ON THE MULTIPLICATION GROUP OF A LOOP

BY

C. R. B. WRIGHT[1]

Introduction

A loop is a set, L, with one binary operation, $\cdot$, with the property that the mappings $R_x : y \longrightarrow y \cdot x$ and $L_x : y \longrightarrow x \cdot y$ are permutations of L for each x in L and with an element 1 for which R_1 and L_1 are the identity. The multiplication group of L, $\mathfrak{M}_L$, is the group of permutations of L generated by the set of mappings R_x and L_x for x in L. A given group may be the multiplication group of several loops, so that it is generally impossible to recapture a loop L from a knowledge of $\mathfrak{M}_L$. Certain conditions on $\mathfrak{M}_L$, however, impose restrictions sufficient to determine L to within a small range of possibilities. This paper contains results connected with the problem of determining such conditions together with an account of some families of simple loops and simple algebras which arise in connection with the problem.

In Section 1 we consider coset groupoids, a hybrid of factor groups and sets of translations in $\mathfrak{M}_L$. The main results give necessary and sufficient conditions that a coset groupoid arising from a group be a loop.

The next section deals with relations between the normal structure of a finite loop and the structure of $\mathfrak{M}_L$. We show that $\mathfrak{M}_L$ is nilpotent if and only if L is a direct product of nilpotent loops of prime-power orders. If L is solvable, $\mathfrak{M}_L$ need not be solvable, but if L is nilpotent, then $\mathfrak{M}_L$ is solvable (although not necessarily nilpotent). If L is a finite Moufang loop and if $\mathfrak{M}_L$ is solvable, then L is solvable. The remainder of the paper stems from an effort to prove a similar result without the Moufang condition. We succeed in replacing "Moufang" by "alternative".

Suppose that L is a finite simple loop whose multiplication group contains an abelian normal subgroup. In Section 3 we show that L can be constructed from a type of non-associative algebra in a natural way. We call loops obtained from such algebras *linear loops*. The next two sections give a complete description of the finite simple linear loops of dimensions 1, 2 and 3 (1-dimensional ones are trivial, and there are no 2-dimensional ones) and summarize the basic facts about the automorphisms and multiplication groups of the 3-dimensional ones. Finally, there is a discussion in Section 6 of the difficulities to be encountered in handling higher-dimensional cases.

Received October 10, 1967.

[1] The bulk of this work was supported by two Faculty Summer Research Awards from the Office of Scientific and Scholarly Research of the University of Oregon. I am also indebted to G. Glauberman for suggesting the lines of thought leading to Theorems 2 and 5.

1. Coset groupoids

Let L be a loop with multiplication group $\mathfrak{M}_L$ and inner mapping group $\mathfrak{J}_L$. (Unexplained notation is that of [2] or of [6]). $\mathfrak{M}_L$ is a transitive permutation group on L and $\mathfrak{J}_L$ is the subgroup fixing the element 1. The set $R_L = \{R_x \mid x \in L\}$ forms a right transversal of $\mathfrak{J}_L$ in $\mathfrak{M}_L$. For each x in L, R_x is the unique member of R_L sending 1 to x, $R_x \cdot R_y$ and R_{xy} agree on 1 and a knowledge of the particular permutations in R_L is enough to determine the multiplication table of L.

With this situation in mind, we define a (right) *coset groupoid* to be a groupoid $(L, \cdot)$ with an element 1 such that $1 \cdot x = x$ for all x and with the property that for each x in L the translation $R_x : y \rightarrow y \cdot x$ is a permutation of L. If L is a coset groupoid let $R_L = \{R_x \mid x \in L\}$, let $\mathfrak{S}_L$ be the group of all permutations of L and let $\mathfrak{R}_L$ be the subgroup of $\mathfrak{S}_L$ generated by R_L. If $G \leq \mathfrak{S}_L$ let G_1 be the subgroup of G fixing 1. The following facts are easy to check.

PROPOSITION 1. (I) *If G is a group with subgroup H and if* $\mathbf{G}$ *is a (right) transversal of H in G define $\circ$ on* $\mathbf{G}$ *by $x \circ y \in Hxy \cap \mathbf{G}$. Then $(\mathbf{G}, \circ)$ is a coset groupoid.*

(II) *If $(L, \cdot)$ is a coset groupoid and if $\mathfrak{S}_L \geq G \geq \mathfrak{R}_L$, then R_L is a transversal of G_1 in G. If $\circ$ is defined on R_L as in (I), then the mapping $x \rightarrow R_x$ is an isomorphism of $(L, \cdot)$ onto $(R_L, \circ)$.*

This proposition shows that coset groupoids are precisely transversals with an obvious multiplication. Since choice of representatives of H in G is not "canonical," we do not generally get a "canonical" way of multiplying cosets of H in G. The obvious exception is the case in which $H \trianglelefteq G$.

Loops are clearly coset groupoids. Every loop is a coset groupoid for the pair $(\mathfrak{M}_L, \mathfrak{J}_L)$, by (II). If G is a group with subgroup H, which loops can have G as multiplication group and H as inner mapping group? We consider the more general question of which loops can be coset groupoids of the pair (G, H). The proof of the following proposition is straightforward.

PROPOSITION 2. *Under the hypotheses of Proposition 1, $(\mathbf{G}, \circ)$ is a quasigroup if and only if* $\mathbf{G}$ *is a transversal for every conjugate of H, and $(\mathbf{G}, \circ)$ has a two-sided identity if and only if the representative of the coset H belongs to every conjugate of H.*

PROPOSITION 3. *Let n be finite. If T is a subset of the symmetric group S_n which has n elements, then T is a transversal for every conjugate of $(S_n)_1$ in S_n if and only if T is transitive.*

For example, in S_3 there are exactly two transitive subsets of order 3, the set of 2-cycles and A_3. Under $\circ$ they yield the two quasigroups of order 3 with left identity.

Proof of Proposition 3. Since $| T | = n$, T is transitive on $\{1, \cdots, n\}$ if and only if for every a and b in $\{1, \cdots, n\}$ no two members of T send a to b. And T is a transversal of $x^{-1}(S_n)_1 x$ if and only if no two members of T send $1x$ to the same place. The result follows.

The next result is straightforward to prove.

Proposition 4. *Let G be a transitive subgroup of S_n.*

(I) *If* $(\mathbf{G}, \circ)$ *is a loop, then the non-identity elements of* $\mathbf{G}$ *are regular* (*i.e., have no fixed points*).

(II) *If $1 \in S \subseteq G$, if $| S | = n$ and if the subgroup of G generated by S consists of regular elements* (*together with* 1), *then the identity function is an isomorphism of* $(S, \circ)$ *onto* $(S, \cdot)$.

In particular, if G is a Frobenius group of degree n, then by (I) the only loops $(\mathbf{G}, \circ)$ which can possibly arise are made from the Frobenius kernel K of G and by (II) the only one is the group K itself.

If G is the alternating group A_5 viewed as a transitive subgroup of S_6, then the regular elements are the products of disjoint 3-cycles, and no five of them together with 1 form a transitive subset of G. It follows that there is no transversal of G_1 in G which is a loop of order 6 under $\circ$. Thus not every permutation group of degree n has an associated loop of order n. On the other hand, *every* loop of order n is a coset groupoid for S_n, by Proposition 1 (II).

Loop properties can be translated straightforwardly into conditions on transversals. Some examples (in the notation of Proposition 1) are:

(i) $(\mathbf{G}, \circ)$ is commutative if and only if $(a^1, b^1) \in H$ for all a and b in G;

(ii) $(\mathbf{G}, \circ)$ has the R.I.P. if and only if for each a in $\mathbf{G}$ there exists b in $\mathbf{G}$ with $ab \in \bigcap xHx^{-1}$;

(iii) $(\mathbf{G}, \circ)$ has the L.I.P. if and only if $a \circ b \in aHb$ for all a and b in $\mathbf{G}$.

2. Relations between the normal structures of L and $\mathfrak{M}_L$

If L is a direct product (or sum) of subloops $\{L(i) | i \in I\}$ then $\mathfrak{M}_L$ is the direct product (respectively, sum) of $\{\mathfrak{M}_{L(i)} | i \in I\}$. By Lemma 2.2, p. 98 [2], if L is a finite loop then L is (centrally) nilpotent of p-power order if and only if $\mathfrak{M}_L$ is a p-group. It follows that if L is a direct product of finitely many nilpotent finite p-loops then $\mathfrak{M}_L$ is nilpotent. In fact, we have the following.

Theorem 1. *If L is a finite loop, then L is a direct product of nilpotent loops of prime-power orders if and only if $\mathfrak{M}_L$ is nilpotent.*

Proof. We prove the remaining implication by induction on $| L |$. Say $\mathfrak{M}_L = \mathfrak{P} \times \mathfrak{Q}$ with $\mathfrak{P}$ a non-trivial Sylow subgroup. Let $P = 1\mathfrak{P}$ and $Q = 1\mathfrak{Q}$. Now $| P |$ is $| \mathfrak{P} : \mathfrak{P} \cap \mathfrak{J}_L |$, a p-power, $| Q |$ is prime to p and P and Q are normal in L. Hence, $P \cap Q = 1$. For $H \trianglelefteq L$ let

$$H^* = \{\theta \in \mathfrak{M}_L \,|\, x\theta \in Hx \,\forall\, x \in L\}$$

(see Lemma 1.3, p. 62, [2]). We need the following to complete the proof.

PROPOSITION 5. *If L is a loop, if $\mathfrak{M}_L = \mathfrak{A} \times \mathfrak{B}$, and if* $1\mathfrak{A} \cap 1\mathfrak{B} = 1$, *then* $\mathfrak{A} = (1\mathfrak{A})^*$ *and* $\mathfrak{B} = (1\mathfrak{B})^*$.

Proof. Clearly, $\mathfrak{A} \subseteq (1\mathfrak{A})^*$ and $\mathfrak{B} \subseteq (1\mathfrak{B})^*$. Since

$$1[(1\mathfrak{A})^* \cap (1\mathfrak{B})^*] \subseteq 1(1\mathfrak{A})^* \cap 1(1\mathfrak{B})^* = 1\mathfrak{A} \cap 1\mathfrak{B} = 1,$$

then $(1\mathfrak{A})^* \cap (1\mathfrak{B})^* \subseteq \mathfrak{J}_L$. But $(1\mathfrak{A})^* \cap (1\mathfrak{B})^* \trianglelefteq \mathfrak{M}_L$ and $\mathfrak{J}_L$ is coreless. Hence, $(1\mathfrak{A})^* \cap (1\mathfrak{B})^* = 1$. It follows that $\mathfrak{A} = (1\mathfrak{A})^*$ and $\mathfrak{B} = (1\mathfrak{B})^*$.

Now in the proof of the theorem, we have $\mathfrak{P} = P^*$ and $\mathfrak{Q} = Q^*$, $\mathfrak{M}_{L/P} \simeq \mathfrak{M}_L/P^* \simeq \mathfrak{Q}$, and we may assume inductively that L/P is a direct product of nilpotent q-loops for primes q other than p, and hence that $|L:Q|$ is a p-power. Then $|L:PQ| = 1$, so that $L = P \times Q$. The result now follows by induction.

Since finite diassociative nilpotent loops are direct products of p-loops (Corollary, p. 404 of [6]), Theorem 1 yields the following.

COROLLARY. *If L is a finite diassociative loop, then L is centrally nilpotent if and only if $\mathfrak{M}_L$ is nilpotent.*

The construction at the end of Section 2 of [6] yields a commutative, power-associative, nilpotent loop which is not the direct product of p-loops and hence does not have a nilpotent multiplication group. We can, however, show the following.

THEOREM 2. *If L is a finite nilpotent loop, then $\mathfrak{M}_L$ is solvable.*

Proof. We actually prove slightly more. Suppose that $1 < N \triangleleft L$. The cosets Nx are blocks for the permutation group $\mathfrak{M}_L$, N^* is the kernel of the canonical homomorphism of $\mathfrak{M}_L$ into $\mathfrak{M}_{L/N}$ and for each x restriction of N^* to Nx yields a homomorphism θ_x of N^* into the group of permutations of Nx. Moreover, N^* is a subdirect product of the various image groups $N^*/\mathrm{Ker}\,\theta_x$.

Now $\mathrm{Ker}\,\theta_x$ is the set of members of N^* fixing each nx in Nx and hence is

$$N^* \cap \bigcap \{ (R_n R_x)^{-1} \mathfrak{J}_L R_n R_x \mid n \in N\}.$$

But this subgroup is conjugate to $N^* \cap \bigcap \{R_n^{-1} \mathfrak{J}_L R_n \mid n \in N\} = W$, the largest normal subgroup of N^* in $\mathfrak{J}_L \cap N^*$. Thus N^* is solvable if and only if each $N^*/\mathrm{Ker}\,\theta_x$ is solvable—and they all look like N^*/W.

Let $\mathrm{R} = \{R_n \mid n \in N\} \subseteq \mathfrak{M}_L$. Then $\mathrm{R} \subseteq N^*$. Hence, $\langle \mathrm{R} \rangle \subseteq N^*$ and restriction to N yields a homomorphism of $\langle \mathrm{R} \rangle$ into $\mathfrak{M}_N$ with kernel $\langle \mathrm{R} \rangle \cap W$. If it is true that $\langle \mathrm{R} \rangle \cdot W = N^*$, then N^*/W is a subquotient of $\mathfrak{M}_N$.

To prove the theorem we use induction on the nilpotency class of L and suppose $N \leq Z(L)$. Then $\mathfrak{M}_L/N^*$ is solvable, $W\langle \mathrm{R} \rangle/W$ is abelian, $W = \mathfrak{J}_L \cap N^*$, $W \cdot \mathrm{R} = N^*$ and hence N^* is solvable.

The same proof also shows that if $N \trianglelefteq L$, if L is solvable, if $|N| \leq 4$ and if $\mathfrak{M}_{L/N}$ is solvable then $\mathfrak{M}_L$ is solvable. For in this case N^*/W is a subgroup of the solvable group S_4. This shows that

if L has chief factors of order at most 4, then $\mathfrak{M}_L$ is solvable.

The condition $|N| \leq 4$ is necessary here. There is a solvable power-associative loop of order 10 with a subgroup of order 5 whose multiplication group contains the symmetric group S_5. A worse example may be constructed as follows. In the notation of Section 2 of [6], let C be cyclic of order 5 and let H be a Klein 4-group with elements e, a, b and c. To specify G we need only give the operations $*_{h,k}$ for h and k in H. Let $*_{a,b}$ be ordinary addition, let $*_{b,c}$ be as in Figure 1, let $*_{a,c}$ be arbitrary and let $*_{h,k} = *_{k,h}$. Then G is a commutative, power-associative solvable loop of order 20 in which every element lies in a cyclic subgroup of order 10. However, the group generated by $R_{(1,e)} \cdot R^4_{(1,b)}$ and $R^{10}_{(1,b)}$ is isomorphic to S_5, so that $\mathfrak{M}_G$ is not solvable.

$*_{b,c}$	0	1	2	3	4
0	1	2	3	4	0
1	4	1	0	2	3
2	3	4	1	0	2
3	0	3	2	1	4
4	2	0	4	3	1

FIGURE 1

These examples and Theorems 1 and 2 suggest that, in terms of normal structure, a loop is generally nicer than its multiplication group. If $\mathfrak{M}_L$ is good, then L should be even better. The rest of the paper is concerned with topics which arise in connection with the following conjecture.

If $\mathfrak{M}_L$ is solvable, then L is solvable.

(A solvable loop is one which has abelian groups as composition factors.) We show, among other things, that if $\mathfrak{M}_L$ has an abelian normal subgroup and L is simple and not solvable then L is very special.

Let L be a loop with subloops H and K with $K \trianglelefteq H$. Let

$$\mathfrak{C}_L(H/K) = \{\theta \in \mathfrak{M}_L \mid h\theta \in Kh \,\forall\, h \in H\}$$

and let

$$\mathfrak{G}_L(H) = \langle R_h, L_h \mid h \in H\rangle \leq \mathfrak{M}_L.$$

($\mathfrak{C}_L(L/K)$ is the group K^* used above.) $\mathfrak{G}_L(H)$ normalizes $\mathfrak{C}_L(H/K)$ and the mapping ρ of $\mathfrak{C}_L(H/K) \cdot \mathfrak{G}_L(H)$ into $\mathfrak{S}_{H/K}$ (the group of permutations of H/K) given by $(Kh)(\theta\rho) = K(h\theta)$ is a homomorphism onto $\mathfrak{M}_{H/K}$ with kernel $\mathfrak{C}_L(H/K)$. Thus

$$\mathfrak{M}_{H/K} \simeq \mathfrak{G}_L(H)/\mathfrak{G}_L(H) \cap \mathfrak{C}_L(H/K),$$

a homomorphic image of a subgroup of $\mathfrak{M}_L$. In particular, if $\mathfrak{M}_L$ is nilpotent or solvable, so is $\mathfrak{M}_{H/K}$.

In case $K \trianglelefteq L$, $\mathfrak{C}_L(L/K)$ avoids the quotient $\mathfrak{G}_L(H)/\mathfrak{G}_L(H) \cap \mathfrak{C}_L(H/K)$, so that $\mathfrak{M}_{H/K}$ is a homomorphic image of $\mathfrak{G}_L(H) \cdot \mathfrak{C}_L(L/K)/\mathfrak{C}_L(L/K)$. If both H and K are normal in L it follows that $\mathfrak{M}_{H/K}$ is a quotient of H^*/K^*.

Suppose now that H is a minimal normal subloop of L. If W is a minimal normal subloop of $\mathfrak{C}_L(L/H)$, then since $1W \trianglelefteq L$ and $1W \neq 1$, $1W = H$ and

$|H| = |W:\mathfrak{J}_L \cap W|$, a divisor of $|W|$. As a consequence we have the following.

PROPOSITION 6. *If L is a finite loop with $\mathfrak{M}_L$ solvable, then the chief factors of L have prime-power orders, and for each minimal normal subloop H of L, $\mathfrak{C}_L(L/H)$ has an elementary abelian p-group as its socle, where H has p-power order.*

As we shall see, there exist nonsolvable loops satisfying the conclusion of Proposition 6. It follows from the discussion above, however, that if $\mathfrak{M}_L$ is solvable the composition factors of L also have prime-power orders and solvable multiplication groups. We would thus like to show that if L is a simple loop and if $\mathfrak{M}_L$ is solvable, then L is a cyclic group.

In at least one case Proposition 6 provides the desired result. A Moufang loop of prime-power order is nilpotent (Glauberman and Wright [3] and [4]), so that we have the following.

THEOREM 3. *If L is a finite Moufang loop and if $\mathfrak{M}_L$ is solvable, then L is solvable.*

To attack the general case we need more machinery.

3. Linear loops

PROPOSITION 7. *Let L be a loop. L is simple if and only if $\mathfrak{M}_L$ is a primitive permutation group on L.*

Proof. This is essentially Theorem 8, p. 516, [1].

COROLLARY. *If L is a finite simple loop and if $\mathfrak{M}_L$ contains an abelian minimal normal subgroup A, then $|L| = |A|$, A is the unique minimal normal subgroup of $\mathfrak{M}_L$ and A acts regularly on L.*

THEOREM 4. *Let $(L, \cdot)$ be a finite simple loop such that $\mathfrak{M}_L$ contains an abelian normal subgroup. Then there is a simple (nonassociative) algebra, $(A, +, \cdot)$, over a field of prime order satisfying*

$$(1)\quad a \cdot b = a \text{ only if } a = 0 \text{ and } a \cdot b = b \text{ only if } b = 0$$

and such that, if $a \circ b = a + b - a \cdot b$, then $(A, \circ)$ is a loop isomorphic to $(L, \cdot)$ and $\mathfrak{M}_L$ is imbedded in the affine group on A with $\mathfrak{J}_L$ a subgroup of the general linear group on A.

Proof. By the Corollary to Proposition 7, $\mathfrak{M}_L$ has a unique minimal normal subgroup, A, and for each x in L there is a unique x_A in A such that $1x_A = x$. Write the operation of A inherited from $\mathfrak{M}_L$ additively, so that $(A, +)$ is a vector space over $GF(p)$ for some prime p. $\mathfrak{J}_L$ acts faithfully by conjugation as non-singular linear transformations of $(A, +)$.

Define φ from $\mathfrak{M}_L$ to $\mathfrak{S}_A$ by $x_A(\alpha\varphi) = (x\alpha)_A$ for x in L and α in $\mathfrak{M}_L$. Then

$$x_A((\alpha\beta)\varphi) = (x\alpha\beta)_A = (x\alpha)_A(\beta\varphi) = x_A(\alpha\varphi)(\beta\varphi),$$

so that φ is a homomorphism. Clearly φ is monic. For $\alpha \in \mathfrak{J}_L$, $x_A(\alpha\varphi) = (x\alpha)_A = \alpha^{-1}x_A\alpha$, and hence $\mathfrak{J}_L\varphi$ is contained in $GL(A)$. For y in L, $x_A(y_A\varphi) = x_A + y_A$, so that $A\varphi$ is the group of translations of A and hence φ embeds M_L in Aff(A).

Now define $\circ$ on A by $x_A \circ y_A = (x \cdot y)_A$, so that $(A, \circ)$ is isomorphic to $(L, \cdot)$, and define $x_A \cdot y_A = x_A + y_A - (x_A \circ y_A)$. For x in L let $x_A = \theta_x \cdot R_x$, so that $\theta_x \in \mathfrak{J}_L$. Now

$$\begin{aligned} x_A \cdot y_A = y_A - (x_A \circ y_A - x_A) = y_A - [(xy)x_A^{-1}]_A &= y_A - [yL_x R_x^{-1}\theta_x^{-1}]_A \\ &= y_A - y_A[(T_x^{-1}\theta_x^{-1})\varphi] \\ &= y_A(1 - \tau), \end{aligned}$$

where $\tau \in GL(A)$. Similarly, $x_A \cdot y_A = x_A(1 - (\theta_y^{-1})\varphi)$. Hence, $\cdot$ is bilinear and $(A, +, \cdot)$ is an algebra over $GF(p)$.

If $x_A \cdot y_A = x_A$, then $0 = y_A - x_A \circ y_A = y_A - (xy)_A$, so that $xy = y$. But then $x = 1$, so that $x_A = 0$. Thus and similarly $(A, +, \cdot)$ satisfies (1).

Finally, $(A, +, \cdot)$ is a simple algebra, since if B is an ideal of A, then B is a normal subloop of A.

If $(A, +, \cdot)$ is an algebra over the field K, then we may define $\circ$ on A by $a \circ b = a + b - a \cdot b$ as in the theorem and in ring theory, and we could define quasi-regularity as in ring theory. However, the quasi-regular elements may not form a groupoid, let alone a loop. For example, let

$$A = \langle x, y \mid x^2 = x = y^2, xy = yx = 0\rangle.$$

Then x is not quasi-regular, but y and $-y$ are, and $y \circ (-y) = x$.

The condition (1) on $(A, +, \cdot)$ is equivalent to right and left cancellation in $(A, \circ)$ and is a consequence of the fact that

(2) $y \to y - xy$ and $y \to y - yx$ are permutations of A.

(In fact, these mappings are linear automorphisms of $(A, +)$.)

PROPOSITION 8. *$(A, \circ)$ is a loop if and only if $(A, +, \cdot)$ satisfies* (2).

Call a loop $(A, \circ)$ obtained in this way from an algebra satisfying (2) a *linear loop*.

If we define a *unit* of an algebra A to be an element x such that $y \to x \cdot y$ and $y \to y \cdot x$ are permutations of A, then an algebra satisfies (2) precisely if it can be embedded as the unique maximal ideal of non-units in an algebra with 1. (To see this, embed A in $K \oplus A$, where

$$(k, x) \cdot (k', x') = (kk', kx' + k'x + x \cdot x').)$$

Hence, the study of algebras with (2) may be viewed as the study of radicals of certain "completely primary" algebras. Although most of what follows would be true for algebras over division rings, we are interested primarily in finite loops and so restrict consideration to algebras over fields.

In view of Propositions 6 and 7 and Theorem 3, we would like to show that simple linear loops of certain kinds are, in fact, cyclic groups. Note that $(a, b, c) = 1$ in $(A, \circ)$ if and only if $[a \cdot b] \cdot c = a \cdot [b \cdot c]$ in $(A, \cdot)$ and similarly $(a, b) = 1$ if and only if $a \cdot b = b \cdot a$. In particular, $(A, \circ)$ is power-associative, diassociative or commutative precisely if $(A, \cdot)$ is.

A finite-dimensional power-associative algebra satisfying (1) is a nilalgebra, since a relation $0 = a_0 x^k + \cdots + a_n x^{k+n}$ with $a_0 x^k \neq 0$ gives

$$x^k \in \langle x^{k+1}, \cdots, x^{k+n} \rangle,$$

a contradiction of (1). If A is a finite-dimensional algebra satisfying (1) and the alternative laws $yx \cdot x = y \cdot x^2$ and $x \cdot xy = x^2 \cdot y$, then A is power-associative, by Theorem 3.1 of [5], so that $(A, +, \cdot)$ is nilpotent, by Theorem 3.2 of [5]. But then $A \cdot A = 0$ if A is simple. A consequence of these remarks is the following theorem which includes Theorem 3 as a special case.

THEOREM 5. *Let L be a finite loop. If*

$$(y, x, x) = 1 = (x, x, y) \quad \textit{for all} \quad x \quad \textit{and} \quad y \quad \textit{in} \quad L$$

and if M_L is solvable, then L is solvable.

Before we study linear loops in more detail it may be worthwhile to look at some "nonlinear" simple loops obtained in a related way.

PROPOSITION 9. *Let V be a 2-dimensional vector space over the finite field K. Suppose that θ is a function from V to V satisfying*

(i) *if $u, v \in V$, then $u\theta = v\theta$ or $u\theta - v\theta \notin K(u - v)$,*

(ii) *$0\theta = 0$, and*

(iii) *$V\theta \cap [(-1, 0) + K(0, 1)] = \emptyset$.*

For u in V, if $u\theta = (a, b)$ let

$$R_u = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, \qquad T_u = I + R_u = \begin{bmatrix} 1 + a & b \\ 0 & 1 \end{bmatrix},$$

and define $\circ$ on V by $u \circ v = uT_v + v$. Then $(V, \circ)$ is a loop.

The proof is straightforward. It will follow from results below that these loops (if simple) cannot be linear loops over K.

There really are functions θ satisfying (i), (ii) and (iii). For example, if $|K| \geq 4$ let $\mu, \nu, \lambda \in K$ with $\mu \neq 0$, $\nu \notin \{0, -1, -2\}$, and let S be a non-empty set of units of K. Define θ on $K \times K$ by

$$(c, \lambda c + \mu c^2 + s)\theta = (\nu, \nu\lambda + \nu\mu c) \quad \text{for} \quad s \quad \text{in} \quad S$$

and by

$$(c, d)\theta = (0, -\nu\mu c) \quad \text{if} \quad d \notin \lambda c + \mu c^2 + S.$$

Then

$$(a, b) \circ (c, \lambda c + \mu c^2 + s) = (a + c + \nu a, b + \lambda c + \mu c^2 + s + \nu\lambda a + \nu\mu ac)$$

and

$$(a, b) \circ (c, d) = (a + c, b + d - \nu\mu ac) \quad \text{if} \quad d \notin \lambda c + \mu c^2 + S.$$

(The condition $\nu \neq -2$ is necessary to prevent $\{(a, \lambda a + \mu a^2) \mid a \in K\}$ from being a normal subloop.) If K has prime order, such loops are simple and possess lots of subgroups or very few, depending on whether S is large or small. There is no such function θ if $|K|$ is 2 or 3.

4. 1- and 2-dimensional linear loops

If A is a linear loop over K and if $A \cdot A < A$, then either $A \cdot A = 0$, in which case $(A, \circ)$ is just the abelian group $(A, +)$, or $A \cdot A$ is a proper normal subloop. We are looking for simple linear loops, so that we consider only loops A for which $A \cdot A = A$. (There is a linear loop A for which $A \cdot A = A > Z(A) > 0$, so that $A \cdot A = A$ is not a sufficient condition for simplicity of A.)

A linear loop A of dimension 1 must have $A \cdot A = 0$, since $x \notin A \cdot x$ for $x \neq 0$. Suppose that A is a 2-dimensional linear loop. We claim that A is not simple. A short, *ad hoc* argument would work here, but we prefer to illustrate the general methods, beginning with a fact about multilinear mappings.

LEMMA. *If V is a vector space over the field K of dimension m, then for each positive integer n there is an alternating multilinear map*

$$\varphi_n : V^n \to W,$$

where W is $\binom{m}{n}$-dimensional, such that $\varphi_n(x_1, \cdots, x_n) = 0$ if and only if $\{x_1, \cdots, x_n\}$ is dependent

Proof. If $n > m$ let $\varphi_n = 0$. Suppose that $n \leq m$. Let B be an ordered basis for V. Let W be a vector space over K with basis $C = \{c_\sigma\}$ indexed by the n-element subsets, σ, of B. For each such σ let A_σ be the matrix whose first n rows are $x_1, \cdots, x_n$ in terms of B and whose last $m - n$ rows are the members of $B - \sigma$ listed in order. Let $a_\sigma = \det(A_\sigma)$ and let

$$\varphi_n(x_1, \cdots, x_n) = \textstyle\sum_\sigma a_\sigma c_\sigma .$$

From now on, we shall denote $\varphi_n(x_1, \cdots, x_n)$ by $\langle\langle x_1, \cdots, x_n\rangle\rangle$.

If A is a linear loop, then $A \cdot x < A$ for every x in A. Hence, if A is n-dimensional

$$(3) \qquad \langle\langle x_1 \cdot x, \cdots, x_n \cdot x\rangle\rangle = 0 \quad \forall x_1, \cdots, x_n \in A,$$

and similarly, by symmetry,

$$(3') \qquad \langle\langle x \cdot x_1, \cdots, x \cdot x_n\rangle\rangle = 0 \quad \forall x_1, \cdots, x_n \in A.$$

We can exploit multilinearity to get dependence relations among the products $x \cdot y$ in $A \cdot A$. After gleaning what we can from (3) and (3′), we may also use the fact that, since $x \notin A \cdot x$ for $x \neq 0$, a relation

$$0 = \textstyle\sum \alpha_i(x_i \cdot x - x_i) = (\sum \alpha_i x_i) \cdot x - \sum \alpha_i x_i$$

would force $\sum \alpha_i x_i = 0$. Thus, and symmetrically,

$$(4) \qquad \ll x_1 \cdot x - x_1, \cdots, x_n \cdot x - x_n \gg \neq 0$$

and

$$(4') \qquad \ll x \cdot x_1 - x_1, \cdots, x \cdot x_n - x_n \gg \neq 0$$

for all x in A and all $\{x_1, \cdots, x_n\}$ independent.

We apply (3) and (3′) to the 2-dimensional case and obtain

$$0 = \ll \alpha xx + \beta xy, \alpha yx + \beta yy \gg, \quad 0 = \ll \alpha xx + \beta yx, \alpha xy + \beta yy \gg$$

for all $\alpha, \beta \in K$, $x, y \in A$. Hence, by multilinearity,

$$(5) \qquad 0 = \ll xx, yx \gg$$

$$(6) \qquad 0 = \ll xx, yy \gg + \ll xy, yx \gg$$

$$(7) \qquad 0 = \ll xx, xy \gg$$

for all $x, y \in A$. If $xx \neq 0$ for some x in A, then by (5), $yx \in \langle xx \rangle$ (from now on, "$\langle S \rangle$" denotes the space spanned by S); by (7), $xy \in \langle xx \rangle$ so that $\ll xy, yx \gg = 0$; and by (6), $yy \in \langle xx \rangle$. If $\langle x, y \rangle = A$, then

$$A \cdot A = \langle xx, xy, yx, yy \rangle = \langle xx \rangle < A,$$

so that A is not simple. The only other possibility is that $xx = 0$ for all x in A. Then (3) and (3′) are no help. But if $A = \langle x, y \rangle$, then for all $\alpha, \beta \in K$, by (4),

$$\begin{aligned} 0 &\neq \ll \alpha xx + \beta xy - x, \alpha yx + \beta yy - y \gg \\ &= \ll \beta xy - x, \alpha yx - y \gg \\ &= \alpha \ll \beta xy - x, yx \gg + \ll \beta xy - x, -y \gg, \end{aligned}$$

so that for all β, $0 = \ll \beta xy - x, yx \gg$ and $0 \neq \ll \beta xy - x, -y \gg$. Hence,

$$0 = \ll xy, yx \gg, \quad 0 = \ll x, yx \gg, \quad 0 \neq \beta \ll xy, -y \gg + \ll -x, -y \gg.$$

Thus $0 = \ll xy, -y \gg$, so that $yx \in \langle x \rangle$, $xy \in \langle y \rangle$. However, $0 = (x + y)^2 = xy + yx$, so that $xy = yx = 0$ for all x and y and $A \cdot A = 0$. This argument, together with our earlier remarks, establishes the following.

PROPOSITION 10. *There are no non-abelian simple linear loops of dimensions* 1 *and* 2.

5. The three-dimensional case

The analysis of simple 3-dimensional linear loops is considerably more complex than that of 1- and 2-dimensional loops and involves lengthy computations. We list here only the major mileposts and the end results. Again we begin by considering (3) and (3′). Our first goal is to show that if A is a

3-dimensional linear loop, then either

(i) $xx = 0$ for all x in A,
(ii) $x \cdot A = 0$ for some $x \neq 0$,
(ii′) $A \cdot x = 0$ for some $x \neq 0$ or
(iii) $A \cdot A < A$.

We suppose all four conditions fail, show first that we can choose a basis $\{x, y, z\}$ such that $yz = 0$ and yx and xz are independent, and after appealing to (3) and (3′) show that the possibilities for A must be limited. In fact, A has constants of structure given by

	x	y	z
x	xx	$Gxx + Pxz$	xz
y	yx	$Gyx + Hxz$	0
z	$Fxx + Lyx$	$(GF - HE)xx + (GL + PE)yx + (PF + HL)xz$	$Eyx + Fxz$

with $H, E \neq 0$. Such an algebra need not satisfy one of (i), $\cdots$, (iii), however, and to show that one of them holds we must use (4) and (4′). A few pages of computations give the desired result.

Now of course a simple linear loop cannot satisfy (iii), and a short argument shows that (i) also cannot hold for a simple algebra satisfying (2). We are thus left with (ii) and (ii′), and consider only (ii).

A few pages of carefully selected computations show that in this case it is possible to choose a basis $\{x, y, z\}$ such that the multiplication in A is given by the table

		x	y	z
	x	0	$ax + ez$	$sx + fy + gz$
(8)	y	0	dx	x
	z	0	hx	0

where the constants of structure are arbitrary in K subject to the conditions (implied by (4) and (4′)) that

$$X^2ef + Xg - 1 \quad \text{and} \quad X^2f + XY(df + gh) + Y^2eh + Xs + Ya - 1$$

are irreducible polynomials over K for every Y in K. If K is finite, the second of these conditions implies that $(gh + df)^2 = 4feh$ and $2(gh + df)s = 4af$, and it is possible to write the table as

		x	y	z
	x	0	$stx + bfz$	$sx + fy + cfz$
(9)	y	0	$[2t - c(t^2/b)]x$	x
	z	0	$(t^2/b)x$	0

where $X^2b + Xc - 1$ and $X^2f + Xs - 1$ are irreducible over K. (If $ef = 0$, then $A \cdot A < A$. Thus we suppose that $ef \neq 0$ and hence that $bf \neq 0$.)

An algebra, A, given by (9) does determine a loop satisfying $A \cdot A = A$ and $v \cdot A = A \cdot v = 0$ only if $v = 0$. Note that $\langle x \rangle$ is the left nucleus, N_λ, and that $N_\mu = N_\rho = 0$ unless $t = 0$, in which case $N_\mu = \langle y \rangle$ and $N_\lambda = \langle z \rangle$.

Note also that the non-simple loops which we have discarded need not be groups. For example, the loop given by

	x	y	z
x	0	0	0
y	0	x	0
z	0	0	y

is not associative even though it is commutative and endowed with a center.

To compute $\mathfrak{J}_A$, where A is given by (9), we look at the mappings

$$\lambda_y : a \longrightarrow y \cdot a \quad \text{and} \quad \rho_y : a \longrightarrow a \cdot y \qquad \text{for } y \text{ in } A.$$

It is easy to check that $\mathfrak{J}_A$ is generated by the mappings $\lambda_y \lambda_z \lambda_{zy}^{-1}$, $\rho_y \rho_z \rho_{yz}^{-1}$ and $\rho_y \lambda_y^{-1}$ for y and z in A. A moderate amount of computation shows that $\mathfrak{J}_A$ contains all matrices $I + \alpha E_{ij}$ for α in K and $i \neq j$ and hence contains $SL(3, K)$. The determinants of the members of $\mathfrak{J}_A$ form a subgroup D of K generated by the elements $1 - c\alpha - b\alpha^2$ and $1 - s\alpha - f\alpha^2$ as α ranges over K. If K is finite, D is the group of units of K and $\mathfrak{J}_A = GL(3, K)$. If K is infinite, D may be much smaller than K. In the finite case, $\mathfrak{M}_A = Aff(3, K)$, so that $\mathfrak{M}_A$ acts primitively on A and A is simple. We may summarize the finite results.

THEOREM 5. *If A is a finite, centerless, 3-dimensional linear loop over the field K, and if $A \cdot A = A$, then A is given by* (9) (*or its opposite algebra*) *for suitable constants in K, A is simple, and $\mathfrak{M}_A = Aff(3, K)$.*

Since A may or may not have trivial left nucleus, we see that the loops, A, which have $\mathfrak{M}_A = Aff(3, K)$ are not all isotopic.

The automorphisms of a finite linear loop A of type (9) over the field K with Galois group $\mathfrak{G}(K)$ over its prime field are the semi-linear transformations of the form

$$\begin{bmatrix} \sigma d^2 e & 0 & 0 \\ 0 & \sigma de & 0 \\ 0 & 0 & \sigma d \end{bmatrix},$$

where $\sigma \in \mathfrak{G}(K)$, σ fixes st, t^2/b, s^2/f, c^2/b and (if $ct \neq 0$) t/c and where d and e satisfy $s\sigma = s\,d$, $c\sigma = ce$, $f\sigma = f\,d^2$, $b\sigma = be^2$ and $t\sigma = te$. Hence, the automorphism group of A is of the form $H \times T$ where H is a (cyclic) factor group of $\mathfrak{G}(K)$ and T is a subgroup of the Klein 4-group whose size depends on which of s, c and t are trivial. In particular, it can easily happen that A has no non-trivial automorphism. Such is the case if $K = GF(p)$ and $sc \neq 0$.

An infinite linear loop of type (9) may have other sorts of automorphisms.

For example, if $K = Q(\sqrt{3})$ (Q the rational field) and if $b = 2 + \sqrt{3} = f = t$, $s = 0$ and $c = 2 - 2b$, then $\sigma : b \rightarrow 1/b$ generates $\mathfrak{G}(K)$, and the loop has an automorphism of order 2 given by

$$\begin{bmatrix} -\sigma \cdot (1/b^3) & 0 & 0 \\ 0 & -\sigma \cdot 2/(b^4 - b^3) & \sigma \cdot (b+1)/(b^3 - b^2) \\ 0 & -\sigma \cdot (b+1)/(b^3 - b^2) & \sigma \cdot 2/(b-1) \end{bmatrix}.$$

Even in the infinite case, however, the automorphism group is a group of semi-linear transformations which is an extension of a subgroup of K_4 by a quotient of $\mathfrak{G}(K)$.

6. Higher-dimensional linear loops

Any field K over which there is an irreducible quadratic polynomial can be used to construct loops of form (9). Hence, if K is n-dimensional over F and there is an irreducible quadratic polynomial over K we can obtain simple $3n$-dimensional linear loops over F. Aside from this obvious device, there seems to be no easy way of constructing simple linear loops of dimension 4 or more. Conditions (3) and (3′) still yield relations on the constants of structure which are comparatively easy to deal with. In the n-dimensional case with basis $\{x_1, \cdots, x_n\}$, if we write $x = \alpha_1 x_1 + \cdots + \alpha_n x_n$, then (4) and (4′) become statements that certain polynomial equations in $\alpha_1, \cdots, \alpha_n$ have no solutions. The equations which arise are of degree n in general, but by comparison with the polynomials in (3) and (3′) they reduce to degree $n - 1$. Thus, except in special cases, (4) and (4′) given conditions on the constants of structure expressed as conditions that certain polynomial equations of degree $n - 1$ have no solutions, and it is by no means easy to determine which (if any) constants satisfy the conditions.

By imposing additional restrictions on the desired loops one may be able to depress the degrees of the polynomials involved. For example, the conditions (4) and (4′) on a 4-dimensional commutative linear loop involve insolvability of quadratic equations and can be shown to conflict with an assumption of simplicity. I conjecture that there are no finite simple power-associative linear loops and hence that if L is finite and power-associative and $\mathfrak{M}_L$ is solvable, then L is solvable.

In every case which I have examined it has been necessary to invoke (4) or (4′) as well as (3) and (3′) in order to settle matters. In view of this experience and the additional complexities which arise with higher dimensions it seems most likely that extension of the analysis to higher dimensions will be most successful in cases in which additional restrictions besides simplicity are imposed upon the loops.

Bibliography

1. A. A. Albert, *Quasigroups, I*, Trans. Amer. Math. Soc., vol. 54 (1943), pp. 507–519.
2. R. H. Bruck, *A survey of binary systems*, Springer Verlag, Berlin-Göttingen-Heidelberg, 1958.

3. G. Glauberman, *On loops of odd order, II.*, J. Algebra, vol. 8 (1968), pp. 393–414.
4. G. Glauberman and C. R. B. Wright, *Nilpotence of finite Moufang 2-loops*, J. Algebra, vol. 8 (1968), pp. 415–417.
5. R. D. Schafer, *An introduction to nonassociative algebras*, Academic Press, New York and London, 1966.
6. C. R. B. Wright, *Nilpotency conditions for finite loops*, Illinois J. Math., vol. 9 (1965), pp. 399–409.

University of Oregon
Eugene, Oregon
University of Chicago
Chicago, Illinois