NORMAL ENDOMORPHISMS

BY

R. H. BRUCK[1]

1. Introduction

It should prove helpful to the reader if we begin with some brief remarks not strictly pertaining to the content of the paper. The general topic is the concept and theory of "normal" endomorphisms of a loop. This topic was begun in Chapter IV, §4 of the author's book, *A Survey of Binary Systems* [1]. Most of the references in the paper are to [1], and these take the form "[SIV.4]", "Lemma 3.1 of [SVII]", and so on. The paper is so designed that the reader can follow the earlier sections with only a general knowledge of loop theory but will need progressively more of the lore of Moufang loops. It is, however, the special knowledge which supports the concepts studied in the paper. Accordingly, we shall now discuss the content of the paper with a minimum of definitions and with little regard to order. We adopt a notation appropriate for the discussion, with no intention of using it in the rest of the paper.

The four main classes of "normal" endomorphisms to be studied in this paper are

K_1 : *The seminormal endomorphisms.*

K_2 : *The weakly normal endomorphisms.*

K_3 : *The normal endomorphisms.*

K_4 : *The strongly normal endomorphisms.*

Each of these is defined in §2. Class K_3 was defined in [SIV.4] in terms of "normalized, purely non-abelian" loop words. We use the same definition here but prove some helpful lemmas (Lemmas 2.1, 2.2) about the defining class of loop words. The remaining classes K were studied originally in response to a question (proposed in a letter from Reinhold Baer) as to whether, in the case of a group, K_3 was precisely the set of all endomorphisms commuting with the inner automorphisms. The answer turns out to be affirmative (Corollary to Theorem 3.2), and the introduction of the new classes allows us to place this result among the elementary ones. The method of proof is as follows: For any loop (by definition and Theorem 2.1),

$$K_1 \supset K_2 \supset K_3 \supset K_4 . \tag{1.1}$$

For a group, K_1 and K_4 are easily seen to consist of all endomorphisms commuting with every inner automorphism of the group.

Received August 12, 1958.

[1] This research was supported in part by a grant from the National Science Foundation.

Let us note parenthetically at this point that multiplication and addition of single-valued mappings θ, ϕ of a loop L into itself are defined in the natural manner: For every x in L,

(1.2) $$x(\theta\phi) = (x\theta)\phi, \qquad x(\theta + \phi) = (x\theta)(x\phi).$$

The (right) complement, θ', of θ is defined by

1.3) $$\theta + \theta' = 1 = \text{the identity mapping.}$$

The inner automorphism group of a group G has as its natural analogue the inner mapping group of a loop L; but the inner mapping group need not consist of automorphisms. Commutators (x, y) and associators (x, y, z) are defined by

(1.4) $$xy = [yx](x, y), \qquad (xy)z = [x(yz)](x, y, z).$$

In what follows let θ (but not necessarily θ') denote an endomorphism of a group G or loop L, according to the context. For a group, the usual definition of normality is

$\mathfrak{G}$.1. *θ commutes with every inner automorphism of G.*

For a loop, one might try

$\mathfrak{L}$.1. *θ commutes with every inner mapping of L.*

If L is a Moufang loop, $\mathfrak{L}$.1 is equivalent (Lemma 7.2) to the set of identities

(1.5) $$(x, y)\theta = (x\theta, y) = (x, y\theta),$$

(1.6) $$(x, y, z)\theta = (x\theta, y, z) = (x, y\theta, z) = (x, y, z\theta).$$

In particular, $\mathfrak{G}$.1 is equivalent (as is well known) to (1.5). We use the identities (1.5), (1.6) (for an arbitrary loop) to define the class K_1. In particular, K_1 is a multiplicative semigroup, a property shared with the other classes K. However, so far as is known, the elements of K_1 (or K_2) need not satisfy $\mathfrak{L}$.1. The elements of K_3 do satisfy $\mathfrak{L}$.1.

For a group, a property known to be equivalent to $\mathfrak{G}$.1 is

$\mathfrak{G}$.2. *θ' is an endomorphism of G.*

However, if we let $\mathfrak{L}$.2 denote the corresponding property for a loop L, we get a class in general incomparable with K_1.—Connected, but not in general identical with this class, is the following:

K_0 : *The demi-seminormal endomorphisms.*

Class K_0 consists of all endomorphisms satisfying a weakened form of (1.6):

(1.7) $$(x\theta, y, z) = (x, y\theta, z) = (x, y, z\theta).$$

For a group, K_0 contains every endomorphism and hence is frequently larger than K_1. For a commutative Moufang loop, K_0 is a (nontrivial) ring consisting of every θ having the property that both θ' and $1 + \theta$ are endomorphisms (Theorem 8.1). For an arbitrary Moufang loop, the additive loop generated by K_0 is a group (Lemma 7.8) with remarkable properties. However, K_0 cannot seriously be considered as a class of "normal" endomorphisms.

For a group, each of $\mathfrak{G}.1$, $\mathfrak{G}.2$ is equivalent to the following strengthened form of $\mathfrak{G}.2$:

$\mathfrak{G}.3$. *θ' is an endomorphism of G and $\theta\theta'$ ($= \theta'\theta$) is centralizing (i. e., maps G into its centre).*

The corresponding property $\mathfrak{L}.3$ is used to define the class K_4. Thus, as stated earlier, K_1 and K_4, in the case of a group, both consist of the endomorphisms satisfying $\mathfrak{G}.1$.

It might be remarked here that K_4 seems the most appropriate class to be used for the theory of direct decomposition of loops. First let us note one difficulty: it is not immediately evident that K_4 is closed under multiplication. To prove that K_4 does possess multiplicative closure it seems necessary to establish at least some of the properties of K_3 or K_2. Theorem 3.1 deals with this matter rather thoroughly.

To get back to direct decomposition, a class, K, of "normal" endomorphisms suitable for the theory of direct decompositions should, ideally,

(a) *contain all decomposition endomorphisms,*

(b) *contain all centralizing endomorphisms and the sums of these with any member,*

(c) *contain all centre automorphisms (i. e., automorphisms θ for which θ' is centralizing),*

(d) *contain the complement of each of its members,*

(e) *be closed under multiplication.*

In addition, the elements of K should

(f) *map normal subloops into normal subloops,*

(g) *map centre elements into centre elements.*

Both (f) and (g) will be automatic if the elements of K also

(h) *commute with inner mappings.*

And I would add the requirement that, for all θ, ϕ in K,

(i) $\theta\phi = \phi\theta + (\theta, \phi)$, *where (θ, ϕ) is a centralizing endomorphism.*

In connection with (i), see Theorem 3.3 and the appended remarks.

For K_4, (a)–(d) are obvious, (h) and (i) can be proved quite simply, and (e) then follows easily from (i). And K_4 is probably the smallest intrinsically defined class with properties (a)–(i) which is likely to be proposed.

For K_3, all of (a)–(h) except (d) were proved in [SIV.4]. I would not have conjectured the truth of (d), but it is indeed true (Theorem 4.1). And (i) holds not only for K_3, but also for K_2.

The relation of K_2, K_1 to (d) and (f), and of K_1 to (i), is still uncertain for loops in general. Except for (d), (f), (h) (which implies (f)), and (i), the rest of (a)–(i) are all true. For a Moufang loop L, K_1 satisfies (a)–(i); moreover, K_1 generates a ring S with the property that every endomorphism θ of L which is in S is also in K_1 and has its complement θ' in K_1 as well (Theorem 7.1). Theorem 7.1 is a true generalization of a theorem of Heerema [3] on normal endomorphisms of a group; the proof, however, has to contend with the fact that inner mappings of a Moufang loop need not be automorphisms.—No comparable theorem is known for loops in general (even with K_1 replaced by K_4); indeed, such a theorem would have to involve a modified concept of "ring", presumably a neoring in the sense of [4].

Now let us turn for a moment to a discussion of the definitions of K_1, K_2, K_3. We recall that K_1 was defined by (1.5), (1.6). And K_2 is defined by adding to (1.5), (1.6) a finite set of identities of a similar sort. (They are not very pretty!) We remark that although (1.5), (1.6) have a superficial symmetry—and have an invariant significance for the special case of Moufang loops—the symmetry is not real. For example, in the definition (1.4) of the commutator (x, y), we might reasonably replace the right-hand side by any one of

$$(y, x)[yx], \qquad [yx](x, y), \qquad [y(y, x)]x, \qquad y[(x, y)x],$$

or by other combinations which will occur to the reader. The resultant effect on K_1 is (in general) by no means clear. Similar remarks apply to the associator and to the other functions used in the definition of K_2. One answer is to use all such functions, after a careful examination of the appropriate meaning of "all such". This prepares us for the definition of K_3.—I cannot resist remarking that this motivation (perhaps like most motivations) bears little relation to historical facts. I believe that I came to the definition of K_3 partly through (1.5), but mainly through the theory of rings and, in particular, through observation of the effect of derivations on ring commutators and ring associators. There is also a tenuous connection with cohomology operators.

To return to K_2. The additional defining identities for K_2 were chosen mainly for their relevance to additive properties of endomorphisms (with the theory of commutative Moufang loops as a guide). The particular objective was to prove (i). There is, however, no very strong reason why one should not add to the definition the finitely many identities necessary to ensure (h).

And now K_3 again. Although the defining identities for K_3 have a pleasing symmetry, they are infinite in number. However (Theorem 6.2) the following condition characterizes the elements θ of K_3:

$\mathfrak{K}$.4. *θ and θ' are seminormal endomorphisms of L, and $\theta\theta'$ is a strongly normal endomorphism of L which maps L into $C(L)$ and L' into $Z(L)$.*

Here L' is the commutator-associator subloop of L, $Z(L)$ is the centre of L, and $C(L)$ is the Moufang centre (§4) of L. Condition $\mathfrak{K}$.4 may be translated into a finite set of identities to be satisfied by the mappings θ, θ', $\phi = \theta\theta'$, ϕ', and $\phi\phi'$ of L. For another condition equivalent to $\mathfrak{N}.4$, see Theorem 6.1.

So far, we have avoided the question as to whether two of the K_i may not coincide for all loops. (To be exact, we did remark that, for a group, K_0 consists of all endomorphisms.) For a Moufang loop, $K_2 = K_3$ (Theorem 7.3); whether the same result holds for all loops is still unknown. In §8 we examine the containing relations

$$K_i \supset K_{i+1} \qquad (0 \leqq i < 4),$$

for a commutative Moufang loop L. If $i \neq 2$, L can be chosen so that

$$K_i \neq K_{i+1} ;$$

and L can also be chosen so as to possess an endomorphism not in K_0. Nevertheless, K_2, K_3, and K_4 cannot differ greatly, regardless of the particular type of loop which may be in question. For any loop, the square of each element of K_2 is in K_4 (Corollary to Theorem 3.1), and every element of K_3 is a sum of two elements of K_4 (Theorem 5.1). Moreover, if L is a loop for which K_3 contains K_4 properly, then L possesses an associator which lies in the centre of L and generates a group of order three.—This last remark is a trivial corollary of $\mathfrak{N}.4$ which, nevertheless, deserves mention.

One final remark. I would hazard a guess that an analogue of the definition of K_3 would prove useful in the study of (general) algebras. Here I refer, not to $\mathfrak{N}.4$, but to the definition (see §2) in terms of words.

2. Four definitions of normality of endomorphisms

Let G be a multiplicative loop. We define the operations of left division ($\backslash$) and right division ($/$) by

$$(2.1) \qquad x(x\backslash y) = y, \qquad (y/x)x = y$$

for all x, y in G. And we define the commutator (x, y) and the associator (x, y, z) by

$$(2.2) \qquad xy = (yx)(x, y), \qquad (xy)z = [x(yz)](x, y, z)$$

for all x, y, z in G. Equivalently,

$$(2.3) \qquad (x, y) = (yx)\backslash(xy), \qquad (x, y, z) = [x(yz)]\backslash[(xy)z].$$

An endomorphism θ of G will be called *seminormal* provided it satisfies the identities

$$(2.4) \qquad (x, y)\theta = (x\theta, y) = (x, y\theta),$$

$$(2.5) \qquad (x, y, z)\theta = (x\theta, y, z) = (x, y\theta, z) = (x, y, z\theta)$$

for all x, y, z in G.

For the purpose of providing certain expansion formulas we define functions

$p(x, y, z)$, $q(x, y, z)$, $P_i(w, x, y, z)$, and $Q_i(w, x, y, z)$, where $i = 1, 2, 3$, as follows:

$$(xy, z) = [(x, z)(y, z)] \cdot p(x, y, z), \tag{2.6}$$

$$(x\backslash y, z) = [(x\backslash 1, z)(y, z)] \cdot q(x, y, z), \tag{2.7}$$

$$(wx, y, z) = [(w, y, z)(x, y, z)] \cdot P_1(w, x, y, z), \tag{2.8}$$

$$(y, wx, z) = [(y, w, z)(y, x, z)] \cdot P_2(w, x, y, z), \tag{2.9}$$

$$(y, z, wx) = [(y, z, w)(y, z, x)] \cdot P_3(w, x, y, z), \tag{2.10}$$

$$(w\backslash x, y, z) = [(w\backslash 1, y, z)(x, y, z)] \cdot Q_1(w, x, y, z), \tag{2.11}$$

$$(y, w\backslash x, z) = [(y, w\backslash 1, z)(y, x, z)] \cdot Q_2(w, x, y, z), \tag{2.12}$$

$$(y, z, w\backslash x) = [(y, z, w\backslash 1)(y, z, x)] \cdot Q_3(w, x, y, z) \tag{2.13}$$

for all w, x, y, z in G.

An endomorphism θ of G will be called *weakly normal* provided θ is seminormal and also satisfies the following eight identities for all w, x, y, z in G:

$$p(x, y, z)\theta = p(x\theta, y, z) = p(x, y\theta, z); \tag{2.14}$$

$$q(x, y, z)\theta = q(x\theta, y, z) = q(x, y\theta, z); \tag{2.15}$$

$$P_i(w, x, y, z)\theta = P_i(w\theta, x, y, z) = P_i(w, x\theta, y, z), \quad i = 1, 2, 3; \tag{2.16}$$

$$Q_i(w, x, y, z)\theta = Q_i(w\theta, x, y, z) = Q_i(w, x\theta, y, z), \quad i = 1, 2, 3. \tag{2.17}$$

We note in passing that the class of seminormal endomorphisms and the class of weakly normal endomorphisms are each defined in terms of a finite set of identities. The definition of a weakly normal endomorphism is (quite obviously) lacking in symmetry; and this is also true of the definition of a seminormal endomorphism, in view of the asymmetry in (2.3). By contrast, the definition of a normal endomorphism (given in [SIV.4] and repeated below) is highly symmetric but involves a countably infinite set of identities.

Before defining a normal endomorphism, we shall prove two simple lemmas on loop words. Let n be a positive integer, and let F_n be the free loop [SI.3] on n free generators $X_1, \cdots, X_n$. By a *loop word* W_n we mean an element of F_n. If $a_1, \cdots, a_n$ are arbitrary elements of a loop G, $W_n(a_1, \cdots, a_n)$ denotes the image of W_n under the uniquely defined homomorphism of F_n into G which maps X_i upon a_i for $i = 1, 2, \cdots, n$.

LEMMA 2.1. *Let G be a loop with centre Z, and let W_n be a loop word. Then*

$$W_n(x_1 c_1, \cdots, x_n c_n) = W_n(x_1, \cdots, x_n)W_n(c_1, \cdots, c_n) \tag{2.18}$$

for all x_i in G and c_i in Z.

Sketch of proof. We first observe that $W_n(c_1, \cdots, c_n)$ is in Z for all c_i in Z. Next we define H to be the subset of F_n consisting of all W_n in F_n for which (2.18) holds. Then we verify that H contains each of the generators $X_1, \cdots, X_n$, and that H is closed under multiplication and under the two division operations. It follows that $H = F_n$. This completes the proof of Lemma 2.1.

We recall that the *commutator-associator* subloop G' of a loop G may be characterized in either of the following ways:

(a) G' is the subloop of G generated by the set of all commutators (x, y) and associators (x, y, z), where x, y, z range over G;

(b) G' is the smallest normal subloop K of G such that the quotient loop G/K is an abelian group.

LEMMA 2.2. *If W_n is an element of the free loop F_n on n free generators, each of the following statements implies the other two*:

(i) *W_n is an element of the commutator-associator subloop F'_n.*

(ii) *W_n vanishes on every abelian group. That is, if $a_1, \cdots, a_n$ are elements of an abelian group, then*

$$W_n(a_1, \cdots, a_n) = 1. \tag{2.19}$$

(iii) *If G is a loop with centre Z, then*

$$W_n(x_1 c_1, \cdots, x_n c_n) = W_n(x_1, \cdots, x_n) \tag{2.20}$$

for all x_i in G and c_i in Z.

DEFINITION. A loop word W_n will be called *purely non-abelian* if it possesses one of the equivalent properties (i)–(iii) of Lemma 2.2.

Proof. (i) $\rightarrow$ (ii). Assume that W_n satisfies (i). Let $a_1, \cdots, a_n$ be elements of an abelian group A, and let θ be the homomorphism of F_n upon A which maps X_i upon a_i, $i = 1, 2, \cdots, n$. Then $W_n \theta = W_n(a_1, \cdots, a_n)$. Since $F_n \theta$ is a subgroup of A and hence an abelian group, the kernel of θ contains F'_n. Since W_n is in F'_n, $W_n \theta = 1$. Then W_n satisfies (ii). Thus (i) implies (ii).

(ii) $\rightarrow$ (iii). Since the centre of a loop is an abelian group, the implication is clear from Lemma 2.1.

(iii) $\rightarrow$ (ii). We first observe that $W_n(1, \cdots, 1) = 1$ for any loop word. Consequently, if (2.20) holds, we set $x_i = 1$ for each i and deduce that $W_n(c_1, \cdots, c_n) = 1$ for all c_i in Z. The special case that G is an abelian group then gives (ii). Hence (iii) implies (ii).

(ii) $\rightarrow$ (i). Let θ be the natural homomorphism of F_n upon F_n/F'_n. Then $X_1 \theta, \cdots, X_n \theta$ are elements of the abelian group F_n/F'_n, so, if we assume (ii),

$$W_n \theta = W_n(X_1 \theta, \cdots, X_n \theta) = 1.$$

Hence W_n lies in the kernel of θ, that is, in F'_n. Thus (ii) implies (i). This completes the proof of Lemma 2.2.

We need one further notion. A loop word $W_n = W_n(X_1, \cdots, X_n)$ will be called *normalized* if it reduces to the identity element whenever one of the X_i is replaced by the identity element. To illustrate this concept, let us consider the loop word f_4 defined by

$$(2.21) \qquad (X_1 X_2)(X_3 X_4) = [(X_1 X_3)(X_2 X_4)] \cdot f_4(X_1, X_2, X_3, X_4).$$

We observe, using any one of the criteria of Lemma 2.2, that f_4 is purely non-abelian. However,

$$f_4(X_1, X_2, 1, X_4) = (X_1, X_2, X_4),$$

so f_4 is not normalized. In this connection the following two remarks seem worth recording:

(a) The loop word f_4 turns up quite naturally when one is trying to decide whether the sum of two given endomorphisms of a loop G is also an endomorphism of G. The fact that f_4 is not normalized seems to complicate this problem a good deal.

(b) The concepts of being purely non-abelian or normalized can of course be applied to associative words (that is, to elements of free groups instead of free loops), and the theory which follows has a natural analogue in group theory. It is significant that the associative word corresponding to f_4 is a product of the purely non-abelian words (X_2, X_3) and $((X_2, X_3), X_4)$, each of which is normalized as an element of the free group on its own arguments, but not normalized as an element of the free group on X_1, X_2, X_3, X_4.

Returning to the topic on hand, we observe that the defining identities for seminormal or weakly normal endomorphisms can all be put in the form

$$(2.22) \qquad W_n(x_1, \cdots, x_n)\theta = W_n(x_1 \theta, \cdots, x_n),$$

where n is a suitably chosen positive integer, W_n is a normalized purely non-abelian loop word, and the elements $x_1, \cdots, x_n$ are required to range over the loop G. For example, the identities (2.4) are equivalent to a pair of identities of type (2.22) with $n = 2$, where for W_2 we use in turn the loop word (X_1, X_2) and the loop word (X_2, X_1). Both of these words are easily seen to be normalized and purely non-abelian. Similarly, the identities (2.5) are equivalent to three identities of type (2.22) where $n = 3$ and W_3 is normalized purely non-abelian. And a like fact is true about the identities given by each of (2.14)–(2.17). Indeed, the definition (2.11) of the function Q_1, for example, was influenced by the desire to ensure that the loop words $W_4 = Q_1(X_1, X_2, X_3, X_4)$ and $W_4 = Q_1(X_2, X_1, X_3, X_4)$ were not only purely non-abelian but also normalized. Now we are ready for a definition:

An endomorphism θ of a loop G will be called *normal* provided (2.22) holds for every choice of a positive integer n, a normalized purely non-abelian loop word W_n, and elements $x_1, \cdots, x_n$ of G.

We see at once that a normal endomorphism is both weakly normal and seminormal. In addition, since F_n' is countable for each positive integer n, the set of inequivalent defining identities for a normal endomorphism is countably infinite. The definition is highly symmetric in that it involves all normalized purely non-abelian loop words. We may note as well that (2.22) can be given a more symmetric form (comparable with (2.4) or (2.5)) in which the right-hand side is replaced in turn by each of

$$W_n(x_1, x_2\theta, \cdots, x_n), \cdots, W_n(x_1, \cdots, x_n\theta).$$

To see this, we need only observe that if W_n is a normalized purely non-abelian word, and if $i \to i'$ is a permutation of $1, 2, \cdots, n$, the loop word V_n defined by

$$V_n(X_1, \cdots, X_n) = W_n(X_{1'}, \cdots, X_{n'})$$

is also normalized purely non-abelian.

Our final definition must be preceded by some brief remarks. If λ, μ are two single-valued mappings of a loop G into itself, we define their ordered product $\lambda\mu$ and their ordered sum $\lambda + \mu$ as follows:

$$(2.23) \qquad x(\lambda\mu) = (x\lambda)\mu, \qquad x(\lambda + \mu) = (x\lambda)(x\mu)$$

for all x in G. The system $(S, +, \cdot)$, consisting of the set of all single-valued mappings of G into G under the operations just defined, is a semigroup under $\cdot$ and a loop under $+$. Moreover,

$$(2.24) \qquad \lambda(\mu + \nu) = \lambda\mu + \lambda\nu$$

for all λ, μ, ν in S, and

$$(2.25) \qquad (\lambda + \mu)\theta = \lambda\theta + \mu\theta$$

for all λ, μ in S provided θ is an endomorphism of G. The *zero mapping*, 0, and the *identity mapping*, 1, are defined as follows:

$$(2.26) \qquad x0 = 1, \qquad x1 = x$$

for all x in G. Each element λ of S uniquely determines a (right-hand) *complement*, λ', such that

$$(2.27) \qquad \lambda + \lambda' = 1 = \text{the identity mapping.}$$

An element λ of S is called *centralizing* provided that $G\lambda$ is contained in the centre Z of G.

We define an endomorphism θ of G to be *strongly normal* provided that
(i) θ' is an endomorphism of G;
(ii) $\theta'\theta$ is centralizing.
Here θ' is the complement of θ (cf. (2.27)).

THEOREM 2.1. *Let θ be an endomorphism of a loop G. Then each of the following statements (after the first) implies those which precede it:*
(i) *θ is seminormal.*
(ii) *θ is weakly normal.*

(iii) θ *is normal.*
(iv) θ *is strongly normal.*

Proof. In view of the preceding discussion, we need only prove that (iv) implies (iii). Accordingly we assume (iv). Let W_n be a normalized purely non-abelian loop word, and let $x_1, x_2, \cdots, x_n$ be arbitrary elements of G. Then, since $1 = \theta + \theta'$ and since θ, θ' are endomorphisms of G,

$$\begin{aligned} W_n(x_1\theta, x_2, \cdots, x_n) &= [W_n(x_1\theta, x_2, \cdots, x_n)\theta][W_n(x_1\theta, x_2, \cdots, x_n)\theta'] \\ &= W_n(x_1\theta^2, x_2\theta, \cdots, x_n\theta)W_n(x_1\theta\theta', x_2\theta', \cdots, x_n\theta'). \end{aligned}$$

Since $\theta = (\theta + \theta')\theta = \theta^2 + \theta'\theta$, and since $\theta'\theta$ is centralizing,

$$x_1\theta^2 = (x_1\theta)c$$

for some c in Z. Therefore, since W_n is purely non-abelian,

$$\begin{aligned} W_n(x_1\theta^2, x_2\theta, \cdots, x_n\theta) &= W_n(x_1\theta\cdot c, x_2\theta, \cdots, x_n\theta) \\ &= W_n(x_1\theta, x_2\theta, \cdots, x_n\theta) \\ &= W_n(x_1, x_2, \cdots, x_n)\theta. \end{aligned}$$

Since $\theta^2 + \theta\theta' = \theta(\theta + \theta') = \theta = (\theta + \theta')\theta = \theta^2 + \theta'\theta$, then $\theta\theta' = \theta'\theta$. Accordingly, since $\theta'\theta$ is centralizing, and since W_n is both purely non-abelian and normalized,

$$W_n(x_1\theta\theta', x_2\theta', \cdots, x_n\theta') = W_n(1, x_2\theta', \cdots, x_n\theta') = 1.$$

Now we have

$$W_n(x_1\theta, x_2, \cdots, x_n) = W_n(x_1, x_2, \cdots, x_n)\theta,$$

which shows that θ is normal. This completes the proof of Theorem 2.1.

The following theorem is informative but is not essential for the sequel:

THEOREM 2.2. *Let G be a loop. Then*
(i) *Every centralizing endomorphism of G is strongly normal.*
(ii) *If θ, θ' are a pair of complementary decomposition endomorphisms of G (that is, a pair of idempotent endomorphisms of G such that $\theta + \theta' = 1$), then θ and θ' are strongly normal.*

3. Elementary properties

In order not to interrupt the flow of the discussion which follows we begin by recalling a few standard definitions.

To each element x of a loop G correspond two permutations $R(x)$, $L(x)$ of G, the *right* and *left multiplication by x*, respectively, defined by

$$yR(x) = yx, \qquad yL(x) = xy \tag{3.1}$$

for all y in G. The set of all right and left multiplications of G generates the *multiplication group*, $\mathfrak{M}(G)$. The *inner mapping group*, $\mathfrak{I}(G)$, is the subgroup of $\mathfrak{M}(G)$ consisting of all α in $\mathfrak{M}(G)$ such that $1\alpha = 1$ where 1 is the identity element of G. The inner mapping group is generated by the set of all permutations $R(x, y)$, $L(x, y)$, $T(x)$, where x, y range over G. Here

$$(3.2)\qquad \begin{gathered} R(x, y) = R(x)R(y)R(xy)^{-1}, \qquad L(x, y) = L(x)L(y)L(yx)^{-1}, \\ T(x) = R(x)L(x)^{-1}. \end{gathered}$$

The *nucleus*, $N = N(G)$, of G, consists of all c in G such that

$$(3.3)\qquad (c, x, y) = (x, c, y) = (x, y, c) = 1$$

for all x, y in G. The nucleus is a subgroup of G. The centre, $Z = Z(G)$, consists of all c in N such that

$$(3.4)\qquad (c, x) = 1.$$

Now we turn to the study of the four classes of endomorphisms defined in §2.

LEMMA 3.1. *Let θ, ϕ, ψ be single-valued mappings of a loop G into itself such that*

(a) $\theta + \phi = \psi$;

(b) *some two of θ, ϕ, ψ are endomorphisms of G.*

A necessary and sufficient condition that the third mapping be also an endomorphism of G is that

$$(3.5)\qquad [(x\theta)(x\phi)][(y\theta)(y\phi)] = [(x\theta)(y\theta)][(x\phi)(y\phi)]$$

for all x, y in G.

Remark. In terms of (2.21), (3.5) is equivalent to

$$f_4(x\theta, x\phi, y\theta, y\phi) = 1.$$

Proof. First assume that θ, ϕ are endomorphisms of G. Then the left-hand side of (3.5) is equal to $(x\psi)(y\psi)$ and the right-hand side of (3.5) is equal to $(xy)\psi$. Therefore (3.5) is necessary and sufficient in order that ψ be an endomorphism of G.

Next assume that θ, ψ are endomorphisms of G. Then the left-hand side of (3.5) is equal to

$$(x\psi)(y\psi) = (xy)\psi = [(xy)\theta][(xy)\phi] = [(x\theta)(y\theta)][(xy)\phi].$$

Therefore (3.5) is necessary and sufficient in order that ϕ be an endomorphism of G.

Similarly, if ϕ, ψ are endomorphisms of G, then (3.5) is necessary and sufficient in order that θ be an endomorphism of G. This completes the proof of Lemma 3.1.

LEMMA 3.2. *Let θ' be the complement of the endomorphism θ of the loop G. Then the following identities ensure that θ' is an endomorphism of G:*

$$
\begin{aligned}
&\text{(i)} & (x\theta, x\theta', y) &= 1,\\
&\text{(ii)} & (x\theta', y\theta, y\theta') &= 1,\\
&\text{(iii)} & (x\theta', y\theta) &= 1,\\
&\text{(iv)} & (y\theta, x\theta', y\theta') &= 1,\\
&\text{(v)} & (x\theta, y\theta, x\theta'\cdot y\theta') &= 1,
\end{aligned}
$$

for all x, y in G.

Proof. By the definition (2.27), $\theta + \theta' = 1$. Since θ and 1 are endomorphisms, we need only prove (3.5) with ϕ replaced by θ'. Using (i)–(v) in order, we get

$$
\begin{aligned}
[(x\theta)(x\theta')][(y\theta)(y\theta')] &= (x\theta)\{(x\theta')[(y\theta)(y\theta')]\}\\
&= (x\theta)\{[(x\theta')(y\theta)](y\theta')\}\\
&= (x\theta)\{[(y\theta)(x\theta')](y\theta')\}\\
&= (x\theta)\{(y\theta)[(x\theta')(y\theta')]\}\\
&= [(x\theta)(y\theta)][(x\theta')(y\theta')]
\end{aligned}
$$

for all x, y in G. This completes the proof of Lemma 3.2.

LEMMA 3.3. *If θ is a normal endomorphism of a loop G, then θ commutes with every inner mapping of G.*

Proof. See Lemma 4.1(ii) of [SIV.4].

LEMMA 3.4. *Let G be a loop with commutator-associator subloop G', centre Z. Let θ, ϕ be seminormal endomorphisms of G. Then*

(i) $\theta + \phi = \phi + \theta$;

(ii) *$\theta\phi$ is a seminormal endomorphism*;

(iii) *$a\theta = a\theta^3$ for every a in G'*;

(iv) *$a\theta\phi = a\phi\theta$ for every a in G'.*

Remark. In connection with (i), we do not claim that $\theta + \phi$ is an endomorphism.

Proof. This has been proved in [SIV.4], ostensibly for normal endomorphisms, but the proof really uses the hypothesis of seminormality except for one point. We need to observe for the present lemma that the product of two seminormal endomorphisms is seminormal, as is obvious from the definition.

LEMMA 3.5. *Let G be a loop with commutator-associator subloop G', centre Z. Let θ, ϕ be weakly normal endomorphisms of G. Then each of the following statements implies the other:*

(i) *There exists a centralizing endomorphism κ of G such that $\phi = \theta + \kappa$.*

(ii) *$a\theta = a\phi$ for every a in G'.*

Proof. (i) $\to$ (ii). If κ is a centralizing endomorphism, $G\kappa$ is an abelian group. Hence $G'\kappa = 1$. Therefore, if (i) holds, and if a is in G', $a\phi = (a\theta)(a\kappa) = a\theta$. Thus (i) implies (ii).

(ii) $\rightarrow$ (i). Define the mapping κ by $\phi = \theta + \kappa$. Suppose temporarily that κ is a centralizing mapping of G. Then, for all x, y in G,

$$[(x\theta)(x\kappa)][(y\theta)(y\kappa)] = [(x\theta)(y\theta)][(x\kappa)(y\kappa)].$$

Hence, by Lemma 3.1, κ is a (centralizing) endomorphism of G.

In order to prove that κ is centralizing, we must show that

$$(x\kappa, y, z) = (x, y\kappa, z) = (x, y, z\kappa) = (x\kappa, y) = 1$$

for all x, y, z in G. Since the details are similar in each case, we shall be content to show that (ii) implies that $(x\kappa, y) = 1$ for all x, y in G. We first observe that $x\kappa = (x\theta)\backslash(x\phi)$ for all x in G. Thus, by (2.7),

$$(x\kappa, z) = [(x\theta\backslash 1, z)(x\phi, z)]\cdot q(x\theta, x\phi, z).$$

Since ϕ is seminormal (in fact, weakly normal),

$$(x\phi, z) = (x, z)\phi.$$

Since (x, z) is in G', and since $a\phi = a\theta$ for each a in G',

$$(x, z)\phi = (x, z)\theta.$$

Since θ is seminormal,

$$(x, z)\theta = (x\theta, z).$$

Therefore

$$(x\phi, z) = (x\theta, z).$$

Similarly, but using this time the full hypothesis of weak normality, we prove that

$$q(x\theta, x\phi, z) = q(x\theta, x, z)\phi = q(x\theta, x, z)\theta = q(x\theta, x\theta, z).$$

Therefore

$$(x\kappa, z) = [(x\theta\backslash 1, z)(x\theta, z)]\cdot q(x\theta, x\theta, z) = (x\theta\backslash x\theta, z) = (1, z) = 1.$$

This completes the proof of Lemma 3.5.

THEOREM 3.1. *Let G be a loop with commutator-associator subloop G', centre Z. If θ is an endomorphism of G, each of the following statements implies all the others:*

(i) *θ commutes with every inner mapping of G, and $x\theta \equiv x\theta^2 \bmod Z$ for every x in G.*

(ii) *θ is seminormal, and $x\theta \equiv x\theta^2 \bmod Z$ for every x in G.*

(iii) *θ is weakly normal, and $a\theta = a\theta^2$ for every a in G'.*

(iv) *θ is normal, and $a\theta = a\theta^2$ for every a in G'.*

(v) *θ is strongly normal.*

COROLLARY. *The square of every weakly normal endomorphism is strongly normal.*

Proof. Let θ' denote the complement of θ. Thus $1 = \theta + \theta'$, $\theta = \theta^2 + \theta\theta'$, $\theta\theta' = \theta'\theta$.

(v) $\rightarrow$ (i), (ii), (iii), (iv). If θ is strongly normal, $\theta\theta'$ is a centralizing endomorphism. Thus $x\theta \equiv x\theta^2 \bmod Z$, and, moreover, $a\theta = a\theta^2$ for every a in G'. In addition, θ is normal, weakly normal, and seminormal. And, by Lemma 3.3, θ commutes with every inner mapping of G. Hence (v) implies all the other statements.

(iv) $\rightarrow$ (iii) $\rightarrow$ (ii). Certainly (iv) implies (iii). If (iii) holds, then, by Lemma 3.5, $\theta\theta'$ is a centralizing endomorphism. Thus $x\theta \equiv x\theta^2 \bmod Z$ for every x in G. Moreover, θ is seminormal. Hence (iii) implies (ii).

(ii) $\rightarrow$ (v). If (ii) holds, then, since $x\theta \equiv x\theta^2 \bmod Z$ for every x in G, the mapping $\theta\theta' = \theta'\theta$ is centralizing. We use this fact, together with the seminormality of θ, to prove the conditions (i)–(v) of Lemma 3.2. For example, (i) of Lemma 3.2 holds since

$$(x\theta, x\theta', y) = (x, x\theta'\theta, y) = 1;$$

and (v) of Lemma 3.2 holds since

$$(x\theta, y\theta, x\theta' \cdot y\theta') = (x\theta, y, x\theta'\theta \cdot y\theta'\theta) = 1.$$

The others are proved quite similarly. Hence θ' is an endomorphism, and $\theta\theta'$ is a centralizing endomorphism. This means that θ is strongly normal. Hence (ii) implies (v).

(i) $\rightarrow$ (v). If (i) holds, then $\theta'\theta$ is a centralizing mapping of G, and θ commutes with every inner mapping of G. We use these facts to prove the identities (i)–(v) of Lemma 3.2. First consider (i) of Lemma 3.2. This identity can be written as $[(x\theta)(x\theta')]y = (x\theta)[(x\theta')y]$ or as

$$(x\theta)R(x\theta', y) = x\theta.$$

Since θ commutes with every inner mapping,

$$(x\theta)R(x\theta', y) = xR(x\theta', y)\theta = x\theta R(x\theta'\theta, y\theta).$$

However, $R(x\theta'\theta, y\theta)$ is the identity mapping of G, since, for every z in G,

$$[z(x\theta'\theta)](y\theta) = z[(x\theta'\theta)(y\theta)]$$

by virtue of the fact that $\theta'\theta$ is centralizing. Consequently, (i) of Lemma 3.2 is true. The remaining identities of Lemma 3.2 are proved with a similar use of inner mappings. Hence (i) implies (v).

This completes the proof of Theorem 3.1. The corollary follows from Theorem 3.1 and Lemma 3.4 (iii). For if θ is weakly normal or even seminormal, $a\theta^2 = a(\theta^2)^2$ for every a in G'.

THEOREM 3.2. *Let G be a loop with centre Z, nucleus N. Let θ be a nuclearizing endomorphism of G, that is, an endomorphism mapping G into N. Let θ' denote the complement of θ. Then each of the following statements implies all the others:*

(i) $(x\theta, y\theta') = 1$ *for all x, y in G.*

(ii) $(x, y)\theta = (x\theta, y)$ *for all x, y in G.*

(iii) *θ' is an endomorphism of G.*
(iv) *θ commutes with every inner mapping of G.*
(v) *θ is seminormal.*
(vi) *θ is weakly normal.*
(vii) *θ is normal.*
(viii) *θ is strongly normal.*

COROLLARY. *If G is a group, and if θ is any endomorphism of G, each of the statements* (i)–(viii) *implies all the others.*

Proof. We first observe that the corollary is the special case of Theorem 3.2 in which $G = N$.

The implications

$$(\text{viii}) \rightarrow (\text{vii}) \rightarrow (\text{vi}) \rightarrow (\text{v})$$

follow from Theorem 2.1. The implication

$$(\text{vii}) \rightarrow (\text{iv})$$

follows from Lemma 3.3. The implications

$$(\text{v}) \rightarrow (\text{ii}), \qquad (\text{viii}) \rightarrow (\text{iii})$$

are a consequence of the definitions of seminormal and strongly normal endomorphisms, respectively. Hence it will suffice to prove the following:
(A) (i) $\leftrightarrow$ (iii).
(B) (iv) $\rightarrow$ (ii) $\rightarrow$ (i) $\rightarrow$ (viii).

Proof of (A). Since $\theta + \theta' = 1$, and since θ, 1 are endomorphisms of G, we see from Lemma 3.1 that θ' will be an endomorphism of G if and only if G satisfies the identity

$$[(x\theta)(x\theta')][(y\theta)(y\theta')] = [(x\theta)(y\theta)][(x\theta')(y\theta')].$$

Since $G\theta$ is part of N, this identity is easily seen to be equivalent to

$$(x\theta')(y\theta) = (y\theta)(x\theta').$$

Hence (i) is equivalent to (iii).

Proof of (B). First we assume (iv). Then, since $G\theta$ is part of the group N,

$$x\theta T(y) = xT(y)\theta = x\theta T(y\theta) = (y\theta)^{-1}(x\theta)(y\theta) = (x\theta)(x\theta, y\theta),$$

and

$$(x\theta)y = y[x\theta T(y)] = y[(x\theta)(x\theta, y\theta)] = [y(x\theta)](x\theta, y\theta),$$

showing that

$$(x\theta, y) = (x\theta, y\theta) = (x, y)\theta.$$

Therefore (iv) implies (ii).

Before assuming (ii) we note that, since $(x, yz)\theta = (x\theta, y\theta \cdot z\theta)$, and since $G\theta$ is a group, a known identity for commutators in a group gives

$$(3.6) \qquad (x, yz)\theta = (x\theta, z\theta)(z\theta)^{-1}(x\theta, y\theta)(z\theta).$$

Now we assume (ii). From (3.6),

$$1 = (y, y)\theta = (y, y\theta \cdot y\theta')\theta = (y\theta, y\theta'\theta)(y\theta'\theta)^{-1}(y\theta, y\theta^2)(y\theta'\theta).$$

However, by (ii),

$$(y\theta, y\theta^2) = (y, y\theta)\theta = (y\theta, y\theta) = 1.$$

Therefore, by (ii) again,

$$1 = (y\theta, y\theta'\theta) = (y, y\theta')\theta = (y\theta, y\theta').$$

Thus we see that

$$y = (y\theta)(y\theta') = (y\theta')(y\theta)$$

for every y.

We use this last fact in (3.6) to get

$$(x, y)\theta = (x, y\theta' \cdot y\theta)\theta = (x\theta, y\theta^2)(y\theta^2)^{-1}(x\theta, y\theta'\theta)(y\theta^2).$$

However, by (ii),

$$(x\theta, y\theta^2) = (x, y\theta)\theta = (x\theta, y\theta) = (x, y)\theta,$$

allowing us to conclude, first, that

$$1 = (y\theta^2)^{-1}(x\theta, y\theta'\theta)(y\theta^2),$$

and thence that

$$1 = (x\theta, y\theta'\theta) = (x, y\theta')\theta = (x\theta, y\theta').$$

Hence (ii) implies (i).

Finally we assume (i). Consider any x in G, and set $c = x\theta\theta' = x\theta'\theta$. Then, by hypothesis, c is in N. Moreover, for any y: since $c = x\theta\theta'$, then $(c, y\theta) = 1$, and, since $c = x\theta'\theta$, then $(c, y\theta') = 1$. Hence

$$\begin{aligned} cy &= c[(y\theta)(y\theta')] = [c(y\theta)](y\theta') = [(y\theta)c](y\theta') \\ &= (y\theta)[c(y\theta')] = (y\theta)[(y\theta')c] = [(y\theta)(y\theta')]c \\ &= yc. \end{aligned}$$

This means that c is in the centre Z. Since $c = x\theta\theta'$ is in Z for each x, the mapping $\theta\theta'$ is centralizing. Since (i) implies (iii) (by (A)), θ' is an endomorphism of G. Therefore θ is strongly normal. That is, (i) implies (viii).

This completes the proof of Theorem 3.2.

When G is a group (in view of the Corollary to Theorem 3.2) any one of the statements (i)–(viii) of Theorem 3.2 can be used to define a "normal" endomorphism of G. The usual definition is (iv) (with "mappings" replaced by "automorphisms"). The equivalence of (iii), (iv) for groups is certainly well known; and the equivalence of (iv), (viii) for groups is probably known also. On the other hand, the equivalence of (iv), (vii) for groups is certainly new, and a direct proof would probably be very difficult.

THEOREM 3.3. *If θ, ϕ are weakly normal endomorphisms of a loop G, then the commutator-mapping (θ, ϕ), defined by*

$$\theta\phi = \phi\theta + (\theta, \phi), \tag{3.7}$$

is a centralizing endomorphism of G.

Remarks. 1. Theorem 3.3 generalizes Specht's Lemma (W. SPECHT, *Gruppentheorie*, p. 227, Satz 7) in two respects. Specht stated his lemma (a) only for groups, and (b) only for the case that θ and ϕ are idempotent.

2. As the proof will show, Lemma 3.5 may also be regarded as a generalization of Specht's Lemma.

Proof. Since θ, ϕ are (a fortiori) seminormal, Lemma 3.4(iii) tells us that $a\theta\phi = a\phi\theta$ for every a in G'. Since the product of two weakly normal endomorphisms is easily seen to be weakly normal, Lemma 3.5 now allows us to conclude that (θ, ϕ) is a centralizing endomorphism of G. This completes the proof of Theorem 3.3.

4. The complement of a normal endomorphism

One of the conclusions that may be drawn from the Corollary to Theorem 3.2 is the (well-known) fact that the complement of a normal endomorphism of a *group* is itself a normal endomorphism. Our first use of the lemma which follows will be to prove the corresponding fact for loops.

LEMMA 4.1. *Let W_n be any normalized purely non-abelian loop word. Let θ be a normal endomorphism, with complement θ', of a loop G. Then*

(I) *If $x_1, \cdots, x_n$ are arbitrary elements of G,*

$$W_n(x_1\theta', x_2, \cdots, x_n) = W_n(x_1, x_2, \cdots, x_n)\theta', \tag{4.1}$$

$$W_n(x_1\theta\theta', x_2, \cdots, x_n) = W_n(x_1, x_2, \cdots, x_n)\theta\theta'. \tag{4.2}$$

(II) *If either*

(a) *n is even, and $x_1, \cdots, x_n$ are arbitrary elements of G, or*

(b) *n is odd, and $x_1, \cdots, x_n$ are elements of G subject only to the restriction that (if $n > 1$) some two are equal,*

then

$$W_n(x_1, x_2, \cdots, x_n)\theta\theta' = 1. \tag{4.3}$$

Proof. Since $1 = \theta + \theta'$ and θ is an endomorphism, we may introduce a mapping ϕ which satisfies

$$\theta\theta' = \theta'\theta = \phi, \tag{4.4}$$

$$\theta = \theta^2 + \phi. \tag{4.5}$$

In the course of the proof we shall need the loop words P_{n+1}, Q_{n+1} defined by

(4.6) $W_n(XY, Z_2, \cdots, Z_n)$
$$= [W_n(X, Z_2, \cdots, Z_n)W_n(Y, Z_2, \cdots, Z_n)]P_{n+1}(X, Y, Z_2, \cdots, Z_n),$$

(4.7) $W_n(X\backslash Y, Z_2, \cdots, Z_n)$
$$= [W_n(X\backslash 1, Z_2, \cdots, Z_n)W_n(Y, Z_2, \cdots, Z_n)]Q_{n+1}(X, Y, Z_2, \cdots, Z_n).$$

We observe here that P_{n+1}, Q_{n+1} are normalized and purely non-abelian. Our first step is to prove the following:

(A) *If n is even,*

$$W_n(x_1, x_2, \cdots, x_n)\phi = 1 = W_n(x_1\phi, x_2, \cdots, x_n) \tag{4.8}$$

for all $x_1, x_2, \cdots, x_n$ in G.

Proof of (A). By Lemma 3.4, since θ is a normal endomorphism,

$$a\theta = a\theta^3 \tag{4.9}$$

for every a in G'. Moreover,

$$W_n(x_1, \cdots, x_n)\theta = W_n(x_1\theta, \cdots, x_n\theta) = W_n(x_1, \cdots, x_n)\theta^n. \tag{4.10}$$

Since $W_n(x_1, \cdots, x_n)$ is in G', and since n is even, we deduce from (4.9), (4.10) that

$$W_n(x_1, \cdots, x_n)\theta = W_n(x_1, \cdots, x_n)\theta^2 \tag{4.11}$$

for all x_i in G. By (4.11) and (4.5),

$$W_n(x_1, \cdots, x_n)\phi = 1 \tag{4.12}$$

for all x_i in G. Again, by (4.11), (4.7), and the fact that θ is an endomorphism,

$$Q_{n+1}(x, y, z_2, \cdots, z_n)\theta = Q_{n+1}(x, y, z_2, \cdots, z_n)\theta^2 \tag{4.13}$$

for all $x, y, z_2, \cdots, z_n$ in G.

We see by (4.5) that $x\phi = x\theta^2\backslash x\theta$ for all x in G. Thence, by (4.7),

(4.14) $W_n(x\phi, z_2, \cdots, z_n)$
$$= [W_n(x\theta^2\backslash 1, z_2, \cdots, z_n)W_n(x\theta, z_2, \cdots, z_n)]Q_{n+1}(x\theta^2, x\theta, z_2, \cdots, z_n).$$

Using (4.11), along with the fact that θ is a normal endomorphism, we get

$$\begin{aligned} W_n(x\theta^2\backslash 1, z_2, \cdots, z_n) &= W_n(x\backslash 1, z_2, \cdots, z_n)\theta^2 \\ &= W_n(x\backslash 1, z_2, \cdots, z_n)\theta \\ &= W_n(x\theta\backslash 1, z_2, \cdots, z_n). \end{aligned}$$

Similarly, by use of (4.13),

$$\begin{aligned} Q_{n+1}(x\theta^2, x\theta, z_2, \cdots, z_n) &= Q_{n+1}(x, x\theta, z_2, \cdots, z_n)\theta^2 \\ &= Q_{n+1}(x\theta, x\theta, z_2, \cdots, z_n). \end{aligned}$$

On making the two indicated changes in the right-hand side of (4.14), we get a product which is equal, by (4.7), to

$$W_n(x\theta\backslash x\theta, z_2, \cdots, z_n) = 1.$$

Consequently,

$$W_n(x\phi, z_2, \cdots, z_n) = 1$$

for all $x, z_2, \cdots, z_n$ in G. And this, taken along with (4.12), completes the proof of (A).

(B) *If n is odd, and if some two of $x_1, \cdots, x_n$ are equal,*

$$W_n(x_1, \cdots, x_n)\phi = 1. \tag{4.15}$$

Proof of (B). We may assume without loss of generality that $n > 1$. Then the loop word U_{n-1} defined by

$$U_{n-1}(X, Z_3, \cdots, Z_n) = W_n(X, X, Z_3, \cdots, Z_n)$$

is normalized and purely non-abelian. Since $n - 1$ is even, we deduce from (A) that

$$U_{n-1}(x, z_2, \cdots, z_n)\phi = 1$$

for all $x, z_3, \cdots, z_n$ in G. This proves (4.15) for the case that $x_1 = x_2$. The proof for the remaining cases is quite similar.

(C) *If n is odd, then*

$$W_n(x_1\theta', x_2, \cdots, x_n) = W_n(x_1, x_2, \cdots, x_n)\theta', \tag{4.16}$$

$$W_n(x_1\phi, x_2, \cdots, x_n) = W_n(x_1, x_2, \cdots, x_n)\phi \tag{4.17}$$

for all x_i in G.

Proof of (C). Since $n + 1$ is even, we may apply (A) to any loop word V_{n+1}. If P_{n+1} is defined by (4.6) and V_{n+1} by

$$V_{n+1}(X, Y, Z_2, \cdots, Z_n) = P_{n+1}(Y, X, Z_2, \cdots, Z_n),$$

we deduce in particular that

$$P_{n+1}(y, x, z_2, \cdots, z_n)\phi = 1 = P_{n+1}(y, x\phi, z_2, \cdots, z_n) \tag{4.18}$$

for all $x, y, z_2, \cdots, z_n$ in G. Since $x = (x\theta)(x\theta')$, (4.6) yields

$$\begin{aligned} &W_n(x, z_2, \cdots, z_n) \\ &= [W_n(x\theta, z_2, \cdots, z_n)W_n(x\theta', z_2, \cdots, z_n)]P_{n+1}(x\theta, x\theta', z_2, \cdots, z_n). \end{aligned} \tag{4.19}$$

Since θ is a normal endomorphism,

$$P_{n+1}(x\theta, x\theta', z_2, \cdots, z_n) = P_{n+1}(x, x\theta'\theta, z_2, \cdots, z_n) = 1$$

by (4.4), (4.18). In addition,

$$W_n(x\theta, z_2, \cdots, z_n) = W_n(x, z_2, \cdots, z_n)\theta.$$

Therefore, by (4.19),

$$(4.20)\quad W_n(x, z_2, \cdots, z_n) = [W_n(x, z_2, \cdots, z_n)\theta]W_n(x\theta', z_2, \cdots, z_n)$$

for all $x, z_2, \cdots, z_n$ in G. Since $y = (y\theta)(y\theta')$ for all y in G, (4.20) implies that

$$W_n(x\theta', z_2, \cdots, z_n) = W_n(x, z_2, \cdots, z_n)\theta'$$

for all $x, z_2, \cdots, z_n$ in G. That is, (4.16) holds. By (4.16), (4.4), and the normality of θ we immediately get (4.17), completing the proof of (C).

(D) *If n is even, then* (4.16), (4.17) *hold for all x_i in G.*

Proof of (D). Since $n + 1$ is odd, we may apply (C) and (B) to any loop word V_{n+1}. We deduce in particular that

$$P_{n+1}(x, x\phi, z_2, \cdots, z_n) = P_{n+1}(x, x, z_2, \cdots, z_n)\phi = 1.$$

Consequently, as in the proof of (C), the equation (4.19) leads to the equation (4.20). Moreover, (4.20) implies (4.16) and hence (4.17). This completes the proof of (D).

In view of (C), (D), we have proved (I) of Lemma 4.1. And in view of (A), (B), we have proved (II) of Lemma 4.1. This completes the proof of Lemma 4.1.

THEOREM 4.1. *If θ is a normal endomorphism of a loop G, the complement, θ', of θ is also a normal endomorphism of G. Moreover, θ is the complement of θ': $\theta = (\theta')'$.*

Proof. By (4.1) of Lemma 4.1, θ' will be normal if θ' is an endomorphism. And θ' will be an endomorphism if the identities (i)–(v) of Lemma 3.2 are valid. To prove (i) we apply Lemma 4.1 to the associator word

$$W_3(X_1, X_2, X_3) = (X_1, X_2, X_3),$$

getting

$$(x\theta, x\theta', y) = (x, x\theta'\theta, y) = (x, x, y)\theta\theta' = 1.$$

The proofs of (ii), (iii), (iv) are quite similar. To prove (v) we need the word P_3 of (2.10). (Note that, despite the subscript, P_3 is a (normalized, purely non-abelian) word W_4.) We have

$$(x\theta, y\theta, x\theta' \cdot y\theta') = [(x\theta, y\theta, x\theta')(x\theta, y\theta, y\theta')]P_3(x\theta', y\theta', x\theta, y\theta).$$

By the normality of θ and by application of Lemma 4.1, each of the three factors is equal to 1. This proves (v). Thus θ' is an endomorphism. Finally, since

$$(x\theta, x\theta') = (x, x)\theta\theta' = 1$$

for all x in G, we have $\theta' + \theta = \theta + \theta' = 1$, whence we see that $\theta = (\theta')'$. This completes the proof of Theorem 4.1.

5. The Moufang centre

The *Moufang centre*, $C = C(G)$, of a loop G is defined to be the set of all elements a in G such that

$$(ax)(ay) = a^2(xy) \tag{5.1}$$

for all x, y in G. Passing reference to the Moufang centre is made in [SVI.1]. Here we need to study the concept more closely.

LEMMA 5.1. *The Moufang centre $C = C(G)$ of a loop G is a subloop of G. An element a of G is in C if and only if*

$$ax = xa, \tag{5.2}$$

$$(ax)(ya) = [a(xy)]a \tag{5.3}$$

for all x, y in G.

Remark. A loop is called a *Moufang* loop if (5.3) holds for all elements a, x, y of the loop. Thus, we have a corollary of Lemma 5.1: *the Moufang centre of a loop is a commutative Moufang subloop.*

Proof. We shall make use of the set P of all ordered pairs (θ, ϕ) of permutations θ, ϕ of G such that

$$(x\theta)(y\theta) = (xy)\phi \tag{5.4}$$

for all x, y in G. Clearly P is a group under componentwise multiplication. That P is appropriate for the proof of Lemma 5.1 may be seen as follows:

Let us call an element a of G a *P-element* provided there exists at least one permutation ϕ of G such that $(L(a), \phi)$ is in P. Equivalently,

$$(ax)(ay) = (xy)\phi \tag{5.5}$$

for all x, y in G. By (5.1), an element a of G is in C if and only if (5.5) holds with

$$\phi = L(a^2). \tag{5.6}$$

On the other hand, from (5.5) with $x = a$, we derive (5.6). That is, *the P-elements are precisely the elements of C.*

Taking first $x = 1$ and then $y = 1$ in (5.5), we find that

$$\phi = L(a)^2, \tag{5.7}$$

$$\phi = L(a)R(a). \tag{5.8}$$

By (5.5), (5.7), (5.8), a P-element a satisfies (5.2), (5.3). Conversely, an element a satisfying (5.2), (5.3) is a P-element.

Let a be a P-element, and let x be any element of G. From (5.5), (5.7) we get

$$L(a)L(ax) = L(x)\phi = L(x)L(a)^2.$$

From this and the fact that P is a group we deduce that ax is a P-element precisely when x is. Since, in addition, $ax = xa$ for all x in G, we have proved that C is a subloop of G. This completes the proof of Lemma 5.1.

For the next lemma we need the concept of the *upper central series* $\{Z_i\}$ of a loop G. Here $Z_0 = 1$, $Z_1 = Z =$ the centre of G, and, for $i \geqq 0$, Z_{i+1} is the uniquely defined subloop containing Z_i such that Z_{i+1}/Z_i is the centre of G/Z_i. For the properties of central series see [SVI].

LEMMA 5.2. *Let θ be a normal endomorphism of a loop G with commutator-associator subloop G', upper central series $\{Z_i\}$, and Moufang centre C. Set $\phi = \theta\theta'$, where θ' is the complement of θ. Then ϕ is a normal endomorphism of G such that*

$$\text{(i)} \quad G'\phi \subset Z, \qquad \text{(ii)} \quad G\phi \subset C \cap Z_2 .$$

Proof. By Theorem 4.1, θ' is a normal endomorphism of G. It is easily verified (and an explicit proof is given in [SIV.4]) that *the product of two normal endomorphisms is a normal endomorphism.* Hence $\phi = \theta\theta' = \theta'\theta$ is a normal endomorphism. We complete the proof in several stages.

(A) *If W_n is a normalized purely non-abelian loop word, then*

$$(5.9) \quad W_n(xy, z_2, \cdots, z_n)\phi = [W_n(x, z_2, \cdots, z_n)\phi][W_n(y, z_2, \cdots, z_n)\phi]$$

for all $x, y, z_2, \cdots, z_n$ in G. Analogous formulas hold when the product xy appears in any other position on the left side of (5.9).

Proof of (A). If n is even, each of the three terms in (5.9) is equal to 1 by Lemma 4.1. Certainly, then, (5.9) holds for even n. If n is odd, so that $n + 1$ is even, and if P_{n+1} is the loop word defined by (4.6), then

$$P_{n+1}(x, y, z_2, \cdots, z_n)\phi = 1$$

by Lemma 4.1, whence (5.9) holds for odd n. This proves (5.9) in all cases. As to the concluding sentence of (A), we recall that if $i \rightarrow i'$ is a permutation of $1, 2, \cdots, n$, and if

$$V_n(X_1, X_2, \cdots, X_n) = W_n(X_{1'}, X_{2'}, \cdots, X_{n'}),$$

then V_n is a normalized purely non-abelian loop word. This completes the proof of (A).

(B) *The loop $G\phi$ is commutative. Moreover, $(G\phi, G) = 1$.*

Proof of (B). Applying Lemma 4.1 to the commutator word, we see that

$$(5.10) \qquad (x, y)\phi = 1 = (x\phi, y)$$

for all x, y in G.

(C) *The formulas*

$$(5.11) \qquad (x, x, y)\phi = (x, y, x)\phi = (y, x, x)\phi = 1,$$

(5.12) $$(wx, y, z)\phi = [(w, y, z)\phi][(x, y, z)\phi],$$

(5.13) $$(y, wx, z)\phi = [(y, w, z)\phi][(y, x, z)\phi],$$

(5.14) $$(y, z, wx)\phi = [(y, z, w)\phi][(y, z, x)\phi],$$

(5.15) $$1 = [(x, y, z)\phi][(y, x, z)\phi] = [(z, x, y)\phi][(y, x, z)\phi],$$

(5.16) $$(x, y, z)\phi = (z, x, y)\phi = (y, z, x)\phi,$$

hold for all w, x, y, z *in* G.

Proof of (C). By applying Lemma 4.1 to the word $W_2 = (X, X, Y)$, we get $(x, x, y)\phi = 1$ for all x, y in G, and similarly for the rest of (5.11). The formulas (5.12), (5.13), (5.14) are special cases of (A). By (5.11) and (5.12),

$$1 = (xy, xy, z)\phi = [(x, xy, z)\phi][(y, xy, z)\phi].$$

By (5.13) and (5.11),

$$(x, xy, z)\phi = (x, y, z)\phi, \qquad (y, xy, z)\phi = (y, x, z)\phi.$$

Therefore

$$1 = [(x, y, z)\phi][(y, x, z)\phi].$$

Similarly, by (5.11), (5.14), (5.12), and (5.11),

$$1 = (yz, x, yz)\phi = [(yz, x, y)\phi][(yz, x, z)\phi] = [(z, x, y)\phi][(y, x, z)\phi].$$

This proves (5.15); and (5.15) implies (5.16).

(D) $G'\phi \subset Z$.

Proof of (D). As a special case of (B), we have

(5.17) $$(G'\phi, G) = 1.$$

To complete the proof of (D), we must show that if a is a commutator or associator of G, then $a\phi$ lies in the nucleus N of G. By (5.10), if $a = (x, y)$, then $a\phi = 1 \in N$. There remains the case that $a = (x, y, z)$ for some x, y, z in G. In view of (5.12), the mapping

$$x \longrightarrow (x, u, v)\phi$$

is an endomorphism of G for each pair u, v of elements of G. Hence

$$\begin{aligned}(a, u, v)\phi &= \big((x, u, v)\phi, (y, u, v)\phi, (z, u, v)\phi\big)\\ &= \big((x, u, v), (y, u, v), (z, u, v)\big)\phi.\end{aligned}$$

However, by applying Lemma 4.1 to the loop word

$$W_6 = \big((X_1, X_4, X_5), (X_2, X_4, X_5), (X_3, X_4, X_6)\big),$$

we deduce in particular that

$$W_6(x, y, z, u, v, v)\phi = 1$$

for all x, y, z, u, v in G. Therefore

$$(a\phi, u, v) = (a, u, v)\phi = 1$$

for all u, v. Similarly

$$(u, a\phi, v) = (u, v, a\phi) = 1,$$

whence we see that $a\phi$ lies in N. This completes the proof of (D).

(E) $G\phi \subset Z_2$.

Proof of (E). To prove (E) we must show that

$$(G\phi, x, y) \equiv (x, G\phi, y) \equiv (x, y, G\phi) \equiv (G\phi, x) \equiv 1 \mod Z$$

for all x, y in G. But these congruences are clear from (D), (B), and the normality of ϕ.

(F) $G\phi \subset C$.

Proof of (F). Let x be an arbitrary element of G, and set $c = x\phi$. To prove (F) we must show that

$$(5.18) \qquad (cy)(cz) = c^2(yz)$$

for all y, z in G. We shall transform the left-hand side of (5.18) into the right-hand side. By the normality of ϕ, together with (5.14), (5.11), (5.16),

$$\begin{aligned}(c, y, cz) &= (x, y, cz)\phi = [(x, y, c)\phi][(x, y, z)\phi] \\ &= [(x, y, x)\phi^2][(y, z, x)\phi] = (y, z, x)\phi \\ &= (y, z, c).\end{aligned}$$

Moreover, by (D), (y, z, c) is in Z. Hence

$$(5.19) \qquad (cy)(cz) = c[y(cz)](y, z, c).$$

Next, by (5.10) and (5.11), $(c, G) = (x, G)\phi = 1$, and $(c, c, G) = (x, x, G)\phi = 1$. Therefore (5.19) becomes

$$(cy)(cz) = c[y(zc)](y, z, c) = c[(yz)c] = c[c(yz)] = (cc)(yz).$$

This proves (F).

We note that (D) implies (i), and that (E), (F) imply (ii) of Lemma 5.2. This completes the proof of Lemma 5.2.

LEMMA 5.3. *Let θ be a normal endomorphism, with complement θ', of a loop G. Then $\phi = \theta\theta'$ is a strongly normal endomorphism of G.*

Proof. We have shown already that θ' and ϕ are normal endomorphisms. Next we prove that

$$(5.20) \qquad \begin{aligned}\phi + (\alpha + \beta) = (\phi + \alpha) + \beta, \qquad (\alpha + \phi) + \beta = \alpha + (\phi + \beta), \\ (\alpha + \beta) + \phi = \alpha + (\beta + \phi), \qquad \alpha + \phi = \phi + \alpha\end{aligned}$$

for all seminormal endomorphisms α, β of G. To begin with, by Lemma 4.1, $(x, x, x)\phi = 1$, and hence

$$(x\phi, x\alpha, x\beta) = (x\alpha, x\phi, x\beta) = (x\alpha, x\beta, x\phi) = (x, x, x)\phi\alpha\beta = 1$$

for all x in G. This is enough to prove the first three equations of (5.20). The last comes from the fact that $(x\alpha, x\phi) = (x, x)\phi\alpha = 1$ for all x in G.

From (5.20) together with the equations (4.4), (4.5), and $\theta = (\theta')'$, we deduce that

$$\begin{aligned} 1 = \theta + \theta' &= (\theta^2 + \phi) + \theta' = \theta^2 + (\phi + \theta') \\ &= \phi + (\theta^2 + \theta') = \phi + [(\theta')^2 + \theta]. \end{aligned} \tag{5.21}$$

In particular, the complements of ϕ and θ^2 are given by

$$\phi' = \theta^2 + \theta' = (\theta')^2 + \theta, \tag{5.22}$$

$$(\theta^2)' = \phi + \theta'; \tag{5.23}$$

and these complements are normal endomorphisms by Theorem 4.1.

Since $\phi = \theta\theta' = \theta'\theta$, we see from (5.22), (5.23) that

$$\phi\phi' = \phi[(\theta')^2 + \theta] = \theta(\theta')^3 + \theta\phi, \tag{5.24}$$

$$\theta^2(\theta^2)' = \theta^2(\phi + \theta') = \theta^3\theta' + \theta\phi. \tag{5.25}$$

Since, in addition, θ and θ' are normal endomorphisms, we see from (5.24), (5.25), and Lemma 3.4 that

$$a\phi\phi' = a(\phi + \theta\phi) = a\theta^2(\theta^2)' \tag{5.26}$$

for every a in G'.

By (5.26) and Lemma 3.5,

$$\phi\phi' = \theta^2(\theta^2)' + \kappa, \tag{5.27}$$

where κ is a centralizing endomorphism. However, by the Corollary to Theorem 3.1, θ^2 is strongly normal, whence $\theta^2(\theta^2)'$ is centralizing. Hence $\phi\phi'$ is centralizing, ϕ is strongly normal; and the proof of Lemma 5.3 is complete.

We are now in a position to state

THEOREM 5.1. *If θ is a normal endomorphism of a loop G, then θ can be expressed in at least one way as a sum of two strongly normal endomorphisms of G. In particular, $\theta = \theta^2 + \theta\theta'$; and θ^2, $\theta\theta'$ are strongly normal endomorphisms of G.*

Proof. The theorem follows from the Corollary to Theorem 3.1 and from Lemma 5.3.

6. Characterizations of normality

Under the hypotheses of Lemma 5.2, the subloop

$$M = G\phi \tag{6.1}$$

of G is, in particular, by (ii) (of Lemma 5.2), a commutative Moufang loop. In addition, by (i) or (ii),

$$M' \subset G'\phi \cap M \subset Z(G) \cap M \subset Z(M),$$

and therefore

$$M = Z_2(M). \tag{6.2}$$

Thus it is clear that the following lemma is appropriate to our present study:

LEMMA 6.1. *Let W_n be a normalized purely non-abelian loop word. Let ϕ be a homomorphism of a loop G such that $M = G\phi$ is a commutative Moufang loop satisfying* (6.2), *where $\{Z_i(M)\}$ is the upper central series of M. Then either*

(i) $W_n(x_1, \cdots, x_n)\phi = 1$ *for all $x_1, \cdots, x_n$ in G; or*

(ii) $n = 3$, *and there exists an integer t, depending only on W_3 and having the value* 1 *or* 2, *such that*

$$W_3(x, y, z)\phi = [(x, y, z)\phi]^t \tag{6.3}$$

for all x, y, z in G.

COROLLARY. *The conclusions* (i) *or* (ii) *are valid when $\phi = \theta\theta'$ where θ is a normal endomorphism of G.*

Proof. The remarks preceding Lemma 6.1 show that the corollary follows from Lemma 6.1.

Now consider an arbitrary but fixed positive integer n. As shown in Bruck [2] (p. 316, Theorem 9A) there exists a unique "freest" commutative Moufang loop H such that

(a) H is generated by n elements $g_1, \cdots, g_n$;

(b) $H = Z_2(H)$;

(c) if $a_1, \cdots, a_n$ are elements of a commutative Moufang loop M satisfying (6.2), the mapping

$$g_i \to a_i \qquad (i = i, \cdots, n)$$

can be extended (uniquely) to a homomorphism of H into M.

In addition, if $n < 3$, $H' = 1$, and, if $n \geqq 3$, H' is an abelian group of exponent 3 with a minimal basis consisting of the associators

$$(g_i, g_j, g_k), \qquad 1 \leqq i < j < k \leqq n.$$

We begin by considering the element

$$w = W_n(g_1, \cdots, g_n) \tag{6.4}$$

of H. Since W_n is purely non-abelian, w is in H'. Hence, if $n < 3$, $w = 1$, and, if $n \geqq 3$,

$$(6.5) \qquad w = \prod\nolimits_{i<j<k} (g_i, g_j, g_k)^{a(i,j,k)}$$

for uniquely defined integral exponents in the range 0, 1, 2. Now suppose that $n > 3$, and consider any triple i, j, k with

$$1 \leqq i < j < k \leqq n.$$

By (c), H possesses a unique endomorphism which leaves each of g_i, g_j, g_k fixed and maps the remaining generators on 1. Since W_n is normalized, this endomorphism must map w on 1. Thus

$$1 = (g_i, g_j, g_k)^{a(i,j,k)}$$

for each such triple i, j, k; and hence $w = 1$. Finally, suppose $n = 3$, and set $t = a(1, 2, 3)$; then

$$(6.6) \qquad w = (g_1, g_2, g_3)^t,$$

and $t = 0$, 1, or 2. Thus the only case in which $w \neq 1$ is that in which $n = 3$ and $t = 1$ or 2.

In view of property (c) of H, we now can specify the values of W_n on any commutative Moufang loop M subject to (6.2). Since ϕ is a homomorphism of G upon a loop,

$$W_n(x_1, \cdots, x_n)\phi = W_n(x_1\phi, \cdots, x_n\phi)$$

for all $x_1, \cdots, x_n$ in G. This is enough for the proof of Lemma 6.1.

Now we are ready for a characterization of normal endomorphisms.

THEOREM 6.1. *The conditions* (I), (II) *below are both necessary and sufficient in order that the endomorphism θ of the loop G be a normal endomorphism of G:*

(I) *θ and its complement, θ', are endomorphisms of G such that the associator identity*

$$(6.7) \qquad (x, y, z)\kappa = (x\kappa, y, z)$$

holds both for $\kappa = \theta$ and for $\kappa = \theta'$, and for all x, y, z in G.

(II) *$\phi = \theta\theta'$ is a normal endomorphism of G such that the loop $M = G\phi$ is a commutative Moufang loop satisfying $M = Z_2(M)$ where $\{Z_i(M)\}$ is the upper central series of M.*

When (I), (II) *hold, θ' is a normal endomorphism of G, ϕ is a strongly normal endomorphism of G, and $M \subset C \cap Z_2$, where C is the Moufang centre of G and $\{Z_i\}$ is the upper central series of G.*

Proof. (A) *Necessity.* Let θ be a normal endomorphism of G. Then, by Theorem 4.1, θ' is also a normal endomorphism. Therefore (I) holds. Moreover, (II) holds by Lemma 5.2 and the Corollary to Lemma 6.1. In addition,

$M \subset C \cap Z_2$, and ϕ is strongly normal by Lemma 5.3. Consequently, the properties stated in the last sentence of Theorem 6.1 are all true.

(B) *Sufficiency.* We now assume that (I), (II) are true. If W_n is a normalized purely non-abelian loop word, we must prove that

$$W_n(x_1\theta, x_2, \cdots, x_n) = W_n(x_1, x_2, \cdots, x_n)\theta \tag{6.8}$$

for all $x_1, \cdots, x_n$ in G. Hence we fix our attention on some such W_n.

The equations (4.4), (4.5) are valid on the ground that θ is an endomorphism. By (4.5), (4.6), and the normality of ϕ, we have

$$W_n(x_1\theta, x_2, \cdots, x_n) = (AB)C$$

for all x_i in G, where

$$A = W_n(x_1\theta^2, x_2, \cdots, x_n), \qquad B = W_n(x_1, x_2, \cdots, x_n)\phi,$$
$$C = P_{n+1}(x_1\theta^2, x_1, x_2, \cdots, x_n)\phi.$$

If $B = 1$ for all x_i, then, by (4.6), $C = 1$ for all x_i also. In the contrary case, by Lemma 6.1, $n = 3$. Then $n + 1 = 4$, and thus, by Lemma 6.1 again, $C = 1$ for all x_i. Thus $C = 1$ in all cases. At this point we replace $x_2, \cdots, x_n$ by $x_2\theta, \cdots, x_n\theta$, respectively. Since θ is an endomorphism, we get the formula

$$\begin{aligned} &W_n(x_1, x_2, \cdots, x_n)\theta \\ &\quad = W_n(x_1\theta^2, x_2\theta, \cdots, x_n\theta)[W_n(x_1, x_2\theta, \cdots, x_n\theta)\phi] \end{aligned} \tag{6.9}$$

for all x_i in G.

On the other hand, if we operate in turn on the left-hand side of (6.8) by the endomorphisms θ and θ', and use the facts that $1 = \theta + \theta'$ and ϕ is normal, we get

$$\begin{aligned} &W_n(x_1\theta, x_2, \cdots, x_n) \\ &\quad = W_n(x_1\theta^2, x_2\theta, \cdots, x_n\theta)[W_n(x_1, x_2\theta', \cdots, x_n\theta')\phi] \end{aligned} \tag{6.10}$$

for all x_i in G.

By comparison of (6.8), (6.9), (6.10), we see that (6.8) will hold if and only if

$$W_n(x_1, x_2\theta, \cdots, x_n\theta)\phi = W_n(x_1, x_2\theta', \cdots, x_n\theta')\phi \tag{6.11}$$

for all x_i in G. According to Lemma 6.1, (6.11) will be true for all x_i and for each choice of W_n provided that the identity

$$[(x, y\theta, z\theta)\phi]^t = [(x, y\theta', z\theta')\phi]^t \tag{6.12}$$

holds for all x, y, z in G and for $t = 1, 2$. Clearly we need only prove (6.12) for $t = 1$.

Since (6.7) holds for $\kappa = \theta$, and since $\phi = \theta\theta'$, we have

$$(x, y\theta, z\theta)\phi = (x\theta, y\theta, z\theta)\theta' = (x, y, z)\theta\theta' = (x, y, z)\phi.$$

Similarly, since (6.7) holds for $\kappa = \theta'$, and since $\phi = \theta'\theta$,

$$(x, y\theta', z\theta')\phi = (x, y, z)\phi.$$

This proves (6.12) for $t = 1$ and completes the proof that the endomorphism θ is normal. And now the proof of Theorem 6.1 is complete.

We observe that the conditions (I), (II) of Theorem 6.1 could be improved—from an aesthetic standpoint—by strengthening them. In particular, it seems a little odd to have to refer the normality of θ to the normality of ϕ. The following theorem meets this objection and others:

THEOREM 6.2. *Let θ be a single-valued mapping of a loop G into itself. Then the following two conditions are necessary and sufficient in order that θ be a normal endomorphism of G:*

(I′) *θ and its complement, θ', are seminormal endomorphisms of G.*

(II′) *$\phi = \theta\theta'$ is a strongly normal endomorphism of G which maps G' into Z and G into C, where G' is the commutator-associator subloop, Z is the centre, and C is the Moufang centre of G.*

Proof. By Theorem 6.1, (I′) and (II′) are certainly necessary. Moreover, (I′) implies (I). Before comparing (II′) and (II) we note that, if ϕ is a strongly normal (or even seminormal) endomorphism mapping G into a commutative loop and G' into Z, then ϕ maps G into Z_2. Hence (II′) implies that $M = G\phi$ is in $C \cap Z_2$ and (consequently) satisfies $M = Z_2(M)$. Therefore (II′) implies (II). Hence (I′), (II′) are sufficient. This completes the proof of Theorem 6.2.

7. Special loops

We now obtain a more intimate view of the various types of "normal" endomorphisms by studying them for special classes of loops. We begin by relating endomorphisms to the inner mapping group. (The generators of the latter are given by (3.2).)

A loop G is called *diassociative* if, for each pair x, y of elements of G, the subloop generated by x, y is associative (and hence a group).

LEMMA 7.1. *Let θ be an endomorphism of a diassociative loop G. A necesary and sufficient condition that*

$$T(x)\theta = \theta T(x) \tag{7.1}$$

for all x in G is that

$$(x, y)\theta = (x\theta, y) = (x, y\theta) \tag{7.2}$$

for all x, y in G.

Proof. Let x, y be arbitrary elements of G. By diassociativity,

$$yT(x) = x^{-1}yx = y(y, x), \tag{7.3}$$

$$(x, y) = (y, x)^{-1}. \tag{7.4}$$

In view of (7.3), we see that (7.1) holds for all x if and only if

$$(y, x)\theta = (y\theta, x)$$

for all x, y. In view of (7.4), the latter condition is equivalent to (7.2). This proves Lemma 7.1.

As previously noted, a loop G is called *Moufang* if and only if

$$(7.5) \qquad (xy)(zx) = [x(yz)]x$$

for all x, y, z. For the theory of Moufang loops, see [SVII], [SVIII].

LEMMA 7.2. *Let θ be an endomorphism of a Moufang loop G. A necessary and sufficient condition that θ commute with every inner mapping of G is that θ be seminormal.*

Proof. By Moufang's Theorem [SVII.4], G is diassociative. Hence Lemma 7.1 applies. For the rest of the proof, and for subsequent use, we need the following identities, taken from Lemma 5.4 of [SVII]. *These are valid in every Moufang loop G:*

$$(7.6) \qquad R(x^{-1}, y^{-1}) = L(x, y) = L(y, x)^{-1};$$

$$(7.7) \qquad xL(z, y) = x(x, y, z)^{-1};$$

$$(7.8) \qquad (x, y, z) = (x, yz, z) = (x, y, zy) = (x, y, zx);$$

$$(7.9) \qquad (x, y, z) = (xy, z, y)^{-1};$$

$$(7.10) \qquad y[x(x, y, z)^{-1}] = (yx)(y, x, z).$$

By (7.7), a necessary and sufficient condition that

$$(7.11) \qquad L(z, y)\theta = \theta L(z, y)$$

for all y, z in G is that

$$(7.12) \qquad (x, y, z)\theta = (x\theta, y, z)$$

for all x, y, z. Next we note that (7.10) can be written in the form

$$(x, y, z)^{-1} = (y, x, z)L(x, y)^{-1}.$$

Thus, if the equivalent identities (7.11), (7.12) are valid, we also have[2]

$$(7.13) \qquad (x, y, z)\theta = (x, y\theta, z)$$

for all x, y, z. Finally, from (7.13) and (7.9), we get

$$(7.14) \qquad (x, y, z)\theta = (x, y, z\theta)$$

[2] (*Added December* 23, 1958) I wish to thank Charles Wright for pointing out that I have nodded here; (7.13) does not follow from (7.11) in the manner suggested. Nevertheless, Lemma 7.2 is true: a valid proof will be given in an Appendix at the end of the paper.

for all x, y, z. Therefore if (7.11) holds for all y, z, then

$$(7.15) \qquad (x, y, z)\theta = (x\theta, y, z) = (x, y\theta, z) = (x, y, z\theta)$$

for all x, y, z in G. Conversely, (7.15) implies (7.12) and hence (7.11).

On the other hand, by (7.6), we see that (7.11) holds for all y, z if and only if $R(x, y)\theta = \theta R(x, y)$ for all x, y.

Combining these results with Lemma 7.1, we see that the identities (7.2), (7.15) are necessary and sufficient in order that θ commute with every inner mapping of G. Since (7.2), (7.15) are the defining identities for a semi-normal endomorphism, the proof of Lemma 7.2 is now complete.

Next we turn to additive properties of endomorphisms. The following lemma is quite obvious from Lemma 3.1:

LEMMA 7.3. *Let θ be an endomorphism of a diassociative loop G. A necessary and sufficient condition that $\theta + \theta$ be an endomorphism of G is that $G\theta$ be commutative.*

It will be convenient to specialize temporarily to the consideration of power-mappings and power-endomorphisms of a loop. A loop G is called *power-associative* provided that, for each x in G, the subloop generated by x is a cyclic group. If G is power-associative, we may associate with each integer n a *power-mapping*, (n), of G, defined by

$$(7.16) \qquad x(n) = x^n$$

for all x in G. The power-mappings form an associative ring, since

$$(7.17) \qquad (m + n) = (m) + (n), \qquad (mn) = (m)(n)$$

for all integers m, n. However, we have the following:

LEMMA 7.4. *Let G be a diassociative loop. A necessary and sufficient condition that every power-mapping of G be an endomorphism of G is that G be commutative.*

For the proof, apply Lemma 7.3 with $\theta = 1$. The next two lemmas have a little more substance.

LEMMA 7.5. *Let G be a diassociative loop. If the power-mapping (n) is an endomorphism of G, then the complement $(1 - n)$ is also an endomorphism of G. Moreover, for all x, y of G,*

$$(7.18) \qquad (x, y)^n = (x^n, y) = (x, y^n).$$

Proof. For (7.18) we apply Lemma 7.1 with $\theta = (n)$; diassociativity ensures the truth of (7.1). The fact that $(1 - n)$ is an endomorphism is essentially due to Baer (see Lemma 5.2 of [SVII]). The connection with normal endomorphisms of groups should also be clear.

LEMMA 7.6. *Let G be a Moufang loop, and let the power-mapping (n) be an* *endomorphism of G. Then (n) and its complement $(1 - n)$ are seminormal endomorphisms of G. If $n \equiv 0$ or $1 \bmod 3$, then (n) is a strongly normal endomorphism of G, and (hence) $(n - n^2)$ is a centralizing endomorphism of G. If $n \equiv 2 \bmod 3$, (n^2) and $(n - n^2)$ are strongly normal endomorphisms of G, and $(n - n^2)$ maps G into its Moufang centre. In addition, $(n - n^3)$ is a centralizing endomorphism of G.*

COROLLARY. *If, under the hypotheses of Lemma 7.6, $n \equiv 2 \bmod 3$, then a necessary and sufficient condition that (n) be normal is that $(n - n^2)$ map the commutator-associator subloop G' of G into the centre Z of G.*

Remark. Lemma 7.6 and its corollary allow us to show rather easily that seminormal endomorphisms need not be normal. However, by delaying this question until later, we shall be able to say a good deal more.

Proof. We shall need the following facts:

(a) *Every power-mapping of a Moufang loop G commutes with every inner mapping of G.*

(b) *If H is a commutative Moufang loop, the cube-mapping (3) is a centralizing endomorphism of H.*

Both (a) and (b) are proved in [SVII]. For (a), see Lemma 3.2 and formula (4.1) of [SVII]. For (b), see Lemma 5.7 of [SVII].

By comparing (a) with Lemma 7.2, we see that power-endomorphisms of the Moufang loop G are automatically seminormal. We set $\theta = (n)$. By Lemma 7.5, since θ is an endomorphism, so is the complement $\theta' = 1 - \theta$. Hence so are $\phi = \theta\theta' = \theta - \theta^2$ and $\phi' = 1 - \phi$. Since θ, ϕ are seminormal,

$$(x, y)\theta = (x\theta, y\theta) = (x, y)\theta^2,$$

and hence

$$(x\phi, y) = (x, y)\phi = (x, y)(\theta - \theta^2) = 1$$

for all x, y. Thus $(G\phi, G) = 1$. Since G is Moufang, the Moufang centre, C, of G consists of all c in G such that $(c, G) = 1$. Therefore we have shown that $G\phi$ is part of C.

Since $G\phi$ is a commutative Moufang loop, the power-mapping $k\phi = \phi(k)$ is a seminormal endomorphism of G for every integer k. From this fact, combined with (b), we deduce that 3ϕ is a centralizing endomorphism of G. We now must treat two cases.

First suppose that $n \equiv 0$ or $1 \bmod 3$. Then $n - n^2 = 3k$ for some integer k, and hence $\phi^2 = k\phi(3)$. In this case, ϕ^2 is a centralizing endomorphism of G. However, since ϕ is seminormal, ϕ and ϕ^3 coincide on G'. Thus we see, first, that $G'\phi = 1$ and, secondly, that ϕ is centralizing. Since θ, θ' are endomorphisms and $\phi = \theta\theta'$ is a centralizing endomorphism, then θ is strongly normal.

Next suppose that $n \equiv 2 \bmod 3$. In this case, $n^2 \equiv 1 \bmod 3$, and $n - n^2 \equiv 1 \bmod 3$. Consequently, by the preceding considerations applied with n replaced by n^2 and $n - n^2$, respectively, the endomorphisms θ^2 and $\phi = \theta - \theta^2$

are strongly normal. Since θ^2 has complement $1 - \theta^2$, then $\theta - \theta^3 = \theta(1 - \theta^2)$ is an endomorphism. Since, also, $\theta - \theta^3 = \phi(1 + n)$ and $1 + n \equiv 0 \bmod 3$, we see that $\theta - \theta^3$ is centralizing. This last fact could also be obtained directly by use of seminormality.

The corollary comes by consideration of Theorem 6.2. We already know that θ and θ' are seminormal endomorphisms, and that $\phi = \theta\theta'$ is a strongly normal endomorphism mapping G into C. The sole remaining condition for the normality of θ is that ϕ map G' into Z. This completes the proof of Lemma 7.6 and its corollary.

In our subsequent study of the additive properties of endomorphisms it will prove interesting to relax the requirement of seminormality. Some terminology is convenient, but we introduce the following with some misgivings: An endomorphism θ of a loop G will be called *demi-seminormal* if and only if

$$(7.19) \qquad (x\theta, y, z) = (x, y\theta, z) = (x, y, z\theta)$$

for all x, y, z in G. We note that the condition makes no reference to commutators; in addition, (7.19) requires less than (2.5). If θ, ϕ are demi-seminormal endomorphisms of a loop G, then so is $\theta\phi$; moreover,

$$(7.20) \qquad (x, y, z)\theta = (x\theta, y\theta, z\theta) = (x\theta^3, y, z) = (x, y\theta^3, z) = (x, y, z\theta^3),$$

$$(7.21) \qquad (x\theta\phi, y, z) = (x, y\theta, z\phi) = (x\phi\theta, y, z)$$

for all x, y, z in G. *If, in addition, either*

(a) *G is Moufang, or*

(b) *G is diassociative and $\theta\phi^2$ is seminormal, then*

$$(7.22) \qquad (xy, x\theta\phi^2, y) = 1$$

for all x, y in G. In case (b), (7.22) follows immediately from the fact that $(xy, x, y) = 1$ by diassociativity. To prove (7.22) in case (a), we recall that (7.9) is valid in any Moufang loop and that Moufang loops are diassociative. Thus

$$(xy, x\theta\phi^2, y)^{-1} = (x, y, x\theta\phi^2) = (x, y\theta\phi^2, x) = 1.$$

The hypotheses of the next lemma are phrased so as to ensure (7.22).

LEMMA 7.7. *Let θ, ϕ be demi-seminormal endomorphisms of a loop G, and assume that either* (i) *G is Moufang, or* (ii) *G is diassociative and $\theta\phi^2$ (or $\phi\theta^2$) is seminormal. Then a necessary and sufficient condition that $\theta + \phi$ be an endomorphism of G is that*

$$(7.23) \qquad (x\theta, y\phi) = 1$$

for all x, y in G.

Proof. We actually prove the lemma under the hypothesis that G is diassociative and (7.22) holds. If, in (ii), it is $\phi\theta^2$ which is assumed seminormal, a slightly different "right-left-dual" proof is required.

By Lemma 3.1, $\theta + \phi$ will be an endomorphism of G if and only if

$$[(x\theta)(x\phi)][(y\theta)(y\phi)] = [(x\theta)(y\theta)][(x\phi)(y\phi)] \tag{7.24}$$

for all x, y in G. We denote the left- and right-hand sides of (7.24) by L and R, respectively, and begin by transforming L. Since

$$(z, y\theta, y\phi) = (z\theta\phi, y, y) = 1$$

for all y, z in G, we take $z = (x\theta)(x\phi)$ and get

$$L = M\cdot(y\phi) \quad \text{where} \quad M = [(x\theta)(x\phi)](y\theta).$$

Since, in addition,

$$(x\theta, x\phi, y\theta) = (x, x, y\theta^2\phi) = 1,$$

we have $M = (x\theta)\cdot N$ and hence

$$L = [(x\theta)\cdot N](y\phi) \quad \text{where} \quad N = (x\phi)(y\theta). \tag{7.25}$$

Next we transform R. Since

$$(x\theta\cdot y\theta, x\phi, y\phi) = (x\theta\cdot y\theta, x, y\phi^2) = (xy, x\theta\phi^2, y),$$

we use (7.22) to get

$$R = S\cdot(y\phi) \quad \text{where} \quad S = [(x\theta)(y\theta)](x\phi).$$

This is the only point at which we use (7.22). Next, since

$$(x\theta, y\theta, x\phi) = (x, y\theta^2\phi, x) = 1,$$

we have $S = (x\theta)\cdot T$ and

$$R = [(x\theta)\cdot T](y\phi) \quad \text{where} \quad T = (y\theta)(x\phi).$$

And now, by comparison with (7.25), $R = L$ if and only if $(y\theta, x\phi) = 1$. Equivalently, $\theta + \phi$ will be an endomorphism of G if and only if (7.23) holds for all x, y in G. This completes the proof of Lemma 7.7.

It will help to prepare the reader for the next lemma if we first discuss a difficult question. (A similar question can be posed for loops in general, but we keep to a case for which we have adequate tools.) Let G be a Moufang loop with inner mapping group $\mathfrak{J}$, and let $(S, +)$ be the additive loop generated by the set of all seminormal endomorphisms of G. Consider an endomorphism θ of G which is contained in S; is θ seminormal? If $\mathfrak{J}$ consists entirely of automorphisms of G, the answer is clearly affirmative; indeed, in this case, every element of S commutes with every element of $\mathfrak{J}$. But what can we say in case $\mathfrak{J}$ does not consist entirely of endomorphisms? The easier course is to avoid this possibility. The price to be paid (combine Lemma 2.1, Theorem 2.1 of [SVII] or see Bruck [2]) may be presented as follows:

If G is a Moufang loop with nucleus N, then N is a normal subgroup of G. A necessary and sufficient condition that the inner mapping group of G consist entirely of automorphisms of G is that G/N be commutative of exponent 3.

It is known that if G is the multiplicative loop of the Cayley division algebra over the field of reals, then G is Moufang, and N consists of the real numbers. Therefore G/N is not commutative.—This example has obvious generalizations.

A more rewarding attack on our question is to start from the obvious fact that seminormal endomorphisms are demi-seminormal. We begin as follows:

LEMMA 7.8. *Let G be a Moufang loop, and let $(L, +)$ be the additive loop generated by the set of all demi-seminormal endomorphisms of G. Then $(L, +)$ is a group, and $(L, \cdot)$ is a semigroup. Moreover,*

(i) *If x, y are in G, the subset $xL \cup yL \cup (xy)L$ of G generates a subgroup $H(x, y)$ of G.*

(ii) *If $\theta + \phi = \psi$ for elements θ, ϕ, ψ of L, some two of which are endomorphisms of G, then the third will be an endomorphism of G if and only if*

$$(x\theta, y\phi) = 1 \tag{7.26}$$

for all x, y in G.

(iii) *If θ is an endomorphism of G contained in L, a necessary and sufficient condition that the complement, θ', be an endomorphism of G is that*

$$(x, y)\theta = (x\theta, y) = (x, y\theta) \tag{7.27}$$

for all x, y in G. When the condition holds, $(\theta')' = \theta$.

(iv) *If $(P, +)$ is a commutative subgroup of $(L, +)$ which is generated by a multiplicative semigroup M of endomorphisms of G, then $(P, +, \cdot)$ is an (ordinary, two-sided distributive) associative ring.*

(v) *If $(Q, +)$ is a subgroup of $(L, +)$ which is generated by a multiplicative semigroup M of endomorphisms of G, then a necessary and sufficient condition that $(Q, +, \cdot)$ be a ring of endomorphisms of G is that* (7.26) *hold for all θ, ϕ in M and x, y in G. When $(Q, +, \cdot)$ is a ring of endomorphisms of G (and Q is part of L), then* (7.26) *actually holds for all θ, ϕ in Q and x, y in G.*

(vi) *If K is the set of all endomorphisms of G which are contained in L and map G into its Moufang centre C, then $(K, +, \cdot)$ is a ring. If θ is an endomorphism of G contained in L, then θK is part of K, and*

$$\theta + \kappa = \kappa + \theta$$

is an endomorphism of G for every κ in K. If, in addition, θ satisfies (7.27) *for all x, y in G, then $K\theta$ is part of K.*

Proof. In order to prove at one stroke that L and the P, Q of (iv), (v) are multiplicative semigroups, we begin with the following proposition:

(*) *If $(R, +)$ is an additive loop generated by a multiplicative semigroup M of endomorphisms of a loop G, then $(R, \cdot)$ is a semigroup.*

Proof of (*). We do not require that G be Moufang. If θ is in M, consider the set R' of all α in R such that $\alpha\theta$ is in R. Since θ is an endomorphism, we may use the "restricted" right distributive law (2.25) for mappings; and we are able to conclude that $(R', +)$ is a subloop of $(R, +)$. However, R' contains M, and M generates $(R, +)$. This tells us that RM is part of R. At this point, if α is in R, we consider the set of all β in R such that $\alpha\beta$ is in R. This time, since the left distributive law (2.24) is "unrestricted", we deduce in the same manner that αR, and thence that RR, is part of R. Since multiplication of mappings is associative, we have proved (*).

Next, let S be the set of all single-valued mappings of a loop G into itself. For each nonempty subset T of S and for each element x of G, let xT denote the subset of G consisting of all elements $x\alpha$ where α ranges over T. If $(T, +)$ is a subloop of $(S, +)$, then, for each x, xT is a subloop of G, and the mapping $\alpha \rightarrow x\alpha$ is a homomorphism of $(T, +)$ upon xT. Combining these homomorphisms as x ranges over G, we see that each subloop $(T, +)$ of $(S, +)$ is isomorphic to a subdirect product of the subloops xT of G. These simple remarks will render our task easy.

Now we impose the condition that G be Moufang. First let M be the multiplicative semigroup of all demi-seminormal endomorphisms of G. Thus M generates $(L, +)$ and, by (*), $(L, \cdot)$ is a semigroup. For each x in G we have

$$(xM, xM, G) = 1 \tag{7.28}$$

since

$$(x\theta, x\phi, y) = (x, x, y\theta\phi) = 1$$

for all x, y in G and θ, ϕ in M. Similarly, for all x, y in G,

$$([xy]M, xM, yM) = 1, \tag{7.29}$$

since, as in the proof of (7.22), if x, y are in G and θ, ϕ, ψ are in M,

$$\begin{aligned}([xy]\theta, x\phi, y\psi) &= (xy, x\theta\phi\psi, y) = (x, y, x\theta\phi\psi)^{-1} \\ &= (x, y\theta\phi\psi, x)^{-1} = 1.\end{aligned}$$

Next we choose some x, y in G and set

$$A = (xy)M, \qquad B = xM, \qquad C = yM.$$

Since (7.28), (7.29) hold for all x, y in G, we have

$$(A, A, G) = (B, B, G) = (C, C, G) = (A, B, C) = 1;$$

and this is the hypothesis of Theorem 4.2 of [SVII]. Therefore we may conclude that $A \cup B \cup C$ is contained in a subgroup H of G. However, for each z in G, the subloop generated by zM is zL. Consequently, H contains

$$(xy)L \cup xL \cup yL.$$

This proves (i). In particular, xL is a group for each x, so $(L, +)$ must be a group.

Let us note at this point that L contains the identity mapping. Thus the group xL contains x, and the group $H(x, y)$ contains both x and y.

Hereafter, that is to say, in the proof of (iv), (v), (vi), M will denote the appropriate generating set. Our proof now consists in some simple observations about groups. We prove (ii), (iii) together as follows: An element α of L is an endomorphism of G if and only if α induces an endomorphism of each group $H(x, y)$. And an identity such as (7.26) or (7.27), where the elements of L involved are understood to be fixed, holds for all x, y in G if and only if it holds as x, y range over each group $H(p, q)$. Therefore (ii), (iii) are valid since we know them to be true when G is a group. The only point at issue in (iv) is the right distributive law for all elements of P. We choose two elements α, β of P and observe that the mapping

$$\gamma \to (\alpha + \beta)\gamma - \alpha\gamma - \beta\gamma$$

is an endomorphism of the abelian group $(P, +)$ and maps the generating set M into 0. This proves (iv). At this stage, (v), like (ii) and (iii), need only be reduced to a proposition about groups. In essence, we have to prove that, if x, y are elements of G such that $xM \cup yM \cup (xy)M$ generates an abelian group—where M generates $(Q, +)$—and such that

$$(xy)\theta = (x\theta)(y\theta) \tag{7.30}$$

for every θ in M, then (7.30) holds for every θ in Q. This is obvious. Finally, we observe that (vi) follows directly from (i)–(v) and the fact that C consists of those elements of G which commute with every element of G. This completes the proof of Lemma 7.8.

It will prove fruitful to recall another concept. A permutation α of a loop G is called a *pseudo-automorphism* of G provided that there exists at least one element c of G, called a *companion* of α, such that

$$[(xy)\alpha]c = (x\alpha)[(y\alpha)c] \tag{7.31}$$

for all x, y in G. By Lemma 3.2 of [SVII], *every inner mapping of a Moufang loop G is a pseudo-automorphism of G.* Hence the following lemma is highly relevant to the question raised before Lemma 7.8:

LEMMA 7.9. *Let G be a Moufang loop, and let $(L, +)$ be the additive group generated by the demi-seminormal endomorphisms of G. Let α be a pseudo-automorphism (for example, an inner mapping) of G. If L' is the set of all θ in L such that $\theta\alpha = \alpha\theta$, then $(L', +)$ is a subgroup of $(L, +)$.*

Proof. In the proof of Lemma 7.8 we showed that (7.28) held for all x in G, where M was the set of demi-seminormal endomorphisms of G. From this and Lemmas 4.3, 4.1 of [SVII], we get

$$(xL, xL, G) = (xL, G, xL) = (G, xL, xL) = 1 \tag{7.32}$$

for every x in G. And (7.32) is more than enough for our purpose.

Suppose now that $\theta + \phi = \psi$ for elements θ, ϕ, ψ of L, some two of which are in L'. Let x be any element of G. By (7.32),

$$(x\alpha\psi)c = [(x\alpha\theta)(x\alpha\phi)]c = (x\alpha\theta)[(x\alpha\phi)c].$$

By (7.31),

$$(x\psi\alpha)c = \{[(x\theta)(x\phi)]\alpha\}c = (x\theta\alpha)[(x\phi\alpha)c].$$

Therefore, by comparison, all three of θ, ϕ, ψ are in L'. This completes the proof of Lemma 7.9.

Now we are ready to settle the question we raised earlier.

THEOREM 7.1. *Let $(S, +)$ be the additive group generated by the set of all seminormal endomorphisms of a Moufang loop G. Then*

(i) *$S = (S, +, \cdot)$ is a ring.*

(ii) *An endomorphism θ of G is in S if and only if θ is seminormal.*

(iii) *The complement of a seminormal endomorphism is a seminormal endomorphism.*

(iv) *If R is the set of all seminormal endomorphisms of G which map G into its Moufang centre C, then $R = (R, +, \cdot)$ is an ideal of S. The quotient ring S/R is commutative.*

(v) *If θ is a seminormal endomorphism of G, then θ^2 is a strongly normal endomorphism of G, $\phi = \theta - \theta^2$ is a strongly normal endomorphism of G belonging to R, and $\psi = \theta - \theta^3$ is a centralizing endomorphism of G.*

COROLLARY. *The strongly normal endomorphisms of a Moufang loop G generate the same ring S as do the seminormal endomorphisms of G.*

Remarks. 1. When G is a group, Theorem 7.1(i) reduces to Theorem 1 of Heerema [3].

2. The Corollary to Theorem 7.1 suggests an interesting conjecture about loops in general.

Proof. Let M denote the set of all seminormal endomorphisms of G.

(i) We apply Lemma 7.8. M is a multiplicative semigroup contained in L. Also $\theta + \phi = \phi + \theta$ for θ, ϕ in M, since

$$(x\theta, x\phi) = (x, x)\theta\phi = 1$$

for all x in G. Hence $(S, +)$ is a commutative subgroup of $(L, +)$; and hence, by Lemma 7.8(iv), $S = (S, +, \cdot)$ is a ring.

(ii) By Lemma 7.9 and Lemma 7.2, every element of S commutes with every inner mapping of G. By Lemma 7.2 again, every endomorphism in S is in M.

(iii) This follows from Lemma 7.8(iii) and from (ii) of the present theorem.

(iv) R, as the intersection of the ring S with the ring K of Lemma 7.8(vi), is clearly a subring of S. Moreover, if θ is a seminormal endomorphism, θR

and $R\theta$ are part of S and of K, and therefore of R. Hence R is an ideal of S. To prove that S/R is commutative, we need only show that

$$\theta\phi = \phi\theta + (\theta, \phi) \tag{7.33}$$

where (θ, ϕ) is in R, under the assumption that θ, ϕ are in M. Equivalently, for each pair x, y of elements of G, we must show that $(\theta, \phi) = \kappa$ satisfies $(xy)\kappa = (x\kappa)(y\kappa)$ and $(x\kappa, y) = 1$. This can be settled inside the group $H(x, y)$ of Lemma 7.8(i); and it is true since θ, ϕ induce normal endomorphisms in each group $H(x, y)$.

(v) The complements of θ and θ^2 are $1 - \theta$ and $1 - \theta^2$, respectively. Thus $\phi = \theta(1 - \theta)$ and $\psi = \theta(1 - \theta^2)$ are seminormal endomorphisms of G. Noting that θ coincides with θ^2 on any commutator and with θ^3 on any associator, we conclude that ϕ maps G into the Moufang centre C, and that ψ is centralizing. Then $\theta^2(1 - \theta^2) = \theta\psi$ is centralizing, so θ^2 is strongly normal. In addition, we verify that

$$\phi(1 - \phi) = 3\phi + (\theta - 2)\psi.$$

The second term on the right is centralizing, since ψ is. And 3ϕ is centralizing since the cube mapping (3) induces a centralizing endomorphism of the commutative Moufang loop $G\phi$. Therefore $\phi(1 - \phi)$ is centralizing, and we conclude that ϕ is strongly normal. This proves Theorem 7.1. The corollary is immediate from (v).

We should perhaps point out that *the mapping* (θ, ϕ) *of* (7.33) *is a centralizing endomorphism of* G. Indeed, if θ, ϕ, and (θ, ϕ) are seminormal endomorphisms, linked by (7.33), of an arbitrary loop G (not necessarily Moufang), then (θ, ϕ) maps G' into 1 and hence maps G into Z. It will be recalled that our procedure in connection with Theorem 3.3 was quite different: In order to show that (θ, ϕ) was an endomorphism, we first had to show that (θ, ϕ) was a centralizing mapping; and for this we needed the hypothesis that θ and ϕ were weakly normal.

By combining Lemmas 7.8, 7.1, 7.9, Theorem 7.1 can be broadened as follows:

THEOREM 7.2. *Let G be a Moufang loop, and let $(S_1, +)$ be the additive group generated by all demi-seminormal endomorphisms of G which satisfy* (7.27). *Then $(S_1, +, \cdot)$ is a ring. If θ is an endomorphism of G contained in S_1, then θ satisfies* (7.27), *$\theta' = 1 - \theta$ is an endomorphism of G contained in S_1, and $\theta\theta'$ maps G into its Moufang centre C.*

It will be observed that we have had no need for the concept of a weakly normal endomorphism of a Moufang loop. The next theorem gives a simple explanation:

THEOREM 7.3. *Every weakly normal endomorphism of a Moufang loop G is a normal endomorphism of G.*

Proof. Let θ be a weakly normal endomorphism of G. Then θ is seminormal, and hence, by Theorem 7.1, $\phi = \theta - \theta^2$ is a strongly normal endomorphism which maps G into its Moufang centre C. According to Theorem 6.2, the only additional condition for the normality of θ is that ϕ map the commutator-associator subloop G' into the centre Z of G. We shall verify this condition.

We shall have to return to the definition of weak normality in §2. Let us first consider formula (2.8). Since θ is seminormal,

$$(w\theta \cdot x\theta, y, z) = (wx, y, z)\theta$$

for all w, x, y, z in G. Evaluating each side of this equality by (2.8) and comparing, we get

$$P_1(w\theta, x\theta, y, z) = P_1(w, x, y, z)\theta. \tag{7.34}$$

Since θ is weakly normal, we may use (2.16) with $i = 1$; this allows us to replace the left-hand side of (7.34) by

$$P_1(w, x, y, z)\theta^2.$$

Therefore, since $\phi = \theta - \theta^2$, we have $P_1 \phi = 1$. From this and (2.8),

$$(wx, y, z)\phi = [(w, y, z)\phi][(x, y, z)\phi] \tag{7.35}$$

for all w, x, y, z in G.

The rest of the proof uses properties of commutative Moufang loops which will be discussed in detail in the section which follows. Setting

$$W = w\phi, \qquad X = x\phi, \qquad Y = y\phi, \qquad Z = z\phi,$$

we deduce from (7.35) and the seminormality of ϕ that

$$(WX, Y, Z) = (W, Y, Z)(X, Y, Z) \tag{7.36}$$

for all W, X, Y, Z in the commutative Moufang loop $G\phi$. This means (see (8.8) below) that $G\phi$ coincides with its *distributor subloop* D. As a consequence (see (8.10) below),

$$((G\phi, G\phi, G\phi), G\phi, G\phi) = 1.$$

Thence, since ϕ is seminormal and $G\phi$ is commutative Moufang, we deduce quite directly that $G'\phi$ is part of the centre Z of G. This completes the proof of Theorem 7.3.

In deriving (7.35), we did not need the full hypothesis that θ was weakly normal. However, (7.35) is essentially a formula for the commutative Moufang loop $G\phi$. In any diassociative loop, the six functions P_i, Q_i of formulas (2.8)–(2.13) can (quite trivially) be reduced to three; in a commutative Moufang loop they can be reduced to one.

8. Commutative Moufang loops

Let G be a commutative Moufang loop. It will be convenient to begin by assembling a number of facts and formulas concerning commutative Moufang loops. The proofs of these are spread over most of §§2–6 of [SVIII], and too much space would be required to give exact references.

The associator satisfies the identities

$$(8.1) \qquad (x, y, z) = (y, x, z)^{-1} = (z, y, x)^{-1},$$

$$(8.2) \qquad (x, y, z)^n = (x^n, y, z) = (x, y^n, z) = (x, y, z^n),$$

$$(8.3) \qquad (x, y, z)^3 = 1,$$

$$(8.4) \qquad ((w, x, y), w, z) = ((w, z, y), w, x)^{-1},$$

$$(8.5) \qquad (wx, y, z) = (w, y, z)(x, y, z)((w, y, z), w, x)((x, y, z), x, w)$$

for all w, x, y, z in G and for every integer n. Moreover,

$$(8.6) \qquad (wx)(yz) = [(wy)(xz)]h(w, x, y, z)$$

for all w, x, y, z in G, where

$$(8.7) \qquad h(w, x, y, z) = (w, x, y)^{-1}(x, y, z)(y, z, w)^{-1}(z, w, x).$$

The following fact is needed for (8.5), (8.7): *If K is a commutative Moufang loop generated by five or less elements, then the commutator-associator subloop K' is an abelian group.* This assures us, in particular, that the right-hand sides of (8.5), (8.7) are unambiguous.

The *distributor*, $D = D(G)$, of a commutative Moufang loop G, is the set of all elements d in G such that

$$(8.8) \qquad (xy, z, d) = (x, z, d)(y, z, d)$$

for all x, y, z in G. The distributor is a characteristic normal subloop of G which contains (often properly) the second term $Z_2(G)$ of the upper central series of G. An element d of G is in D if and only if one of the following formulas holds for all w, x, y, z in G:

$$(8.9) \qquad ((w, x, y), w, d) = 1;$$

$$(8.10) \qquad ((w, x, y), z, d) = 1;$$

$$(8.11) \qquad ((d, w, x), y, z) = ((d, w, y), x, z)^{-1}.$$

To repeat: if one of (8.8)–(8.11) holds for fixed d in G and all w, x, y, z in G, then all of them hold.

We are now ready to begin a study of the endomorphisms of a commutative Moufang loop.

LEMMA 8.1. *Let θ, ϕ be endomorphisms of a commutative Moufang loop G. A necessary and sufficient condition that $\theta + \phi$ be an endomorphism of G is that*

$$(8.12) \qquad (x\theta, x\phi, y\theta) = (x\theta, x\phi, y\phi)$$

for all x, y in G.

Proof. By comparing (8.6) with Lemma 3.1, we see that $\theta + \phi$ will be an endomorphism of G if and only if

$$h(x\theta, x\phi, y\theta, y\phi) = 1 \tag{8.13}$$

for all x, y in G. By (8.7), (8.1), condition (8.13) can be written as

$$f(x, y) = f(y, x)$$

where

$$f(x, y) = (x\theta, x\phi, y\theta)(x\theta, x\phi, y\phi)^{-1}.$$

In view of (8.2), we see that

$$f(x^{-1}, y) = f(x, y), \qquad f(y, x^{-1}) = f(y, x)^{-1}.$$

Therefore, if $\theta + \phi$ is an endomorphism, we have

$$f(x, y)^2 = f(x, y)f(x^{-1}, y) = f(y, x)f(y, x^{-1}) = 1$$

for all x, y. In view of (8.3), this implies $f(x, y) = 1$, an equation equivalent to (8.12). Conversely, if $f(x, y) = 1$ for all x, y, then (8.13) holds for all x, y, and therefore $\theta + \phi$ is an endomorphism. This completes the proof of Lemma 8.1.

LEMMA 8.2. *Let θ be an endomorphism of the commutative Moufang loop G. Then each of the following statements implies the other two:*

(i) *θ is demi-seminormal.*

(ii) *$1 + \theta$ and $1 - \theta$ are endomorphisms of G.*

(iii) *The identity*

$$(x, x\theta, y) = 1 \tag{8.14}$$

holds for all x, y in G.

Proof. By Lemma 8.1, $1 + \theta$ will be an endomorphism of G if and only if

$$(x, x\theta, y) = (x, x\theta, y\theta) \tag{8.15}$$

for all x, y in G. Replacing θ in (8.15) by $-\theta = (-1)\theta = \theta(-1)$ and using (8.2), we see that $1 - \theta$ will be an endomorphism if and only if

$$(x, x\theta, y)^{-1} = (x, x\theta, y\theta) \tag{8.16}$$

for all x, y in G.

If (i) holds, all four of the associators in (8.15), (8.16) can be put in the form $(x, x, y\phi)$ where $\phi = \theta$ or θ^2. Since G is diassociative, we see that (i) implies (ii).

If (ii) holds, then (8.15), (8.16) hold for all x, y. Combining these with (8.3), we deduce that (iii) holds. Hence (ii) implies (iii).

Finally, let us assume (iii). Then, by (8.1), (8.14), (8.5), we have

$$1 = (x\theta \cdot y\theta, xy, z) = pq(p, x\theta, y\theta)(q, y\theta, x\theta) \tag{8.17}$$

for all x, y, z in G, where

$$p = (x\theta, xy, z), \qquad q = (y\theta, xy, z).$$

Again, by (8.1), (8.5), (8.14),

$$p^{-1} = (xy, x\theta, z) = (y, x\theta, z)\big((y, x\theta, z), y, x\big).$$

The last factor is 1 by (8.1), (8.2), (8.4), (8.14), since it equals

$$\big((y, z, x\theta), y, x\big)^{-1} = \big((y, x, x\theta), y, z\big) = 1.$$

Thus for p and similarly for q,

$$p = (x\theta, y, z), \qquad q = (x, y\theta, z)^{-1}.$$

Now we see that if, in (8.17), x is replaced by x^{-1}, then p and q are replaced by their inverses whereas the other two factors are unchanged. This tells us, in view of (8.3), that $pq = 1$ or

$$(x\theta, y, z) = (x, y\theta, z)$$

for all x, y, z in G. In view of (8.1), we see that (i) holds. Thus (iii) implies (i), and the proof of Lemma 8.2 is complete.

If θ is a demi-seminormal endomorphism, we see from (8.2) that $-\theta$ is also demi-seminormal. If, in addition, ϕ is a demi-seminormal endomorphism, then, by Lemma 8.1, $\theta + \phi$ is an endomorphism, and, by (8.5),

$$\text{(8.18)} \qquad \big(x(\theta + \phi), y, z\big) = (x\theta, y, z)(x\phi, y, z)$$

for all x, y, z in G. By combining (7.20), (8.18), we find that

$$\text{(8.19)} \qquad (x\theta, y, z)[(x, y, z)\theta]^{-1} = \big(x(\theta - \theta^3), y, z\big)$$

for every demi-seminormal endomorphism θ and all x, y, z in G. If

$$\text{(8.20)} \qquad \theta\phi = \phi\theta + (\theta, \phi),$$

then (7.21), (8.18) yield

$$\text{(8.21)} \qquad \big(x(\theta, \phi), y, z\big) = 1$$

for all demi-seminormal endomorphisms θ, ϕ and all x, y, z in G. These results yield the following theorem:

THEOREM 8.1. *The demi-seminormal endomorphisms of a commutative Moufang loop G form a ring, E, namely the unique maximal ring of endomorphisms of G which contains the identity endomorphism of G. Moreover*

(i) *θ is in E if and only if θ, $1 + \theta$, and $1 - \theta$ are endomorphisms of G.*
(ii) *An element θ of E is seminormal if and only if $\theta - \theta^3$ is centralizing.*
(iii) *If θ and ϕ are in E, then (θ, ϕ) is centralizing.*
(iv) *If θ is in E, then 3θ is centralizing.*

Proof. Apply Lemma 8.2 and formulas (8.18)–(8.21) and (8.1)–(8.3).

By Theorem 7.1, applied to the commutative Moufang loop G, the set R of all seminormal endomorphisms of G is also a ring; and R is a subring of the ring E of Theorem 8.1. We also note that the set F of centralizing endomorphisms of G is an ideal of R and of E, and that E/F is a commutative ring of characteristic 3.

Since the structure of commutative Moufang loops is fairly well developed, it seems reasonable to expect answers to the followlng questions: *Does there exist a commutative Moufang loop G possessing an endomorphism θ which is*

(i) *not demi-seminormal?*
(ii) *demi-seminormal but not seminormal?*
(iii) *seminormal but not weakly normal?*
(iv) *weakly normal but not normal?*
(v) *normal but not strongly normal?*

In view of Theorem 7.3, (iv) must be answered in the negative. We shall show, on the other hand, that (i)–(iii) and (v) have affirmative answers. We begin with the following lemma, which shows how to construct certain "inner" demi-seminormal endomorphisms.

LEMMA 8.3. *Let G be a commutative Moufang loop with distributor D. To each d in D and p in G there corresponds a demi-seminormal endomorphism $\theta(p, d)$ of G, defined by*

$$x\theta(p, d) = (x, p, d) \tag{8.22}$$

for all x in G. Moreover,

$$\theta(p, d)\theta(q, d') = 0 \tag{8.23}$$

for all p, q in G and d, d' in D. In particular, a necessary and sufficient condition that $\theta(p, d)$ be seminormal for all p in G and d in D is that $D = Z_2(G)$.

Proof. That $\theta = \theta(p, d)$ is an endomorphism follows from (8.8); that it is demi-seminormal follows from (8.11), (8.1). Again, by (8.10),

$$(x, y, z)\theta = 1$$

for all x, y, z in G; and this is enough to prove (8.23). By (8.23), $\theta^3 = 0$. Thence, by Theorem 8.1(ii), θ will be seminormal if and only if θ is centralizing. If, for some d in D, $\theta(p, d)$ is centralizing for every p in G, we deduce that

$$(d, x, y) \equiv 1 \mod Z$$

for all x, y in G; and thence that d is in $Z_2(G)$. We noted earlier that $Z_2(G)$ is part of D. Therefore $\theta(p, d)$ will be seminormal for all p in G, d in D precisely when $D = Z_2(G)$. This completes the proof of Lemma 8.3.

By the criterion discussed in §7, every inner mapping of a commutative Moufang loop G is an (inner) automorphism. If we set

$$L(p, q) = 1 + \phi$$

for some p, q in G, then $L(p, q)$ will be demi-seminormal precisely when ϕ is a demi-seminormal endomorphism. By (7.7), (8.1),

$$x\phi = (x, p, q)$$

for all x in G. Consequently, a necessary and sufficient condition that $L(p, q)$ be demi-seminormal for all p, q in G is that $G = D$, or, equivalently in view of (8.10), (8.1), that $G = D = Z_2(G)$.

Lemma 8.3 and the remarks of the preceding paragraph show that (i) and (ii) may be answered in the affirmative by producing a commutative Moufang loop G such that $D(G) \neq Z_2(G)$. Now consider the commutative Moufang loop H constructed in [SVIII.1]. It is pointed out in [SVIII] that H is a commutative Moufang loop of exponent 3, that $1 = Z(H) = Z_2(H)$, and that H' is both infinite and part of $D(H)$. This disposes of (i), (ii). The same loop H will dispose of (iii). For if $\theta = (-1)$ is the inverse mapping of H, then $\phi = \theta\theta' = (-2) = 1$; θ is seminormal but not normal, since $H\phi$ is not part of $Z_2(H)$; and therefore θ is not weakly normal either.

To dispose of (v) we choose a commutative Moufang loop G such that $G = Z_2(G) \neq Z(G)$; such loops were discussed in the proof of Lemma 6.1. In this case the inverse mapping (-1) is normal; but it is not strongly normal, since, in view of (8.3), the mapping (-2) is not centralizing.

Appendix

(Added December 23, 1958)

As pointed out in footnote 2, the proof of Lemma 7.2 contains a hole; in order to obtain a valid proof, we are forced to probe much more deeply. For this reason it will be convenient to derive Lemma 7.2 in the following stronger form:

LEMMA 7.2*. *Let G be a Moufang loop, and let θ be an endomorphism of G with complement θ'. Then each of the following three statements implies the other two:*

(i) *θ commutes with every inner mapping of G.*

(ii) *θ^2 and $\phi = \theta\theta'$ are weakly normal endomorphisms of G, and $G\phi$ is commutative.*

(iii) *θ is seminormal.*

In addition, each of (i)–(iii) *implies the following:*

(iv) *θ' is a seminormal endomorphism of G, and $(\theta')' = \theta$.*

(v) *θ^2 and ϕ are strongly normal endomorphisms of G.*

Proof. Let K denote the set of all endomorphisms θ of G which commute with every inner mapping of G. We begin by noting that an endomorphism θ of G is in K if and only if

$$(1) \qquad (x, y)\theta = (x\theta, y) = (x, y\theta),$$

$$(2) \qquad (x, y, z)\theta = (x\theta, y, z)$$

for all x, y, z in G. Indeed, by Lemma 7.1, (1) holds for all x, y in G if and only if $\theta T(x) = T(x)\theta$ for all x in G; and, by the (valid) first part of the proof of Lemma 7.2, (2) holds for all x, y, z in G if and only if $\theta L(z, y) = L(z, y)\theta$ for all y, z in G. Since, in a Moufang loop, $R(x, y) = L(x^{-1}, y^{-1})$ for all x, y, we see that (1), (2) hold identically if and only if θ is in K; that is, θ satisfies (i).

We shall have frequent use for the obvious fact that K is closed under multiplication.

(iii) $\rightarrow$ (i). If θ is seminormal, then θ certainly satisfies (1), (2). Hence (iii) implies (i).

(ii) $\rightarrow$ (iii). We assume that (ii) holds and indicate how to prove (iii). To prove (iii) we must prove (1), (2), and each of the identities (7.13), (7.14). However (as correctly shown in the proof of Lemma 7.2), (7.13) is equivalent to (7.14). Moreover, as shown in the proof of Lemma 7.1, (1) is equivalent to the identity $(x, y)\theta = (x\theta, y)$. We shall prove (7.13) in detail and indicate how to prove the remaining identities.

To prove (7.13) we use (2.9). Since $\theta = \theta^2 + \phi$ and since θ^2, ϕ are weakly normal endomorphisms, (2.9) yields

$$\begin{aligned}(y, x\theta, z) &= (y, x\theta^2 \cdot x\phi, z)\\ &= [(y, x\theta^2, z)(y, x\phi, z)]P_2(x\theta^2, x\phi, y, z)\\ &= [(y, x, z)\theta][P_2(x, x, y, z)\phi\theta^2]\end{aligned}$$

for all x, y, z in G. Therefore we may prove (7.13) by showing that

$$P_2(x, x, y, z)\phi = 1 \tag{3}$$

for all x, y, z in G. We do this as follows: By (2.9) again,

$$(y, x^2, z) = (y, x, z)^2 \cdot P_2(x, x, y, z) \tag{4}$$

for all x, y, z in G. Since ϕ is an endomorphism and $G\phi$ is a commutative Moufang loop,

$$(y, x^2, z)\phi = (y, x, z)^2\phi$$

by properties of the associator in a commutative Moufang loop (see [SVIII.2]). Hence, by applying ϕ to both sides of (4), we get (3). This proves (7.13).

For the rest of the proof that (ii) implies (iii), we employ formulas (2.6), (2.8) in a similar manner.

(i) $\rightarrow$ (ii). Finally we assume that (i) holds, that is, that θ is in K. Our main objective is to prove (ii). In the course of the proof we show that θ' is in K, that $(\theta')' = \theta$, and that θ^2 and ϕ are strongly normal. Thus when (ii) has been proved, we will have completed the proof of Lemma 7.2*. Our proof requires several steps.

(A) *If x, y are in G, the subloop generated by x, $x\theta$, and y is a group.*

Proof of (A). Since θ is in K, and since G is diassociative,

$$(x\theta, x, y) = (x, x, y)\theta = 1\theta = 1.$$

Hence, by Moufang's Theorem (see [SVII.4]) the three elements $x\theta$, x, y generate a group. This proves (A).

(B) *The formulas*

$$(x, y\theta') = (x, y)\theta', \tag{5}$$

$$(x\theta, y\theta') = (x, y)\phi = 1 \tag{6}$$

hold for all x, y in G.

Proof of (B). By definition, $y = y\theta \cdot y\theta'$. Hence $y\theta' = y^{-1}\theta \cdot y$. By (A), the elements $y^{-1}\theta$, y, x lie in a group. Hence, by formulas from group theory,

$$(x, y\theta') = (x, y^{-1}\theta \cdot y) = (x, y)(x, y^{-1}\theta)\big((x, y^{-1}\theta), y\big).$$

Since θ is in K, the last two factors may be replaced by $p\theta$ where

$$p = (x, y^{-1})\big((x, y^{-1}), y\big) = (x, y)^{-1}(x, y^{-1}y) = (x, y)^{-1}.$$

Hence, if $c = (x, y)$, we have

$$(x, y\theta') = c \cdot c^{-1}\theta = c^{-1}\theta \cdot c \cdot (c, c^{-1}\theta) = c\theta' \cdot \{(c, c^{-1})\theta\} = c\theta'.$$

This proves (5). By (5) and the fact that θ is in K, we have

$$(x\theta, y\theta') = c\theta\theta' = c\phi$$

where $c = (x, y)$. However, since θ is in K, and since $\theta = \theta^2 + \phi$,

$$c\theta^2 \cdot c\phi = c\theta = (x\theta, y\theta) = c\theta^2,$$

whence $c\phi = 1$. This proves (6) and completes the proof of (B).

(C) *θ' is in K, and $(\theta')' = \theta$.*

Proof of (C). Since $x\theta' = x^{-1}\theta \cdot x$ for all x, we have

$$(xy)\theta' = (xy)^{-1}\theta \cdot xy = \{y^{-1}\theta \cdot x^{-1}\theta\} \cdot xy$$

for all x, y. Moreover, since θ is in K,

$$(y^{-1}\theta, x^{-1}\theta, xy) = (y^{-1}, x^{-1}\theta, xy)\theta = 1\theta = 1$$

by (A). By this and by two uses of (A),

$$(xy)\theta' = (y^{-1}\theta)\{x^{-1}\theta \cdot xy\} = y^{-1}\theta \cdot (x\theta' \cdot y) = (y^{-1}\theta \cdot x\theta')y.$$

By (B), $(y^{-1}\theta, x\theta') = 1$. By this and by (A),

$$(xy)\theta' = (x\theta' \cdot y^{-1}\theta)y = x\theta' \cdot (y^{-1}\theta \cdot y) = x\theta' \cdot y\theta'.$$

Therefore θ' is an endomorphism of G.

To prove that θ' is in K, we shall show that $\theta'\alpha = \alpha\theta'$ for every inner mapping α of G. If α is an inner mapping of G, then (see [SVII], Lemma 3.2) α is a pseudo-automorphism of G; that is, there exists an element p of G such that

$$(7) \qquad [(xy)\alpha]p = (x\alpha)[(y\alpha)p]$$

for all x, y of G. Since $x\theta' = x^{-1}\theta \cdot x$, and since $\theta\alpha = \alpha\theta$, we use (7) to get

$$(x\theta'\alpha)p = [(x^{-1}\theta \cdot x)\alpha]p = (x^{-1}\theta\alpha)(x\alpha \cdot p) = (x^{-1}\alpha\theta)(x\alpha \cdot p).$$

It follows in particular from (7) that $x^{-1}\alpha = (x\alpha)^{-1}$. Moreover, by (A), the elements $x\alpha\theta$, $x\alpha$, p lie in a group. Hence

$$(x\theta'\alpha)p = [(x\alpha)^{-1}\theta \cdot x\alpha]p = (x\alpha\theta')p.$$

Therefore $x\theta'\alpha = x\alpha\theta'$ for all x, whence we see that θ' is in K.

Finally, since $(x\theta, x\theta') = (x, x)\phi = 1$ by (B), we see that $1 = \theta + \theta' = \theta' + \theta$, whence $(\theta')' = \theta$. This proves (C).

(D) *$G\phi$ is commutative. Moreover, the identities*

$$(8) \qquad (x, y, z)\phi = (x\theta, y, z)\theta' = (x, y\theta, z)\theta' = (x, y, z\theta)\theta',$$

$$(9) \qquad (x, y, z)\phi = (x, y, z)\theta^2\phi$$

hold for all x, y, z in G.

Proof of (D). By (B), $G\phi$ is commutative. We proceed to prove (8). Since $\phi = \theta\theta'$, and since θ is in K, certainly

$$(x, y, z)\phi = (x\theta, y, z)\theta'$$

for all x, y, z in G. Next we use the identity (7.10). Since $L(x, y)^{-1} = L(y, x)$ for all x, y (by (7.6)), we may write this as

$$(10) \qquad (x, y, z)^{-1} = (y, x, z)L(y, x).$$

We also recall that $(x\alpha)^{-1} = x^{-1}\alpha$ for every x in G and every inner mapping α of G. Therefore, by (10) and the fact that θ, θ' are in K,

$$(x, y\theta, z)\theta' = (y\theta, x, z)^{-1}L(y\theta, x)\theta' = (y, x, z)^{-1}\theta\theta' L(y\theta, x).$$

Since $G\phi$ is a commutative Moufang loop,

$$(y, x, z)^{-1}\phi = (x, y, z)\phi$$

by properties of the associator in a commutative Moufang loop (see [SVIII.2]). By this and the fact that $\phi = \theta\theta'$ is in K,

$$(x, y\theta, z)\theta' = (x, y, z)\phi L(y\theta, x) = (x, y, z)L(y\theta, x)\phi.$$

However, by (7.7),

$$(x, y, z)L(y\theta, x)\phi = \{(x, y, z)\big((x, y, z), x, y\theta\big)^{-1}\}\phi.$$

By further properties [SVIII.2] of the associator in a commutative Moufang loop,

$$\begin{aligned}((x, y, z), x, y\theta)^{-1}\phi &= (y\theta, x, (x, y, z))\phi \\ &= (y, x, (x, y, z))\theta\phi \\ &= 1\theta\phi = 1.\end{aligned}$$

Hence

$$(x, y\theta, z)\theta' = (x, y, z)\phi$$

for all x, y, z in G. Combining this with (7.9) we get

$$(x, y, z\theta)\theta' = (xy, z\theta, y)^{-1}\theta' = (xy, z, y)^{-1}\phi = (x, y, z)\phi$$

for all x, y, z in G. This completes the proof of (8).

Since θ is an endomorphism of G,

$$(x, y, z)\phi = (x, y, z)\theta\theta' = (x\theta, y\theta, z\theta)\theta'$$

for all x, y, z in G. By this, (8), and the fact that $\theta\theta' = \theta'\theta$,

$$(x, y, z)\phi = (x, y, z)\theta^3\theta' = (x, y, z)\theta^2\phi$$

for all x, y, z. This proves (9) and completes the proof of (D).

(E) *ϕ and θ^2 are strongly normal.*

Proof of (E). We need the formulas

$$(11) \qquad (\theta^2)' = \phi + \theta',$$

$$(12) \qquad \phi' = \theta^2 + \theta'$$

for the complements of θ^2 and ϕ. We obtain these as follows: By (A), if x, y are in G, the elements x, $x\theta$, y lie in a group. Equivalently, since $x = x\theta \cdot x\theta'$, the elements $x\theta'$, $x\theta$, y lie in a group. In particular, on replacing x, y by $x\theta$, $x\theta'$, respectively, we see that $x\phi$, $x\theta^2$, $x\theta'$ lie in a group. However, by (B) and the fact that θ, θ', ϕ are in K, each two of $x\phi$, $x\theta^2$, $x\theta'$ commute; therefore the three elements lie in an abelian group. Now we see that

$$1 = \theta + \theta' = (\theta^2 + \phi) + \theta' = \theta^2 + (\phi + \theta') = \phi + (\theta^2 + \theta'),$$

whence (11), (12) follow immediately.

Next we wish to prove that

$$(13) \qquad a\phi = a\theta^2\phi$$

for every element a in the commutator-associator subloop G'. Since θ, ϕ are endomorphisms of G, we need only verify (13) when a is an arbitrary commutator or associator of G. However, if a is a commutator, (13) follows from the fact (see (D)) that $G\phi$ is commutative; and, if a is an associator, (13) follows from (9).

For a in G', by (13),

$$a\theta^2\phi = a\phi = a[\theta^2 + (\theta^2)']\phi = (a\theta^2\phi)[a(\theta^2)'\phi].$$

From this and (11)

$$1 = a(\theta^2)'\phi = a(\phi + \theta')\phi = (a\phi^2)(a\theta'\phi).$$

Therefore

$$(a\phi^2)^{-1} = a\theta'\phi = a\theta\phi \tag{14}$$

for every a in G', the second equality coming by interchange of θ and θ'. In view of (14),

$$(a\phi^2)^{-2} = (a\theta\phi)(a\theta'\phi) = a(\theta + \theta')\phi = a\phi$$

for a in G'. However, since $G\phi^2$, like $G\phi$, is commutative Moufang,

$$(a\phi^2)^{-2} = a\phi^2$$

for a in G'. (See [SVIII.2].) Thus

$$a\phi^2 = a\phi = a\phi(\phi + \phi') = (a\phi^2)(a\phi\phi') \tag{15}$$

for every a in G'. In view of (15), $\phi\phi'$ maps G' upon 1.

Since $\phi = \theta\theta'$ and (hence) ϕ' are in K, then $\phi\phi'$ is in K. Consequently, since $G'\phi\phi' = 1$, the defining relation (2) of K tells us that the subloop $G\phi\phi'$ is part of the left nucleus of G. For a Moufang loop, the left nucleus coincides with the nucleus ([SVII], Theorem 2.1); hence $G\phi\phi'$ is part of the nucleus of G. In addition, by (1), $G\phi\phi'$ commutes elementwise with G. Hence $G\phi\phi'$ lies in the centre of G. Therefore $\phi\phi'$ is centralizing, and ϕ is strongly normal.

If a is in G', we use (11), (13), (14), (15) to get

$$a\theta^2(\theta^2)' = a\theta^2(\phi + \theta') = (a\theta^2\phi)(a\theta\phi) = (a\phi)(a\phi^2)^{-1} = 1.$$

Therefore $\theta^2(\theta^2)'$ maps G' into 1. Consequently, by the same arguments as employed in connection with ϕ, we see that θ^2 is strongly normal. This completes the proof of (E).

To sum up: by assuming (i) we were able to prove (E), (D), and (C). Thus (i) implies (ii) (so that (i), (ii), (iii) are equivalent), and, moreover, (i) implies (iv) and (v). This completes the proof of Lemma 7.2* and repairs the hole in the proof of Lemma 7.2.

References

1. Richard Hubert Bruck, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete, N.F., Heft 20, Berlin-Göttingen-Heidelberg, Springer-Verlag, 1958.
2. ———, *Contributions to the theory of loops*, Trans. Amer. Math. Soc., vol. 60 (1946), pp. 245–354.
3. Nickolas Heerema, *Sums of normal endomorphisms*, Trans. Amer. Math. Soc., vol. 84 (1957), pp. 137–143.
4. R. H. Bruck, *Analogues of the ring of rational integers*, Proc. Amer. Math. Soc., vol. 6 (1955), pp. 50–58.

University of Wisconsin
Madison, Wisconsin