a and $R_+(x)$ for x in V as products of conjugates of t. Now a^p is easily seen to have the form

$$\begin{bmatrix} 1 & 0 & ? \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

whence $a^{p^2} = 1$. Thus a has odd order $2n+1$, say. Then it is easily checked that $a = (a^{-n}ta^n)t$. If $x \in V$, say $x = (-2)(u, v, w)$, let $y = (u+v, 0, w+2v)$ and $z = (v, 0, v)$. Then

$$R_+(x) = t(a^{-1}ta)(a^{-1}R_+(z)\,tR_+(-z)\,a)(R_+(y)\,tR_+(-y)).$$

Q thus generates G. To show that Q and G satisfy the hypothesis of Proposition 3, it only remains to check the condition on the order of xy for x, y conjugates of t. If H is

https://doi.org/10.1017/S0305004100052634 Published online by Cambridge University Press

the subgroup of G generated by $\{a, t\}$, it is easily verified that $G = \{\alpha R_+(x) | \alpha \in H, x \in V\}$, where $\alpha R_+(x) . \beta R_+(y) = \alpha\beta R_+(z)$ for some z. Hence the product of two conjugates of t is of the form

$$\begin{aligned}\delta &= (\alpha R_+(x)\, t R_+(-x)\, \alpha^{-1})\,(\beta R_+(y)\, t R_+(-y)\, \beta^{-1}) \\ &= \alpha t \alpha^{-1} \beta t \beta^{-1} R_+(z) = \gamma R_+(z), \text{ say, for some } z.\end{aligned}$$

Now the matrix of γ has diagonal terms $(1, 1, 1)$, so γ has order p or p^2, and

$$\delta^{p^2} = \gamma^{p^2} R_+(w) = R_+(w)$$

for some w, whence $\delta^{p^3} = R_+(pw) = 1$. Thus every product of two conjugates of t has order p^n for some $n \leqslant 3$.

Defining $\circ$ on Q as before, $(Q, \circ)$ is a right distributive quasigroup by Proposition 3. However, it is not left distributive: e.g. if $x \in V - \{0\}$,

$$R_+(x)\, t \circ (at \circ t) \neq (R_+(x)\, t \circ at) \circ (R_+(x)\, t \circ t).$$

This paper was written while the author held the Charles and Katharine Darwin Research Fellowship at Darwin College, Cambridge.

I am grateful to the referee for many helpful suggestions.

REFERENCES

(1) Belousov, V. D. O strukture distributivnih kvazigrupp. *Mat. Sbornik* **50** (1960), 267–298. MR **22**, 11059.
(2) Bruck, R. H. *A survey of binary systems* (Berlin, Springer, 1971).
(3) Fischer, B. Distributive Quasigruppen endlicher Ordnung. *Math. Z.* **83** (1964), 267–303.
(4) Glauberman, G. On loops of odd order. *J. Algebra* **1** (1964), 374–396.
(5) Glauberman, G. On loops of odd order II. *J. Algebra* **8** (1968), 393–414.
(6) Manin, Ju. I. *Kubičeskie formy* (Moskva, Nauka, 1972).
(7) Manin, Ju. I. (trans. Hazewinkel, M.) *Cubic forms* (Amsterdam, North-Holland, 1974).

https://doi.org/10.1017/S0305004100052634 Published online by Cambridge University Press