

DIRECT DECOMPOSITIONS

BY
REINHOLD BAER

Introduction. The theorem of Wedderburn and Remak asserting the isomorphism of indecomposable direct decompositions of finite groups has been extended by Krull and O. Schmidt to all operator groups satisfying the double chain condition for admissible subgroups. If the hypotheses imposed upon the operator group do not assure the existence of decompositions into indecomposable direct summands, then one can only try to prove a refinement theorem asserting the existence of isomorphic refinements to any two given direct decompositions; Koříněk has proved such a refinement theorem for all operator groups meeting the requirement that the descending chain condition be satisfied by all of the subgroups, whether admissible or not, of the operator center. Clearly Schmidt's and Koříněk's theorems are independent of each other in the sense that neither is a consequence of the other one.

It is the principal objective of the present investigation to obtain a refinement theorem of such a generality that in particular the theorems of O. Schmidt and Koříněk and their recent generalizations by Kurosh are special cases of it. However, one ought to remember the limitations as to the generality that is attainable. For there exist ordinary abelian groups possessing direct decompositions without isomorphic refinements (Baer [1]⁽¹⁾). Krull [2] has given an example of an abelian operator group satisfying the ascending chain condition for admissible subgroups, but possessing non isomorphic indecomposable direct decompositions. Kurosh [3] has constructed a very elegant example of a (not commutative) group satisfying the ascending chain condition for all its subgroups, though possessing non isomorphic direct decompositions into two indecomposable direct summands.

It has long been noticed that the difficulties encountered when studying direct decompositions have their source in properties of the center. For instance, it is quite easy to prove that direct decompositions of groups without a center possess common, not only isomorphic refinements⁽²⁾. Finally Kurosh and Koříněk showed that it suffices to impose conditions on the center in order to obtain a refinement theorem. Thus every investigation of the refinement theorems will have to concern itself quite fundamentally with the center.

The methods used in investigations of the refinement theorems may be

Presented to the Society, November 30, 1946; received by the editors December 26, 1945, and, in revised form, October 1, 1946.

⁽¹⁾ Numbers in brackets refer to the bibliography at the end of the paper.

⁽²⁾ See, for example, Zassenhaus [1, p. 82].

divided broadly into two classes. There is firstly Fitting's method which is based on the observation that direct decompositions are defined by their decomposition endomorphisms and which works fundamentally with products of these decomposition endomorphisms. Jacobson's presentation of the decomposition theorems, for instance, gives a very clear and convincing account of Fitting's method. It was Kořinek's discovery mainly which showed that we need not consider all these endomorphisms, but only those which map the group into part of its center. Secondly one may attempt to work within the partially ordered set of the normal and admissible subgroups. This has been done systematically by Ore [1] and partly also by Kurosh [2, 3]. The basis for this approach is the observation that it is possible to define isomorphy of direct decompositions in terms of an exchange property of which their (center) isomorphy is a trivial consequence. The difficulties that seem, at least at present, to stand in the way of using this method may be indicated shortly: isomorphy of direct decompositions in the sense of the exchange property is a much deeper proposition than ordinary isomorphy; witness the free abelian groups of rank 2 which possess direct decompositions into cyclic direct summands that are not exchange isomorphic. More difficult still is the fact that the center of a group cannot be characterized in terms of the partially ordered set of subgroups—after all there exist abelian groups that have essentially the same system of subgroups as certain nonabelian groups. Thus it appears natural to use a "mixed method": most of our hypotheses, contentions and many of our arguments deal with the system of subgroups only; but there are some proofs where essential use has been made of the elements, their addition and subtraction.

When studying the various proofs of decomposition theorems, one notices that the hypotheses imposed upon the operator group are mainly used to prove what we have termed elsewhere^(*) 'splitting criteria for endomorphisms. Thus it seems only natural to base our discussion on the hypothesis that certain rather special endomorphisms split; in this fashion we obtain a very comprehensive refinement theorem—as a matter of fact, it does not seem impossible to obtain necessary and sufficient conditions for the validity of a refinement theorem by proceeding far enough in this direction—and by applying the splitting criteria that we obtained elsewhere it may be shown how great a range this theorem has.

§§1 to 4 are devoted to preparations, some of which may be of independent interest. In §5 we prove first a very sharp refinement theorem for decompositions into two direct summands; and from this special refinement theorem the general refinement theorem is deduced by arguments that deal with the system of subgroups only. In §6 groups without abelian direct summands are treated; they have rather interesting special properties; in particu-

(*) Baer [4].

lar it is possible to determine the refinements uniquely by the original decompositions. In §7 we discuss direct decompositions into summands that are either abelian and indecomposable or else they do not possess abelian direct summands, not 0. They have the important property that center isomorphism implies exchange isomorphism and that the exchange property may be proved in a strict form. In §8 we give finally the applications of the splitting criteria to the general refinement theorem.

As is natural in an investigation that concerns itself mainly with the endomorphisms of groups, no real use is made of the associative law. Thus we develop the whole theory immediately for loops⁽⁴⁾. This does not involve any noticeable extra work, partly for the reason given, partly because the principal difficulties stem from the center and the center is an abelian group⁽⁵⁾.

1. Fundamental concepts and notations. In this section we collect for ready reference a number of concepts and results established elsewhere.

Throughout we are going to consider a loop L admitting a certain system M of operators. Thus there exists the sum $x+y$ of any elements x, y in L and the product mx of every m in M and x in L . These compositions meet the usual requirements; see, for example, Baer [3, 4, 5]. As usual we term the subloop S of L *admissible* or an *M -subloop*, if $MS \leq S$. (The reader will notice that the definition of admissibility is almost the only use made of the operators.)

The center of L consists of all those elements in L which commute with every element in L and which associate with every pair of elements in L . The center is a commutative subgroup of L , but in general it is not admissible. Thus we consider, following Kořínek [1], the *M -center* $Z_M(L)$ of L which is the uniquely determined greatest M -subgroup of the center of L ; see Baer [5].

An *M -homomorphism* of L is a single-valued mapping η of L into some M -loop, meeting the requirements:

$$(x + y)\eta = x\eta + y\eta \quad \text{and} \quad m(x\eta) = (mx)\eta$$

for x, y in L and m in M . The system $K(\eta)$ of all the elements in L which are mapped upon 0 by η is termed the *kernel* of η . The kernels form a special class of M -subloops of L , called *normal* M -subloops; for an intrinsic characterization of normal subloops see Albert [1], Smiley [1]. It should be noted that every M -subloop of the center is normal.

An *M -homomorphism* effects a 1:1 mapping if, and only if, its kernel is 0; in this case we speak of an *M -isomorphism*.

(4) Jónsson and Tarski [1] have undertaken a generalization in this direction which goes far beyond operator loops. Our results, however, are not special cases of theirs.

(5) This investigation had originally been planned as a joint enterprise with Professor A. A. Albert. The pressure of war work, however, forced Professor Albert to withdraw. The author gratefully acknowledges the stimulation these original discussions have given to him; see furthermore footnote (9) below. The author is very much indebted to Professors Bruck and Good for their careful reading of a draft of this paper and for their helpful suggestions and criticisms.

The M -homomorphism η of L is termed an M -endomorphism of L if $L\eta \leq L$. The powers η^i for $0 < i$ of an M -endomorphism η are M -endomorphisms too; thus we may form the ascending chain $K(\eta^i)$ of normal M -subloops of L . Their compositum (join) $R(\eta)$ is termed *the radical of η* . It is a normal M -subloop of L with these properties:

x is in $R(\eta)$ if, and only if, there exists an integer $i = i(x)$ such that $x\eta^i = 0$;

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

η induces an M -endomorphism in $R(\eta)$ and an M -isomorphism in $L/R(\eta)$.

For elementary properties of the radical see Baer [4].

An M -subloop C of L is termed a *complement of the M -endomorphism η* if every coset of $L/R(\eta)$ contains one and only one element in C , and if $C = C\eta$. Thus η induces an M -automorphism in C which is essentially the same as the one induced by η in $L/R(\eta)$, and C and $L/R(\eta)$ are essentially the same M -loops. If there exists a complement of η , then η *splits L* or is a *splitting M -endomorphism of L* ; for splitting criteria see Baer [4].

Trivially splitting M -endomorphisms are the M -automorphisms whose radical is 0 and whose complement is L and the *nil endomorphisms* whose radical is L and whose complement is 0.

The M -endomorphism η of L is a *centralizing endomorphism*, if $L\eta \leq Z_M(L)$. These enjoy a number of convenient properties.

(a) The set $\theta_M(L)$ of all the centralizing M -endomorphisms of L is a ring with respect to the operations of addition and multiplication defined in the usual fashion; for properties of this ring see Baer [5].

(b) If η is a centralizing nil endomorphism of L , then $1 + \eta$ is an automorphism of L . For a simple proof see Baer [5].

(c) If C is a complement of the centralizing M -endomorphism η of L , then $C = C\eta \leq L\eta \leq Z_M(L)$. Thus C is a commutative group and a normal M -subloop of L . Anticipating a concept introduced in the next section, this implies that

$$L = C \oplus R(\eta).$$

Loops will be called *abelian* whenever they are commutative and associative, that is, whenever they are commutative groups.

2. Direct decompositions and decomposition endomorphisms. The M -loop L is the *direct sum*⁽⁶⁾ of A and B , in symbols: $L = A \oplus B$, if A and B are normal M -subloops of L whose cross cut is 0 and whose sum is L . Then every element in A commutes with every element in B and associates with every pair of elements in B . The M -loop L is therefore the direct sum of its normal M -subloops A and B if, and only if, every element in L may be represented in one and only one way in the form $a + b = b + a$ for a in A and b in B .

If $L = A \oplus B$, then there exist uniquely determined M -endomorphisms α

⁽⁶⁾ See Albert [1] for fundamental properties of direct sums of loops.

and β of L such that $x = x\alpha$ and $0 = x\beta$ for x in A , $0 = y\alpha$, $y = y\beta$ for y in B . These endomorphisms satisfy⁽⁷⁾

$$(1) \quad \alpha^2 = \alpha, \quad \beta^2 = \beta, \quad \alpha\beta = \beta\alpha = 0, \quad \alpha + \beta = \beta + \alpha = 1.$$

If conversely the M -endomorphisms α, β satisfy the conditions (1), then

$$(2) \quad L = L\alpha \oplus L\beta, \quad K(\alpha) = L\beta, \quad K(\beta) = L\alpha.$$

Thus we shall term any pair α, β of M -endomorphisms, satisfying (1), a *pair of complementary decomposition endomorphisms*; any member of a pair of complementary decomposition endomorphisms shall be called a decomposition endomorphism. We note in passing the useful fact that a centralizing M -endomorphism is a decomposition endomorphism if, and only if, it is idempotent.

The M -loop L is the direct sum of $S(1), \dots, S(n)$, in symbols: $L = S(1) \oplus \dots \oplus S(n)$, if L is, for every i , the direct sum of $S(i)$ and of the compositum of the $S(j)$ for $j \neq i$. Then it is possible again to represent every element in L in one and, apart from the order of summands, only one way in the form $s(1) + \dots + s(n)$ for $s(i)$ in $S(i)$.

If $L = S(1) \oplus \dots \oplus S(n)$, then the compositum of $S(1), \dots, S(i)$ is a normal M -subloop of L , a direct summand of L , and is the direct sum of $S(1), \dots, S(i)$. Direct sums of direct sums are direct sums, in particular

$$S(1) \oplus \dots \oplus S(n) = [S(1) \oplus \dots \oplus S(i)] \oplus [S(i+1) \oplus \dots \oplus S(n)],$$

and a number of similar formulas.

If $L = S(1) \oplus \dots \oplus S(n)$, then denote by $\sigma(i), \sigma'(i)$ the pair of complementary decomposition endomorphisms of L satisfying

$$L\sigma(i) = S(i), \quad L\sigma'(i) = S(1) \oplus \dots \oplus S(i-1) \oplus S(i+1) \oplus \dots \oplus S(n).$$

Then $\sigma'(i) = \sigma(1) + \dots + \sigma(i-1) + \sigma(i+1) + \dots + \sigma(n)$ and

$$(3) \quad \sigma(i)^2 = \sigma(i), \quad \sigma(i)\sigma(j) = 0 \quad \text{for } i \neq j, \quad \sigma(1) + \dots + \sigma(n) = 1.$$

The remainder of this section is devoted to the derivation of a number of simple and often used properties of *products of decomposition endomorphisms*.

LEMMA 1. *Decomposition endomorphisms of the M -loop L map center elements upon center elements and normal M -subloops of L upon normal M -subloops of L .*

Proof. If δ is a decomposition endomorphism of L , then $L = L\delta \oplus K(\delta)$, and δ maps every center element of L upon a center element of $L\delta$, every normal M -subloop of L upon a normal M -subloop of $L\delta$. But center elements of $L\delta$ are center elements of L and normal M -subloops of $L\delta$ are normal M -subloops of L , as we claimed.

⁽⁷⁾ The sum of the mappings α and β is, as usual, defined by the rule: $x(\alpha + \beta) = x\alpha + x\beta$ for every x .

COROLLARY 1. *Products of decomposition endomorphisms map center elements upon center elements and normal admissible subloops upon normal admissible subloops.*

This is an immediate consequence of Lemma 1.

LEMMA 2. *If σ, τ is a pair of complementary decomposition endomorphisms of the M -loop L , and if γ, η, κ are products of decomposition endomorphisms of L , then $\gamma\sigma\eta\tau\kappa$ is a centralizing endomorphism of L .*

Proof. If ϵ, δ is a pair of complementary decomposition endomorphisms of L , and if x and y are elements in L such that $x\delta = y\delta$ and $x\epsilon = y\epsilon$, then $x = y$. Hence we shall refer to $x\delta$ and $x\epsilon$ as to the δ - and ϵ -components of x .

Assume now that σ, τ and α, β are pairs of complementary decomposition endomorphisms of L . We want to show that every $z\sigma\alpha\tau$ for z in L is a center element of L .

Consider an element x in L . Then we prove:

$$(1) \quad z\sigma + x\tau = x\tau + z\sigma.$$

This is true, since $z\sigma$ is the σ -component and $x\tau$ the τ -component of both sides of equation (1).

$$(2) \quad z\sigma\alpha + x\tau = x\tau + z\sigma\alpha.$$

Both sides of (2) have the β -component $x\tau\beta$; and they have the same α -component, since it follows from (1) that

$$\begin{aligned} (z\sigma\alpha + x\tau)\alpha &= z\sigma\alpha + x\tau\alpha = (z\sigma + x\tau)\alpha = (x\tau + z\sigma)\alpha \\ &= x\tau\alpha + z\sigma\alpha = (x\tau + z\sigma\alpha)\alpha. \end{aligned}$$

$$(3) \quad z\sigma\alpha\tau + x = x + z\sigma\alpha\tau.$$

Both sides of (3) have the σ -component $x\sigma$; and their τ -components are equal since, by (2), $(z\sigma\alpha\tau + x)\tau = z\sigma\alpha\tau + x\tau = (z\sigma\alpha + x\tau)\tau = (x\tau + z\sigma\alpha)\tau = x\tau + z\sigma\alpha\tau = (x + z\sigma\alpha\tau)\tau$.

Consider elements x, y in L . Then we prove

$$(4) \quad z\sigma + (x\tau + y\tau) = (z\sigma + x\tau) + y\tau.$$

Both sides have the σ -component $z\sigma$ and the τ -component $x\tau + y\tau$.

$$(5) \quad z\sigma\alpha + (x\tau + y\tau) = (z\sigma\alpha + x\tau) + y\tau.$$

Both sides of (5) have the β -component $(x+y)\tau\beta$, and their α -components are equal, since it follows from (4) that

$$\begin{aligned} [z\sigma\alpha + (x\tau + y\tau)]\alpha &= [z\sigma + (x\tau + y\tau)]\alpha = [(z\sigma + x\tau) + y\tau]\alpha \\ &= [(z\sigma\alpha + x\tau) + y\tau]\alpha. \end{aligned}$$

$$(6) \quad z\sigma\alpha\tau + (x + y) = (z\sigma\alpha\tau + x) + y.$$

Both sides of (6) have the σ -component $(x+y)\sigma$, and their τ -components are equal, since we infer from (5) that

$$\begin{aligned} [z\sigma\alpha\tau + (x+y)]\tau &= z\sigma\alpha\tau + (x+y)\tau = [z\sigma\alpha + (x\tau + y\tau)]\tau \\ &= [(z\sigma\alpha + x\tau) + y\tau]\tau = (z\sigma\alpha\tau + x\tau) + y\tau \\ &= [(z\sigma\alpha\tau + x) + y]\tau. \end{aligned}$$

The other formulas assuring that $z\sigma\alpha\tau$ associates with every pair of elements x, y in L are proven in a fashion similar to the proof of (6). (3) assures that $z\sigma\alpha\tau$ commutes with every element in L , and thus it follows that $z\sigma\alpha\tau$ is a center element of L .

We may now make the induction hypothesis that $z\sigma\nu\tau$ is a center element of L whenever ν is the product of less than n decomposition endomorphisms. If δ is a decomposition endomorphism, then

$$z\sigma\nu\delta\tau = z\sigma\nu\sigma\delta\tau + z\sigma\nu\tau\delta\tau.$$

It is a consequence of the induction hypothesis that $z\sigma\nu\tau$ is a center element, and it follows from what we showed in the first part of the proof that $(z\sigma\nu)\sigma\delta\tau$ is a center element. We infer from Corollary 1 that $(z\sigma\nu\tau)\delta\tau$ is a center element, and thus $z\sigma\nu\delta\tau$ is a center element as a sum of center elements. This completes the induction proof of the fact that $z\sigma\eta\tau$ is a center element whenever σ, τ is a pair of complementary decomposition endomorphisms and η is a product of decomposition endomorphisms.

Now it follows from Corollary 1 that $L\gamma\sigma\eta\tau\kappa$ is an M -subloop of L which consists of center elements only; $\gamma\sigma\eta\tau\kappa$ is therefore a centralizing endomorphism of L .

Remark on Fitting's concept of normal endomorphisms. Fitting⁽⁸⁾ has introduced into the theory of associative groups a concept of normal endomorphism whose place will be taken in the present investigation by the class of centralizing endomorphisms characterized in Lemma 2 (see [4, splitting hypothesis]). The following remarks will indicate the relations between these concepts.

(1) According to Fitting's definition the following three classes are subclasses of the class of normal endomorphisms: the products of decomposition endomorphisms; the centralizing endomorphisms; the endomorphisms of the form $1-\eta$ for η a centralizing endomorphism. It is evident that the endomorphisms discussed in Lemma 2 form a common subclass of the first two of these classes so that this class is certainly much smaller than the class of normal endomorphisms.

(2) Fitting's definition of normal endomorphism involves the concept of inner automorphism. But it seems to be just this concept which provides most of the difficulties when attempting the step from group theory to loop theory.

⁽⁸⁾ Fitting [1, p. 19].

Thus it is not quite obvious how to define for loops the exact equivalent of the normal endomorphisms in the sense of Fitting⁽⁹⁾.

(3) Even the definition of normal endomorphism as a centralizing endomorphism which is a product of decomposition endomorphisms does not seem satisfactory, though this too would be a proper subclass of the class of normal endomorphisms in the sense of Fitting. For the endomorphisms, discussed in Lemma 2, are completely characterized by properties of the system of M -subloops of L . But the M -center, and hence the concept of centralizing endomorphism, cannot be defined in terms of this system, since it is well known that abelian groups and nonabelian groups may have essentially the same system of subgroups.

DEFINITION. *If A and B are M -subloops of the M -loop L , if ρ is an M -isomorphism of A upon B such that $x \equiv x\rho$ modulo $Z_M(L)$ and such that ρ and ρ^{-1} are induced by products of decomposition endomorphisms of L , then ρ is a center isomorphism, and A and B are center isomorphic M -subloops of L .*

This definition is narrower than the one usually adopted, insofar as we require that both ρ and ρ^{-1} are induced by products of decomposition endomorphisms. It should be noted that a "center isomorphism" need not be a "centralizing endomorphism," though there will be little danger of actual confusion of these two concepts.

COROLLARY 2. *If σ, σ' and τ, τ' are pairs of complementary decomposition endomorphisms of the M -loop L such that $L\sigma' = L\tau'$, then τ induces a center isomorphism of $L\sigma$ upon $L\tau$ such that*

$$x\tau = x + x\sigma\tau\sigma' \quad \text{for } x \text{ in } L\sigma.$$

Proof. From $L\tau'\sigma = L\sigma'\sigma = 0$ we infer $\tau'\sigma = 0$; $\sigma'\tau = 0$ is shown likewise. If x is an element in $L\sigma$, then

$$x\tau = x\tau\sigma + x\tau\sigma' = (x\tau\sigma + x\tau'\sigma) + x\tau\sigma' = x\sigma + x\tau\sigma' = x + x\sigma\tau\sigma',$$

since $x = x\sigma$; and likewise we prove for y in $L\tau$ that

$$y\sigma = y + y\tau\sigma\tau'.$$

If x is in $L\sigma$, then $x\tau\sigma = x\sigma + x\sigma\tau\sigma'\sigma = x$; and if y is in $L\tau$, then $y\sigma\tau = y\tau + y\tau\sigma\tau'\tau = y$. This implies that τ and σ induce reciprocal isomorphisms between $L\sigma$ and $L\tau$; and these are center isomorphisms, since $\sigma\tau\sigma'$ and $\tau\sigma\tau'$ are, by Lemma 2, centralizing endomorphisms.

3. Elementary exchange properties. The following simple proposition will be used continuously.

LEMMA 1. *If the M -loop $L = A \oplus B$, and if the M -subloop S contains A , then $S = A \oplus (S \cap B)$.*

⁽⁹⁾ A. A. Albert is in possession of a theory of a class of endomorphisms which is the exact analogue of the normal endomorphisms in the sense of Fitting.

The simple proof may be left to the reader.

LEMMA 2. *If the M -loop $L = D \oplus A(1) \oplus \cdots \oplus A(n) = D \oplus B$, then:*

- (a) $B(i) = [D \oplus A(i)] \cap B$ is a normal M -subloop of L which is center isomorphic to $A(i)$;
- (b) $D \oplus A(i) = D \oplus B(i)$;
- (c) $B = B(1) \oplus \cdots \oplus B(n)$.

Proof. (b) is an immediate consequence from Lemma 1 and (a) is readily deduced from (b) and §2, Corollary 2.

Denote by B' the compositum of the $B(i)$. This is clearly a normal M -subloop of L which is part of B so that in particular $D \cap B' = 0$. It follows from (b) that the compositum of D and B' is the same as the compositum of D and the $A(i)$; and thus we have shown that $L = D \oplus B'$. From $L = D \oplus B$, $B' \leq B$, and Lemma 1 we infer that $B = B'$; and thus we have shown that B is the compositum of the $B(i)$.

Denote by $B'(i)$ the compositum of the $B(j)$ for $j \neq i$. Then

$$B'(i) \cap B(i) \leq [D \oplus B'(i)] \cap [D \oplus B(i)] \cap B = 0,$$

since it follows from (b) that

$$D \oplus B'(i) = D \oplus A(1) \oplus \cdots \oplus A(i-1) \oplus A(i) \oplus \cdots \oplus A(n),$$

$$D \oplus B(i) = D \oplus A(i)$$

so that the cross cut of these two loops is just D . This completes the proof of (c).

LEMMA 3. *If α, β and ρ, σ are pairs of complementary decomposition endomorphisms of the M -loop L , and if $\alpha\rho\alpha$ induces an automorphism in $L\alpha$, then $L = L\alpha \oplus L\beta$.*

Proof. It is a consequence of §2, Corollary 1 that $L\alpha\rho$ is a normal M -subloop of L , since the decomposition endomorphism ρ maps the normal subloop $L\alpha$ upon a normal subloop.

If x belongs to the cross cut of $L\alpha\rho$ and $L\beta$, then there exists an element y such that $y = y\alpha$ and $x = y\alpha\rho$. Since x is in $L\beta$, we have $0 = x\alpha = y\alpha\rho\alpha$. But $\alpha\rho\alpha$ induces an automorphism in $L\alpha$ and y is in $L\alpha$. Hence $y = 0$; this implies $x = 0$ and therefore $L\alpha\rho \cap L\beta = 0$.

If x is an element in $L\alpha$, then $x = x\alpha$ and there exists an element y in $L\alpha$ such that $x = y\alpha\rho\alpha$. Then $y\alpha\rho = y\alpha\rho\alpha + y\alpha\rho\beta = x + y\alpha\rho\beta$. Since $y\alpha\rho$ is in $L\alpha\rho$ and $y\alpha\rho\beta$ is in $L\beta$, it follows that x is in the compositum $L\alpha\rho \oplus L\beta$. Thus we have shown that $L\alpha \leq L\alpha\rho \oplus L\beta$, proving $L = L\alpha\rho \oplus L\beta$.

COROLLARY 1. *The following properties of the pairs of complementary decomposition endomorphisms α, β and ρ, σ of the M -loop L imply each other.*

- (i) $L = L\rho \oplus L\beta = L\alpha \oplus L\sigma$.

- (ii) *An automorphism is induced by $\alpha\rho\alpha$ in $L\alpha$ and by $\rho\alpha\rho$ in $L\rho$.*
 (iii) *An automorphism is induced by $\beta\sigma\beta$ in $L\beta$ and by $\sigma\beta\sigma$ in $L\sigma$.*

Proof. Clearly it suffices to prove the equivalence of the properties (i) and (ii). If (ii) is valid, then we infer from Lemma 3 that $L = L\alpha\rho \oplus L\beta = L\rho\alpha \oplus L\sigma$. Furthermore $L\alpha\rho \leq L\rho = L\rho(\rho\alpha\rho) \leq L\alpha\rho$ or $L\rho = L\alpha\rho$; hence $L\rho\alpha = L\alpha\rho\alpha = L\alpha(\alpha\rho\alpha) = L\alpha$. Thus (i) is a consequence of (ii). Assume finally the validity of (i). Then it follows from §2, Corollary 2 that α induces an isomorphism of $L\rho$ upon $L\alpha$ and that ρ induces an isomorphism of $L\alpha$ upon $L\rho$; (ii) is an immediate consequence of these facts.

LEMMA 4. *If α, β is a pair of complementary decomposition endomorphisms of the M -loop L , and if the decomposition endomorphism ρ of L satisfies $L\rho \leq L\alpha$, $L\beta \leq K(\rho)$, then $\rho = \rho\alpha = \alpha\rho$.*

Proof. It is a consequence of the second hypothesis that α leaves invariant every element in $L\rho$, proving $\rho\alpha = \rho$; it is a consequence of the last hypothesis that $\beta\rho = 0$ so that $\rho = \alpha\rho + \beta\rho = \alpha\rho$.

COROLLARY 2. *If α, β and δ, ϵ are pairs of complementary decomposition endomorphisms of the M -loop L , if $L\alpha = U \oplus V$, and if $\alpha\delta\alpha$ induces an automorphism in U , then $L = U\delta \oplus V \oplus L\beta$.*

Proof. Since $L = L\alpha \oplus L\beta = U \oplus (V \oplus L\beta)$, there exist complementary decomposition endomorphisms ρ, σ such that $L\rho = U$, $L\sigma = V \oplus L\beta$. It follows from Lemma 4 that $\rho = \rho\alpha = \alpha\rho$. If x is an element in U , then $x\alpha\delta\alpha$ belongs to U and thus both x and $x\alpha\delta\alpha$ are left invariant by ρ . Hence $x\alpha\delta\alpha = x\rho\alpha\delta\alpha\rho = x\rho\delta\rho$ so that $\alpha\delta\alpha$ and $\rho\delta\rho$ induce the same automorphism in U . Hence we may deduce from Lemma 3 that

$$L = L\rho\delta \oplus L\sigma = U\delta \oplus V \oplus L\beta,$$

as we claimed.

4. The splitting hypothesis. The M -loops whose direct decomposition we are going to study will be required to satisfy the following fundamental condition.

SPLITTING HYPOTHESIS. *If δ, ϵ is a pair of complementary decomposition endomorphisms of the M -loop L , and if α is a decomposition endomorphism of L , then the endomorphism $\alpha\delta\alpha\epsilon\alpha$ of L possesses one and only complement.*

It is a consequence of §2, Lemma 2, that $\alpha\delta\alpha\epsilon\alpha$ is a centralizing endomorphism of L . The uniquely determined complement C of $\alpha\delta\alpha\epsilon\alpha$ is therefore part of the M -center of L , and we have $L = C \oplus R(\alpha\delta\alpha\epsilon\alpha)$. At the same time C is part of $L\alpha$; thus C is an abelian direct summand of L and $L\alpha$.

The criteria for the validity of the splitting hypothesis will be discussed in §8.

LEMMA 1. *If the splitting hypothesis is satisfied by the M -loop L , then it is satisfied by every direct summand of L .*

Proof. Suppose that $L = U \oplus V$, that δ, ϵ is a pair of complementary decomposition endomorphisms of U , and that α is a decomposition endomorphism of U . Then there exist uniquely determined decomposition endomorphisms α', δ' of L which coincide with α and δ respectively on U and which both map V upon 0; and there exists a uniquely determined decomposition endomorphism ϵ' of L which coincides with ϵ on U and which leaves invariant every element in V . Then δ', ϵ' are complementary decomposition endomorphisms of L , $\alpha'\delta'\alpha'\epsilon'\alpha'$ and $\alpha\delta\alpha\epsilon\alpha$ coincide on U and $\alpha'\delta'\alpha'\epsilon'\alpha'$ maps L into U . Thus complements of $\alpha'\delta'\alpha'\epsilon'\alpha'$ are part of U , proving that $\alpha\delta\alpha\epsilon\alpha$ and $\alpha'\delta'\alpha'\epsilon'\alpha'$ have the same complements. It follows from the splitting hypothesis that $\alpha'\delta'\alpha'\epsilon'\alpha'$ possesses one and only one complement. Hence $\alpha\delta\alpha\epsilon\alpha$ possesses one and only one complement, as we claimed.

The proof of the main consequence of the splitting hypothesis we precede by the proof of the following proposition which holds independently of the splitting hypothesis.

LEMMA 2. *If ρ and σ are M -endomorphisms of the M -loop L such that $x = x\rho + x\sigma$ for every x in L , then⁽¹⁰⁾:*

- (i) $\rho\sigma = \sigma\rho$;
- (ii) $R(\rho\sigma) = R(\rho) \oplus R(\sigma)$;
- (iii) *An automorphism is induced by ρ in $R(\sigma)$ and by σ in $R(\rho)$.*

Proof. If x is an element in L , then

$$x\rho^2 + x\sigma\rho = (x\rho + x\sigma)\rho = x\rho = x\rho^2 + x\rho\sigma \quad \text{or} \quad x\sigma\rho = x\rho\sigma,$$

proving (i). Next we are going to prove:

- (iv) $R(\rho)\sigma = R(\rho)$ and $R(\sigma)\rho = R(\sigma)$.

If x is an element in $R(\rho)$, then there exists an integer $i = i(x)$ such that $x\rho^i = 0$. Hence it follows from (i) that $x\sigma\rho^i = x\rho^i\sigma = 0$. Consequently $R(\rho)\sigma \leq R(\rho)$. Suppose conversely that x is in $R(\rho)$. Then $x\rho^i = 0$ is clearly in $R(\rho)\sigma$. Assume that we have already shown that $x\rho^j = 0$ for $0 < j \leq i$ is in $R(\rho)\sigma$. Then

$$x\rho^{i-1} = (x\rho^{i-1})\rho + (x\rho^{i-1})\sigma = x\rho^i + x\rho^{i-1}\sigma.$$

The first of these terms is in $R(\rho)\sigma$ because of the induction hypothesis; the second term is in $R(\rho)\sigma$, since $x\rho^{i-1}$ is in $R(\rho)$. Hence $x\rho^{i-1}$ is in $R(\rho)\sigma$; it now follows by complete induction that x itself is in $R(\rho)\sigma$. Consequently $R(\rho)\sigma = R(\rho)$; $R(\sigma)\rho = R(\sigma)$ is shown likewise.

If x is in the cross cut of $R(\rho)$ and $R(\sigma)$, then there exists a smallest not negative integer i such that $x\rho^i = x\sigma^i = 0$. If x were different from 0, then

⁽¹⁰⁾ This theorem may be considered as a generalization of such propositions as Fitting [1, p. 19, Hilfssatz 4] and Jacobson [1, p. 11, lemma].

$0 < i$, and we could infer that

$$x\rho^{i-1} = (x\rho^{i-1})\rho + (x\rho^{i-1})\sigma = x\rho^{i-1}\sigma;$$

from this equation and from (i) we would infer that $x\rho^{i-1} = x\rho^{i-1}\sigma^i = x\sigma^i\rho^{i-1} = 0$. Since $x\sigma^{i-1} = 0$ could be shown likewise, we have arrived at a contradiction, proving $x = 0$, or:

$$(v) \quad R(\rho) \cap R(\sigma) = 0.$$

Since $R(\rho)$ and $R(\sigma)$ are both normal subloops of L , it follows from (v) that their compositum is their direct sum $R(\rho) \oplus R(\sigma)$.

If x is in $R(\rho)$, then $x\rho^i = 0$ for some i ; it follows from (i) that $x(\rho\sigma)^i = x\rho^i\sigma^i = 0$, proving that $R(\rho) \leq R(\rho\sigma)$. Likewise we see that $R(\sigma) \leq R(\rho\sigma)$, proving that $R(\rho) \oplus R(\sigma) \leq R(\rho\sigma)$.

Since $K((\rho\sigma)^0) = K(1) = 0$ is certainly part of $R(\rho) \oplus R(\sigma)$, we may make the induction hypothesis that $K((\rho\sigma)^{i-1})$, for positive i , is part of $R(\rho) \oplus R(\sigma)$. If x is in $K((\rho\sigma)^i)$, then $x\rho\sigma$ is in $K((\rho\sigma)^{i-1})$; and we infer from the induction hypothesis the existence of elements x' and x'' in $R(\rho)$ and $R(\sigma)$ respectively such that $x\rho\sigma = x' + x''$. We infer from (iv) the existence of an element y in $R(\rho)$ such that $x' = y\sigma$; and there exists one and only one element z such that $x\rho = y + z$. Since x'' is in $R(\sigma)$, there exists a positive integer j such that $x''\sigma^j = 0$. Hence

$$y\sigma^{i+1} = x'\sigma^i = x'\sigma^i + x''\sigma^i = (x' + x'')\sigma^i = x\rho\sigma^{i+1} = y\sigma^{i+1} + z\sigma^{i+1}$$

or $z\sigma^{i+1} = 0$. Thus z belongs to $R(\sigma)$. Since y belongs to $R(\rho)$, we have shown that $x\rho = y + z$ belongs to $R(\rho) \oplus R(\sigma)$; likewise we see that $x\sigma$ is in $R(\rho) \oplus R(\sigma)$. Consequently $x = x\rho + x\sigma$ is in $R(\rho) \oplus R(\sigma)$, proving that $K((\rho\sigma)^i) \leq R(\rho) \oplus R(\sigma)$. Since $R(\rho\sigma)$ is the compositum of all the $K((\rho\sigma)^i)$, it follows that $R(\rho\sigma) \leq R(\rho) \oplus R(\sigma)$, completing the proof of (ii).

We infer from (ii) or (v) that $K(\rho) \cap R(\sigma) \leq R(\rho) \cap R(\sigma) = 0$. Hence we may deduce from (iv) that ρ induces an automorphism in $R(\sigma)$; that σ induces an automorphism in $R(\rho)$ is seen likewise, completing the proof.

LEMMA 3. *If α, β and δ, ϵ are pairs of complementary decomposition endomorphisms of the M -loop L , and if $\alpha\delta\alpha\epsilon\alpha$ possesses one and only complement C , then there exists one and only one direct decomposition $L\alpha = U \oplus V$ such that:*

$$(a) \quad V \leq R(\alpha\epsilon\alpha);$$

(b) *an automorphism is induced in U by $\alpha\epsilon\alpha$ and in V by $\alpha\delta\alpha$, and we have $U = C \oplus [L\alpha \cap R(\alpha\delta\alpha)]$, $V = L\alpha \cap R(\alpha\epsilon\alpha)$.*

Proof. A. We show first that $U = C \oplus [L\alpha \cap R(\alpha\delta\alpha)]$, $V = L\alpha \cap R(\alpha\epsilon\alpha)$ constitute a direct decomposition of $L\alpha$, satisfying (a) and (b).

It is clear that U and V are part of $L\alpha$ and that $V \leq R(\alpha\epsilon\alpha)$.

Since $\alpha\delta\alpha\epsilon\alpha$ is, by §2, Lemma 2, a centralizing endomorphism of L , its complement C is part of the M -center of L , and we have

$$L = R(\alpha\delta\alpha\epsilon\alpha) \oplus C.$$

Since $K(\alpha)$ is part of $R(\alpha\delta\alpha)$, $R(\alpha\epsilon\alpha)$ and $R(\alpha\delta\alpha\epsilon\alpha)$, and since $L = L\alpha \oplus K(\alpha)$, it follows from §3, Lemma 1 that

$$\begin{aligned} R(\alpha\delta\alpha) &= K(\alpha) \oplus [L\alpha \cap R(\alpha\delta\alpha)], \\ R(\alpha\epsilon\alpha) &= K(\alpha) \oplus [L\alpha \cap R(\alpha\epsilon\alpha)], \\ R(\alpha\delta\alpha\epsilon\alpha) &= K(\alpha) \oplus [L\alpha \cap R(\alpha\delta\alpha\epsilon\alpha)]; \end{aligned}$$

and we note furthermore the often used fact that the second term is always the radical of the endomorphism induced in $L\alpha$.

The identity is induced in $L\alpha$ by $\alpha = \alpha\delta\alpha + \alpha\epsilon\alpha$. Hence it follows from Lemma 2 and $L = K(\alpha) \oplus L\alpha$ that

$$\begin{aligned} (\alpha\delta\alpha)(\alpha\epsilon\alpha) &= (\alpha\epsilon\alpha)(\alpha\delta\alpha), \\ L\alpha \cap R(\alpha\delta\alpha\epsilon\alpha) &= [L\alpha \cap R(\alpha\delta\alpha)] \oplus [L\alpha \cap R(\alpha\epsilon\alpha)], \end{aligned}$$

and an automorphism is induced in $L\alpha \cap R(\alpha\delta\alpha)$ by $\alpha\epsilon\alpha$ and in $L\alpha \cap R(\alpha\epsilon\alpha)$ by $\alpha\delta\alpha$.

We infer first that

$$\begin{aligned} R(\alpha\delta\alpha\epsilon\alpha) &= K(\alpha) \oplus [L\alpha \cap R(\alpha\delta\alpha\epsilon\alpha)] \\ &= K(\alpha) \oplus [L\alpha \cap R(\alpha\delta\alpha)] \oplus [L\alpha \cap R(\alpha\epsilon\alpha)] \\ &= R(\alpha\delta\alpha) \oplus [L\alpha \cap R(\alpha\epsilon\alpha)] = [L\alpha \cap R(\alpha\delta\alpha)] \oplus R(\alpha\epsilon\alpha). \end{aligned}$$

Since $\alpha\delta\alpha$ maps $R(\alpha\delta\alpha)$ into itself and induces an automorphism in $L\alpha \cap R(\alpha\epsilon\alpha)$, it follows that $\alpha\delta\alpha$ induces an endomorphism in $R(\alpha\delta\alpha\epsilon\alpha)$; that $\alpha\epsilon\alpha$ induces an endomorphism in $R(\alpha\delta\alpha\epsilon\alpha)$ is seen likewise. Furthermore we have

$$L = R(\alpha\delta\alpha\epsilon\alpha) \oplus C = K(\alpha) \oplus [L\alpha \cap R(\alpha\delta\alpha)] \oplus [L\alpha \cap R(\alpha\epsilon\alpha)] \oplus C.$$

The three last summands are part of $L\alpha$, since $C = C\alpha\delta\alpha\epsilon\alpha$; hence it follows from $L = K(\alpha) \oplus L\alpha$ and §3, Lemma 1 that⁽¹¹⁾

$$L\alpha = C \oplus [L\alpha \cap R(\alpha\delta\alpha)] \oplus [L\alpha \cap R(\alpha\epsilon\alpha)] = U \oplus V,$$

and we note that $\alpha\delta\alpha$ induces an automorphism in V .

Suppose now that w is an element in C such that $w\alpha\epsilon\alpha$ is in $R(\alpha\delta\alpha\epsilon\alpha)$. Since $\alpha\delta\alpha$ has been shown to map $R(\alpha\delta\alpha\epsilon\alpha)$ into itself, it follows that $w(\alpha\epsilon\alpha)(\alpha\delta\alpha) = w(\alpha\delta\alpha)(\alpha\epsilon\alpha) = w\alpha\delta\alpha\epsilon\alpha$ is in $R(\alpha\delta\alpha\epsilon\alpha)$. Thus it follows from elementary properties of the radical that w itself is in $R(\alpha\delta\alpha\epsilon\alpha)$. Hence $w = 0$ as an element in $C \cap R(\alpha\delta\alpha\epsilon\alpha) = 0$. Consequently

$$C\alpha\epsilon\alpha \cap R(\alpha\delta\alpha\epsilon\alpha) = 0.$$

Since both $\alpha\delta\alpha$ and $\alpha\epsilon\alpha$ map $R(\alpha\delta\alpha\epsilon\alpha)$ into itself, they induce both endomor-

⁽¹¹⁾ Kořinek [1] and Kurosh [2, 3] have based their discussion on a three term decomposition of $L\alpha$ very similar to this one.

phisms in $L/R(\alpha\delta\alpha\epsilon\alpha)$. But their product $\alpha\delta\alpha\epsilon\alpha$ induces an automorphism in C and therefore in $L/R(\alpha\delta\alpha\epsilon\alpha)$. Hence each of the factors $\alpha\delta\alpha$ and $\alpha\epsilon\alpha$ induces an automorphism in $L/R(\alpha\delta\alpha\epsilon\alpha)$. This implies in particular that every coset of $L/R(\alpha\delta\alpha\epsilon\alpha)$ contains one (and only one) element in $C\alpha\epsilon\alpha$. Since finally

$$C\alpha\epsilon\alpha(\alpha\delta\alpha\epsilon\alpha) = C(\alpha\epsilon\alpha)(\alpha\delta\alpha)(\alpha\epsilon\alpha) = C(\alpha\delta\alpha\epsilon\alpha)(\alpha\epsilon\alpha) = C\alpha\epsilon\alpha,$$

we have shown that $C\alpha\epsilon\alpha$ is a complement of $\alpha\delta\alpha\epsilon\alpha$. But $\alpha\delta\alpha\epsilon\alpha$ possesses only one complement, proving that

$$C = C\alpha\epsilon\alpha$$

(and $C = C\alpha\delta\alpha$ may be shown likewise).

From $R(\alpha\epsilon\alpha) \leq R(\alpha\delta\alpha\epsilon\alpha)$ we infer now that $\alpha\epsilon\alpha$ induces an automorphism in C . Since $\alpha\epsilon\alpha$ induces an automorphism in $L\alpha \cap R(\alpha\delta\alpha)$, it follows that $\alpha\epsilon\alpha$ induces an automorphism in U ; thus we have shown that U and V meet all the requirements.

B. Consider now a direct decomposition $L\alpha = U' \oplus V'$, meeting the requirements (a) and (b). It follows from (a) that $V' \leq L\alpha \cap R(\alpha\epsilon\alpha) = V$; hence it follows from 3, Lemma 1 and $L\alpha = U' \oplus V'$ that $V = V' \oplus (U' \cap V)$. Since $\alpha\epsilon\alpha$ induces, by (b), an automorphism in U' and, by (a), a nil endomorphism in V , it follows that $U' \cap V = 0$ or $V = V'$.

Since $\alpha\epsilon\alpha$ induces an automorphism in U' , and since $\alpha = \alpha\delta\alpha + \alpha\epsilon\alpha$ leaves invariant every element in $U' \leq L\alpha$, it follows that $\alpha\delta\alpha$ maps U' into itself. If x is an element in $L\alpha \cap R(\alpha\delta\alpha) \leq L\alpha = U' \oplus V'$, then there exist elements u and v in U' and V' respectively such that $x = u + v$, and there exists an integer i such that

$$0 = x(\alpha\delta\alpha)^i = u(\alpha\delta\alpha)^i + v(\alpha\delta\alpha)^i.$$

Since $\alpha\delta\alpha$ has just been shown to map U' into itself, and since $\alpha\delta\alpha$ induces an automorphism in V' , the elements $u(\alpha\delta\alpha)^i$ and $v(\alpha\delta\alpha)^i$ belong to U' and V' respectively. Since $U' \cap V' = 0$, we have $0 = u(\alpha\delta\alpha)^i = v(\alpha\delta\alpha)^i$. Since $\alpha\delta\alpha$ induces an automorphism in V' , this implies $v = 0$ so that $x = u$ is in U' . Thus we have shown that $L\alpha \cap R(\alpha\delta\alpha) \leq U'$.

We have shown before that $L\alpha = [L\alpha \cap R(\alpha\delta\alpha)] \oplus [L\alpha \cap R(\alpha\epsilon\alpha)] \oplus C$. Hence we may infer from 3, Lemma 1, that

$$\begin{aligned} U' &= [L\alpha \cap R(\alpha\delta\alpha)] \oplus [U' \cap (C \oplus [L\alpha \cap R(\alpha\epsilon\alpha)])] \\ &= [L\alpha \cap R(\alpha\delta\alpha)] \oplus [U' \cap (C \oplus V)] \end{aligned}$$

and hence

$$\begin{aligned} L &= K(\alpha) \oplus L\alpha = K(\alpha) \oplus U' \oplus V' = K(\alpha) \oplus V \oplus U' \\ &= K(\alpha) \oplus [L\alpha \cap R(\alpha\epsilon\alpha)] \oplus [L\alpha \cap R(\alpha\delta\alpha)] \oplus [U' \cap (C \oplus V)] \\ &= R(\alpha\delta\alpha\epsilon\alpha) \oplus [U' \cap (C \oplus V)]. \end{aligned}$$

Since $\alpha\epsilon\alpha$ maps into itself V , U' , and C , it maps $U' \cap (C \oplus V)$ into itself; the same holds of $\alpha\delta\alpha$, since $\alpha = \alpha\delta\alpha + \alpha\epsilon\alpha$ leaves invariant each of the elements in $U' \cap (C \oplus V)$. Thus this subloop is mapped into itself by $\alpha\delta\alpha\epsilon\alpha$, and is consequently a complement of $\alpha\delta\alpha\epsilon\alpha$. However, $\alpha\delta\alpha\epsilon\alpha$ possesses but one complement, proving that $C = U' \cap (C \oplus V)$, and that therefore

$$U' = [L\alpha \cap R(\alpha\delta\alpha)] \oplus [U' \cap (C \oplus V)] = [L\alpha \cap R(\alpha\delta\alpha)] \oplus C = U,$$

completing the proof.

REMARK. It is clear that this lemma may be used whenever the splitting hypothesis is satisfied by the M -loop L under consideration. It may be of interest to note that this will be the only⁽¹²⁾ explicit use that we are going to make of the splitting hypothesis. Instead we shall only use the present lemma.

COROLLARY. *If the splitting hypothesis is satisfied by the M -loop L , if α , β and δ , ϵ are pairs of complementary decomposition endomorphisms of L , and if S is a direct summand of $L\alpha$ such that $\alpha\delta\alpha$ and (therefore) $\alpha\epsilon\alpha$ induce endomorphisms in S , then there exists a direct decomposition $S = U \oplus V$ such that:*

- (a) $V \leq R(\alpha\epsilon\alpha)$;
- (b) *An automorphism is induced by $\alpha\epsilon\alpha$ in U and by $\alpha\delta\alpha$ in V .*

Proof. $L\alpha = S \oplus T$, since S is a direct summand of $L\alpha$. Hence there exists one and only one decomposition endomorphism σ of L such that $L\sigma = S$ and $K(\sigma) = T \oplus K(\alpha)$. We infer from §3, Lemma 4, that $\alpha\sigma = \sigma\alpha = \sigma$. We infer from Lemma 3 the existence of one and only one direct decomposition $S = U \oplus V$ such that $V \leq R(\sigma\epsilon\sigma)$ and such that an automorphism is induced in U by $\sigma\epsilon\sigma$ and in V by $\sigma\delta\sigma$. If x is an element in S , then $x\alpha\epsilon\alpha$ and $x\alpha\delta\alpha$ are elements in S . Hence x , $x\alpha\delta\alpha$, and $x\alpha\epsilon\alpha$ are left invariant by σ ; thus it follows that $x\alpha\delta\alpha = x\sigma\alpha\delta\alpha\sigma = x\sigma\delta\sigma$ and $x\alpha\epsilon\alpha = x\sigma\alpha\epsilon\alpha\sigma = x\sigma\epsilon\sigma$. Hence (a) and (b) are satisfied by U and V , completing the proof.

5. The main theorems. The following proposition will prove useful.

LEMMA. *If α , β and δ , ϵ are pairs of decomposition endomorphisms of the M -loop L , and if the direct decompositions*

$$(d) \quad L\alpha = A' \oplus A'', \quad L\beta = B' \oplus B'', \quad L\delta = D' \oplus D'', \quad L\epsilon = E' \oplus E''$$

have the properties

- α induces an isomorphism of D' upon A' and of E'' upon A'' ,
- β induces an isomorphism of E' upon B' and of D'' upon B'' ,
- (i) δ induces an isomorphism of A' upon D' and of B'' upon D'' ,
- ϵ induces an isomorphism of B' upon E' and of A'' upon E''

then they satisfy the equations:

⁽¹²⁾ With the exception of the proof of 6, Theorem 2.

$$\begin{aligned}
 (e) \quad & L\alpha \oplus B' = L\alpha \oplus E', & L\alpha \oplus B'' = L\alpha \oplus D'', \\
 & L\beta \oplus A' = L\beta \oplus D', & L\beta \oplus A'' = L\beta \oplus E'', \\
 & L\delta \oplus E' = L\delta \oplus B', & L\delta \oplus E'' = L\delta \oplus A'', \\
 & L\epsilon \oplus D' = L\epsilon \oplus A', & L\epsilon \oplus D'' = L\epsilon \oplus B''.
 \end{aligned}$$

Proof. Since $\beta\epsilon\beta$ induces an automorphism in B' , it follows from §3, Corollary 2, that $L = L\alpha \oplus B'\epsilon \oplus B'' = L\alpha \oplus E' \oplus B''$; this implies in particular that $0 = L\alpha \cap E'$. It is clear that $E'\alpha \leq L\alpha \oplus E'$ and hence $B' = E'\beta \leq L\alpha \oplus E'$. Since an automorphism is induced in B'' by $\beta\delta\beta$, it follows from §3, Corollary 2, that $L = L\alpha \oplus B' \oplus B'' = L\alpha \oplus B' \oplus B''\delta = L\alpha \oplus B' \oplus D''$. Hence it follows from §3, Lemma 1 and $L\alpha \oplus B' \leq L\alpha \oplus E'$ that

$$L\alpha \oplus E' = (L\alpha \oplus B') \oplus [(L\alpha \oplus E') \cap D''].$$

If x is an element in $L\alpha \cap (E' \oplus D'')$, then $x\beta = 0$ and there exist elements y and z in E' and D'' respectively such that $x = y + z$. Hence $0 = y\beta + z\beta$ where $y\beta$ is in $E'\beta = B'$ and where $z\beta$ belongs to $D''\beta = B''$. Since $B' \cap B'' = 0$, it follows that $y\beta = z\beta = 0$. Hence y is in the cross cut of $L\alpha$ and E' and z is in the cross cut of $L\alpha$ and D'' , and both these cross cuts are 0. Thus $0 = y = z = x$, proving that $L\alpha \cap (E' \oplus D'') = 0$. The compositum of $L\alpha$ and E' , D'' is therefore their direct sum, implying that $D'' \cap (L\alpha \oplus E') = 0$. Hence $L\alpha \oplus B' = L\alpha \oplus E'$; the other equations (e) may be proven in a like fashion.

SPECIAL REFINEMENT THEOREM. *If the splitting hypothesis is satisfied by the M -loop L , and if $L = A \oplus B = D \oplus E$, then there exist direct decompositions*

$$A = A' \oplus A'', \quad B = B' \oplus B'', \quad D = D' \oplus D'', \quad E = E' \oplus E''$$

such that

$$\begin{aligned}
 A' \oplus B' &= B' \oplus D' = D' \oplus E' = E' \oplus A', \\
 A'' \oplus D'' &= D'' \oplus E'' = E'' \oplus B'' = B'' \oplus A''.
 \end{aligned}$$

Proof. Denote by α, β and δ, ϵ the pairs of complementary decomposition endomorphisms such that $L\alpha = A$, $L\beta = B$, $L\delta = D$ and $L\epsilon = E$. Then we infer from 4, Lemma 3, the existence of uniquely determined M -subloops A', A'' and D', D'' such that

$$\begin{aligned}
 A &= A' \oplus A'', & D &= D' \oplus D'', \\
 A'' &\leq R(\alpha\delta\alpha), & D'' &\leq R(\delta\alpha\delta),
 \end{aligned}$$

and an automorphism is induced in A' by $\alpha\delta\alpha$, in A'' by $\alpha\epsilon\alpha$, in D' by $\delta\alpha\delta$ and in D'' by $\delta\beta\delta$.

We define

$$B' = B \cap (D' \oplus E), \quad B'' = D''\beta, \quad E' = E \cap (A' \oplus B), \quad E'' = A''\epsilon.$$

Since $\delta\beta\delta$ induces an automorphism in D'' , and since $\alpha\epsilon\alpha$ induces an auto-

morphism in A'' , it follows from §3, Corollary 2, that

$$(1) \quad \begin{aligned} L &= A' \oplus A'' \oplus B = A' \oplus A''\epsilon \oplus B = A' \oplus E'' \oplus B \\ &= D' \oplus D'' \oplus E = D' \oplus D''\beta \oplus E = D' \oplus B'' \oplus E. \end{aligned}$$

Since $B'' \leq B$ and $E'' \leq E$, we deduce from (1) and §3, Lemma 1, that

$$B = B' \oplus B'', \quad E = E' \oplus E''.$$

Our first object is to prove that the decompositions of A , B , D , and E , thus obtained, satisfy the conditions (i) of the preceding lemma.

Since $\delta\beta\delta$ induces an automorphism in D'' , it is clear that β induces an isomorphism of D'' upon B'' and that δ induces an isomorphism of B'' upon D'' , and since $\alpha\epsilon\alpha$ induces an automorphism in A'' , an isomorphism of A'' upon E'' is induced by ϵ and an isomorphism of E'' upon A'' is induced by α .

Since $\alpha\delta\alpha$ induces an automorphism in A' , we infer from §3, Corollary 2, that $L = A' \oplus A'' \oplus B = A'\delta \oplus A'' \oplus B$. Since $A'\delta$ is thus a direct summand of L and part of D , we deduce from §3, Lemma 1, that

$$(2) \quad D = A'\delta \oplus [D \cap (A'' \oplus B)].$$

If x is an element in $A'\delta$ such that $x\delta\alpha\delta = 0$, then there exists an element y in A' such that $x = y\delta$ and such that $0 = y\delta(\delta\alpha\delta)$. This implies $0 = y(\delta\alpha\delta)\alpha = y\alpha\delta\alpha\delta\alpha = y(\alpha\delta\alpha)^2$. But $\alpha\delta\alpha$ induces an automorphism in A' , proving that $y = 0$. Hence $x = 0$ too. Furthermore $A'\delta(\delta\alpha\delta) = A'(\alpha\delta\alpha)\delta = A'\delta$, proving that

$$(2') \quad \delta\alpha\delta \text{ induces an automorphism in } A'\delta.$$

If x is an element in $D \cap (A'' \oplus B)$, then $x = x\delta$ and there exist elements u and v in A'' and in B respectively such that $x = u + v$. Hence $x\delta\alpha\delta = x\alpha\delta = (u + v)\alpha\delta = (u\alpha + v\alpha)\delta = u\delta$. Since u belongs to $A'' \leq R(\alpha\delta\alpha)$, there exists an integer i such that $u(\alpha\delta\alpha)^i = 0$. Consequently $x(\delta\alpha\delta)^{i+1} = u\delta(\delta\alpha\delta)^i = u(\alpha\delta\alpha)^i\delta = 0$, proving that x is in $R(\delta\alpha\delta)$ and that therefore

$$(2'') \quad D \cap (A'' \oplus B) \leq R(\delta\alpha\delta).$$

We infer from (2), (2'') and §3, Lemma 1, that

$$D \cap R(\delta\alpha\delta) = [D \cap (A'' \oplus B)] \oplus [D \cap R(\delta\alpha\delta) \cap A'\delta].$$

Since $\delta\alpha\delta$ induces a nil endomorphism in $R(\delta\alpha\delta)$ and, by (2'), an automorphism in $A'\delta$, it follows that $R(\delta\alpha\delta) \cap A'\delta = 0$. Hence $D \cap R(\delta\alpha\delta) = D \cap (A'' \oplus B)$; it follows from §4, Lemma 3 (or 2) that

$$(2''') \quad \text{an automorphism is induced in } D \cap (A'' \oplus B) \text{ by } \delta\beta\delta.$$

The decomposition (2) of D meets therefore the requirements which determined, by §4, Lemma 3, uniquely the decomposition $D = D' \oplus D''$. Thus it follows that

$$(3') \quad D' = A'\delta, \quad D'' = D \cap (A'' \oplus B);$$

and likewise we see that

$$(3'') \quad A' = D'\alpha, \quad A'' = A \cap (D'' \oplus E).$$

Since $\alpha\delta\alpha$ induces an automorphism in A' and $\delta\alpha\delta$ in D' , it follows from (3') and (3'') that α induces an isomorphism of D' upon A' and that δ induces an isomorphism of A' upon D' .

If x is an element in E' , then $x = x\epsilon$, $0 = x\delta$ and there exist elements y and z in A' and B respectively such that $x = y + z$. Hence $0 = y\delta + z\delta$, showing that $z\delta$ and $y\delta$ belong to $A'\delta = D'$, by (3'). Since $z = z\epsilon + z\delta$ belongs to B , we have shown that z belongs to $B \cap (E \oplus D')$. From $x\beta = y\beta + z\beta = z$ we infer now that $E'\beta \leq B' = B \cap (E \oplus D')$. If in particular $0 = x\beta = z$, then $x = y$ belongs to the cross cut of E and A' . Since $\alpha\delta\alpha$ induces an automorphism in A' , we infer now that $x\alpha\delta\alpha = x\delta\alpha = 0$ implies $x = 0$; and thus we have shown:

$$(4') \quad \beta \text{ induces an isomorphism of } E' \text{ into } B';$$

and one verifies likewise that

$$(4'') \quad \epsilon \text{ induces an isomorphism of } B' \text{ into } E'.$$

It follows in particular from (4') and (4'') that $\epsilon\beta\epsilon$ induces an isomorphism of E' into E' . Since ϵ leaves invariant every element in $E' \leq E$, and since $\epsilon = \epsilon\alpha\epsilon + \epsilon\beta\epsilon$, it follows that $\epsilon\alpha\epsilon$ too maps E' into itself. Since E' is a direct summand of E , we infer now from §4, corollary, the existence of a direct decomposition $E' = U \oplus V$ such that $V \leq R(\epsilon\beta\epsilon)$ and such that an automorphism is induced in U by $\epsilon\beta\epsilon$ and in V by $\epsilon\alpha\epsilon$. Thus $U = U\epsilon\beta\epsilon \leq E'\epsilon\beta\epsilon$, and it follows from §3, Lemma 1, that $E'\epsilon\beta\epsilon = U \oplus (V \cap E'\epsilon\beta\epsilon)$. But $\epsilon\beta\epsilon$ induces a nil endomorphism in V and an isomorphism in E' , and hence in $E'\epsilon\beta\epsilon \leq E'$. Hence $V \cap E'\epsilon\beta\epsilon = 0$ or $U = E'\epsilon\beta\epsilon$. An automorphism is therefore induced by $\epsilon\beta\epsilon$ in $E'\epsilon\beta\epsilon$. Since $\epsilon\beta\epsilon$ induces an isomorphism of E' upon $E'\epsilon\beta\epsilon \leq E'$, it follows now that $\epsilon\beta\epsilon$ induces an automorphism in E' . Now we deduce from (4') and (4'') that

$$E' = E'\epsilon\beta\epsilon = E'\beta\epsilon \leq B'\epsilon \leq E' \quad \text{or} \quad E' = B'\epsilon;$$

this shows in conjunction with (4'') that ϵ induces an isomorphism of B' upon E' . That β induces an isomorphism of E' upon B' may be shown likewise. This completes the proof of the fact that our decompositions of A , B , D , E meet the requirements (i) of the preceding lemma. Consequently they satisfy the equations (e) of that same lemma.

It follows from (e) that $P = B \oplus A' = B \oplus D'$ and $Q = E \oplus A' = E \oplus D'$. Then $B \cap P \cap Q = B \cap Q = B \cap (E \oplus D') = B'$ and $E \cap P \cap Q = E \cap P = E \cap (B \oplus A') = E'$. Since A' and D' are both direct summands of P and Q , we infer from §3, Lemma 1 that

$$\begin{aligned}
P \cap Q &= A' \oplus (B \cap P \cap Q) = A' \oplus B' \\
&= A' \oplus (E \cap P \cap Q) = A' \oplus E' \\
&= D' \oplus (B \cap P \cap Q) = D' \oplus B' \\
&= D' \oplus (E \cap P \cap Q) = D' \oplus E',
\end{aligned}$$

proving the first set of desired equations.

It follows from (e) that $H = B \oplus A'' = B \oplus E''$ and that $K = D \oplus A'' = D \oplus E''$. Then $D \cap H \cap K = D \cap H = D \cap (B \oplus A'') = D''$ by (3'). Since E'' and A'' are both direct summands of H and of K , it follows from §3, Lemma 1 that

$$\begin{aligned}
H \cap K &= A'' \oplus (H \cap K \cap D) = A'' \oplus D'' \\
&= E'' \oplus (H \cap K \cap D) = E'' \oplus D''.
\end{aligned}$$

It follows from (e) that $S = E \oplus D'' = E \oplus B''$ and that $T = A \oplus D'' = A \oplus B''$. Then $A \cap S \cap T = A \cap S = A \cap (E \oplus D'') = A''$ by (3''). Since B'' and D'' are direct summands of S and of T , it follows from §3, Lemma 1, that

$$\begin{aligned}
S \cap T &= B'' \oplus (A \cap S \cap T) = B'' \oplus A'' \\
&= D'' \oplus (A \cap S \cap T) = D'' \oplus A''.
\end{aligned}$$

Thus we have shown that $B'' \oplus A'' = A'' \oplus D'' = D'' \oplus E''$. It is clear that E'' and B'' are both contained in this M -subloop of L . Hence we infer from (e) that

$$E' \oplus (E'' \oplus D'') = E \oplus D'' = E \oplus B'' = E' \oplus (E'' \oplus B''),$$

and from $E'' \oplus B'' \leq E'' \oplus D''$ and §3, Lemma 1, that $E'' \oplus B'' = E'' \oplus D''$, completing the proof.

REMARK 1. If we let, in the notation of the theorem,

$$\begin{aligned}
L' &= A' \oplus B' = B' \oplus D' = D' \oplus E' = E' \oplus A', \\
L'' &= A'' \oplus D'' = D'' \oplus E'' = E'' \oplus B'' = B'' \oplus A'',
\end{aligned}$$

then $L = L' \oplus L''$; these decompositions constitute refinements of the original decomposition which meet an exchange requirement that is much stronger than all the other exchange conditions that we are going to discuss.

REMARK 2. It is an immediate consequence of §2, Corollary 2, that A' and D' , B' and E' , A'' and E'' , B'' and D'' are center isomorphic direct summands of L .

DEFINITION 1. The permutation: $i \rightarrow i^*$ of the integers from 1 to n effects an exchange isomorphism of the direct decomposition $L = A(1) \oplus \cdots \oplus A(n)$ upon the direct decomposition $L = B(1) \oplus \cdots \oplus B(n)$ of the M -loop L , if

$$(5.E) \quad L = A(1) \oplus \cdots \oplus A(i-1) \oplus B(i^*) \oplus A(i+1) \oplus \cdots \oplus A(n)$$

for every i .

The term "exchange isomorphism" ought to be used with some care, since products and inverses of exchange isomorphisms need not be exchange isomorphisms. Note the center isomorphism of $A(i)$ and $B(i^*)$.

GENERAL REFINEMENT THEOREM. *If the splitting hypothesis is satisfied by the M -loop L , then any two direct decompositions of L possess exchange isomorphic refinements.*

Here we term as usual the direct decomposition (U) of L a *refinement* of the direct decomposition (V) of L if every component of (V) is the direct sum of suitable components of (U) .

The general refinement theorem will be deduced from the special refinement theorem by purely structural arguments. It will be seen that the contention of the general refinement theorem is true whenever the contention of the special refinement theorem is valid for every direct summand.

The proof of our theorem will be effected by a double induction. In order to do so, it is necessary to prove a somewhat stronger theorem which will be useful in later applications, namely the following proposition.

(T. m, n) *If the splitting hypothesis is satisfied by the M -loop L if*

$$L = A(1) \oplus \cdots \oplus A(m) = B(1) \oplus \cdots \oplus B(n),$$

then there exist direct decompositions

$$A(i) = A(i, 1) \oplus \cdots \oplus A(i, n), \quad B(j) = B(j, 1) \oplus \cdots \oplus B(j, m)$$

such that L is, for every $i=1, \dots, m$ and for every set J of integers between 1 and n , the direct sum of the $A(k)$ for $k \neq i$, the $A(i, j)$ for j in J , and the $B(j, i)$ for j not in J .

(T. m, n) asserts the existence of an exchange isomorphism of the direct decomposition into the $A(i, j)$ upon the direct decomposition into the $B(j, i)$ which permits us to substitute (comparatively freely) $B(j, i)$ for $A(i, j)$.

Proof of (T. 2, n). Since (T. 2, 2) is nothing but a weaker form of the special refinement theorem, we may make the induction hypothesis that (T. 2, $n-1$) is valid in order to prove (T. 2, n).

Assume that $L = D \oplus E = A(1) \oplus \cdots \oplus A(n)$ and let $A = A(1) \oplus \cdots \oplus A(n-1)$, $B = A(n)$. Then $L = A \oplus B = D \oplus E$; we infer from the special refinement theorem the existence of direct decompositions

$$(1) \quad A = A' \oplus A'', \quad B = B' \oplus B'', \quad D = D' \oplus D'', \quad E = E' \oplus E''$$

such that

$$(2) \quad \begin{aligned} L' &= A' \oplus B' = B' \oplus D' = D' \oplus E' = E' \oplus A', \\ L'' &= A'' \oplus D'' = D'' \oplus E'' = E'' \oplus B'' = B'' \oplus A''. \end{aligned}$$

Clearly $L = L' \oplus L''$.

It is a consequence of §4, Lemma 1, that the splitting hypothesis is satisfied by every direct summand of the M -loop L . Thus we may apply (T.2, $n-1$) upon the direct decompositions $A = A' \oplus A'' = A(1) \oplus \cdots \oplus A(n-1)$ of the direct summand A of L . Consequently there exist direct decompositions $A(i) = A'(i) \oplus A''(i)$ for $i < n$, $A' = U(1) \oplus \cdots \oplus U(n-1)$, $A'' = V(1) \oplus \cdots \oplus V(n-1)$, meeting the following requirements:

(a') If J is a set of numbers between 1 and $n-1$, then A is the direct sum of A' , the $V(j)$ for j in J , and the $A''(j)$ for j not in J .

(a'') If J is a set of integers between 1 and $n-1$, then A is the direct sum of A'' , the $U(j)$ for j in J , and the $A'(j)$ for j not in J .

Let $D(i) = D' \cap (E' \oplus U(i))$ for $i < n$. Then it follows from $E' \oplus A' = E' \oplus D'$, $A' = U(1) \oplus \cdots \oplus U(n-1)$, and from 3, Lemma 2, that $D' = D(1) \oplus \cdots \oplus D(n-1)$ and $E' \oplus U(i) = E' \oplus D(i)$.

Likewise we let $E(i) = E'' \cap (D'' \oplus V(i))$ and find that $E'' = E(1) \oplus \cdots \oplus E(n-1)$ and $D'' \oplus V(i) = D'' \oplus E(i)$.

Finally we let $B' = A''(n)$, $B'' = A'(n)$, $D'' = D(n)$, $E' = E(n)$. Then we have $A(i) = A'(i) \oplus A''(i)$ for every $i = 1, \dots, n$ and $D = D(1) \oplus \cdots \oplus D(n)$, $E = E(1) \oplus \cdots \oplus E(n)$. In order to show that these direct decompositions meet all the requirements of (T.2, n) we have to show the validity of the following two contentions.

(d) If J is a set of integers between 1 and n , then L is the direct sum of D , the $E(j)$ for j in J , and the $A''(j)$ for j not in J .

(e) If J is a set of integers between 1 and n , then L is the direct sum of E , the $D(j)$ for j in J , and the $A'(j)$ for j not in J .

For reasons of symmetry it suffices to verify one of these properties, say (d). We distinguish two cases.

Case 1. n does belong to J .

Then we may assume without loss in generality that J consists of n and the integers $1, 2, \dots, i$ for some $i < n$. Then

$$\begin{aligned}
 L &= D \oplus E = D \oplus E(1) \oplus \cdots \oplus E(n) \\
 &= L' \oplus D'' \oplus E(1) \oplus \cdots \oplus E(n-1) \quad (\text{since } L' = D' \oplus E' = D' \oplus E(n)) \\
 &= L' \oplus D'' \oplus V(1) \oplus \cdots \oplus V(n-1) \quad (\text{since } D'' \oplus E(j) = D'' \oplus V(j) \\
 &\hspace{15em} \text{for } j < n) \\
 &= L' \oplus D'' \oplus V(1) \oplus \cdots \oplus V(i) \oplus A''(i+1) \oplus \cdots \oplus A''(n-1) \\
 &\hspace{15em} (\text{because of (a')} \text{ and } L' = A' \oplus B') \\
 &= L' \oplus D'' \oplus E(1) \oplus \cdots \oplus E(i) \oplus A''(i+1) \oplus \cdots \oplus A''(n-1) \\
 &\hspace{15em} (\text{as before}) \\
 &= D \oplus E(1) \oplus \cdots \oplus E(i) \oplus A''(i+1) \oplus \cdots \oplus A''(n-1) \oplus E(n),
 \end{aligned}$$

as we claimed.

Case 2. n does not belong to J . Then we may assume without loss in generality that J consists of the integers $1, 2, \dots, i$ for some $i < n$. From what we showed under Case 1 it follows that

$$\begin{aligned} L &= D \oplus E(1) \oplus \dots \oplus E(i) \oplus A''(i+1) \oplus \dots \oplus A''(n-1) \oplus E(n) \\ &= L' \oplus D'' \oplus E(1) \oplus \dots \oplus E(i) \oplus A''(i+1) \oplus \dots \oplus A''(n-1) \\ &= D' \oplus B' \oplus D'' \oplus E(1) \oplus \dots \oplus E(i) \oplus A''(i+1) \oplus \dots \oplus A''(n-1) \\ &= D \oplus E(1) \oplus \dots \oplus E(i) \oplus A''(i+1) \oplus \dots \oplus A''(n-1) \oplus A''(n), \end{aligned}$$

completing the verification of (d).

Thus (T.2, n) is a consequence of (T.2, $n-1$), completing the inductive proof of (T.2, n) for every n .

Proof of (T.m, n). Since we have already verified (T.2, n) for every n , we may make the induction hypothesis of the validity of (T.m-1, n) in order to prove (T.m, n).

Let $L = A(1) \oplus \dots \oplus A(m) = B(1) \oplus \dots \oplus B(n)$ and put $D = A(1) \oplus \dots \oplus A(m-1)$, $E = A(m)$. Applying (T.2, n) upon the direct decompositions $L = D \oplus E = B(1) \oplus \dots \oplus B(n)$ we obtain direct decompositions $B(i) = B'(i) \oplus B''(i)$, $D = D(1) \oplus \dots \oplus D(n)$, $E = E(1) \oplus \dots \oplus E(n)$, meeting the following requirements.

(d) If J is a set of integers between 1 and n , then L is the direct sum of D , the $E(j)$ for j in J , and the $B''(j)$ for j not in J .

(e) If J is a set of integers between L and n , then L is the direct sum of E , the $D(j)$ for j in J , and the $B'(j)$ for j not in J .

From (e) we infer in particular that

$$(f) \quad L = E \oplus B'(1) \oplus \dots \oplus B'(n),$$

and that is all we shall use of property (e).

Let $V(i) = D \cap (E \oplus B'(i))$. Then it follows from $L = E \oplus D$, (f) and §3, Lemma 2, that $D = V(1) \oplus \dots \oplus V(n)$, $E \oplus B'(i) = E \oplus V(i)$. Since D is a direct summand of L , the splitting hypothesis is satisfied by D . Thus we may apply the induction hypothesis (T.m-1, n) upon the direct decompositions

$$D = A(1) \oplus \dots \oplus A(m-1) = V(1) \oplus \dots \oplus V(n).$$

Consequently there exist direct decompositions

$$A(i) = A(i, 1) \oplus \dots \oplus A(i, n), \quad V(j) = V(j, 1) \oplus \dots \oplus V(j, m-1)$$

with the property:

(g) If $0 < i < m$, and if J is a set of integers between 1 and n , then D is the direct sum of the $A(j)$ for $j \neq i$, the $A(i, k)$ for k in J , and the $V(k, i)$ for k not in J .

Let $B(i, j) = B'(i) \cap (E \oplus V(i, j))$. Then we infer from §3, Lemma 2, $E \oplus B'(i) = E \oplus V(i)$ and $V(i) = V(i, 1) \oplus \dots \oplus V(i, m-1)$ that

$$B'(i) = B(i, 1) \oplus \cdots \oplus B(i, m-1), \quad E \oplus V(i, j) = E \oplus B(i, j).$$

Finally we let $B''(i) = B(i, m)$ and $E(i) = A(m, i)$. Then it is clear that

$$A(i) = A(i, 1) \oplus \cdots \oplus A(i, n), \quad B(j) = B(j, 1) \oplus \cdots \oplus B(j, m)$$

for $i=1, \dots, m$ and $j=1, \dots, n$. In order to show that these direct decompositions have the property enunciated in $(T.m, n)$, we distinguish two cases.

Case 1. $i < m$. We may assume without loss in generality that J is the set of integers $1, 2, \dots, k$ for some $k \leq n$, and that $i=1$. Then

$$\begin{aligned} L &= A(1) \oplus \cdots \oplus A(m) = A(1) \oplus \cdots \oplus A(m-1) \oplus E \\ &= A(1, 1) \oplus \cdots \oplus A(1, n) \oplus A(2) \oplus \cdots \oplus A(m-1) \oplus E \\ &= A(1, 1) \oplus \cdots \oplus A(1, k) \oplus V(k+1, 1) \oplus \cdots \oplus V(n, 1) \\ &\quad \oplus A(2) \oplus \cdots \oplus A(m-1) \oplus E \quad (\text{because of } (g)) \\ &= A(1, 1) \oplus \cdots \oplus A(1, k) \oplus B(k+1, 1) \oplus \cdots \oplus B(n, 1) \oplus E \\ &\quad \oplus A(2) \oplus \cdots \oplus A(m-1) \quad (\text{since } E \oplus V(j, 1) = E \oplus B(j, 1)) \\ &= A(1, 1) \oplus \cdots \oplus A(1, k) \oplus B(k+1, 1) \oplus \cdots \oplus B(n, 1) \\ &\quad \oplus A(2) \oplus \cdots \oplus A(m-1) \oplus A(m), \end{aligned}$$

as we claimed.

Case 2. $i=m$. Without loss in generality we may assume that J consists of the integers from 1 to k for some $k \leq n$. Then

$$\begin{aligned} L &= A(1) \oplus \cdots \oplus A(m) = D \oplus A(m) \\ &= D \oplus A(m, 1) \oplus \cdots \oplus A(m, n) = D \oplus E(1) \oplus \cdots \oplus E(n) \\ &= D \oplus E(1) \oplus \cdots \oplus E(k) \oplus B''(k+1) \oplus \cdots \oplus B''(n) \quad (\text{because of } (d)) \\ &= A(1) \oplus \cdots \oplus A(m-1) \oplus A(m, 1) \oplus \cdots \oplus A(m, k) \\ &\quad \oplus B(k+1, m) \oplus \cdots \oplus B(n, m), \end{aligned}$$

completing the proof of the fact that $(T.m, n)$ is a consequence of $(T.m-1; n)$. Thus $(T.m, n)$ is true for every m and n , as we claimed.

DEFINITION 2. The permutation $i \rightarrow i^*$ of the integers from 1 to n effects a center isomorphism of the direct decomposition $L = A(1) \oplus \cdots \oplus A(n)$ upon the direct decomposition $L = B(1) \oplus \cdots \oplus B(n)$ of the M -loop L , if $A(i)$ and $B(i^*)$ are center isomorphic⁽¹³⁾ M -subloops of L (for every i).

REMARK 1. It is readily seen that products and inverses of center isomorphisms between direct decompositions are again center isomorphisms. The relation of center isomorphism between direct decompositions is therefore symmetric and transitive.

REMARK 2. If a center isomorphism of the direct decomposition $L = A(1)$

⁽¹³⁾ In the sense of §2, definition.

$\oplus \cdots \oplus A(n)$ upon the direct decomposition $L = B(1) \oplus \cdots \oplus B(n)$ is effected by the permutation $i \rightarrow i^*$, then one easily constructs an M -automorphism α of L such that $A(i)\alpha = B(i^*)$ and $x \equiv x\alpha$ modulo $Z_M(L)$. Because of our rather restricted definition of center isomorphism of subloops the converse of this statement need not be true; see §2, definition.

REMARK 3. It is a fairly immediate consequence of §2, Corollary 2, that a permutation effects a center isomorphism of two direct decompositions whenever it effects an exchange isomorphism. It is important to note that the converse of this statement is not true, as may be seen from the following simple example. Denote by L the free abelian group of rank 2 and by u, v a basis of L . Denote by A, B, D, E the subgroups of L which are generated by $u, v, u+v$, and $2u+3v$ respectively. Then $L = A \oplus B = A \oplus D = B \oplus D = D \oplus E$, but L is different from $A \oplus E$ and $B \oplus E$. It is readily seen that $A \oplus B$ and $D \oplus B, D \oplus B$ and $D \oplus E$ are exchange isomorphic decompositions of L , but $A \oplus B$ and $D \oplus E$ are not exchange isomorphic, though clearly center isomorphic. Thus we have shown that exchange isomorphism is not transitive and that center isomorphism does not imply exchange isomorphism.

Applying the preceding remarks upon the general refinement theorem we find the following corollary.

COROLLARY. *If the splitting hypothesis is satisfied by the M -loop L , then any two direct decompositions of L possess center isomorphic refinements.*

6. Center indecomposable loops. A direct summand of an M -loop is abelian if, and only if, it is part of the M -center. This justifies the following terminology.

DEFINITION. *The M -loop L is center indecomposable, if 0 is its only abelian direct summand.*

Thus center indecomposable M -loops are not abelian, unless they are 0.

If η is a centralizing endomorphism of the center indecomposable M -loop L , then the complements of η are, by §1, Property (c), abelian direct summands of L . Thus η either does not split L or else 0 is its complement. This proves the equivalence of the following three properties of η :

- (a) η possesses one and only one complement;
- (b) η splits L ;
- (c) η is a nil endomorphism of L .

The splitting hypothesis should be considered and applied in the light of this remark.

Direct summands of center indecomposable M -loops are center indecomposable, since direct summands of direct summands are direct summands.

LEMMA 1. *If the splitting hypothesis is satisfied by the M -loop L , and if L is the direct sum of center indecomposable M -subloops, then L is center indecomposable.*

Proof. Suppose that L is the direct sum of the center indecomposable M -subloops $S(i)$, and that A is an abelian direct summand of L . Then it follows from the refinement theorems (§5, corollary) that A is the direct sum of M -subloops $A(i)$ such that $A(i)$ is isomorphic to a direct summand of $S(i)$. Since $A(i)$ is abelian, and since 0 is the only abelian direct summand of $S(i)$, we have $A(i) = 0$. Hence $A = 0$ as we claimed.

LEMMA 2. *If the M -loop $L = A \oplus B$ is center indecomposable, then 0 is the only direct summand of A which is center isomorphic to an M -subloop of B .*

Proof. Denote by α, β the pair of complementary decomposition endomorphisms of L such that $A = L\alpha$ and $B = L\beta$. Suppose that S is a direct summand of A , that ρ is a product of decomposition endomorphisms of L , and that ρ induces an isomorphism of S into B . Then $\alpha\rho\beta$ induces the same isomorphism of S into B as ρ . But it follows from 2, Lemma 2, that $\alpha\rho\beta$ is a centralizing endomorphism of L . Hence $S\rho = S\alpha\rho\beta$ is abelian. Since S and $S\rho$ are isomorphic, S is an abelian direct summand of the center indecomposable M -loop L . Thus $S = 0$, as we intended to show.

Remark. We proved a little more than we stated in Lemma 2, namely that 0 is the only direct summand of A which is mapped isomorphically into B by a product of decomposition endomorphisms.

THEOREM 1. *If the splitting hypothesis is satisfied by the center indecomposable M -loop L , and if an exchange isomorphism of the direct decomposition $L = A(1) \oplus \cdots \oplus A(n)$ upon the direct decomposition $L = B(1) \oplus \cdots \oplus B(n)$ is effected by the permutation $i \rightarrow i^*$, then this exchange isomorphism has the following property:*

(6.E) *If J is a set of integers between 1 and n , then L is the direct sum of the $B(j^*)$ for j in J and the $A(j)$ for j not in J .*

Proof. The contention (6.E) is certainly true whenever J consists of just one integer (see 5, Definition 1). Hence we may make the induction hypothesis that (6.E) is true whenever J consists of less than i integers. If J consists of i integers, then we may assume without loss in generality that J is the set of integers $1, 2, \dots, i$. Applying the induction hypothesis on the set of integers between 1 and $i-1$ we find

$$(1) \quad L = B(1^*) \oplus \cdots \oplus B((i-1)^*) \oplus A(i) \oplus A(i+1) \oplus \cdots \oplus A(n);$$

and applying the Property (5.E) (of 5, Definition 1) we find

$$(2) \quad L = A(1) \oplus \cdots \oplus A(i-1) \oplus B(i^*) \oplus A(i+1) \oplus \cdots \oplus A(n).$$

We apply the general refinement theorem (T.m, n) upon these two direct decompositions of L . Consequently there exist direct decompositions:

$$\begin{aligned} B(j^*) &= U(j, 1) \oplus \cdots \oplus U(j, n) & \text{for } j < i, \\ A(j) &= U(j, 1) \oplus \cdots \oplus U(j, n) & \text{for } i \leq j, \end{aligned}$$

and

$$\begin{aligned} A(j) &= V(j, 1) \oplus \cdots \oplus V(j, n) && \text{for } j \neq i, \\ B(i^*) &= V(i, 1) \oplus \cdots \oplus V(i, n); \end{aligned}$$

and an exchange isomorphism of the direct decomposition of L into the U 's upon the direct decomposition of L into the V 's is obtained by mapping $U(h, k)$ upon $V(k, h)$.

Applying §2, Corollary 2, we find that $A(i)$ and $B(i^*)$, $U(h, k)$ and $V(k, h)$ are center isomorphic. If $i \neq k$, then the direct summand $U(i, k)$ of $A(i)$ is center isomorphic to the direct summand $V(k, i)$ of $A(k)$; and it follows from Lemma 2 that

$$U(i, k) = V(k, i) = 0 \quad \text{for } i \neq k$$

and hence $A(i) = U(i, i)$. If $k < i$, then the direct summand $V(i, k)$ of $B(i^*)$ is center isomorphic to the direct summand $U(k, i)$ of $B(k^*)$ so that $V(i, k) = U(k, i) = 0$ by Lemma 2. If $i < k$, then the direct summand $V(i, k)$ of $B(i^*)$ is center isomorphic to the direct summand $U(k, i)$ of $A(k)$. Since $B(i^*)$ and $A(i)$ are center isomorphic, one verifies furthermore that $V(i, k)$ is center isomorphic to some direct summand of $A(i)$. The direct summand $U(k, i)$ of $A(k)$ is therefore center isomorphic to a direct summand of $A(i)$ for $i < k$, and it follows from Lemma 2 that $U(k, i)$, and, therefore, $V(i, k)$, is 0. Thus we have shown that

$$V(i, k) = 0 \quad \text{for } i \neq k$$

and hence $B(i^*) = V(i, i)$. Since $V(i, i)$ may be substituted for $U(i, i)$, it follows that

$$L = B(1^*) \oplus \cdots \oplus B((i-1)^*) \oplus B(i^*) \oplus A(i+1) \oplus \cdots \oplus A(n),$$

completing the proof of the induction and of the theorem.

THEOREM 2. *If $L = A(1) \oplus \cdots \oplus A(m) = B(1) \oplus \cdots \oplus B(n)$ are two direct decompositions of the center indecomposable M -loop L , and L satisfies the splitting hypothesis, then there exist uniquely determined direct decompositions*

$$A(i) = A(i, 1) \oplus \cdots \oplus A(i, n), \quad B(j) = B(j, 1) \oplus \cdots \oplus B(j, m)$$

such that

$$\begin{aligned} (6.F) \quad A(i, j) &= A(i) \cap \left[\sum_{k \neq i} A(k) \oplus B(j, i) \right], \\ B(j, i) &= B(j) \cap \left[\sum_{k \neq j} B(k) \oplus A(i, j) \right]. \end{aligned}$$

Remark. It should be noted that the conditions (6.F) imply the following facts:

$$\begin{aligned}
 (1) \quad & \sum_{k \neq i} A(k) \cap B(j, i) = 0, \quad \sum_{k \neq j} B(k) \cap A(i, j) = 0; \\
 & \sum_{k \neq i} A(k) \oplus B(j, i) = \sum_{k \neq i} A(k) \oplus A(i, j), \\
 (2) \quad & \sum_{k \neq j} B(k) \oplus A(i, j) = \sum_{k \neq j} B(k) \oplus B(j, i).
 \end{aligned}$$

These equations (2) are consequences of §3, Lemma 2.

(3) An exchange isomorphism of the decomposition into the $A(i, j)$ upon the decomposition into the $B(j, i)$ is obtained by mapping $A(i, j)$ upon $B(j, i)$ (and conversely), as follows from (2). Thus these direct decompositions are exchange isomorphic refinements of the original decompositions (A) and (B) .

Proof. Denote by $\alpha(i)$, $\alpha'(i)$ and $\beta(i)$, $\beta'(i)$ the pairs of complementary decomposition endomorphisms of L which satisfy:

$$\begin{aligned}
 L\alpha(i) &= A(i), & L\alpha'(i) &= \sum_{k \neq i} A(k) = A'(i), \\
 L\beta(i) &= B(i), & L\beta'(i) &= \sum_{k \neq i} B(k) = B'(i).
 \end{aligned}$$

Then $\alpha'(i) = \sum_{k \neq i} \alpha(k)$ and $\beta'(i) = \sum_{k \neq i} \beta(k)$. Furthermore we define:

$$\begin{aligned}
 U(i, j) &= A(i) \cap R(\alpha(i)\beta'(j)\alpha(i)), & U'(i, j) &= A(i) \cap R(\alpha(i)\beta(j)\alpha(i)), \\
 V(j, i) &= B(j) \cap R(\beta(j)\alpha'(i)\beta(j)), & V'(j, i) &= B(j) \cap R(\beta(j)\alpha(i)\beta(j)).
 \end{aligned}$$

These M -subloops have a number of properties. It will usually suffice to state the one concerning the U 's.

- (a.1) $A(i) = U(i, j) \oplus U'(i, j)$;
- (a.2) $\alpha(i)\beta(j)\alpha(i)\beta'(j)\alpha(i) = \alpha(i)\beta'(j)\alpha(i)\beta(j)\alpha(i)$ is a nil endomorphism;
- (a.3) an automorphism is induced in $U(i, j)$ by $\alpha(i)\beta(j)\alpha(i)$ and in $U'(i, j)$ by $\alpha(i)\beta'(j)\alpha(i)$.

It is a consequence of the splitting hypothesis that $\alpha(i)\beta(j)\alpha(i)\beta'(j)\alpha(i)$ is a nil endomorphism so that in particular $A(i) = A(i) \cap R(\alpha(i)\beta(j)\alpha(i)\beta'(j)\alpha(i))$. Since the identity is induced in $A(i) = L\alpha(i)$ by $\alpha(i) = \alpha(i)\beta(j)\alpha(i) + \alpha(i)\beta'(j)\alpha(i)$, contentions (a) may be deduced from §4, Lemma 2.

(b) If an automorphism is induced in the M -subloop S of L by $\alpha(i)\beta(j)\alpha(i)$, then $S \leq U(i, j)$.

It follows from our hypothesis that $S \leq L\alpha(i)$ and that therefore $\alpha(i)\beta'(j)\alpha(i)$ induces an endomorphism in S . There exists, by (a.2), to every element s in S an integer $k = k(s)$ such that

$$0 = s[\alpha(i)\beta(j)\alpha(i)\beta'(j)\alpha(i)]^k = s[\alpha(i)\beta'(j)\alpha(i)]^k[\alpha(i)\beta(j)\alpha(i)]^k.$$

Since $s[\alpha(i)\beta'(j)\alpha(i)]^k$ is in S , and since an automorphism is induced in S by $[\alpha(i)\beta(j)\alpha(i)]^k$, it follows that $0 = s[\alpha(i)\beta'(j)\alpha(i)]^k$, proving $S \leq U(i, j)$.

(c) if $A(i) = A(i, 1) \oplus \dots \oplus A(i, n)$, $B(j) = B(j, 1) \oplus \dots \oplus B(j, m)$, and if an exchange isomorphism is effected by mapping $A(i, j)$ upon $B(j, i)$, then

$$A(i) = U(i, j) \oplus \sum_{k \neq j} A(i, k) = A(i, j) \oplus U'(i, j).$$

Let $D = \sum_{k \neq j} A(i, k)$. Then it follows from Theorem 1 that L is the direct sum of the $A(k)$ for $k \neq i$, $A(i, j)$ and the $B(k, i)$ for $k \neq j$. Thus D is by §2, Corollary 2, center isomorphic to $D^* = \sum_{k \neq j} B(k, i)$. Likewise we see the center isomorphism of $A(i, j)$ and $B(j, i)$.

Let $A = U'(i, j)$, $B = U(i, j)$ and $E = A(i, j)$. Then it follows from (a.1) that $A(i) = A \oplus B = D \oplus E$. The splitting hypothesis is satisfied by $A(i)$, since $A(i)$ is a direct summand of L . Hence we infer from the special refinement theorem the existence of decompositions

$$(c') \quad A = A' \oplus A'', \quad B = B' \oplus B'', \quad D = D' \oplus D'', \quad E = E' \oplus E''$$

such that

$$(c'') \quad \begin{aligned} A' \oplus B' &= B' \oplus D' = D' \oplus E' = E' \oplus A', \\ A'' \oplus D'' &= D'' \oplus E'' = E'' \oplus B'' = B'' \oplus A''. \end{aligned}$$

It follows from (c'') and §2, Corollary 2, that A'' and E'' , B'' and D'' are center isomorphic. The direct summand E'' of $A(i, j)$ is center isomorphic to a direct summand of $B(j, i)$ and therefore to a direct summand of $B(j)$. It follows from (a.3) that an isomorphism is induced in A by $\beta'(j)$; and $\beta'(j)$ induces therefore an isomorphism of A'' into $B'(j)$. We deduce from Lemma 2 (and the remark appended to it) that A'' and E'' are 0. We noted that D is center isomorphic to D^* and D^* is a direct summand of $B'(j)$. Hence D'' is center isomorphic to a direct summand of $B'(j)$. It follows from (a.3) that an isomorphism is induced in B by $\beta(j)$; and $\beta(j)$ induces therefore an isomorphism of B'' into $B(j)$. Since B'' and D'' are center isomorphic, it follows, as before, that B'' and D'' are 0. Now it follows from the equations (c') and (c'') that

$$A \oplus B = B \oplus D = D \oplus E = E \oplus A,$$

proving (c).

(d) *If the decomposition of $A(i)$ into the $A(i, j)$ and of $B(j)$ into the $B(j, i)$ meet the requirements (6.F), then $A(i, j) = U(i, j)$ and $B(j, i) = V(j, i)$.*

Once we have proved this contention (d), we have verified the uniqueness claim of our theorem.

It is readily deduced from (6.F) that $\alpha(i)$ induces an isomorphism of $B(j, i)$ upon $A(i, j)$, and that $\beta(j)$ induces an isomorphism of $A(i, j)$ upon $B(j, i)$. Thus an automorphism is induced in $A(i, j)$ by $\alpha(i)\beta(j)\alpha(i)$; and hence it follows from (b) that $A(i, j) \leq U(i, j)$. It follows from (a.1) and (c) that $U(i, j) \oplus U'(i, j) = A(i, j) \oplus U'(i, j)$. Hence it follows from §3, Lemma 1, that $A(i, j) = U(i, j)$; $B(j, i) = V(j, i)$ is shown likewise.

(e) $U(i, j)\beta(j) = V(j, i)$ and $V(j, i)\alpha(i) = U(i, j)$.

From (a.3)—and a like statement referring to the V 's—we infer that an automorphism is induced in $U(i, j)$ by $\alpha(i)\beta(j)\alpha(i)$ and in $V(j, i)$ by $\alpha(j)\beta(i)\alpha(j)$. Now one deduces readily that an automorphism is induced in

$U(i, j)\beta(j)$ by $\beta(j)\alpha(i)\beta(j)$ and in $V(j, i)\alpha(i)$ by $\alpha(i)\beta(j)\alpha(i)$. We infer from (b)—and a like statement concerning the V 's—that $U(i, j)\beta(j) \leq V(j, i)$ and $V(j, i)\alpha(i) \leq U(i, j)$; the equations (e) are now readily deduced from (a.3).

(f) *If the $A(i, j)$ and $B(j, i)$ meet the requirements of (c), then L is the direct sum of $A'(i)$, $V(j, i)$ and $\sum_{k \neq j} A(i, k)$.*

It is a consequence of (c) that L is the direct sum of $A'(i)$, $U(i, j)$ and $\sum_{k \neq j} A(i, k)$. Hence it follows from (a.3) and 3, Corollary 2, that L is the direct sum of $A'(i)$, $\sum_{k \neq j} A(i, k)$, and $U(i, j)\beta(j) = V(j, i)$, by (e), as we claimed.

It is a consequence of §5, (T.m, n) that there exist $A(i, j)$ and $B(j, i)$, meeting the requirements of (c). Consequently we may choose decompositions $A(i, j)$ and $B(j, i)$ which meet the requirements of (c) and which have the additional property that as many of the $A(i, j)$ and $B(j, i)$ as possible are equal to $U(i, j)$ and $V(j, i)$ respectively. Then one infers easily from (c) and (f) that each $A(i, j) = U(i, j)$ and each $B(j, i) = V(j, i)$; and one infers from (e) and (a.3) that these decompositions meet the requirement (6.F), completing the proof.

7. Center indecomposable direct decompositions. If there is given a direct decomposition of the M -loop L into components which are either abelian or center indecomposable (in the sense of the preceding section), then we may form the direct sum A of the abelian components and the direct sum J of the center indecomposable components. Then $L = A \oplus J$, A is abelian, and, if we assume the validity of the splitting hypothesis, J is center indecomposable (by §6, Lemma 1). That such a decomposition is essentially unique may be seen from the following proposition.

LEMMA 1. *If the splitting hypothesis is satisfied by the M -loop L , if $L = A \oplus B = D \oplus E$ where A and D are abelian and where B and E are center indecomposable, then $L = A \oplus E = D \oplus B$.*

Proof. We infer from the special refinement theorem (§5) the existence of decompositions

$$A = A' \oplus A'', \quad B = B' \oplus B'', \quad D = D' \oplus D'', \quad E = E' \oplus E''$$

such that

$$\begin{aligned} A' \oplus B' &= B' \oplus D' = D' \oplus E' = E' \oplus A', \\ A'' \oplus D'' &= D'' \oplus E'' = E'' \oplus B'' = B'' \oplus A''. \end{aligned}$$

This implies in particular that A'' and E'' , B'' and D'' are center isomorphic. But A'' and D'' are abelian whereas E'' and B'' are direct summands of center indecomposable loops. Hence $A'' = D'' = E'' = B'' = 0$, and now our contention is an immediate consequence of the preceding equations.

DEFINITION. *The direct decomposition $L = A(1) \oplus \cdots \oplus A(n)$ is center in-*

decomposable, if none of the $A(i)$ possesses an abelian direct summand which is different from 0 and $A(i)$.

The components of a center indecomposable direct decomposition are therefore either abelian and indecomposable or center indecomposable (in the sense of §6, definition).

One verifies readily that every direct decomposition of the M -loop L possesses a center indecomposable refinement whenever the descending or the ascending chain condition is satisfied by the M -subgroups of the M -center of L . Even weaker conditions, like the ascending chain condition for abelian direct summands, suffice. Somewhat deeper is the following criterion.

LEMMA 2. *If the splitting hypothesis is satisfied by the M -loop L , and if there exists a center indecomposable direct decomposition of L , then every direct decomposition of L possesses center indecomposable refinements.*

Proof. Suppose that (A) is a center indecomposable direct decomposition of L and that (B) is some direct decomposition of L . There exist by §5, corollary, center isomorphic refinements (A') and (B') of (A) and (B) respectively. (A') is center indecomposable as a refinement of a center indecomposable direct decomposition. Hence (B') is center indecomposable, since its components are isomorphic to the components of (A') .

Lemma 2 and the preceding remarks may serve as a justification for restricting our considerations to center indecomposable direct decompositions.

THEOREM 1. *Suppose that the splitting hypothesis is satisfied by the M -loop L . Then center indecomposable direct decompositions of L are exchange isomorphic if, and only if, they are center isomorphic.*

Proof. The necessity of our condition is a consequence of §2, Corollary 2. Suppose now that $L = A(1) \oplus \cdots \oplus A(n) = B(1) \oplus \cdots \oplus B(n)$ are center isomorphic and center indecomposable direct decompositions. We may assume without loss in generality that:

- (i) $A(i)$ and $B(i)$ are center isomorphic for every i ;
- (ii) $A(i)$ and $B(i)$ are abelian for $i \leq m$ and are not abelian for $m < i$ where $0 \leq m \leq n$.

We infer from §5, (T. n , n), the existence of decompositions

$$A(i) = A(i, 1) \oplus \cdots \oplus A(i, n), \quad B(j) = B(j, 1) \oplus \cdots \oplus B(j, n)$$

such that an exchange isomorphism is effected by mapping $A(i, j)$ upon $B(j, i)$. Thus $A(i, j)$ and $B(j, i)$ are center isomorphic.

If $i \leq m$, then $A(i)$ is abelian and therefore indecomposable. Hence there exists—assuming that $A(i) \neq 0$ —one and only one integer i' such that $A(i, j) = 0$ for $j \neq i'$, $A(i) = A(i, i')$. Since $A(i)$ is abelian, since $A(i, i')$ is center isomorphic to the direct summand $B(i', i)$ of $B(i')$, and since $B(j)$ for

$m < j$ does not possess abelian direct summands not equal to 0, it follows that $i' \leq m$. Hence $B(i')$ is abelian and indecomposable, proving that $B(i') = B(i', i)$ and $B(i', j) = 0$ for $j \neq i'$. One verifies now readily that:

$i \rightarrow i'$ is a permutation of the integers from 1 to m such that $A(i) = A(i, i')$ and $B(i') = B(i', i)$.

If $m < i$ and $j \leq m$, then $A(i, j)$ is center isomorphic to the direct summand $B(j, i)$ of the abelian $B(j)$. But $A(i, j)$ is a direct summand of the center indecomposable $A(i)$ whose only abelian direct summand is 0. Thus $A(i, j) = 0$. Likewise we see that $B(i, j) = 0$, if $m < i$ and $j \leq m$.

Suppose now that $m < i$, $m < j$ and $i \neq j$. Then $A(i, j)$ is center isomorphic to the direct summand $B(j, i)$ of $B(j)$. But $B(j)$ is, by (i), center isomorphic to $A(j)$; and thus we have shown that the direct summand $A(i, j)$ of $A(i)$ is center isomorphic to a direct summand of $A(j)$.

It is a consequence of §6, Lemma 1 and (ii), that $A(m+1) \oplus \cdots \oplus A(n)$ is center indecomposable. Hence it follows from §6, Lemma 2, that 0 is the only direct summand of $A(i)$ for $m < i$ which is center isomorphic to a direct summand of $A(j)$ for $m < j \neq i$. Thus we have shown that

$$A(i, j) = 0 \quad \text{for } m < i \neq j;$$

and this implies that

$$B(i, j) = 0 \quad \text{for } m < i \neq j,$$

since $B(i, j)$ and $A(j, i)$ are center isomorphic. It follows now that

$$A(i) = A(i, i) \quad \text{and} \quad B(i) = B(i, i) \quad \text{for } m < i.$$

Thus we have shown that the exchange isomorphic refinements $A(i, j)$ and $B(j, i)$ of (A) and (B) are actually identical with the original decompositions, proving their exchange isomorphy as we claimed.

Remark. The importance of this theorem stems from the fact that center isomorphy of direct decompositions is a symmetric and transitive relation whereas a like claim cannot be made, in general, for exchange isomorphy; see §5, Remark 3.

THEOREM 2. *If the splitting hypothesis is satisfied by the M -loop L , and if the center indecomposable direct decompositions $L = A(1) \oplus \cdots \oplus A(n) = B(1) \oplus \cdots \oplus B(n)$ are center isomorphic, then there exists to every permutation ρ of the integers from 1 to n a permutation σ of the integers from 1 to n such that*

$$(7.E) \quad L = B(1^\sigma) \oplus \cdots \oplus B(i^\sigma) \oplus A((i+1)^\rho) \oplus \cdots \oplus A(n^\rho)$$

for every i .

Remark. This exchange property (7.E) is weaker than (6.E), but stronger than (5.E).

Proof. We are going to prove by complete induction with respect to i the

validity of the following proposition.

($\rho.i$) *There exist integers $1'$ to i' between 1 and n such that*

$$(\rho.i, j) \quad L = B(1') \oplus \cdots \oplus B(j') \oplus A((j+1)^\rho) \oplus \cdots \oplus A(n^\rho)$$

for $j \leq i$.

Since ($\rho.0$) is trivially true, we may make the induction hypothesis of the validity of ($\rho.i$) in order to prove ($\rho.i+1$). It is a consequence of §2, Corollary 2, that the direct decompositions ($\rho.i, j$) and ($\rho.i, j-1$) are center isomorphic. Hence it follows from the transitivity of center isomorphy that the direct decomposition ($\rho.i, i$) is center isomorphic to the direct decomposition $L = A(1) \oplus \cdots \oplus A(n)$ and therefore to the direct decomposition $L = B(1) \oplus \cdots \oplus B(n)$. We infer from Theorem 1 that the direct decomposition ($\rho.i, i$) is exchange isomorphic to the direct decomposition (B); and hence there exists an integer $(i+1)'$ such that

$$L = B(1') \oplus \cdots \oplus B(i') \oplus B((i+1)') \oplus A((i+2)^\rho) \oplus \cdots \oplus A(n^\rho);$$

and now it is easy to verify the validity of ($\rho.i+1$).

Thus we have in particular ($\rho.n$). Consider the direct decomposition ($\rho.n, n$). It shows that the mapping: $i \rightarrow i'$ is necessarily a permutation of the integers from 1 to n , completing the proof.

THEOREM 3. *If the splitting hypothesis is satisfied by the M -loop L , then any two direct decompositions of L into indecomposable direct summands are exchange isomorphic and meet requirement (7.E)⁽¹⁴⁾.*

This is an almost immediate consequence of the general refinement theorem and of Theorem 2.

Remark. This Theorem 3 invites comparison with the main theorem of Ore [1]; see his Theorem 18 on p. 591. In this theorem he makes the hypothesis that certain "regular decompositions" do exist. It is not difficult to see that this condition may be restated as follows: if α and β are decomposition endomorphisms such that $L\alpha$ and $L\beta$ are indecomposable, then there exist integers n and m such that $L = L(\alpha\beta)^m \oplus K((\alpha\beta)^n)$. It appears that this condition is a kind of splitting hypothesis, though stronger than the one used by us. The main advantage of our splitting hypothesis seems to be that it refers to centralizing endomorphisms only and that we do not have to assume the existence of decompositions into indecomposable direct summands. See also §8, Remark 1.

It should be noted that the results of the present section would remain valid if we substituted for the splitting hypothesis everywhere the assumption that the contentions of the refinement theorems are valid.

As in §6 it would be possible to attain our ends with a slightly weakened

⁽¹⁴⁾ The contention of this theorem is exactly the same as is found in the presentations of group theory; see Jacobson [1, p. 12, Theorem 11] or Zassenhaus [1, p. 79, Satz 7 (c)].

form of our splitting hypothesis. Remember that this hypothesis asserts the existence of *one and only one* complement to every endomorphism of the form $\alpha\delta\alpha\epsilon\alpha$ where δ, ϵ is a pair of complementary decomposition endomorphisms and where α is a decomposition endomorphism. To prove the refinement theorems for center indecomposable direct decompositions we would have to apply this hypothesis only in case $L\alpha$ is either abelian and indecomposable or not abelian and center indecomposable. The existence of a complement to $\alpha\delta\alpha\epsilon\alpha$ assures that either $L\alpha$ is abelian and $\alpha\delta\alpha\epsilon\alpha$ induces an automorphism in $L\alpha$ or else $\alpha\delta\alpha\epsilon\alpha$ is a nil endomorphism; in either case the uniqueness of the complement is a consequence of its existence.

8. Application of splitting criteria to refinement theorems. Every criterion assuring the existence of one and only one complement to every centralizing endomorphism will lead us automatically to a decomposition theorem by applying this criterion to the refinement theorems of §5 (or to the results of §§6 and 7), since these criteria imply the validity of the splitting hypothesis. We are going to use criteria derived elsewhere (Baer [4]); all these criteria assure what we termed "uniform splitting" and this implies the existence of one and only one complement.

Centralizing endomorphisms map L upon M -subgroups of $Z_M(L)$. The following three properties of an M -subgroup S of $Z_M(L)$ are easily seen to be equivalent.

- (i) *There exists a centralizing endomorphism η of L such that $S = L\eta$*
- (ii) *S is an M -homomorphic image of L .*
- (iii) *S is an M -homomorphic image of L_A .*

Here L_A signifies the M -loop L made abelian, that is, $L_A = L/G$ where G is the "commutator associator subloop"⁽¹⁵⁾ of L , that is, the uniquely determined smallest normal M -subloop of L modulo which L is abelian.

DEFINITION 1. *The M -subgroup S of $Z_M(L)$ is an L - M -subgroup if it satisfies the above properties (i) to (iii).*

For shortness sake we shall state all the following results in the form: "The splitting hypothesis is satisfied, if" The reader ought to remember that the validity of the splitting hypothesis assures the validity of the contentions of all the refinement theorems of §5, and so on.

THEOREM A. *The splitting hypothesis is satisfied by the M -loop L if every L - M -subgroup S of $Z_M(L)$ meets the following requirement.*

(A) *If s is an element in S and η an M -endomorphism of S , then the set of elements $s\eta, s\eta^2, \dots, s\eta^i, \dots$ is finite.*

Proof. Consider a centralizing M -endomorphism η of L . Then $S = L\eta$ is an L - M -subgroup of $Z_M(L)$ and the elements $x\eta^{i+1}$ for x in L are iterated images of the element $x\eta$ in S . It follows from (A) that the set of elements of the form $x\eta^i$ is for every fixed x in L a finite set. Thus η is, in the terminology

⁽¹⁵⁾ See Bruck [1].

of Baer [4], almost periodical, and such endomorphisms have been shown to be uniformly splitting. Thus every centralizing endomorphism possesses one and only one complement, proving the validity of the splitting hypothesis.

Remark. If $Z_M(L)$ happens to be the additive group of rational numbers modulo 1 (or some similar group), then condition (A) is satisfied, and the existence of center indecomposable decompositions of L is assured. But none of the chain conditions is satisfied by the subgroups of $Z_M(L)$. Kurosh [3, Theorem 3] is readily seen to be a consequence of Theorem A.

The following property has been considered by various writers; see, for example, Baer [2]:

(Q) *If N is a normal M -subloop of the M -loop H such that H and H/N are M -isomorphic, then $N=0$.*

Of the various criteria for the validity of (Q) we mention here only the most trivial one, namely the ascending chain condition for normal M -subloops.

THEOREM B. *The splitting hypothesis is satisfied by the M -loop L if every L - M -subgroup S of $Z_M(L)$ meets the following requirement:*

(B) *Property (Q) and the descending chain condition are satisfied by the M -subgroups of S .*

Proof. In Baer [4] we have shown that the centralizing endomorphism η of L splits L uniformly and possesses therefore one and only one complement if it meets the following two requirements (which we state for brevity's sake in an unnecessarily strict form):

(a) If the M -subgroup T of $Z_M(L)$ satisfies $T\eta \leq T$, then there exists an integer i such that $T\eta^i = T\eta^{i+1}$.

(b) If the M -subgroup T of $Z_M(L)$ satisfies $T\eta = T$, then there exists an integer j such that $T \cap K(\eta^j) = T \cap R(\eta)$.

Now consider some centralizing endomorphism η of L . Then $S = L\eta$ is an L - M -subgroup of $Z_M(L)$. If $T \leq Z_M(L)$ and $T\eta \leq T$, then $T\eta \leq S$ and the descending chain $T\eta^i$ breaks off after a finite number of steps, showing the validity of (a). If $T = T\eta$, then $T \leq S$ and $T \cap K(\eta) = 0$ because of (Q), proving (b). Thus (a) and (b) are satisfied by η , proving that η possesses one and only one complement.

This theorem may be dualized. In order to do so we need the following dual of property (Q).

(S) *If U is an M -subloop of the M -loop H which is M -isomorphic to H , then $H = U$.*

Of the various criteria for the validity of (S) we mention here only the most trivial one, namely the descending chain condition for M -subloops of H ; see Baer [2], Beaumont [1], Cohen [1], Kaplansky [1].

THEOREM C. *The splitting hypothesis is satisfied by the M -loop L if every*

L-M-subgroup S of $Z_M(L)$ meets the following requirement:

(C) *Property (S) and the ascending chain condition are satisfied by the M -subgroups of S .*

Proof. Consider a centralizing endomorphism η of L . It clearly suffices to verify the validity of the conditions (a) and (b) stated in the course of the proof of Theorem B.

$L\eta = S$ is an L - M -subgroup of $Z_M(L)$. If T is an M -subgroup of $Z_M(L)$, then $T\eta \leq S$ and the $T\eta \cap K(\eta^i)$ form an ascending chain of M -subgroups of S . Thus there exists an integer $n = n(T)$ such that

$$T\eta \cap K(\eta^n) = \cdots = T\eta \cap K(\eta^{n+i}) = \cdots = T\eta \cap R(\eta).$$

This implies in particular the validity of condition (b). Suppose now that $T\eta \leq T$. If x is an element in $T\eta^{n+1} \cap K(\eta)$, then there exists an element t in T such that $t\eta^{n+1} = x$ and $0 = x\eta = t\eta^{n+2}$. Thus $t\eta$ is an element in $T\eta \cap K(\eta^{n+1}) = T\eta \cap K(\eta^n)$, proving that $x = t\eta^{n+1} = 0$. Hence $0 = K(\eta) \cap T\eta^{n+1}$, proving that η induces an isomorphism of $T\eta^{n+1} \leq S$ into itself. It follows from Property (S) that $T\eta^{n+1} = T\eta^{n+2}$, proving that (a) too is satisfied by η . This completes the proof.

Remark 1. Theorems B and C should be compared with Ore [1, p. 594–595, Theorems 1 and 2]. The main difference consists in the fact that the hypotheses of Theorems B and C refer to the M -center only whereas Ore's conditions refer to the whole structure.

THEOREM D. *The splitting hypothesis is satisfied by the M -loop L if every L - M -subgroup S of $Z_M(L)$ meets the following requirements:*

(D') *The descending chain condition is satisfied by the M -subgroups of S .*

(D'') *If the M -subgroup T of S is a cyclic M -group, then the ascending chain condition is satisfied by the M -subgroups of T .*

Proof. In Baer [4] we have shown that every endomorphism η of L which satisfies $L\eta \leq S \leq Z_M(L)$ splits uniformly provided (D') and (D'') are satisfied by S . From this remark our theorem may be inferred in the usual fashion.

Remark 2. Whether or not condition (D'') may be omitted without invalidating Theorem D is still an open question. It is unknown in particular whether or not the refinement theorems can be deduced from condition (D') alone. It is known, however, that (D') alone does not assure the splitting of all centralizing endomorphisms of L ; but for our purposes we need only the uniform splitting of very special endomorphisms.

Remark 3. The impossibility of deducing the splitting hypothesis or the refinement theorems from the ascending chain condition for M -subgroups of the center is a fact that has been known for a long time; see in this respect Krull [2] and the very elegant example in Kurosh [3], apart from §5, Remark 3.

Remark 4. Conditions (D') and (D'') are certainly satisfied whenever the double chain condition is satisfied by the M -subgroups of the L - M -subgroup S of $Z_M(L)$. Thus Theorem 2 of Kurosh [3] is a special case of our refinement theorems.

DEFINITION 2. *If S is an M -subgroup of $Z_M(L)$, then $E(S) = E_M(S)$ is the ring of endomorphisms of the abelian group S which is generated by the identity and by those endomorphisms of S which are induced in S by the elements in M , and $E^*(S) = E_M^*(S)$ is the center of the ring $E_M(S)$.*

COROLLARY. *The splitting hypothesis is satisfied by the M -loop L if every L - M -subgroup S of $Z_M(L)$ meets either of the following requirements:*

(D.1) *The descending chain condition is satisfied by the M -subgroups of S and every right ideal in $E_M(S)$ is two-sided.*

(D.2) *The descending chain condition is satisfied by the $E^*(S)$ -subgroups of S .*

Proof. It has been shown in Baer [6] that (D.1) as well as (D.2) (as well as some similar conditions) implies the conditions (D') and (D'') of Theorem D so that the present corollary is a consequence of Theorem D.

Remark 5. If we assume the validity of one of the conditions (B) to (D) not only for the L - M -subgroups of $Z_M(L)$, but for $Z_M(L)$ itself, then we are assured of the existence of center indecomposable refinements to every given direct decomposition of L . In that case we are not only assured of the validity of the splitting hypothesis and the refinement theorems of §5, but also of the results of §7, in particular the stricter form (7.E) of the exchange property. One sees now that our theorems include as special cases also the strong form of the theorem of O. Schmidt and the theorem of Kořinek.

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 decomposition of enumerable, primary abelian groups into direct summands*, Quart. J. Math. Oxford Ser. vol. 6 (1935) pp. 217-221.
2. *Groups without proper isomorphic quotient groups*, Bull. Amer. Math. Soc. vol. 50 (1944) pp. 267-278.
3. *The homomorphism theorems for loops*, Amer. J. Math. vol. 67 (1945) pp. 450-460.
4. *Splitting endomorphisms*, Trans. Amer. Math. Soc. vol. 61 (1947) pp. 508-516.
5. *Endomorphism rings of operator loops*, Trans. Amer. Math. Soc. vol. 61 (1947) pp. 517-529.
6. *The double chain condition in cyclic operator groups*, Amer. J. Math. vol. 69 (1947) pp. 37-45.

R. A. BEAUMONT

1. *Groups with isomorphic proper subgroups*, Bull. Amer. Math. Soc. vol. 51 (1945) pp. 381-386.

- R. H. BRUCK
1. *Contributions to the theory of loops*, Trans. Amer. Math. Soc. vol. 60 (1946) pp. 245–354.
- I. S. COHEN
1. *Groups and rings of finite rank*, Bull. Amer. Math. Soc. Abstract 52-5-110.
- H. FITTING
1. *Über die direkten Produktzerlegungen einer Gruppe in direkt unzerlegbare Faktoren*, Math. Zeit. vol. 39 (1934) pp. 16–30.
- O. N. GOLOWIN
1. *On factors without centers in direct decompositions of groups*, Rec. Math. (Mat. Sbornik) N.S. vol. 6 (1939) pp. 423–426.
- N. JACOBSON
1. *The theory of rings*, Mathematical Surveys, vol. 2, 1943.
- B. JÓNSSON and A. TARSKI
1. *On direct products of algebras*, Bull. Amer. Math. Soc. Abstract 51-9-149.
2. *A generalization of Wedderburn's theorem*, Bull. Amer. Math. Soc. Abstract 51-9-150.
- I. KAPLANSKY
1. *A note on groups without isomorphic subgroups*, Bull. Amer. Math. Soc. vol. 51 (1945) pp. 529–530.
- V. KOŘÍNEK
1. *Sur la décomposition d'un groupe en produit direct des sousgroupes*, Časopis pro pěstování matematiky a fyziky vol. 66 (1937) pp. 261–286.
- W. KRULL
1. *Über verallgemeinerte endliche Abelsche Gruppen*, Math. Zeit. vol. 23 (1925) pp. 161–196.
2. *Matrizen, Moduln und verallgemeinerte Abelsche Gruppen im Bereich der ganzen algebraischen Zahlen*, Sitzungsberichte der Heidelberger Akademie der Wissenschaften, mathematisch-naturwissenschaftliche Klasse, 1932, pp. 13–38.
- A. KUROSU
1. *Zur Zerlegung unendlicher Gruppen*, Math. Ann. vol. 106 (1932) pp. 107–113.
2. *Isomorphisms of direct decompositions*, I, Bull. Acad. Sci. URSS. vol. 7 (1943) pp. 185–202.
3. *Isomorphisms of direct decompositions*, II, Bull. Acad. Sci. URSS. vol. 10 (1946) pp. 47–72.
- O. ORE
1. *Direct decompositions*, Duke Math. J. vol. 2 (1936) pp. 581–596.
- R. REMAK
1. *Über die Zerlegungen der endlichen Gruppen in direkte unzerlegbare Faktoren*, J. Reine Angew. Math. vol. 139 (1911) pp. 293–308.
- O. SCHMIDT
1. *Über unendliche Gruppen mit endlicher Kette*, Math. Zeit. vol. 29 (1929) pp. 34–41.
- M. F. SMILEY
1. *An application of lattice theory to quasigroups*, Bull. Amer. Math. Soc. vol. 50 (1944) pp. 782–786.
- J. H. MACLAGAN WEDDERBURN
1. *On the direct product in the theory of finite groups*, Ann. of Math. vol. 10 (1909) pp. 173–176.
- H. ZASSENHAUS
1. *Lehrbuch der Gruppentheorie*, I, Hamburger Mathematische Einzelschriften, vol. 21, 1937.

UNIVERSITY OF ILLINOIS,
URBANA, ILL.