SPLITTING ENDOMORPHISMS

BY REINHOLD BAER

In their analysis of the direct decompositions of operator groups Fitting and Kořínek have introduced an important concept which after abstraction from the special situation considered by these authors may be stated as follows: if η is an endomorphism of the operator group G, then the kernels of the endomorphisms η , $\eta^2 \cdots$, $\eta^i \cdots$ form an ascending chain of admissible and normal subgroups; their compositum $R(\eta)$ is a normal and admissible subgroup of G which we term the radical of n. An isomorphism is induced by η in $G/R(\eta)$. An admissible subgroup C of G which contains one and only one element in every coset of $G/R(\eta)$ is termed a complement of η , provided η induces an automorphism in C. Whenever there exists a complement of η , we say that η splits G, since η behaves in the radical like a nilendomorphism and in the complement like an automorphism. The problem of the present note is to find criteria for endomorphisms to split; we obtain two different types of such criteria: individual ones which assure the splitting of an individual endomorphism by considering properties essentially involving this endomorphism, and universal ones which apply to whole classes of endomorphisms and which are expressed in terms of chain conditions for certain classes of subgroups. Various applications of these results and concepts will be discussed in later publications.

As is usual with discussions involving primarily endomorphisms, the associative law is not used at all; thus we obtain all our results immediately for loops. The careful reader will notice that no simplification of our arguments would have been obtained if we had restricted ourselves to groups.

Another, perhaps more important, generalization could have been obtained as follows. Instead of considering the system of all admissible subloops of the given operator loop we could have given preference to some distinguished system of admissible subloops with the property that cross cuts and composita of each of its subsets belong to it. Though this could have been done without much difficulty, it would have involved a few nice points, when defining the admissible endomorphisms; thus we refrained from doing more than mentioning this possibility.

1. Fundamental concepts. We are considering a loop(1) L. The composition of the elements in L is written as addition x+y. The loop L admits the elements in the set M as (left-) multipliers so that there exists for every m

Presented to the Society, November 30, 1946; received by the editors July 27, 1946.

⁽¹⁾ The elementary facts on loop theory that we shall use may be found in various papers on the subject; see the bibliography.

in M and every x in L a uniquely determined element mx in L. This multiplication is distributive, that is, m(x+y) = mx + my for m in M, x, y in L.

An endomorphism η of the M-loop L maps every element x in L upon a uniquely determined element $x\eta$ in L in such a way that

$$(x + y)\eta = x\eta + y\eta$$
 and $m(x\eta) = (mx)\eta$ for m in M and x, y in L.

The kernel $K(\eta)$ of η is the set of all the elements x in L such that $x\eta = 0$; it is a normal M-subloop of L.

If η is an endomorphism of L, so are $\eta^2, \dots, \eta^i, \dots$. Thus we may form their kernels $K(\eta^i)$ too; it is seen without difficulty that they form an ascending chain of normal M-subloops of $L: 0 \leq K(\eta) \leq K(\eta^2) \leq \dots \leq K(\eta^i) \leq \dots$. Their compositum $R(\eta)$ is, therefore $L: 0 \leq K(\eta) \leq K(\eta^2) \leq \dots \leq K(\eta^i) \leq \dots$. Their compositum $L: 0 \leq K(\eta) \leq K(\eta^i) \leq \dots \leq K(\eta^i) \leq$

x is in
$$R(\eta)$$
 if, and only if, $x\eta$ is in $R(\eta)$.

This important fact is verified by observing the equivalence of the following propositions: x is in $R(\eta)$; $0 = x\eta^{i+1} = (x\eta)\eta^i$ for some positive i; $x\eta$ is in $R(\eta)$.

One of the fundamental consequences of the preceding observation is the fact that:

η induces an isomorphism of the M-loop $L/R(\eta)$ into itself.

In all the situations that will be investigated in the present note this isomorphism will be an automorphism of $L/R(\eta)$; but as follows from trivial examples, this need not be the case in general.

DEFINITION 1. The M-subloop C of the M-loop L is a complement of the endomorphism η if $L = R(\eta) + C$, $0 = R(\eta) \cap C$, $C = C\eta$.

The first two of these conditions(*) just assert that every coset of $L/R(\eta)$ contains one and only one element in C so that L is a splitting extension of $R(\eta)$ by $L/R(\eta)$. Thus η induces essentially the same automorphism in C and in $L/R(\eta)$. It might seem better justified to substitute for the third condition the weaker condition $C\eta \leq C$, but this would lead us to unnecessary complication, since $C\eta \leq C$ will imply $C\eta = C$ whenever η induces an automorphism in $L/R(\eta)$. Note that C need not be a normal subloop of L.

Whenever there exists a complement of η , we shall say that η is a splitting endomorphism of L or that η splits L.

It is easy to give examples of endomorphisms that do not split and of

⁽²⁾ The fact that the compositum of normal subloops is itself a normal subloop is easiest verified by using Bruck's "inner mapping group"; see Bruck [1]. Numbers in brackets refer to the bibliography at the end of the paper.

⁽³⁾ It should be noted that the compositum of the subloops S and T is S+T=T+S, whenever S is a normal subloop of the compositum of S and T; see, for example, Baer [1].

endomorphisms that possess at least two different complements.

DEFINITION 2. The endomorphism η of the M-loop L is a uniformly splitting endomorphism of L if η induces a splitting endomorphism in every M-subloop S of L satisfying $S\eta \leq S$.

All the splitting criteria obtained in the present investigation assure uniform splitting. But for many applications it suffices to assume simply splitting.

2. Individual splitting criteria. The following notations will prove convenient. If η is an endomorphism of the M-loop L, and if the M-subloop S of L satisfies $S\eta \leq S$, then S is admissible for the extended system of operators M, η , and we shall say that S is an M- η -subloop of L. Of particular interest to us are the cyclic M- η -subloops of L; they are smallest M- η -subloops generated by a single element x in L; we denote them by (x, η) and remark that (x, η) is the smallest M- η -subloop generated by x or the smallest M-subloop generated by the sequence of elements: $x, x\eta, x\eta^2, \cdots, x\eta^i, \cdots$

The main object of the present section is the proof of the following comprehensive criterion.

THEOREM A. The endomorphism η of the M-loop L splits L uniformly if, and only if, it meets the following two requirements:

- (D) To every cyclic M- η -subloop Z of L there exists an integer i = i(Z) such that $Z\eta^i = Z\eta^{i+1}$.
- (A) If the subloop V is the compositum of the cyclic M- η -subloops Z' and Z'' satisfying $Z' = Z'\eta$ and $Z'' = Z''\eta$, then there exists an integer k = k(V) such that $V \cap K(\eta^k) = V \cap K(\eta^{k+1})$.

The proof of this proposition will be effected by proving a number of lemmas which will often assert more than is contained in Theorem A.

LEMMA 1. Every uniformly splitting endomorphism meets requirement (D).

Proof. Consider the cyclic M- η -subloop $Z = (x, \eta)$ of L. Clearly $Z\eta \leq Z$. Since η splits uniformly, it induces a splitting endomorphism in Z. The radical of this endomorphism of Z is $Z \cap R(\eta)$. Denote by U some complement of the endomorphism which η induces in Z. Then there exists one and only one element y in U such that $x \equiv y \mod Z \cap R(\eta)$. If z is the uniquely determined element such that x = y + z, then z is in $R(\eta)$. Hence $z\eta^i = 0$ for some positive i, implying that $x\eta^i = y\eta^i$. From $U = U\eta$ we infer now that

$$U = U\eta^i \le Z\eta^i = (x\eta^i, \eta) = (y\eta^i, \eta) \le (y, \eta) \le U$$
 or $U = Z\eta^i$.

Now $Z\eta^{i} = Z\eta^{i+1}$ is an immediate consequence from $U = U\eta$.

LEMMA 2. Suppose that η meets requirement (D) and that C is a complement of η . Then the element x in L belongs to C if, and only if, $(x, \eta)\eta = (x, \eta)$.

Proof. If x is an element in C, then $(x, \eta) \le C$, since $C = C\eta$. From (D) we infer the existence of a positive integer i such that $(x, \eta)\eta^i = (x, \eta)\eta^{i-1}$. But η

induces an automorphism in the complement C of η , and (x, η) is part of C. Hence $(x, \eta)\eta = (x, \eta)$ is a consequence of the preceding equation, showing the necessity of our condition.

Suppose conversely that $(x, \eta)\eta = (x, \eta)$. Since C is a complement of η , there exists one and only one element y in C such that $x \equiv y \mod R(\eta)$; this is equivalent to saying that there exists an integer i such that $x\eta^i = y\eta^i$. Consequently

$$(x, \eta) = (x, \eta)\eta^i = (x\eta^i, \eta) = (y\eta^i, \eta) \le (y, \eta) \le C,$$

since y is in C and $C = C\eta$. Hence x itself is in C, proving the sufficiency of our condition.

LEMMA 3. If the splitting endomorphism η meets requirement (D), then it meets requirement (A).

Proof. If C is a complement of η , and if Z' and Z'' are cyclic M- η -subloops of L satisfying $Z' = Z'\eta$ and $Z'' = Z''\eta$, then it follows from Lemma 2 that both Z' and Z'' are part of C. Hence their compositum V is part of C which implies that $V \cap K(\eta^i) \leq V \cap R(\eta) \leq C \cap R(\eta) = 0$. Hence $V \cap K(\eta^i) = 0$ for every positive i, a statement that appears to be slightly sharper than (A).

LEMMA 4. If S is an M-subloop of L such that $S = S\eta$ and

$$S \cap K(\eta^i) = S \cap K(\eta^{i+1})$$

for some positive i, then $S \cap R(\eta) = 0$.

Proof. If x is in $S \cap R(\eta)$, then there exists a smallest positive integer j such that $x\eta^j = 0$. Since $S = S\eta$, we have $S = S\eta^i$; and thus there exists an element y in S such that $x = y\eta^i$. Hence

$$0 = x\eta^{i} = y\eta^{i+i} = (y\eta^{i-1})\eta^{i+1}.$$

Thus $y\eta^{i-1}$ belongs to $S \cap K(\eta^{i+1}) = S \cap K(\eta^i)$, proving that

$$0 = (y\eta^{j-1})\eta^{i} = y\eta^{i+j-1} = x\eta^{j-1}.$$

From the choice of j it follows now that j-1=0 or 0=x, proving our contention that $S \cap R(\eta) = 0$.

LEMMA 5. If η meets requirements (D) and (A), then it splits L.

Proof. Consider the set T of all the elements x in L such that $(x, \eta)\eta = (x, \eta)$. We show first:

(+)
$$(x, \eta)\dot{\eta} = (x, \eta)$$
 if, and only if, $(x, \eta) \cap R(\eta) = 0$.

If $(x, \eta)\eta = (x, \eta)$, then we infer from (A) the existence of a positive integer i such that $(x, \eta) \cap K(\eta^i) = (x, \eta) \cap K(\eta^{i+1})$ —letting $Z' = Z'' = V = (x, \eta)$ —and it follows from Lemma 4 that $(x, \eta) \cap R(\eta) = 0$. If conversely $(x, \eta) \cap R(\eta) = 0$,

then η induces an isomorphism of (x, η) into itself. We infer from (D) the existence of a smallest positive integer i such that $(x, \eta)\eta^{i} = (x, \eta)\eta^{i-1}$. But $(x, \eta)\eta^{i-1} \leq (x, \eta)$ and η effects an isomorphism in (x, η) . If i-1 were positive, then our equation would imply $(x, \eta)\eta^{i-1} = (x, \eta)\eta^{i-2}$, contradicting our choice of i. Hence $(x, \eta)\eta = (x, \eta)$, completing the proof of (+).

Suppose now that x and y are elements in T and that z is some element in the compositum V of the M-subloops (x, η) and (y, η) . It follows from (A) and Lemma 4 that $V \cap R(\eta) = 0$. Since z is in V, (z, η) is part of $V = V\eta$. Hence $(z, \eta) \cap R(\eta) \leq V \cap R(\eta) = 0$, and it follows from (+) that $(z, \eta)\eta = (z, \eta)$. Now one verifies immediately that T is the compositum of all the cyclic M- η -subloops Z of L which satisfy $Z = Z\eta$. Thus T is in particular an M-subloop of L satisfying $T = T\eta$ and, by (+), $T \cap R(\eta) = 0$. If finally w is some element in L, then we infer from (D) the existence of a positive integer k such that $(w, \eta)\eta^k = (w, \eta)\eta^{k+1}$. This implies $(w\eta^k, \eta) = (w\eta^k, \eta)\eta$ so that in particular $(w\eta^k, \eta) \leq T$. But $(w\eta^k, \eta)$ is mapped upon itself by η , and contains therefore an element v such that $v\eta^k = w\eta^k$. Clearly $v \equiv w$ modulo $R(\eta)$ and v is in T, proving that T is the desired complement of η .

Proof of Theorem A. If η is a uniformly splitting endomorphism of the M-loop L, then we infer the validity of (D) from Lemma 1 and subsequently the validity of (A) from Lemma 3. If conversely conditions (A) and (D) are satisfied by η , then they are satisfied by the endomorphism induced by η in the M- η -subloop S of L. It follows from Lemma 5 that this induced endomorphism splits S so that η is a uniformly splitting endomorphism of L.

COROLLARY. If η is a uniformly splitting endomorphism of the M-loop L, then it possesses one and only one complement $C = C(\eta)$. If S is an M- η -subloop of L, then $S \cap R(\eta)$ is the radical and $S \cap C(\eta)$ is the (uniquely determined) complement of the endomorphism which η induces in S.

These are almost immediate consequences of Theorem A and Lemma 2. From Theorem A we want to deduce a more special splitting criterion. To do so, we need the following concept.

DEFINITION 3. The isomorphism α of the M-loop H is almost periodic if there exists to every x in H a positive integer i = i(x) such that $x = x\alpha^i$.

Note that i may change from element to element so that α need not be of finite order.

THEOREM B. If η induces an almost periodic isomorphism in $L/R(\eta)$, then η is a uniformly splitting endomorphism of the M-loop L.

Proof. If x is an element in L, then $R(\eta)+x$ is an element in $L/R(\eta)$. Hence there exists a positive integer i such that $x = x\eta^i$ modulo $R(\eta)$; this implies the existence of a positive integer j such that $x\eta^j = x\eta^{i+j}$. Hence

$$(x, \eta)\eta^{j} = (x\eta^{j}, \eta) = (x\eta^{i+j}, \eta) = (x, \eta)\eta^{i+j} \le (x, \eta)\eta^{j+1} \le (x, \eta)\eta^{j}$$

or $(x, \eta)\eta^{i} = (x, \eta)\eta^{i+1}$, proving the validity of condition (D).

Assume next that $(x, \eta)\eta = (x, \eta)$. There exist, as before, positive integers i and j such that $x\eta^{i} = x\eta^{i+j}$. Hence

$$(x, \eta) = (x, \eta)\eta^{j} = (x\eta^{j}, \eta)$$

is the *M*-subloop of *L* which is generated by the elements $x\eta^i$, $x\eta^{i+1}$, \cdots , $x\eta^{i+i-1}$. Clearly η effects a cyclic permutation of order i among these elements, if we have chosen i, as we may, as small as possible. But this implies in particular that η^i leaves invariant each of these i generators of the *M*-loop (x, η) . Hence η^i leaves invariant every element in (x, η) .

Suppose now that Z' and Z'' are cyclic M- η -subloops of L satisfying $Z' = Z'\eta$ and $Z'' = Z''\eta$. We infer from the preceding paragraph of the proof the existence of positive integers i' and i'' such that $\eta^{i'}$ leaves invariant every element in Z' and $\eta^{i''}$ leaves invariant element in Z''. Then i'i'' is a positive integer such that $\eta^{i'i''}$ leaves invariant every element in Z' as well as in Z''. Hence $\eta^{i'i''}$ leaves invariant every element in the compositum V of Z' and Z''. Thus η induces an automorphism of finite order (dividing i'i'') in V; this implies in particular the validity of condition (A). Thus we have shown that conditions (D) and (A) of Theorem A are both satisfied, and Theorem B is a consequence of Theorem A.

A direct verification of Theorem B, without reference to Theorem A, would not prove too difficult.

3. Universal splitting criteria. The basis for the considerations of this section is the following proposition which may be of interest in itself.

LEMMA 6. If the descending chain condition is satisfied by the M-subloops of the M-loop Z, if η is an endomorphism of Z such that Z is a cyclic M- η -loop, then the M-loop Z may be generated by a finite number of elements.

Proof. There exists an element z in Z such that the M-loop Z is generated by the sequence of elements z, $z\eta$, \cdots , $z\eta^i$, \cdots . Denote by Z_i the M-subloop generated by the elements $z\eta^j$ for $i \le j$. Then $Z = Z_0$, $Z_i = Z_{i-1}\eta$ for 0 < i and $Z_i \le Z_{i-1}$ for 0 < i. The Z_i form, therefore, a descending chain of M-subloops of L; hence there exists an integer n such that $Z_n = Z_{n+1} = Z_n\eta$. Since $z\eta^n$ is an element in $Z_n = Z_n\eta$, there exists an element u in Z_n such that $u\eta = z\eta^n$.

Denote by W(k) the M-subloop of Z which is generated by the elements $z\eta^i$ for $n \le j \le n+k$. It is readily seen that every element in Z_n belongs to at least one W(k) and that Z_n is the compositum of the W(k). Consequently there exists a positive integer m such that u belongs to W(m). Since $W(m)\eta$ is generated by the elements $z\eta^{i+1}$ for $n \le j \le n+m$, we have $W(m)\eta \le W(m+1)$. Since u is in W(m), $u\eta = z\eta^n$ belongs to $W(m)\eta$ too; thus $W(m)\eta$ contains the elements $z\eta^i$ for $n \le j \le n+m+1$, proving $W(m+1) \le W(m)\eta$. Thus we have shown that $W(m) \le W(m+1) = W(m)\eta$. This inequality implies in parti-

cular that there exists to every element s in W(m) an element s' in W(m) such that $s = s'\eta$. Hence we may construct inductively a sequence of elements u(i) in W(m) such that u = u(0), $u(i)\eta = u(i-1)$ for 0 < i.

Denote by V(i) the M-subloop of Z which is generated by the elements u(j) for $i \le j$. Then $V(i) \le V(i-1) = V(i)\eta$ for 0 < i. There follows from the descending chain condition the existence of an integer k satisfying $V(k) = V(k+1) = \cdots = V(k+j) = \cdots$ so that in particular $V(k+1) = V(k) = V(k+1)\eta$. Since u(k+1) is in $V(k+1) = V(k+1)\eta$, it follows that V(k) contains all the elements

$$u(k + 1), u(k), \dots, u(0) = z\eta^{n}, z\eta^{n+1}, \dots, z\eta^{n+j}, \dots,$$

proving that Z_n is part of V(k). Consequently

$$Z_n \leq V(k) \leq W(m) \leq Z_n$$
 or $Z_n = W(m)$.

Since W(m) is, by its very definition, a finitely generated M-subloop of Z, so is Z_n . But Z is obtained from Z_n by adjoining not more than n elements, namely z, $z\eta$, \cdots , $z\eta^{n-1}$, and thus Z itself is finitely generated, as we claimed.

THEOREM C. Suppose that the M-subloop H of the M-loop L meets the following two requirements:

- (i) The descending chain condition is satisfied by the M-subloops of H.
- (ii) If F is a finitely generated M-subloop of H, then the ascending chain condition is satisfied by the M-subloops of F.

Then the endomorphism η of L splits L uniformly whenever there exists a positive integer i such that $L\eta^i \leq H$.

Proof. If x is an element in L, then the M-subloops $(x, \eta)\eta^{j}$ for $i \leq j$ form a descending chain of M-subloops of H. Hence it follows from (i) that there exists an integer n, not less than i, such that $(x, \eta)\eta^{n} = (x, \eta)\eta^{n+1}$, proving the validity of condition (D) of Theorem A.

Suppose that Z' and Z'' are cyclic M- η -subloops of L satisfying $Z' = Z'\eta$ and $Z'' = Z''\eta$. Then Z', Z'' and their compositum V are all contained in $L\eta^i \leq H$. Now it follows from (i) and Lemma 6 that Z', Z'' and therefore V are finitely generated. Consider the ascending chain of M-subloops $V \cap K(\eta^i)$ of V. We infer from (ii) the existence of a positive integer m such that $V \cap K(\eta^m) = V \cap K(\eta^{m+1})$, proving the validity of condition (A) of Theorem A. Hence η is a uniformly splitting endomorphism of L, completing the proof.

The conditions (i) and (ii) are certainly satisfied whenever the double chain condition is satisfied by the M-subloops of H. This shows that Fitting's lemma (4) is a special case of Theorem C. It should be noted, however, that (ii) is satisfied often enough when the ascending chain condition is not satis-

⁽⁴⁾ Fitting [1]; for a convenient presentation see Jacobson [1].

fied. Simple examples are groups like the rational numbers modulo 1, groups of type p^{∞} , and so on. See in this context the discussion following the corollary to the present Theorem C.

COROLLARY. Suppose that the M-subloop A of the M-loop L meets the following three requirements:

- (a) A is a commutative group.
- (b) The descending chain condition is satisfied by the M-subgroups of A.
- (c) If Z is a cyclic M-subgroup of A, then the ascending chain condition is. satisfied by the M-subgroups of Z.

Then the endomorphism η of L splits L uniformly whenever there exists an integer i such that $L\eta^i \leq A$.

This is an immediate consequence of Theorem C, if one observes only that the double chain condition is satisfied by the M-subgroups of the commutative M-group A'+A'' whenever it is satisfied by the M-subgroups of A' and of A''.

From the proof of the corollary it is apparent that condition (a) may be weakened in a variety of ways without invalidating the corollary. It would suffice, for instance, to assume that A is a group all of whose M-subgroups are normal. The impossibility of omitting (b) altogether may be seen from so trivial an example as the infinite cyclic group. An example showing that condition (c) cannot be omitted without invalidating the corollary may be constructed as follows: Let R be the additive group of rational numbers and P a group of type p^{∞} . Then P contains, for every n, one and only one cyclic subgroup Z(n) of order p^n , and every element in P is contained in at least one Z(n). Denote by A the direct sum of R and P. If r is a rational number, then denote by r' the uniquely determined endomorphism of A which annihilates P and maps every element in R upon its r-fold. There exists furthermore an endomorphism w of A which annihilates P and effects a homomorphism of Rupon P. Let M be the set composed of w and the r' so that M may be considered in a natural way as a set of multipliers for A. Then one verifies easily that the only M-subgroups of A are 0, Z(n), P, and A. Consider now the (admissible) endomorphism of A which maps every element in A upon its p-fold. The radical of this endomorphism is exactly P. But P is not a direct summand of A, since A is the only M-subgroup of A which is not part of P. Thus we have found an endomorphism of the abelian M-group A which does not split, though the descending chain condition is clearly satisfied by the M-subgroups of A.

Elsewhere (5) we have shown that there exists a great number of special situations where condition (c) may be omitted. We give just samples of the type of results (6). If A is a commutative M-group, then we may form the ring

⁽⁵⁾ Baer [2].

⁽⁶⁾ The proofs may be found in Baer [2].

E of endomorphisms of A which is generated by the identity and those endomorphisms of A which are induced by elements in M. If every ideal in A is a two-sided ideal, then the descending chain condition implies condition (c) of the corollary. Another criterion of the same type may be obtained as follows: Denote by E^* the center of the ring E, just defined. If the descending chain condition is satisfied by the E^* -admissible subgroups of A, then both conditions (b) and (c) of the corollary are satisfied too. This last fact contains a criterion, due to Kořínek [1], as a special case, who assumes that the descending chain condition is satisfied by all the subgroups of A whether admissible or not (and this clearly implies the validity of the descending chain condition for E^* -admissible subgroups of A).

BIBLIOGRAPHY

A. A. ALBERT

1. Quasigroups, I and II, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 507-519 and vol. 55 (1944) pp. 401-419.

R. BAER

- 1. The homomorphism theorems for loops, Amer. J. Math. vol. 67 (1945) pp. 450-460.
- The double chain condition in cyclic operator groups, Amer. J. Math. vol. 69 (1947) pp. 37-45.

R. H. BRUCK

- 1. Contributions to the theory of loops, Trans. Amer. Math. Soc. vol. 60 (1946) pp. 245-354. H. FITTING
 - 1. Über die direkten Produktzerlegungen einer Gruppe in direkt unzerlegbare Faktoren, Math. Zeit. vol. 39 (1934) pp. 16-30.

N. JACOBSON

1. The theory of rings, Mathematical Surveys, vol. 2, 1943.

V. Kořínek

1. Sur la decomposition d'un group en produit direct des sousgroups, Casopis pro pestovaní matematiky a fysiki vol. 66 (1937) pp. 261-286.

University of Illinois, Urbana, Ill.