# A UNIFIED THEORY OF PROJECTIVE SPACES AND FINITE ABELIAN GROUPS

BY

REINHOLD BAER

The similarity between finite-dimensional projective spaces and finite abelian groups has often been noted(1); and thus one may expect that the more general features of these two theories are identical. But the likeness is more than a superficial one; and consequently it is possible to give a unified treatment for spaces and groups.

It may be worthwhile to indicate in a few lines the developments leading up to a scientific situation that made such a joint theory as we are offering here a possibility. The evolution of geometrical thought pertinent to our problem is perhaps best described by two textbooks: Bôcher's *Higher Algebra* which exposed the identity of geometry and the theory of linear equations; and Veblen and Young's *Projective Geometry* whose presentation of the theory broke down the restriction to the two geometries over the real and the complex number field; and enlarged the domain to be considered to the projective geometries over any sort of field, whether finite or infinite, commutative or not. Any further progress had to be a progress in the theory of linear equations; and this was found in the treatment of the theory without using determinants—a concept that had to be thoroughly debunked to make these (and other) extensions possible. This was the starting point for further generalizations, generalizations in a direction that is different from ours—notably the theory of linear equations with infinitely many variables and in particular its geometrical counterpart, J. von Neumann's continuous geometry.

In the theory of finite abelian groups only one generalization was needed. We refer to the extension of this theory by introducing the concept of an abelian group which admits operators from some given ring or some other domain. For this concept makes it possible to consider projective geometry a—rather special—chapter in the theory of abelian groups, since the $n$-dimensional projective space over the (not necessarily commutative) field $F$ of coordinates is nothing but the set of $F$-admissible subgroups of an abelian group of rank $n+1$ over $F$ and the linear forms over this geometry are just the characters of this underlying group. Our problem is now easily stated: to characterize a class of abelian operator groups which comprises both the

Presented to the Society, April 11, 1941; received by the editors February 13, 1941, and, in revised form, September 19, 1941.

(1) See, for example, R. D. Carmichael, *Finite geometries and the theory of groups*, American Journal of Mathematics, vol. 52 (1930), pp. 754–788.

finite abelian groups and the abelian groups over fields as special cases; and to develop a theory of this class of groups which contains finite-dimensional projective geometry and finite commutative group theory as special cases.

It is clear from the preceding remarks that the theory of abelian operator groups may be considered from two rather different points of view, for it is both a special chapter in the theory of groups and a generalization of projective geometry and the theory of linear forms; and according to the point of view preferred, one will write the group composition as "multiplication" or "addition," the operators as "exponents" or "multipliers."

The present investigation has been divided into three parts and this division has been guided by the customary organization of projective geometry. There is first the synthetic theory which deals with the subgroups and their combinations and which does not make any use of the elements of the underlying group, their addition or their multiplication by operators. The analytic theory concerns itself with those facts that either cannot be proved without making use of the group elements and their combinations (or equivalent hypotheses) or which actually involve them in their statement. The third part is devoted to the construction of the underlying abelian operator group to a given partially ordered set meeting certain requirements (=introduction of coordinates in the terminology of projective geometry) and which may be considered the main contribution of this investigation. Though this part takes an intermediate place between the synthetic and the analytic theory, we had to place it at the end for technical reasons.—A little more detailed account of the contents of these three parts will be found in the introductions prefacing them.

## Part I. The synthetic theory

The system of admissible subgroups of an abelian operator group is known to form a partially ordered set, containing the sums and cross-cuts of its elements and obeying Dedekind's law, in short, a *Dedekind set*(2). Thus it is natural to make Dedekind sets the framework around which to build the synthetic theory. The atoms of a projective space are its points; and likewise one may consider as the atoms of a finite abelian group its cyclic subgroups of order a power of a prime. Consequently we choose as the atoms of our theory the *cycles*, that is, elements in a Dedekind set whose parts form a finite ordered set. In order to obtain a satisfactory theory including in particular the theory of dimension (or rank), the existence of complementary subspaces and the basis theorem for finite abelian groups, it turns out to be necessary and sufficient to impose the following two conditions upon the

(2) There exists an extensive literature on partially ordered sets, notably the work of G. Birkhoff and O. Ore; for a survey of this theory, see G. Birkhoff, *Lattice Theory*, American Mathematical Society Colloquium Publications, vol. 25, 1940. It should be noted that we use only very elementary parts of this theory, and that we state in full whatever we use.

Dedekind set under consideration. (1) Every element is a sum of cycles. (2) A quotient system is a cycle if, and only if, it contains at most one smallest element not zero (=subcycle of order 1=point).

To obtain a satisfactory geometry one has to assume that lines carry at least three different points. The group-theoretical counterpart is the restriction to primary groups (=groups of order a power of a prime). Thus we have to prove a generalization of the reduction theorem stating that every finite abelian group is the direct sum of its primary components (=partition into relatively prime, primary components); and we show that restriction to primary systems is equivalent to substituting for condition (2) the following condition. (2′) A quotient system is a cycle if, and only if, it contains at most two different smallest elements not zero.

1. **Preliminaries**[3]. The framework for our investigation of the system of admissible subgroups of a (primary) abelian operator group is provided by concepts like "partially ordered set," "lattice," "structure," and so on. Since these systems will be required to satisfy Dedekind's law, we shall term them "Dedekind sets." Such a Dedekind set is a system $D$ of elements connected by the following three relations: the cross-cut, meet, intersection or product $fg$ of the elements $f$, $g$; the join or sum $f+g$ of the elements $f$ and $g$; the relation $f \leqq g$ (in words: $f$ is a part of or contained in $g$). The rules by means of which the first two operations may be reduced to the third one, and conversely, may be stated as follows:

$fg$ is the greatest element contained in both $f$ and $g$.

$f+g$ is the smallest element containing both $f$ and $g$.

$f \leqq g$; $f=fg$ and $f+g=g$ are equivalent assertions.

Let us add finally that the relation: $f \leqq g$ is reflexive and transitive; and that $f<g$ signifies: $f \neq g$ but $f \leqq g$.

To these elementary rules we add the existence of a null-element 0 and we impose the main requirement, namely

DEDEKIND'S LAW. *If $f$, $g$, $h$ are three elements in $D$, and if $f \leqq g$, then* $f+gh=(f+h)g$.

This is a partial substitute for the distributive law; and we are going to derive from it some further useful formulas.

LEMMA I.1.1. *If the four elements $a$, $b$, $c$, $d$ in the Dedekind set $D$ satisfy* $(a+b)(c+d)=0$, *then*

$$(a+c)(b+d)=ab+cd=(a+d)(b+c).$$

**Proof.** It suffices to prove the first of these equations; and this may be done as follows:

---

[3] In this section we collect a number of elementary facts from the theory of partially ordered sets in the form best suited to our purposes (see Footnote 2).

$$(a+c)(b+d) = (a+c)(a+b+c)(b+d) = (a+c)(b+d)(a+b+c)$$
$$= (a+c)(b+d(d+c)(a+b+c))$$
$$= (a+c)(b+d(c+(d+c)(a+b)))$$
$$= (a+c)(b+dc) = dc+b(a+c) = dc+b(a+b)(a+c)$$
$$= dc+b(a+c(a+b)) = dc+ab.$$

LEMMA I.1.2. *If $a$, $b$, $c$ are three elements in $D$ such that $ab=(a+b)c=0$, then $a(b+c)=b(c+a)=0$.*

For $a(b+c)=a(a+b)(b+c)=a(b+c(a+b))=ab=0$.

The elements $x_1, \cdots, x_n$ are said to be *independent*, if $x_i\sum_{j\neq i}x_j=0$ for $i=1, \cdots, n$; and it is readily inferred(4) from Lemma I.1.1 that the elements $x_1, \cdots, x_n$ *are independent if, and only if,* $0=x_i\sum_{j<i}x_j$ *for* $i=2, \cdots, n$.

If the elements $x_1, \cdots, x_n$ are independent, then $\sum_{i=1}^{n}x_i=s$ is the *direct sum* of the $x_i$ and every summand $x_i$ is a *direct summand* of $s$. The following statements are easily verified. If $x$ is the direct sum of the $x_i$, and if $x_i$ is the direct sum of the elements $x_{ij}$, then $x$ is the direct sum of the $x_{ij}$. If $s$ is the direct sum of $t$ and $u$, and if $v$ is an element between $u$ and $s$, then $v$ is the direct sum of $u$ and $vt$; so that $a$ is a direct summand of $b$, if $a$ is a direct summand of $c$ and if $a\leqq b\leqq c$.

If $u\leqq v$, then the set $v/u$ of all the elements $x$ in $D$ which satisfy $u\leqq x\leqq v$ is a Dedekind set (exactly as $D$) and $u$ is the null-element of $v/u$. If in particular $u=0$, then $v/0$ is the set of all the parts of $v$; and it will be possible to write $v$ instead of $v/0$ without causing confusion.

Any biunivoque and monotonically increasing correspondence, mapping the elements of the Dedekind set $D$ upon the elements of $D'$ is termed an *isomorphism* or a *projectivity*(5) of $D$ upon $D'$. If in particular $u$ and $v$ are two elements in $D$, then *an isomorphism of* $(u+v)/u$ *upon* $v/(uv)$ is defined by mapping $x$ in $(u+v)/u$ upon $xv$ in $v/(uv)$.

2. **Cycles and their orders.** If $u$ and $v$ are elements in a partially ordered set (in particular in a Dedekind set), then $u$ is said to be a *cycle modulo* $v$, if $v\leqq u$, if there exists only a finite number of elements between $v$ and $u$, and if of two elements between $u$ and $v$ one is always part of the other, that is, if $u/v$ is a finite ordered set. If $u$ is a cycle modulo $v$, then we denote by $n(u/v)$ the number of elements between $u$ and $v$ which are different from $v$ and term this number the *order* of the cycle $u/v$. Instead of $n(u/0)$ we write $n(u)$ and we say that $u$ is a cycle instead of saying a cycle modulo 0. If the

(4) Cf. K. Menger, Annals of Mathematics, (2), vol. 37 (1936), pp. 456–482.

(5) As long as only partially ordered sets are discussed, we prefer the term "isomorphism" as the more appropriate one. But as soon as we have to connect the "isomorphisms" of partially ordered sets (of subgroups of a group) with the "isomorphisms" of groups, we shall use the term "projectivity" in order to avoid confusion.

cycle $z$ is part of the element $e$, then we express this fact by saying that $z$ is a *subcycle of* $e$.

THEOREM I.2.1. *If $z$ is a subcycle of a sum of cycles whose orders do not exceed $m$, then the order of $z$ does not exceed $m$ either.*

**Proof.** It is a well known fact(6) that every part of a sum of a finite number of cycles of order 1 (of points in projective geometry) is itself a sum of a finite number of cycles of order 1; and from this fact one readily infers our theorem in the special case $m=1$.

We now proceed by induction with regard to $m$, assuming the theorem to be true for $m$ and proving it for $m+1$. Let $s$ be the sum of the cycles $z_i$ of order not exceeding $m+1$; and suppose that $z$ is a subcycle of $s$. If $n(z_i)=m+1$, then denote by $y_i$ the uniquely determined subcycle of order $m$ of $z_i$; and if $n(z_i)\leqq m$, then put $z_i=y_i$. If $t$ is the sum of the $y_i$, then it follows from the induction hypothesis that the subcycle $tz$ of $t$ has an order not exceeding $m$. We note furthermore that $s/t$ is the sum of the cycles $(t+z_i)/t$ whose orders do not exceed 1, since they are isomorphic to $z_i/(z_it)$ and since $y_i\leqq z_it$. Thus it follows from the special case $m=1$ that the subcycle $(z+t)/t$ of $s/t$ is of an order not exceeding 1 so that $n(z/(zt))\leqq 1$. Since we already pointed out that $n(zt)\leqq m$, we find now that $n(z)=n(zt)+n(z/(zt))\leqq m+1$, as was to be shown.

THEOREM I.2.2. *If $z$ is a subcycle of the direct sum $s$ of the cycles $z_i$, if $n$ is a positive integer, if $y_i$ is the uniquely determined subcycle of $z_i$ whose order is exactly the minimum of the numbers $n$ and $n(z_i)$, and if $y$ is the sum of the cycles $y_i$, then $n(z)\leqq n$ is a necessary and sufficient condition for $z\leqq y$.*

REMARK. It is easy to give examples showing that the independence of the cycles $z_i$ is indispensable for the validity of this theorem.

**Proof.** It is a consequence of Theorem I.2.1 that the orders of the subcycles of $y$ do not exceed $n$, since $n(y_i)\leqq n$.—Thus assume conversely that $n(z)\leqq n$. If $k$ is the number of cycles $z_i$, then we put $s(i)=\sum_{j=1}^{i}y_j+\sum_{j=i+2}^{k}z_j$ and $t(i)=s(i)+z_{i+1}$ so that in particular $t(0)=s$ and $t(k)=y$. Since $z$ is a subcycle of $t(0)$ we are going to prove by complete induction with regard to $i$ that $z$ is a subcycle of each $t(i)$. Thus we assume that $z\leqq t(i)$ and we have to prove that $z\leqq t(i+1)$. From the induction hypothesis it follows that $s(i)\leqq s(i)+z\leqq t(i)=s(i)+z_{i+1}$. Since $(s(i)+z)/s(i)$ and $z/(zs(i))$ are isomorphic cycles, and since the order of $z$ does not exceed $n$, it follows that $n((s(i)+z)/s(i))\leqq n$. Since $s$ is the direct sum of the cycles $z_j$, it follows that $0=s(i)z_{i+1}$ so that $z_{i+1}$ and $t(i)/s(i)$ are isomorphic cycles. Consequently $s(i)+z\leqq s(i)+y_{i+1}=t(i+1)$; and this completes the proof.

We note without proof the important fact that *the maximum and the minimum conditions are satisfied by the parts of a sum of a finite number of*

(6) Cf. Menger, loc. cit.

*cycles*; it is an obvious consequence of the fact(7) that the maximum and minimum conditions are satisfied by the parts of $a+b$, if they are satisfied by the parts of $a$ and of $b$.

3. **Direct decompositions.** The part $v$ of the element $w$ (in the Dedekind set $D$) is said to be *closed in*(8) $w$, if to every cycle $z \leqq w$ such that $zv \neq 0$ there exists a cycle of order $n(z)$ between $zv$ and $v$.

THEOREM I.3.1. *Every direct summand of $w$ is closed in $w$.*

**Proof.** If $w$ is the direct sum of $u$ and $v$, if $z$ is a subcycle of $w$ such that $vz \neq 0$, then $c=v(u+z)$ is between $zv$ and $v$. Thus $cu=0$ and $zu=0$ are consequences of the fact that the only subcycle of order 1 of the cycle $z$ is in $v$. Hence $c=c/(cu)$ is isomorphic to $(c+u)/u=(v(u+z)+u)/u$ $=((v+u)(u+z))/u=(w(u+z))/u=(u+z)/u$ as follows from Dedekind's law; and $(u+z)/u$ being isomorphic to $z/(uz)=z$, it follows that $c$ and $z$ are isomorphic so that they are cycles of equal order.

THEOREM I.3.2. *If $z$ is a subcycle of maximum order of the direct sum $s$ of the cycles $c(1), \cdots, c(k)$, then there exists an $i$ such that $s$ is the direct sum of $z$ and of the cycles $c(j)$ for $j \neq i$.*

**Proof.** We may assume that $n(c(i))=n(z)$ if, and only if, $1 \leqq i \leqq h$; and we note that $0<h$ by Theorem I.2.1. If $v(i)=\sum_{j \neq i} c(j)$, then $\prod_{i=1}^{h} v(i)=\sum_{h<j} c(j)$ $=v$. Since $v$ is a direct summand of $s$, $v$ is closed in $s$ by Theorem I.3.1; and since the maximum order of the subcycles of $v$ is smaller than $n(z)$—by Theorem I.2.1—$vz=0$. Thus there exists at least one $i$ between 1 and $h$ such that the subcycle $z^*$ of order 1 of $z$ is not contained in $v(i)$; since thus $zv(i)=0$, and since $s$ is the direct sum of $v(i)$ and of the cycle $c(i)$ of order $n(z)$, it follows finally that $s$ is the direct sum of $z$ and of $v(i)$.

COROLLARY I.3.3. *Every part of $w$ is a direct sum of cycles if, and only if, the following conditions are satisfied.*

(i) *Every part of $w$ is a sum of cycles.*

(ii) *If $z$ is a subcycle of maximum order of the part $v$ of $w$, then $z$ is a direct summand of $v$.*

The necessity is an immediate consequence of Theorem I.3.2, the sufficiency may be proved inductively, since every part $v \neq 0$ of $w$ is the direct sum of a subcycle of maximum order (in $v$) and of some smaller element, and since (i) implies the minimum condition for the parts of $w$.

COROLLARY I.3.4. *If the element $s$ is both the direct sum of the cycles $c(i)$*

---

(7) Cf. Birkhoff, loc. cit.

(8) This concept has been introduced by H. Prüfer into the theory of primary abelian groups (under the name "Servanzuntergruppe"); cf. H. Prüfer, Mathematische Zeitschrift, vol. 17 (1923), pp. 35–61.

*and the direct sum of the cycles $d(j)$, then the number of cycles $c(i)$ of order $n$ is the same as the number of cycles $d(j)$ of order $n$.*

For if $d(1)$ is a cycle of maximum order in $s$, then it follows from Theorem I.3.2 that $s$ is the direct sum of $d(1)$ and of the $c(i)$ for $i \neq k$. Thus $d(1)$ and $c(k)$ are of the same order and $\sum_{1<i} d(i)$ and $\sum_{j \neq k} c(j)$ are isomorphic; and now the statement may be proved by induction.

The element $w$ *splits*, if every part of $w$ is a direct sum of (a finite number of) cycles, and if every closed part of any element $v \leqq w$ is a direct summand of $v$. The following characterization of splitting elements will be needed in the proof of the main theorem of this section.

THEOREM I.3.5. *The element $w$ splits if, and only if, it satisfies the following conditions.*

(i) *Every part of $w$ is a sum of cycles.*

(ii) *If $t < s \leqq w$, if $t$ is a subcycle of maximum order of $s$, and if $s/t$ is a cycle, then $s$ contains a cycle of order 1 which is not part of $t$; and if $p$ is a subcycle of order 1 not part of $t$, then $s$ is the direct sum of $t$ and of a cycle containing $p$.*

**Proof.** If $w$ splits, and if $s$ and $t$ satisfy the hypotheses of (ii), then $t$ is closed in $s$, therefore a direct summand of $s$ so that $s$ is the direct sum of $t$ and of some cycle $z$. Thus there exist subcycles of order 1 of $s$ which are not in $t$. If $p$ is some such cycle of order 1, then denote by $c$ a cycle of greatest order between $p$ and $v$. Then $c$ is closed in $v$ and therefore a direct summand of $v$. Since $n(z) \leqq n(t)$, it follows now from Corollary I.3.4 that $n(c) = n(z)$; and $tc = 0$ implies now that $v$ is the direct sum of $c$ and $t$. Thus splitting elements satisfy (i) and (ii).

For the sufficiency proof it will be convenient to say that the part $r$ of $s$ is *weakly closed in* $s$, if subcycles of order 1 of $r$ which are contained in subcycles of order $n$ of $s$ are contained in subcycles of the same order $n$ of $r$.

Suppose now that $w$ satisfies (i) and (ii), that $r < v \leqq w$ and that $r$ is weakly closed in $v$. Since $r$ and $v$ are sums of cycles, there exists a subcycle $x$ of smallest order of $v$ which is not part of $r$. If $x^*$ is the subcycle of order 1 of $x$, then $x^* \leqq r$ would imply the existence of a cycle $y$ of order $n(x)$ between $x^*$ and $r$. It follows from Theorem I.2.1 that $n(y)$ is the maximum order of the subcycles of $x+y$; and thus it follows from (ii) that $y$ is a direct summand of $x+y$ which proves the existence of a cycle of order smaller than $n(x)$ which is part of $v$ but not of $r$. This contradiction shows that $xr = 0$. Thus there exists a subcycle $z$ of $v$ such that $zr = 0$ and such that the order of $z$ is as big as possible. Since $z \neq 0$, this implies $r < r+z$. Suppose now that $p$ is a subcycle of order 1 of $r+z$, that $b$ is a cycle between $p$ and $v$. If $p \leqq r$, then there exists a cycle of order $n(b)$ between $p$ and $r$. If the inequality $p \leqq r$ does not hold, then $br = 0$ so that $n(b) \leqq n(z)$. Thus we may assume that $pz = 0$ in order to

prove that $r+z$ is weakly closed in $v$. Then $q=r(p+z)$ is a cycle of order 1, since $p$ and $(p+z)/z=(q+z)/z$ are isomorphic. Since $qz=0$, it follows from (ii) that $b+z$ is the direct sum of $z$ and of a cycle $d$ containing $q$. Since $bz=0$, $n(b)=n(d)$. Since $q\leqq r$, and since $r$ is weakly closed in $v$, there exists a cycle $e$ of order $n(d)$ between $q$ and $r$. Since $p\leqq q+z\leqq e+z$, there exists by (ii) a cycle $f$ containing $p$ such that $e+z$ is the direct sum of $f$ and $z$. It follows from Corollary I.3.4 that $n(f)=n(d)=n(b)$; and thus we have finally shown that $r+z$ is weakly closed in $v$. Since by (i) the maximum condition is satisfied by the parts of $w$, it follows now by induction that $v$ is the direct sum of $r$ and of some cycles. Thus we have shown that (i), (ii) imply the splitting of $w$ and imply that *every weakly closed part is a direct summand* (and therefore closed).

If the element $v$ is part of the element $u$, then $u$ splits modulo $v$, whenever $u$ splits in the Dedekind set $u/v$ (which consists of all the elements between $v$ and $u$ and whose null is $v$). The element $w$ *splits completely*, if every part $u$ of $w$ splits modulo each of its parts $v$. We mention the important and well known fact that both finite abelian groups([9]) and finite-dimensional projective geometries([10]) split completely.

THEOREM I.3.6. *The element $w$ splits completely if, and only if, it satisfies the following conditions.*

(i) *Every part of $w$ is a sum of cycles.*

(ii) *If $r\leqq s\leqq w$, and if $s/r$ contains at most one subcycle of order 1, then $s/r$ is a cycle.*

**Proof.** The necessity of these conditions is an immediate consequence of the fact that subcycles of maximum order are closed, and that $s/r$ is a sum of cycles, if $s$ is a sum of cycles.

Before proving the sufficiency of (i) and (ii) we prove the following helpful lemma.

(I.3.6.1) *If $s$ is a sum of cycles, if $t<s$ and if $s/t$ is a cycle then there exists a cycle $z$ such that $s=t+z$.*

For there exists between $t$ and $s$ one and only one element $r$ such that $s/r$ is a cycle of order 1. Since $r<s$, not every subcycle of $s$ is part of $r$. If $z$ is a subcycle of $s$, though not of $r$, then the inequality $t+z\leqq r$ does not hold so that $t+z=s$, since $s/t$ is a cycle.

Suppose now that (i) and (ii) are satisfied by $w$, that $t<s\leqq w$, that $t$ is a subcycle of maximum order of $s$ and that $s/t$ is a cycle. Since $s$ is therefore not a cycle, it follows from (ii) that $s$ contains at least two different subcycles of order 1, one of which is certainly not part of $t$. Suppose now that $p$ is a sub-

([9]) Cf. Prüfer, loc. cit.

([10]) The central importance of this fact for projective geometry has been stressed by Menger, loc. cit., and by G. Birkhoff, Annals of Mathematics, (2), vol. 36 (1935), pp. 743–748.

cycle of order 1 of $s$ and that the inequality $p \leqq t$ does not hold or $pt = 0$. Denote by $b$ a cycle of greatest order between $p$ and $s$. If $g$ is an element between $b$ and $s$ such that $g/b$ is a cycle of order 1, then $g$ is no cycle so that $g$ contains by (ii) a subcycle $q$ of order 1 different from $p$. Since it follows from (I.3.6.1) that $s$ is the sum of $t$ and of some other cycle, it follows that the sum $s^*$ of all the subcycles of order 1 of $s$ is the sum of any two of its (different) subcycles (of order 1) so that $s^* = p+q$ or $g = b+s^*$. Thus $s/b$ contains one and only one subcycle of order 1; and (ii) implies consequently that $s/b$ is a cycle. Hence it follows from (I.3.6.1) that $s$ is the sum of $b$ and of some cycle so that $n(s/b) \leqq n(t)$. Since $tb = 0$, it follows now that $s$ is the direct sum of $t$ and of the cycle $b$ containing $p$. Thus we showed that the conditions of Theorem I.3.5 are satisfied by $w$, if $w$ satisfies (i) and (ii); that is, if $w$ satisfies our conditions (i) and (ii), then $w$ splits. But if $w$ satisfies conditions (i) and (ii), and if $u \leqq v \leqq w$, then $v/u$ satisfies these conditions so that $v/u$ splits too. Thus $w$ splits completely, if it satisfies the conditions (i) and (ii).

The elements $u$ and $v$ are termed *relatively prime*, if $u$ and $v$ are not both 0, if $uv = 0$, and if $x \leqq u+v$ implies $x = xu+xv$. The decomposition of a finite abelian group into its primary components is an example of a decomposition into a sum of relatively prime elements. The elements $u$ and $v$ are said to be relatively prime modulo their common part $t$, if they are relatively prime elements in the Dedekind set $(u+v)/t$. Finally we say that the element $w$ is *primary*, if there does not exist any triplet of elements $u$, $v$, $t$ such that $t \leqq uv \leqq u+v \leqq w$ and such that $u$ and $v$ are relatively prime modulo $t$. The system of subgroups of an abelian group of order a power of a prime furnishes an example of a primary system; and projective geometries whose lines carry at least three points are primary too.

If the sum of the two cycles $p$ and $q$ of order 1 contains just these two cycles and no further cycles (of order 1), then $p$ and $q$ are relatively prime.—If $u$ and $v$ are relatively prime, and if $u$ and $v$ are sums of cycles, then $u$ contains a cycle $p$ of order 1, $v$ contains a cycle $q$ of order 1, and $p+q$ contains just these two cycles and no further ones. Combining these remarks with Theorem I.3.6 we obtain the following fundamental theorem.

THEOREM I.3.7. *The element $w$ splits completely and is primary if, and only if, it satisfies the following conditions.*

(i) *Every part of $w$ is a sum of cycles.*

(ii) *If $r \leqq s \leqq w$, and if $s/r$ contains at most two different subcycles of order 1, then $s/r$ is a cycle.*

An $n$-dimensional projective geometry whose lines carry at least three points possesses systems of $n+1$ points no $n$ of which are on a hyperplane. To generalize this property which will be of importance in the future we say that the elements $v(i)$ form a *partial sum* of the elements $u(i)$, if $v(i) \leqq u(i)$ for $i = 1, \cdots, n$. If we have $v(i) < u(i)$ for at least one $i$, then the $v(i)$ form a

*proper partial sum* of the $u(i)$. If the $u(i)$ are independent, and if the $v(i)$ form a partial sum of the $u(i)$, then they form a proper partial sum if, and only if, $\sum_{i=1}^{n} v(i) < \sum_{i=1}^{n} u(i)$.

LEMMA I.3.8. *If the primary element $s$ is the direct sum of the cycles $c(i)$, if the parts of $s$ are sums of cycles, then there exists a subcycle of $s$ which is not contained in any proper partial sum of the $c(i)$; if the subcycle $z$ of $s$ is not contained in any proper partial sum of the $c(i)$, then $z$ is a subcycle of maximum order of $s$ and $s$ is the direct sum of $z$ and of the $c(i)$ for $i \neq k$, provided $c(k)$ is of maximum order too.*

**Proof.** If we denote by $c(i)'$ the uniquely determined subcycle of $c(i)$ such that $c(i)/c(i)'$ is a cycle of order 1 and by $s'$ the sum of the $c(i)'$, then $s/s'$ is an $(n-1)$-dimensional projective geometry (a direct sum of the cycles $c(i)/c(i)'$ of order 1). Hence there exists in $s/s'$ a cycle $c$ of order 1 which is not part of any proper partial sum of the $c(i)/c(i)'$. But $c$ may be seen to be the sum of $s'$ and of a cycle $z$ which meets the requirements.—The second statement is obvious.

4. **Partition into relatively prime, primary components.** The elements $u_1, \cdots, u_k$ *constitute a partition of their sum $s$*, if $s$ is the direct sum of the $u_i$, and if $u_i$ and $\sum_{j \neq i} u_j$ are relatively prime for every $j$. Note that the primary components of a finite abelian group constitute a partition of this group. If $w$ is a completely splitting element in a Dedekind set, then $w$ is the direct sum of cycles and therefore of primary elements; but there exist examples of completely splitting elements which do not admit of a partition into relatively prime, primary elements.

THEOREM I.4.1. (a) *The element $w$ in the Dedekind set $D$ admits of at most one partition into (relatively prime) primary elements.* (b) *The completely splitting element $w$ admits of a partition into (relatively prime) primary elements if, and only if, any two subcycles with non-primary sum are relatively prime.*

**Proof.** Assume first that the elements $u_i$ as well as the elements $v_i$ constitute a partition of the element $w$. Then the elements $u_i v_j \neq 0$ for $j = 1, \cdots, h$ constitute a partition of $u_i$ so that the elements $u_i v_j \neq 0$ constitute a partition of $w$. Statement (a) is now a consequence of the fact that primary elements do not admit of partitions into (more than one) relatively prime element.

Suppose now that the primary elements $p_1, \cdots, p_k$ constitute a partition of the completely splitting element $w$. If $z$ is a subcycle not 0 of $w$, $z^*$ the uniquely determined subcycle of order 1 of $z$, then $z = \sum_{i=1}^{k} z p_i$, $z^* = \sum_{i=1}^{k} z^* p_i$. Consequently there exists a subscript $j$ such that $z^* p_j = z^*$, $z^* p_i = 0$ for $i \neq j$; and this implies $z \leqq p_j$, $z p_i = 0$ for $i \neq j$ so that *every subcycle of $w$ is contained in one and only one component $p_i$.*

If $u$ and $v$ are two subcycles of $w$, then they are either contained in the same component $p_i$—in which case their sum is primary—or else they are in

different components and then they are relatively prime proving the necessity of the condition of (b).

Suppose now that the condition of (b) be satisfied by the subcycles of the completely splitting element $w$. If the part $t$ of $w$ is not primary, then there exist elements $x$, $y$ such that $x<y\leqq t$ and such that $y/x$ consists of exactly four elements, namely $x$, $y$ and two cycles of order 1. Since $w$ and therefore $t$ splits completely, this implies the existence of two subcycles $u$, $v$ not 0 of $t$ such that $uv=0$ and such that $u+v$ is not primary. Hence it follows from the hypothesis that $u$ and $v$ are relatively prime.—Suppose now that $s<t$, that $t/s$ is a cycle of order 1, and that $s$ is primary. If we denote by $c'$ the uniquely determined subcycle of order $n(c)-1$ of the cycle $c\neq 0$, then $c'\leqq s$ for every subcycle $c\neq 0$ of $t$ so that in particular $u'+v'\leqq s$. But the inequality $u+v\leqq s$ does not hold since $u+v$ is not primary, though $s$ is primary. Thus not both cycles $u$ and $v$ are subcycles of $s$. Since $t/s=(s+u+v)/s$ is a cycle of order 1 and is isomorphic to $(u+v)/s(u+v)=(u+v)/(su+sv)$—as $u$ and $v$ are relatively prime—it follows now that at least one of the cycles $u$ and $v$ is part of $s$. Thus we assume that $u\leqq s$, and that the inequality $v\leqq s$ does not hold. Since $u+v'\leqq s$, $u+v'$ is primary; and since $u$ and $v$ are relatively prime, this implies $v'=0$ so that $v$ is a cycle of order 1. If now $c$ is a subcycle of order 1 of $s$ which is different from the subcycle $u^*$ of order 1 of $u$, then $u^*+c$ is the direct sum of two cycles of order 1 and is primary as a part of $s$. Hence there exists a subcycle $z$ of order 1 of $u^*+c$ which is different from $c$ and $u^*$ so that $c+u^*=u^*+z=z+c$. Then $c+v=(c+v)/z(c+v)$ is isomorphic to $(z+c+v)/z=(z+u^*+v)/z$ and this is isomorphic to $(u^*+v)/z(u^*+v)=u^*+v$ so that $c$ and $v$ are relatively prime too. If $q$ is any subcycle not 0 of $s$, $q^*$ its subcycle of order 1, then $q^*$ and $v$ are relatively prime; hence $q+v$ is not primary and it follows from the hypothesis that $q$ and $v$ are relatively prime. Since every part of $s$ is a direct sum of cycles, it follows now that $s$ and $v$ are relatively prime. Thus $s$ and the cycle $v$ of order 1 constitute a partition of $t=s+v$ so that every subcycle of $t$ is either part of $s$ or of $v$; and this shows in particular that $v$ is the only subcycle $r$ of $t$ such that $t=s+r$.

Since the maximum condition is satisfied by the parts of $w$, there exists some greatest primary part $p$ of $w$. Certainly $p\neq 0$, if $w\neq 0$, since every subcycle of $w$ is primary. If $p=w$, then $w$ is primary so that we may assume that $0<p<w$. If $z$ is any subcycle of $w$, then either $z\leqq p$ or $p+z$ is not primary. In the latter case $(p+z)/p$ is a cycle different from 0 and there exists a uniquely determined subcycle $c$ of $z$ such that $(p+c)/p$ is a cycle of order 1. From what we have shown in the preceding paragraph of the proof it follows that $c$ is a cycle of order 1 such that $p$ and $c$ are relatively prime. If $x$ is any subcycle of $p$, then $x$ and $c$ are relatively prime; since $x+c\leqq x+z$, it follows that $x+z$ is not primary; and hence it follows from the hypothesis that $x$ and $z$ are relatively prime; and this shows that $p$ and $z$ are relatively prime.

Thus every subcycle of $w$ which is not part of $p$ is relatively prime to $p$.—Denote now by $q$ the sum of all the subcycles of $w$ which are not part of $p$. Then $q=z_1+\cdots+z_h$ where each of the $z_i$ is relatively prime to $p$. If $c$ is a subcycle of order 1 of $p$, then $c$ and $z_1$ are relatively prime. Since $cz_1=0$, we may assume that $cq_{i-1}=0$ for $q_{i-1}=\sum_{j=1}^{i-1}z_j$. If $c(q_{i-1}+z_i)\neq 0$, then $c\leqq q_{i-1}+z_i$. Hence $c+z_i=(c+z_i)(q_{i-1}+z_i)=z_i+q_{i-1}(c+z_i)=z_i$, since $c$ and $z_i$ are relatively prime, and since therefore $q_{i-1}(c+z_i)=q_{i-1}c+q_{i-1}z_i=q_{i-1}z_i$ by the induction hypothesis; but this would imply $c\leqq z_i$, an impossibility which proves $cq=0$. This implies $zq=0$ for every subcycle $z$ of $p$; and hence every subcycle not 0 of $w$ is part of one and only one of the two elements $p$ and $q$. Since the parts of $w$ are sums of cycles, this implies that $p$ and $q$ are relatively prime; and from the validity of maximum and minimum condition for the parts of $w$ one now readily infers that the greatest primary parts of $w$ constitute a partition of $w$ into relatively prime, primary elements.

5. **Sums and products of infinite sets.** It is well known that a great part of the theory of finite abelian groups, in particular the basis theorem, holds true for abelian groups the orders of whose elements are bounded. Crosscuts of any number of subgroups and sums of any number of subgroups are subgroups too; and we propose to give in this section a short analysis of the pertinent concepts.

If $S$ is a set of elements in the Dedekind set $D$, then the element $p$ in $D$ is a product of $S$, if $p$ is a greatest element contained in all the elements in $S$; and the element $s$ in $D$ is a sum of $S$, if $s$ is a smallest element containing every element in $S$. It is readily verified that there exists at most one product and at most one sum of $S$.

The set $S$ of elements not 0 in $D$ is independent, if there exists for every element $t$ in $S$ the sum $S(t)$ of the elements different from $t$ in $S$, and if $tS(t)=0$ for every $t$ in $S$.

THEOREM I.5.1([11]). *Suppose that the element $w$ satisfies the following conditions.*

(i) *If the nonvacuous set $T$ of subcycles of $w$ contains every subcycle of any finite sum of cycles in $T$, then there exists one and only one part $s(T)$ of $w$ such that $T$ is the set of all the subcycles of $s(T)$.*

(ii) *The orders of the subcycles of $w$ are bounded.*

*Then every part of $w$ is the direct sum of each of its closed parts and of a finite or infinite number of cycles if (and only if) every finite sum of subcycles of $w$ splits.*

REMARK. Condition (i) is satisfied in every abelian group without elements of infinite order and is satisfied in the primary abelian operator groups too (see below).—That condition (ii) is indispensable for the validity of the theorem is well known.

([11]) H. Prüfer proved this theorem for primary abelian groups.

**Proof.** We note first that on account of condition (i) sums and products of any number of parts of $w$ exist, that furthermore the subcycle $c$ of $w$ is part of the sum of the set $S$ of parts of $w$ if (and only if) there exists a finite number of elements in $S$ whose sum contains $c$, and that finally the set $S$ of parts not 0 of $w$ is independent if, and only if, every finite subset of $S$ is independent. We recall furthermore that—as in the proof of Theorem I.3.5—the element $u$ is termed weakly closed in the element $v$, if $u \leqq v$, and if there exists a cycle of order $n$ between $p$ and $u$ whenever $p$ is a subcycle of order 1 of $u$ which is contained in a subcycle of order $n$ of $v$.

Suppose now that $u < v \leqq w$ and that $u$ is weakly closed in $v$. Then there exists a subcycle of $v$ which is not part of $u$ and one verifies—exactly as in the proof of Theorem I.3.5—that there exist subcycles not 0 of $v$ which are independent of $u$. Hence it follows from condition (ii) that there exists a subcycle $z$ of $v$ such that $zu = 0$ and such that the order $n(z)$ is as big as possible. To show that the (direct) sum $u+z$ is weakly closed we need consider only subcycles $p$ of order 1 of $u+z$ which satisfy: $pu = pz = 0$. Suppose that $b$ is some cycle between $p$ and $v$. Then $n(b) \leqq n(z)$ and $bz = 0$. That $q = u(p+z)$ is a cycle of order 1 is verified as in the proof of Theorem I.3.5. Thus it follows from Theorem I.3.5 and the fact that the direct sum $b+z$ of the two cycles $b$ and $z$ splits, that there exists a cycle of order $n(b)$ between $q$ and $b+z \leqq v$. Since $q \leqq u$, and since $u$ is weakly closed in $v$, there exists a cycle $d$ of order $n(b)$ between $q$ and $u$. Since $qz = 0$, and since the direct sum $d+z$ of the two cycles $d$ and $z$ splits by hypothesis, it follows from Theorem I.3.5 that there exists a cycle of order $n(d) = n(b)$ between $p$ and $d+z \leqq u+z$; and thus it has been shown that $u+z$ is weakly closed in $v$ too.

If the part $r$ of the element $v \leqq w$ is weakly closed in $v$, then denote by $R$ the set of all the elements $s$ between $r$ and $v$ such that $s$ is weakly closed in $v$ and such that $s$ is the direct sum of $r$ and of a finite or infinite number of cycles. If $x$ and $y$ are two elements in $R$, then $x$ is said to be better than $y$, if $x$ is the direct sum of $y$ and of a finite or infinite number of cycles. From the remarks in the first paragraph of this proof it may be inferred that there exists a best element in $R$; and it is an immediate consequence of the results of the second paragraph of the proof that $v$ itself is the only best element in $R$ so that $v$ is the direct sum of $u$ and of a finite or infinite number of cycles.

If the element $w$ satisfies condition (i) of Theorem I.5.1, then it follows from Theorem I.2.1 that there exists one and only one part $w_n$ of $w$ such that the set of subcycles of $w_n$ is just the set of subcycles of $w$ with an order not exceeding $n$. Every finite sum of subcycles of $w$ is contained in almost every $w_n$; and Theorem I.5.1 may be applied on the $w_n$.

## PART II. THE ANALYTIC THEORY

An abelian operator group may be termed a primary abelian operator group, if the system of its admissible subgroups meets the requirements

imposed in the first part. Not only do abelian groups of prime power order and the abelian operator groups underlying projective geometry belong into this class, but it is even possible to develop a theory of primary abelian operator groups which is fully comparable to both projective geometry and the theory of finite abelian groups. For example, the duality between group and character group may be proved, a fact that specializes, in the case of projective geometry, to the duality between the point space and the hyperplane space and which thus contains the theory of systems of linear equations. Further examples are extensions of the fundamental theorem of projectivity and of the theorem of Pappus.

For our purposes it does not suffice to characterize the primary abelian operator groups as operator groups with specific properties. We have to solve the problem of determining those sets of subgroups of an abelian group which are the systems of all the admissible subgroups of a primary abelian operator group. A set $L$ of subgroups of the abelian group $G$ may be proved to be the system of all the admissible subgroups of $G$ for a suitable set of operators, if $L$ satisfies the following conditions: (a) $L$ contains sums and cross-cuts of its subsets. (b) If the subgroup $Z$ in $L$ is the smallest subgroup in $L$ containing a given element $z$, then the subgroups in $L$ that are part of $Z$ form a finite ordered set. (c) If a subgroup $Z$ in $L$ contains just $n$ subgroups in $L$ and if the subgroups in $L$ that are part of $Z$ form an ordered set, then there exist at least three independent subgroups of this kind in $L$. Under the same hypotheses we may prove that every projectivity of $L$ is induced by an isomorphism of the underlying group $G$. It seems noteworthy that both these theorems are obtained as special cases from one and the same construction.

1. **Construction of endomorphisms and isomorphisms.** The composition of the elements in commutative groups $G$ will be written as addition: $x+y$. A *linear transformation*[12] of $G$ into the commutative group $H$ is a function $\mathfrak{f}$ which maps every element $g$ in $G$ upon a uniquely determined element $g^{\mathfrak{f}}$ in $H$ such that $(g\pm h)^{\mathfrak{f}}=g^{\mathfrak{f}}\pm h^{\mathfrak{f}}$. Linear transformations of $G$ into $G$ are termed *endomorphisms*[13] *of* $G$; and these shall be written usually as multipliers, that is, the endomorphism $f$ of $G$ maps the element $g$ in $G$ upon the element $gf$ in $G$.

If $E$ is a set of endomorphisms of $G$, $S$ is a subset of $G$, then $SE$ is the set of all the elements $se$ for $s$ in $S$, $e$ in $E$; and the subset of $G$ is *$E$-admissible*, if $SE\leqq S$. The system of all the $E$-admissible subgroups of $G$ shall be denoted by $D(G; E)$. It is one of the objects of this section to determine all the systems $D(G; E)$ meeting certain requirements.

If $L$ is a set of subgroups of $G$, then the endomorphism $e$ of $G$ is *$L$-admissible*, if $Se\leqq S$ for every subgroup $S$ in $L$; and the set $K(G; L)$ of all the $L$-admissible endomorphisms of $G$ is a ring, provided addition and multiplica-

(12) Often termed "homomorphism."

(13) Often called "auto-homomorphism," "(proper or improper) automorphism," and so on.

tion are defined as customary. If in particular $L=D(G; E)$ for some system $E$ of endomorphisms of $G$, then $E \leqq K(G; L)$ and $L=D(G; K(G; L))$, though in general it may happen that $L<D(G; K)$.

The system $L$ of subgroups of $G$ shall be termed a *ring of subgroups*, if $L$ contains 0, $G$ and the cross-cuts and the sums (=join-groups) of each of its subsets. It is well known that rings of subgroups are Dedekind sets; and their importance for us lies in the fact that the sets $D(G; E)$ are rings of subgroups.

If $L$ is a ring of subgroups of the commutative group $G$, and if $X$ is a subset of $G$, then the cross-cut of all the subgroups in $L$ which contain $X$ is a subgroup in $L$; and we call this subgroup the $L$-subgroup $XL$ of $G$ or the *$L$-subgroup generated by $X$*. If $Z$ is an *$L$-subgroup* of $G$ such that the $L$-subgroups contained in $Z$ form a cycle (in the meaning of §I.2), then $Z$ is called a *cycle* in $L$; if the $L$-subgroup $Z$ is a cycle different from 0 in $L$, then $Z$ contains elements which are not contained in any proper $L$-subgroup of $Z$. If $z$ is such an element in $Z$, then $Z=zL$ so that we may say that cycles are cyclic. Since in general not every cyclic subgroup is a cycle, we define: The ring $L$ of subgroups of $G$ is *primary*, if every cyclic subgroup $gL$ in $L$ is a cycle in $L$.

If $S$ and $T<S$ are $L$-subgroups of $G$, then the $L$-subgroups $X$ between $T$ and $S$ define the $L$-subgroups $X/T$ of $S/T$. If $L$ is a primary ring of subgroups of $G$, then the $L$-subgroups of $S/T$ form a primary ring of subgroups too.

If $L$ is a primary ring of subgroups of $G$, $Z$ a cycle in $L$, then either $Z=0$ or $Z$ contains a uniquely determined subcycle $Z^*$ of order 1 (in $L$), a notation which we shall use occasionally.

If $g$ is an element in $G$, $L$ a primary ring of subgroups of $G$, then $gL$ is a cycle; and thus we may define the *$L$-order of $g$* by the equation $n(g)=n(gL)$, the order of the cycle $gL$ in $L$. It is an immediate consequence of Theorem I.2.1 that *the order of the element $g$ in $G$ does not exceed $n$, if $g$ is the sum of elements in $G$ whose orders do not exceed $n$.*

If $x$ and $y$ are two elements of $L$-order 1, then either $xL=yL$ or else the cross-cut of $xL$ and $yL$ is 0. In the latter case $x+y$ is not contained in $xL$ and not in $yL$ so that $xL+yL$ contains at least three subgroups of order 1. From this remark one infers readily that $G$ is primary in the Dedekind set $L$ (using the definition of §I.3), if $L$ is a primary ring of subgroups of $G$ [14].

We note finally that the elements $x, y, \cdots$ are termed ($L$-) *independent*, if the subgroups $xL, yL, \cdots$ are independent elements of the Dedekind set $L$ (that is, if the cross-cut of $xL$ and of the sum $yL+\cdots$ is 0 and so on).

The following general theorem contains as special cases both the existence of the coordinates and the existence of the semi-linear transformations of a projective geometry.

[14] Whether or not a ring of subgroups of an abelian group, satisfying the conditions of Theorem I.3.7 is a primary ring as defined in this section, seems to be an open problem.

THEOREM II.1.1. *If $L$ is a primary ring of subgroups of the abelian group $G$, if $J$ is a primary ring of subgroups of the abelian group $H$, if $L$ either does not contain any cycle of order $n$ or at least three independent ones, if $\mathfrak{p}$ is a projectivity of $L$ upon $J$, if $g$ is an element in $G$ and $h$ an element in $(gL)^{\mathfrak{p}}$, then there exists a linear transformation $\mathfrak{q}$ of $G$ into $H$ such that*

(i) $g^{\mathfrak{q}}=h$,

(ii) $x^{\mathfrak{q}}$ *is for every $x$ in $G$ an element in $(xL)^{\mathfrak{p}}$,*

(iii) $n(x)-n(x^{\mathfrak{q}})=n(g)-n(h)$ *for* $n(g)-n(h)\leqq n(x)$ *and* $x^{\mathfrak{q}}=0$ *for* $n(x)<n(g)-n(h)$.

**Proof**([15]). We note first that $\mathfrak{p}$ maps cycles in $L$ upon cycles in $J$ and that $\mathfrak{p}$ preserves both order of cycles and independence of subgroups. In particular we have $0=0^{\mathfrak{p}}$ and $H=G^{\mathfrak{p}}$. If $X$ is any subset of $G$, then it will prove convenient to put $p(X)=(XL)^{\mathfrak{p}}$.

(II.1.1.1) *If $x$ and $y$ are two independent elements in $G$ such that* $0<n(x)\leqq n(y)$, *then $x$ and $y-x$ are independent,* $n(y-x)=n(y)$ *and the order of the cross-cut of $yL$ and $(y-x)L$ is* $n(y)-n(x)$.

From the hypothesis it follows that $xL+yL$ is the direct sum of $xL$ and $yL$; and it is obvious that it equals $xL+(y-x)L=yL+(y-x)L$. It is a consequence of Theorem I.2.1 that the order of $y-x$ does not exceed $n(y)$. Since $yL$ and $(xL+yL)/(xL)$ are isomorphic, it follows that $(y-x)L$ is, modulo its cross-cut with $xL$, a cycle of order $n(y)$; and this shows that $n(y-x)=n(y)$ and that $y-x$ and $x$ are independent. Since $xL$ and $(xL+yL)/(yL)$ are isomorphic, $(y-x)L$ is, modulo its cross-cut with $yL$, a cycle of order $n(x)$; and the order of the cross-cut of $yL$ and $(y-x)L$ is therefore $n(y-x)-n(x)=n(y)-n(x)$.

(II.1.1.2) *If $x$ and $y$ are two independent elements in $G$ such that* $0<n(x)\leqq n(y)$, *and if $t$ is an element in $p(y)$, then there exists one and only one element $f(x, t; y)$ in $p(x)$ such that $f(x, t; y)\equiv t$ modulo $p(x-y)$. (Note that this statement holds trivially true for $x=0$ in which case $f(x, t; y)=0$.)*

The cross-cut of $p(x)$ and $p(x-y)$ is 0, since the cross-cut of $xL$ and $(x-y)L$ is 0 by (II.1.1.1); and consequently there exists at most one solution of our congruence, since the difference of any two solutions would be an element in the cross-cut of $p(x)$ and $p(x-y)$.—Since $xL+yL=xL+(x-y)L$, it follows that $p(x)+p(y)=p(x)+p(x-y)$; and since $t$ is an element in $p(x)+p(y)$, and $J$ a ring of subgroups, it follows that $t=r+s$ for $r$ in $p(x)$, $s$ in $p(x-y)$ or $r\equiv t$ mod $p(x-y)$ so that $r=f(x, t; y)$ is the required solution of our congruence.

---

([15]) The method used in this proof is an adaptation and extension of a method employed by us previously in proving a similar theorem; cf. R. Baer, American Journal of Mathematics, vol. 61 (1938), pp. 1–44, in particular Footnote 10.

(II.1.1.3) *If $x$ and $y$ are independent elements in $G$ such that $n(x) \leqq n(y)$, and if $t$ is an element in $p(y)$, then $f(x, t; y) = 0$ for $n(x) \leqq n(y) - n(t)$ and $n(f(x, t; y)) = n(x) - (n(y) - n(t))$ for $n(y) - n(t) \leqq n(x)$.*

The order of the cross-cut of $p(y)$ and $p(y-x)$ is $n(y)-n(x)$, since this is —by (II.1.1.1)—the order of the cross-cut of $yL$ and $(y-x)L$. Thus $t$ is an element in this cross-cut and therefore in $p(y-x)$, if $n(t) \leqq n(y)-n(x)$. But if $t$ is in $p(y-x)$, then $f(x, t; y) = 0$ by (II.1.1.2).—It follows from the definition of $f(x, t; y)$ that $tJ+p(x-y) = f(x, t; y)\ J+p(x-y) = d$. Hence $f(x, t; y) = 0$ implies that $t$ is contained in $p(x-y)$ and that therefore $n(t) \leqq n(y)-n(x)$. Thus $f(x, t; y) \neq 0$, if $n(y)-n(x) < n(t)$. Since $xL$ and $(x-y)L$ are independent, so are $p(x)$ and $p(x-y)$; and since $f(x, t; y)$ is an element not 0 in $p(x)$, $f(x, t; y)$ and $p(x-y)$ are independent, so that $n(f(x, t; y)) = n(d/p(x-y))$. But $d/p(x-y)$ is isomorphic to $tJ$ modulo its cross-cut with $p(x-y)$; and this cross-cut equals the cross-cut of $p(y)$ and $p(x-y)$, since $t$ is in $p(y)$, but not in $p(x-y)$. Thus it follows finally from (II.1.1.1) that $n(f, t; y)) = n(t) - (n(y) - n(x))$, as was to be shown.

(II.1.1.4) *If $x, y, z$ are independent elements in $G$ such that $n(x) \leqq n(y) \leqq n(z)$, then $(z-x)L$ is the cross-cut of $zL+xL$ and $(z-y)L+(y-x)L$.*

Clearly $(z-x)L$ is contained in the cross-cut $C$ of $zL+xL$ and $(z-y)L+(y-x)L$.—It is a consequence of (II.1.1.1) that $zL+xL$ is the direct sum of $xL$ and $(z-x)L$; and $(z-x)L < C$ is therefore equivalent to dependence of $xL$ and $C$. But this is impossible, since the cross-cut of $xL$ and $(y-x)L + (z-y)L$ is 0 as a consequence of (II.1.1.1) and our hypotheses; and thus $C = (x-z)L$.

(II.1.1.5) *If $x, y, z$ are three independent elements in $G$ such that $n(x) \leqq n(y) \leqq n(z)$, and if $t$ is an element in $p(z)$, then*

$$f(x, t; z) = f(x, f(y, t; z); y).$$

Since $f(x, f(y, t; z); y) - t = f(x, f(y, t; z); y) - f(y, t; z) + f(y, t; z) - t$ is an element in the cross-cut of $p(xL+zL)$ and $p((x-y)L+(y-z)L)$, and since this cross-cut is $p(x-z)$ by (II.1.1.4), it follows that the element $f(x, f(y, t; z); y)$ is contained in $p(x)$ and satisfies $f(x, f(y, t; z); y) \equiv t \bmod p(x-z)$. But it follows from (II.1.1.2) that $f(x, t; z)$ is the only element meeting these requirements.

(II.1.1.6) *If $x, y, z$ are elements in $G$ such that $xL+yL$ and $zL$ are independent and such that $n(x) \leqq n(y) \leqq n(z)$, and if $t$ is in $p(z)$, then*

$$f(x + y, t; z) = f(x, t; z) + f(y, t; z).$$

The proof of this statement will be effected in three steps.

A. $x$ and $y$ are independent.

In this case the three elements $x$, $y$, $z$ are independent. Then it follows from (II.1.1.1) that $y$ and $z-y$ are independent, that $n(z)=n(z-y)$ so that $(z-y)L$ and $xL+yL$ are independent too. Likewise $y-x$ and $x$ are independent, $n(y)=n(y-x)$ so that the three elements $x$, $y-x$, $z-y$ are independent and satisfy $n(x)\leqq n(y-x)\leqq n(z-y)$. Hence it follows from (II.1.1.4) that the cross-cut of $xL+(z-y)L$ and $(z-x)L+yL=(x-y-x)L+(z-y-(x-y))L$ is just $(z-y-x)L$. Thus the element $v-t=(f(x, t; z)+f(y, t; z))-t$ is contained in $p(x+y-z)$, since it is contained in the cross-cut of $p(xL+(y-z)L)$ and $p(yL+(x-z)L)$. But $v=(v-t)+t$ is contained in the cross-cut $p(x+y)$ of $p(xL+yL)$ and $p((x+y-z)L+zL)=p((x+y)L+zL)$. Thus $v$ has been shown to be an element in $p(x+y)$ such that $v\equiv t \bmod p(x+y-z)$; and this proves the required identity, since $f(x+y, t; z)$ is by (II.1.1.2) the only element satisfying these conditions.

B. $x=-y$.

We may assume $x\neq 0$, since $f(0, t; z)=0$. Then $xL+zL$ is the direct sum of $xL=yL$ and $zL$. Since there exist at least three independent elements of order $n(z)$ in $G$, we may infer from Corollary I.3.4 that there exists an element $v$ of order $n(z)$ in $G$ such that $x=-y$, $v$, $z$ are three independent elements. It is a consequence of (II.1.1.1) that $y$ and $v+x$ are independent elements too, $n(v)=n(v+x)$. Hence it follows from A that

$$\begin{aligned} f(v, t; z) &= f(v+x+y, t; z) = f(v+x, t; z)+f(y, t; z) \\ &= f(v, t; z)+f(x, t; z)+f(y, t; z) \end{aligned}$$

or

$$0 = f(x, t; z)+f(y, t; z).$$

C. $x$ and $y$ are not independent.

We may assume that neither $x$ nor $y$ is 0, since otherwise nothing need be proved. Thus $xL$ and $yL$ are dependent cycles different from 0 so that they have the same subcycle of order 1: $c^*=(xL)^*=(yL)^*$. Since both $z$, $x$ and $z$, $y$ are pairs of independent elements, it follows that $(zL)^*+c^*$ contains every subcycle of order 1 of $xL+zL$ and of $yL+zL$.

If the three elements $x+y$, $y$, $z$ are independent, then $x+y$, $-y$, $z$ are independent too; and it follows from A and B that

$$\begin{aligned} f(x, t; z) &= f(x+y-y, t; z) = f(x+y, t; z)+f(-y, t; z) \\ &= f(x+y, t; z)-f(y, t; z). \end{aligned}$$

Thus we need only handle the case where $x+y\neq 0$ and $x+y$ and $y$ are dependent so that as before $((x+y)L)^*=c^*$. As under B there exists an element $v$ in $G$ such that $n(v)=n(z)$ and such that $v$ and $c^*+zL$ are independent. Then the triplets of elements $x$, $v$, $z$ and $x+y$, $v$, $z$ are triplets of independent elements whose orders do not exceed $n(z)$. Since $c^*$ is the only subcycle of order 1, contained in both $xL+vL$ and $yL+zL$, and since $x$ and $v+x$ are independent, it follows that $y$, $v+x$, $z$ is another triplet of independent elements

whose orders do not exceed $n(z)$. Thus it follows from A that $f(v, t; z)+f(x+y, t; z)=f(x+y+v, t; z)=f(x+v, t; z)+f(y, t; z)=f(v, t; z)+f(x, t; z)+f(y, t; z)$, completing the proof of the identity (II.1.1.6).

(II.1.1.7) *If $x$ and $z$ are two independent elements such that $n(x)\leqq n(z)$, and if $s$ is an element in $p(x)$, then there exists an element $t$ in $p(z)$ such that $s=f(x, t; z)$.*

Since $p(xL+zL)=p((x-z)L+zL)=p(x-z)+p(z)$, and since $s$ is an element in $p(xL+zL)$, there exist elements $r$, $t$ in $p(x-z)$ and $p(z)$, respectively, such that $s=r+t$. Then $s$ is an element in $p(x)$ such that $s\equiv t \bmod p(x-z)$; and since $t$ is in $p(z)$, it follows from (II.1.1.2) that $s=f(x, t; z)$.

We denote by $G_n$ the set of all those elements in $G$ whose $L$-order does not exceed $n$. It has been pointed out at the beginning of this section that $G_n$ is a subgroup in $L$. The set $H_n$ of all the elements in $H$ whose $J$-order does not exceed $n$ is likewise a $J$-subgroup of $H$.

(II.1.1.8) *If $z$ is an element of order $n$ in $G$, and if $t$ is in $p(z)$, then there exists one and only one linear transformation $\mathfrak{f}$ of $G_n$ into $H_n$ such that $z^{\mathfrak{f}}=t$, $x^{\mathfrak{f}}$ is in $p(x)$ for every $x$ in $G_n$, $n(x^{\mathfrak{f}})-n(x)=n(t)-n$ for $n-n(t)\leqq n(x)$, but $x^{\mathfrak{f}}=0$ for $n(x)\leqq n-n(t)$.*

There exist by the hypotheses of Theorem II.1.1 two elements $x$, $y$ of order $n$ such that $x$, $y$, $z$ are three independent elements. We put $r=f(x, t; z)$ and $s=f(y, t; z)$. Since $t$ is an element in $p(z)$ such that $t\equiv r \bmod p(z-x)$, it follows from $n(x)=n$ and (II.1.1.2) that $t=f(z, r; x)$ and likewise that $t=f(z, s; y)$. Applying (II.1.1.5) we find that $f(x, t; z)=f(x, f(y, t; z); y)=f(x, s; y)$ and likewise $f(y, t; z)=f(y, r; x)$. It is a consequence of (II.1.1.3) that $n(r)=n(s)=n(t)$.

Any element $v\neq 0$ in $G_n$ belongs to one and only one of the following three classes.

*Class* 1. $v$ is independent of each of the three subgroups $xL+yL$, $yL+zL$ and $zL+xL$.

*Class* 2. $v$ is independent of two of the three subgroups $xL+yL$, $yL+zL$, $zL+xL$ and depends on the third one; and $v$ is independent of each of the three subgroups $xL$, $yL$, $zL$.

*Class* 3. $v$ is independent of one and only one of the three subgroups $xL+yL$, $yL+zL$, $zL+xL$; and $v$ is dependent of one and only one of the subgroups $xL$, $yL$, $zL$. (Thus dependence of $v$ and $z$ would imply independence of $vL$ and $xL+yL$.) We have to prove that these three classes exhaust all the possibilities. If $v$ is independent of $xL+yL$, then $v$ is independent of both $x$ and $y$. If $v$ is independent of two of the three subgroups $xL+yL$, $yL+zL$ and $zL+xL$, then $v$ is therefore independent of each of the elements $x$, $y$, $z$.— If $v$ depends on both $xL+yL$ and $yL+zL$, then $(vL)^*$ is contained in the cross-cut $yL$ of these two subgroups so that $v$ and $y$ are dependent. But then $v$ is certainly independent of $xL+zL$.

It follows from (II.1.1.2) and this trichotomy that of the three functions $f(u, r; x)$, $f(u, s; y)$ and $f(u, t; z)$ at least two are defined for $u=v$; and it follows from (II.1.1.5) and the properties of $r$, $s$, $t$ that those of these functions which are defined for $u=v$ have the same value $v^f$ for $u=v$. If we put $0^f=0$, then the function $f$ is defined for all the elements in $G_n$; and it follows from (II.1.1.2) and (II.1.1.3) that $v^f$ is a uniquely determined element in $p(v)$ for every $v$ in $G_n$; and that $v^f=0$ for $n(v)\leqq n-n(t)$, $n(v^f)-n(v)=n(t)-n$ for $n-n(t)\leqq n(v)$.

If $v$ and $w$ are any two elements (not both 0) in $G_n$, then at least one of the elements $x$, $y$, $z$ is by Corollary I.3.4 independent of the subgroup $vL+wL$. If, for example, $x$ and $vL+wL$ are independent, then $x$ and each of the three elements $v$, $v+w$, $w$ are independent so that $f(v, r; x)$, $f(v+w, r; x)$ and $f(w, r; x)$ are well determined elements; and since the orders of these elements do not exceed the order $n$ of $x$, it follows from (II.1.1.6) that $(v+w)^f=f(v+w, r; x)=f(v, r; x)+f(w, r; x)=v^f+w^f$; and thus $f$ is a linear transformation meeting all the requirements.

If $g$ is any linear transformation which meets the requirements of (II.1.1.8), and if $v$ and $w$ are two independent elements in $G_n$, $n=n(w)$, then $v^g$ is an element in $p(v)$ such that $v^g\equiv w^g \bmod p(v-w)$, since $v^g-w^g=(v-w)^g$ is an element in $p(v-w)$. If $x$, $y$, $z$ are the three elements used in the construction of $f$, then $x^g=f(x, z^g; z)=f(x, t; z)=r$, $y^g=s$, $z^g=t$—by (II.1.1.2). If $v$ is any element in $G_n$, then $v$ is 0 or independent of at least one of the elements $x$, $y$, $z$; and if $v$ and $x$ are independent, then it follows from (II.1.1.2) that $v^g=f(v, r; x)=v^f$ so that $f=g$.

During the remainder of the proof it will be convenient to term a linear transformation $f$ of $G_n$ into $H_n$ *permissible*, if $x^f$ is for every element in $G_n$ an element in $p(x)$, if $S^f$ is a $J$-subgroup of $H_n$ for every $L$-subgroup $S$ of $G_n$, and if there exists an integer $m\geqq 0$ such that $x^f=0$ for $n(x)\leqq m$ and $n(x)-n(x^f)=m$ for $m\leqq n(x)$.

(II.1.1.9) *Every permissible linear transformation of $G_n$ into $H_n$ is induced by a permissible linear transformation of $G_{n+1}$ into $H_{n+1}$.*

If—as we may assume without loss in generality—$G_n<G_{n+1}$, then there exist at least three independent elements of order $n+1$ in $G$. Let $x$, $y$ be any pair of independent elements of order $n+1$ in $G$, let $z$ be an element of order $n$ in $xL$ and let $f$ be a permissible linear transformation of $G_n$ into $H_n$. Since $z$ and $y$ are independent, (II.1.1.7) implies the existence of an element $t$ in $p(y)$ such that $z^f=f(z, t; y)$. There exists by (II.1.1.8) one and only one permissible linear transformation $g$ of $G_{n+1}$ into $H_{n+1}$ such that $y^g=t$ (put $m=n+1-n(t)$); and as shown in the last paragraph of the proof of (II.1.1.8) we have $z^g=f(z, t; y)=z^f$. Since $g$ induces a permissible linear transformation of $G_n$ into $H_n$, it follows from (II.1.1.8) that $g$ and $f$ coincide on $G_n$, as was to be shown.

Our theorem is now an immediate consequence of (II.1.1.8) and (II.1.1.9), provided the orders of the elements in $G$ are bounded, that is, $G=G_j$ for some integer $j$.—If the orders of the elements in $G$ are not bounded, then our theorem is again an immediate consequence of (II.1.1.8) and (II.1.1.9), if one remembers that every element in $G$ is contained in almost every $G_n$.

THEOREM II.1.2. *If $L$ is a primary ring of subgroups of the abelian group $G$ such that $L$ contains either no subcycle of order $n$ or at least three independent ones, then $L$ is the set $D(G; E)$ of all the $E$-admissible subgroups of $G$ where $E$ is the ring $K(G; L)$ of all the $L$-admissible endomorphisms of $G$.*

**Proof.** If $x$ is any element in $yL$ for $y$ an element in $G$, then there exists by Theorem II.1.1 an endomorphism $\boldsymbol{f}$ of $G$ such that $y^f=x$ and such that $g^f$ is in $gL$ for every $g$ in $G$. Clearly $\boldsymbol{f}$ belongs to $E$; and thus we have shown that $dL=dE$ for every $d$ in $G$, a fact that immediately implies $L=D(G; E)$.

THEOREM II.1.3. *If $L$ is a primary ring of subgroups of the abelian group $G$ such that $L$ contains either no cycles of order $n$ or at least three independent ones*[16], *and if $J$ is a primary ring of subgroups of the abelian group $H$, then every projectivity of $L$ upon $J$ is induced by an isomorphism of $G$ upon the whole group $H$.*

**Proof.** If $\boldsymbol{p}$ is a projectivity of $L$ upon $J$, and if $g$ is an element not 0 in $G$, then $gL$ and $(gL)^p$ are cycles of equal order and there exists therefore an element $h$ such that $(gL)^p=hJ$. Since $n(g)=n(h)$, there exists by Theorem II.1.1 a linear transformation $\boldsymbol{q}$ of $G$ into $H$ with the following properties: $g^q=h$, $x^q$ is for every element $x$ in $G$ an element in $(xL)^p$ such that $n(x)=n(x^q)$. Since therefore $x^q=0$ implies $n(x)=0$, that is, $x=0$, we see that $\boldsymbol{q}$ is an isomorphism such that $S^q\leqq S^p$ for every $L$-subgroup $S$ of $G$. If $u$ is any element not 0 in $S^p$, then $uJ$ is a cycle in $J$ and there exists one and only one subcycle $Z$ of $S$ such that $Z^p=uJ$ (and clearly $n(Z)=n(u)$). There exists in $G$ an element $y$ such that $y$ and $Z$ are independent and such that $n(y)=n(Z)=n(u)=n$. Since $yL$ and $Z$ are independent cycles of order $n$, so are $y^qJ$ and $uJ$; and $y^q-u$ and $u$ are independent elements of order $n$ too. There exists a cycle $T$ of order $n$ in $L$ such that $T^p=(y^q-u)J$ and one verifies that $yL+Z$ is the direct sum of $T$ and $Z$. Hence there exist uniquely determined elements $t$ and $z$ in $T$ and $Z$, respectively, such that $y=t+z$. Since $t^q$ is an element in $(y^q-u)J$, $z^q$ an element in $uJ$, $z^q-u=y^q-u-t^q$ is an element in the cross-cut of $uJ$ and $(y^q-u)J$. But this cross-cut is 0, since the cross-cut of $T$ and $Z$ is 0; and hence we have shown that $u=z^q$, $S^q=S^p$; and this completes the proof of the theorem.

(16) That this condition is indispensable for the validity of the theorem may be seen from simple examples like the groups of order a prime number (though here the theorem would hold true at least for auto-projectivities), or the direct sum of two abelian groups of order $p$ not 2 or 3 (where the theorem would not hold true for auto-projectivities); cf. R. Baer, loc. cit., p. 31.

2. **The ideals of the ring of endomorphisms.** If $L$ is a ring of subgroups of the abelian group $G$, then the endomorphism $e$ of $G$ is said to be $L$-admissible, if $Se \leqq S$ for every subgroup $S$ in $L$; and the set $E=K(G; L)$ of all the $L$-admissible endomorphisms of $G$ is a ring. If on the other hand a ring $E$ of endomorphisms of the abelian group $G$ has been given, then a subgroup $S$ of $G$ is termed *$E$-admissible*, if $Se \leqq S$ for every $e$ in $E$; and the set $L=D(G; E)$ of all the $E$-admissible subgroups of $G$ is a ring of subgroups. If this ring $D(G; E)$ of subgroups of $G$ is a primary ring of subgroups (as defined in §II.1), then we say for short that $G$ is *primary over $E$*; and it is the object of this section to characterize the rings $E$ with primary $D(G; E)$ by inner properties[17]; and to analyze the relations between the ideals in $E$ and the subgroups (in particular: the cycles) in $D(G; E)$. With this in mind we define: the *ring $E$ is primary if*

(i) *$E$ contains a universal unit* 1;

(ii) *every right-ideal in $E$ is two-sided*;

(iii) *the two-sided ideals not* 0 *in $E$ form a (finite or infinite) descending chain (of the order type of part of the negative integers).*

Such a primary ring $E$ contains one and only one greatest two-sided ideal different from $E$ which we shall denote by $P=P(E)$. We derive first some simple properties of $E$ and $P$.

(iv) *An element in $E$ possesses an inverse in $E$ if, and only if, it is not contained in $P$.*

**Proof.** If the element $z$ in $E$ is not in $P$, then the right-ideal $zE$ is not part of $P$ so that $zE=E$ by (ii). There exists therefore an element $z'$ in $E$ such that $zz'=1$. Since $z'$ cannot be in $P$, there exists likewise an element $z''$ such that $z'z''=1$; and thus we have $z=zz'z''=z''$ or $zz'=z'z=1$.—That elements in $P$ do not possess inverses, is obvious.

(v) *Every two-sided ideal not* 0 *in $E$ is a power of $P$ and a principal right-ideal; and* 0 *is the cross-cut of all the $P^i$.*

**Proof.** If $Q$ is a two-sided ideal different from 0 in $E$, then there exists one and only one greatest two-sided ideal $Q'$ which is a proper part of $Q$. There exists an element in $Q$ which is not contained in $Q'$; and if $q$ is any such

[17] G. Köthe, Mathematische Zeitschrift, vol. 39 (1934), pp. 31–44; T. Nakayama, Bulletin of the American Mathematical Society, vol. 44 (1938), pp. 719–723; K. Asano, Japanese Journal of Mathematics, vol. 15 (1939), pp. 231–253; vol. 16 (1939), pp. 1–36 have treated the following problem: Given an abstract ring $R$, to find the necessary and sufficient conditions such that every abelian group admitting the elements in $R$ as operators and satisfying the maximum and minimum condition for admissible subgroups is the direct sum of cyclic admissible subgroups and such that every admissible subgroup of a cyclic group over $R$ is itself cyclic Then it is possible to derive necessary conditions in a trivial fashion by the remark that $R$ is an abelian group over $R$. Clearly our problem is quite different, as we consider a pair: abelian group $G$, ring $E$ of endomorphisms of $G$; and ask for conditions on $G$, $E$ assuring a satisfactory theory for the group $G$ over $E$. Moreover we have to exclude completely those pairs $G$, $E$ where $G$ is cyclic over $E$ whereas we may omit the maximum and minimum condition for admissible subgroups.

element, then $qE$ is a right-ideal contained in $Q$, but not in $Q'$ so that $Q=qE$. Thus $QP=qEP=qP$. If $p$ is an element in $P$, then $qp$ is an element in $Q$. If $qp$ would not be an element in $Q'$, then $Q=qpE$ so that there would exist an element $r$ in $E$, satisfying $q=qpr$. Since $p$ is in $P$, $1-pr$ is not in $P$ and possesses therefore by (iv) an inverse $t$ so that $q=q(1-pr)t=0$, an impossibility which proves that $QP\leqq Q'$. If $x$ is an element in $Q'$, then $x$ is in $Q=qE$ so that there exists an element $y$ satisfying $x=qy$. If $y$ would not be in $P$, then there would exist—by (iv)—the inverse $z$ of $y$ so that $q=qyz=xz$ would be an element in $Q'$, an impossibility which proves that $Q'\leqq QP$. Thus we have shown that $QP=Q'$ of which equality (v) is an immediate consequence.

From (iv) one infers that $P=0$ if, and only if, $E$ is a (not necessarily commutative) field; and in general $E/P$ is a field. Thus it follows from (v) that either $P=0$ or $P$ is the one and only one prime ideal in $E$. Any element $p$ such that $P=pE$ shall be called a *prime* in $E$; and if $p$ is a prime in $E$, then every two-sided ideal different from 0 in $E$ has the form $P^i=p^iE$.

If the number of two-sided ideals in $E$ is finite, then there exists a smallest positive integer $m=m(E)$ such that $P^m=0$; and if the number of two-sided ideals in $E$ is infinite, then we put $m(E)=\infty$. In the first case we infer from (iv) that an element in $E$ is a zero-divisor if and only if, it is contained in $P$; and in the second case it may be shown that none of the elements in $E$ is a zero-divisor.

THEOREM II.2.1. *Suppose that the ring $E$ of endomorphisms of the abelian group $G$ is a primary ring.*

(1) *If $m(E)$ is finite, then the ring $D(G; E)$ of $E$-admissible subgroups of $G$ is a primary ring of subgroups and $m(E)$ is the maximum order of the cycles in $D(G; E)$.*

(2) *$D(G; E)$ is for infinite $m(E)$ a primary ring of subgroups of $G$ if, and only if, there exists to every element $g$ in $G$ an element $e\neq 0$ in $E$ such that $ge=0$; and if $D(G; E)$ is primary, then there exist cycles of every order in $D(G; E)$.*

(3) *The order of the cycle $xE$ in $D(G; E)$ is $i$ if, and only if, $P^i$ is the set of all the elements $e$ in $G$ such that $xe=0$.*

(4) *If $Z$ is a cycle of order $n$ in $D(G; E)$, and if $0\leqq i\leqq n$, then $ZP^i$ is the uniquely determined subcycle of order $n-i$ of $Z$ (in $D(G; E)$) and $P^i$ contains every element $e$ in $E$ such that $Ze\leqq ZP^i$.*

**Proof.** If $g$ is an element in $G$, $N(g)$ the set of all the elements $e$ in $E$ such that $ge=0$, then $N(g)$ is a right-ideal in $E$; and hence it follows from (ii) and (v) that either $N(g)=0$ or $N(g)=P^i$ for suitable $i<m(E)$. If $g\neq 0$, then $N(g)<E$ and therefore $N(g)\leqq P$. If $e$ is an element in $E$ such that $gE=(ge)E$ (for $g\neq 0$ in $G$), then there exists an element $e'$ in $E$ such that $g=gee'$ so that $1-ee'$ is in $N(g)$ and therefore in $P$; and this implies that neither $e$ nor $e'$ is in $P$. Applying (iv) it follows now immediately that

(*) $gE=(ge)E$ for $g\neq 0$ if, and only if, $e$ possesses an inverse in $E$.

If $S$ is an $E$-admissible subgroup of $gE$, then the set of all the elements $e$ in $E$ such that $ge$ is in $S$ is a right-ideal between $N(g)$ and $E$. If $J$ and $J'$ are right-ideals such that $N(g) \leqq J < J'$, then $gJ$ and $gJ'$ are $E$-admissible subgroups such that $gJ < gJ'$ as follows from (ii), (iv), (v) and (*). But now it is clear that $gE$ is a cycle of order $i$ in $D(G; E)$ if, and only if, $N(g) = P^i$. This proves (3). To derive (4) we need note now only that $PN(gP) = N(g)$.

From the fact that $gE$ is a cycle of order $i$ if, and only if, $N(g) = P^i$, we infer that $D(G; E)$ is primary if, and only if, either $m(E)$ is finite, or $m(E)$ is infinite, but there exists to every $g$ in $G$ an $e \neq 0$ in $E$ such that $ge = 0$.—If the maximum order of the cycles in the primary ring $D(G; E)$ of subgroups of $G$ is $k$, and if $e$ is an element in $P^k$, then it follows from (3) that $ge = 0$ for every $g$ in $G$; and this implies $e = 0$, since $e$ is an endomorphism of $G$. This completes the proof of (1) and (2).

THEOREM II.2.2. *If the ring $E$ of endomorphisms of the abelian group $G$ contains the identity element* 1, *if the ring $D(G; E)$ of $E$-admissible subgroups of $G$ is primary and contains at least two independent cycles of order $m$, but no cycles of higher order, then the ring $E$ is a primary ring and contains every $D(G; E)$-admissible endomorphism of $G$.*

**Proof.** If the $E$-admissible subgroup $uE$ of $G$ is a cycle of the maximum order $m$, and if the $E$-admissible subgroup $vE$ of $G$ is independent of $uE$, then $vE$ is a cycle of an order not exceeding $m$ and the smallest $E$-admissible subgroup $W$ of $G$ which contains $u$ and $v$ is the direct sum $W = uE + vE$ of these two cycles. The $E$-admissible subgroup $(u+v)E$ is a cycle of an order not exceeding $m$ in $D(G; E)$ and $W$ is the sum of the cycles $vE$ and $(u+v)E$. If $C$ is the cross-cut of $(u+v)E$ and $vE$, then $uE$, $W/vE$ and $(u+v)E/C$ are isomorphic cycles; and this implies that $C = 0$ and that $(u+v)E$ is a cycle of order $m$ which is independent of $vE$.—Suppose now that $e$ is an element in $E$ such that $ue = 0$. Then $(u+v)e = ve$ is an element in the cross-cut $C$ of $(u+v)E$ and $vE$; and thus it follows that $ue = 0$ implies $ve = 0$, if $uE$ is a cycle of order $m$, and if $uE$ and $vE$ are independent.

Assume now that $uE$ is a cycle of order $m$, that $e$ is an element in $E$ such that $ue = 0$ and that $g$ is some element in $E$. If $gE$ is independent of $uE$, then we have already shown that $ge = 0$. If the cross-cut of $uE$ and $gE$ is different from 0, then there exists—by our hypothesis—an element $s$ in $G$ such that $sE$ is a cycle of order $m$ which is independent of $uE$. Since $gE$ is a cycle, and since $uE$ and $gE$ have their uniquely determined subcycle of order 1 in common, it follows that $sE$ and $gE$ are independent. But we have shown already that $ue = 0$ implies $se = 0$ and that $se = 0$ implies $ge = 0$. Since $e$ is an endomorphism we have therefore proved:

If $uE$ is a cycle of order $m$, and if $e$ is an element in $E$ such that $ue = 0$, then $e = 0$.

If $0 \leqq i \leqq m$, then denote by $(uE)^i$ the uniquely determined subcycle of

order $m-i$ of the cycle $uE$ of order $m$ and by $P_i$ the set of all the elements $e$ in $E$ such that $ue$ is in $(uE)^i$. Clearly every $P_i$ is a right-ideal in $E=P_0$; and we have just proved that $P_m=0$. If $J$ is any right-ideal in $E$, then $uJ$ is an $E$-admissible subgroup of $G$ so that $uJ=(uE)^j=uP_j$ for some $j$; and since $ue=uf$ for $e$ and $f$ in $E$ implies $e=f$, it follows now that $J=P_j$ so that every right-ideal in $E$ is contained in the descending chain of the $m+1$ right-ideals $P_j$. If $e$ is any element in $E$, then $eP_i$ is a right-ideal in $E$ and is hence a $P_j$ too. But $P_i<P_j$ would imply $P_i<eP_i<eP_j=e^2P_i<\cdots$ contradicting the fact that there exists but a finite number of right-ideals between $P_i$ and $E$. Thus $eP_i\leqq P_i$ so that the $P_i$ are two-sided ideals and this shows the primarity of the ring $E$.

Denote now by $F$ the ring of all the $D(G; E)$-admissible endomorphisms of $G$. Then $D(G; E)=D(G; F)$; and thus it follows from what we have shown already that $E\leqq F$, that $F$ is a primary ring and that $uf=0$ implies $f=0$, if $uF=uE$ is a cycle of order $m$. If $w$ is any element in $F$, then $uw$ is in $uE$. Hence there exists an element $e$ in $E$ such that $uw=ue$; and this implies $e=w$, since $uE=uF$ is a cycle of order $m$. Thus $E=F$; and this completes the proof.

THEOREM II.2.3. *If the ring $E$ of endomorphisms of the abelian group $G$ contains every $D(G; E)$-admissible endomorphism of $G$, if $D(G; E)$ is a primary ring of subgroups of $G$ which contains at least two independent cycles of every order $n$, then $E$ is a primary ring with the following property*[18].

(vi) *If $P$ is the prime ideal of $E$, if $e_i$ is an element in $P^i$ for $i=0, 1, 2, \cdots$, then there exists one and only one element $e$ in $E$ such that $e-e_0-e_1-\cdots-e_i$ is an element in $P^{i+1}$ (for every $i$).*

**Proof.** We denote by $G(n)$ the smallest $E$-admissible subgroup of $G$ which contains all the elements $x$ in $G$ such that $xE$ is a cycle of an order not exceeding $n$ (in $D(G; E)$); and we denote by $P(n)$ the set of all the elements $e$ in $E$ such that $G(n)e=0$. Clearly $P(n)$ is a two-sided ideal in $E$. If $x$ is any element in $G(n)$, then $x=x_1+\cdots+x_j$ where the $x_i$ are elements in $G$ such that the $E$-admissible subgroup $x_iE$ is a cycle of an order not exceeding $n$ in $D(G; E)$. Since $xE$ is a subcycle of the sum of the cycles $x_iE$, it follows from Theorem I.2.1 that the order of the cycle $xE$ does not exceed $n$ either; and thus we have shown that the order of the cycle $xE$ in $D(G; E)$ does not exceed $n$ if, and only if, $x$ is in $G(n)$.

Since every element $x$ in $G$ is contained in some $G(n)$, it follows that the cross-cut of the descending chain of two-sided ideals $P(n)$ is 0. If $e_i$ is for $i=0, 1, 2, \cdots$ an element in $P(i)$, and if $a_i=e_0+\cdots+e_i$, then all the endomorphisms $a_n, a_{n+1}, \cdots$ induce the same endomorphism $b_n$ in $G(n)$. Since every element in $G$ is contained in some $G(n)$, there exists therefore one (and only one) endomorphism $e$ of $G$ which coincides with $b_n$ on $G(n)$ (for every $n$).

---

[18] Because of this property (vi) the ring $E$ may be termed a $P$-adic ring.

Since every $a_n$ is $D(G; E)$-admissible, so is $e$; and hence $e$ is an element in $E$ such that $e-a_i$ is in $P(i+1)$.

Suppose that $s$ is any endomorphism in $E$. If $s\neq 0$, then there exists a greatest $n$ such that $s$ is in $P(n)$ (so that $s$ is not in $P(n+1)$) since 0 is the cross-cut of the $P(i)$. Suppose that $t$ is some element in $P(n)$ (which may or may not be in $P(n+1)$). Clearly $E(h)=E/P(h)$ is a ring of endomorphisms of $G(h)$ such that $D(G(h); E(h))$ consists only of the $E$-admissible subgroups of $G(h)$. Thus it follows from Theorem II.2.2 that $E(h)$ is a primary ring of endomorphisms of $G(h)$ whose only right-ideals are by (v) the two-sided ideals $P(i)/P(h)=(P(1)/P(h))^i$ for $0\leqq i\leqq h$. Thus there exists an element $s_h$ in $E$ such that $t-ss_h$ is an element in $P(n+h)$ (for $h=1, 2, \cdots$). Hence $s(s_h-s_{h+1})$ is in $P(n+h)$; and since $s$ is in $P(n)$, but not in $P(n+1)$, it follows that $(P(n+h)+s)E(n+h)=P(n)/P(n+h)$ and that therefore $s_h-s_{h+1}=e_h$ is in $P(h)$. Hence it follows from what has been shown in the preceding paragraph of this proof that there exists one and only one endomorphism $e$ in $E$ such that $e-e_0-\cdots-e_i$ is in $P(i+1)$. Then $t-s(s_0-e)=t-ss_i+s(s_i-s_0-e)$ $=t-ss_i+s(e_0+\cdots+e_{i-1}-e)$ is the sum of two elements in $P(n+i)$ so that $t-s(s_0-e)$ is part of the cross-cut of the $P(n+i)$ and is therefore 0. Consequently $t=s(s_0-e)$; or $P(n)=sE$; and this shows that every right-ideal not 0 in $E$ is one of the two-sided ideals $P(n)$. Hence $E$ is a primary ring of endomorphisms of $G$; and that $E$ satisfies (vi) has been shown in the second paragraph of the proof.

THEOREM II.2.4. *If the ring $E$ of endomorphisms of the abelian group $G$ contains every $D(G; E)$-admissible endomorphism, if $D(G; E)$ is a primary ring of subgroups of $G$ which contains either no subcycle of order $n$ or at least two independent ones, then the following condition is necessary and sufficient for every left-ideal in $E$ to be two-sided.*

(vii) *If $U$ and $V$ are $E$-admissible subgroups of $G$ such that $V$ is the sum of $U$ and of a finite number of cycles in $D(G; E)$, and if there exists at most one cycle of order 1 in $V/U$, then $V/U$ is a cycle.*

**Proof.** If $P=P(E)=0$, then $E$ is a field and every cycle not 0 is of order 1 so that we may assume in the course of the proof that $P\neq 0$.—Suppose first that every ideal in $E$ is two-sided, and the $E$-admissible subgroups $U$ and $V$ meet the requirements of (vii). Then (vii) will be proved as soon as we have shown that there do not exist different cycles of equal order in $V/U$. We note first that the cycle $(U+x)E$ in $V/U$ is of order $n$—on account of the preceding theorems—if, and only if, the cross-cut of $U$ and $xE$ is exactly $xP^n$. If $(U+x)E$ and $(U+y)E$ are cycles of order $n$ in $V/U$, then $(U+x)P^{n-1}$ and $(U+y)P^{n-1}$ are cycles of order 1 in $V/U$ and hence it follows from the requirements on $V$ and $U$ enunciated in (vii) that $(U+x)P^{n-1}=(U+y)P^{n-1}$. If $p$ is any prime in $E$, then this implies the existence of an element $r$ in $E$ such that $U+xp^{n-1}=U+yp^{n-1}r$; and $r$ cannot be an element in $P$ since $xp^{n-1}$ is not

in $U$, though $yp^{n-1}P$ is contained in $U$. Since every left-ideal is assumed to be a right-ideal, there exists an element $s$ in $E$ such that $sp^{n-1}=p^{n-1}r$; and $s$ cannot be in $P$, since $p^{n-1}r$ is not in $P^n$. Since therefore $(x-ys)p^{n-1}=xp^{n-1}-yp^{n-1}r$ is an element in $U$, $((x-ys)E+U)/U$ is a cycle of an order not exceeding $n-1$. If we make now the induction hypothesis that there exists at most one subcycle of order $n-1$ of $V/U$, then it follows that $U+(x-ys)E$ is part of $U+yE$ so that $U+xE\leqq U+yE$; and consequently there exists at most one subcycle of order $n$ of $V/U$. Thus (vii) is a consequence of the fact that all the ideals in $E$ are two-sided.

Suppose now that (vii) is satisfied by $D(G; E)$, that $r$ is an element in $E$, though not in $P$, and that $p$ is a prime in $E$ (so that every right-ideal different from 0 in $E$ is of the form $p^iE$). If there exist cycles of order $n$ in $D(G; E)$, then there exist two independent cycles $xE$ and $yE$ of order $n$ in $D(G; E)$. If $U=(xp-ypr)E$ and $V=xE+yE$, then $U\leqq xP+yP$ so that $V/U$ is not a cycle, since $V/(xP+yP)$ is the direct sum of two cycles of order 1. Since the cross-cut of $U$ and $xE$ is null, it follows that $(U+xP^{n-1})/U$ is a cycle of order 1. Hence it follows from (vii) that there exists a cycle $(U+vE)/U$ of order 1 in $V/U$ which is different from $(U+xP^{n-1})/U$. Thus $v$ is not in $U$, but $vp$ is in $U$ and the cross-cut of $U+xP^{n-1}$ and $U+vE$ is exactly $U$. Furthermore there exist elements $s$, $t$ in $E$ such that $v=xs+yt$. If $t$ would be in $P$, then $t=pf$ for $f$ in $E$ and consequently (since $r$ is not in $P$ and (iv) may be applied)

$$\begin{aligned} v &= xs + ypf = xs + ypr\,r^{-1}f \\ &= x(s + pr^{-1}f) - (xp - ypr)r^{-1}f \\ &\equiv x(s + pr^{-1}f) \bmod U; \end{aligned}$$

and this is impossible, since it would imply $U+vE\leqq U+xE$. Thus $t$ is not in $P$. Since $vp$ is in $U$, there exists an element $g$ in $E$ such that $xsp+ytp=vp=(xp-ypr)g=xpg-yprg$; and from the independence of $xE$ and $yE$ we may infer $xsp=xpg$ and $ytp=yprg$. Since $t$ is not in $P$, we have $yE=ytE$ and hence $(ytp)E=yP=(yprg)E$ or $P=prgE$; and thus $g$ cannot be in $P$. Hence $xP=xpgE=xspE$ or $P=spE$ so that $s$ cannot be in $P$ either. Thus it follows from $xsp=xpg$ that $sp-pg$ is in $P^n$, since $n$ is the order of $xE$; and hence it follows from (iv) that $pg^{-1}\equiv s^{-1}p \bmod P^n$; and from $ytp=yprg$ we obtain likewise that $pr\equiv tpg^{-1}\equiv ts^{-1}p \bmod P^n$. Thus we have obtained the following intermediary result.

(*) If $r$ is in $E$ though not in $P$, if $p$ is a prime in $E$, and if there exist cycles of order $n$ in $D(G; E)$, then there exists an element $q(n)$ in $E$ such that $pr\equiv q(n)p \bmod P^n$.

If the orders of the cycles in $D(G; E)$ are bounded, and if $m$ is the maximum order of the cycles in $D(G; E)$, then $P^m=0$ and (*) implies $pr=q(m)p$.— If the orders of the cycles in $D(G; E)$ are not bounded, then it follows from (*) that $q(n)p\equiv q(n+1)p \bmod P^n$ so that $q(n)\equiv q(n+1) \bmod P^{n-1}$ for every $n$;

and hence it follows from Theorem II.2.3, (vi) that there exists one and only one element $q$ in $E$ such that $q \equiv q(n) \bmod P^{n-1}$ or $pr \equiv q(n)p \equiv qp \bmod P^n$ for every $n$. Since the cross-cut of the ideals $P^n$ is 0, it follows now that $pr = qp$; and thus we have shown

(**) If $r$ is in $E$ though not in $P$, if $p$ is a prime in $E$, then there exists an element $q$ in $E$ such that $pr = qp$.

Since every right-ideal different from 0 is a power of $P$ and of the form $p^iE$, every element not 0 in $E$ has the form $p^ir$ for $p$ a prime in $E$ and $r$ not in $P$. If $p^js$ is another element in this normal form, then there exist elements $q$, $t$ in $E$—by (**) and $sp^iE = p^iE$—such that $p^js\ p^ir = p^j\ p^i\ trs^{-1}\ s = p^iq\ p^js$ so that every left-ideal in $E$ is a right-ideal; and this completes the proof of our theorem.

It is a consequence of this theorem and the other theorems of this section, that by Theorem I.3.6 finite sums of cycles in the ring $D(G; E)$ are completely splitting, primary elements in a Dedekind set, if $E$ is a primary ring all of whose ideals are two-sided, and if there exist either no cycles of order $n$ in $D(G; E)$ or at least two independent ones.

If the ideals in the primary ring $E$ are two-sided, then it is readily verified that the subsets $GP^i$ of the group $G$ are $E$-admissible subgroups (do not only generate $E$-admissible subgroups); and on the basis of this remark one may prove by the customary arguments:

A([19]). *If $E$ is a primary ring of endomorphisms of the abelian group $G$ such that $m(E)$ is finite and such that all the ideals in $E$ are two-sided, then $G$ is a direct sum of cycles in $D(G; E)$.*

B([20]). *If the primary ring $E$ of endomorphisms of the abelian group $G$ contains every $D(G; E)$-admissible endomorphism of $G$, if every ideal in $E$ is two-sided, and if $D(G; E)$ is primary, then every $E$-admissible subgroup $S$ different from 0 of $G$ satisfying $S = SP$ is a direct summand of $G$ and is the direct sum of subgroups([21]) in $D(G; E)$ which contain one and only one cycle of order $n$ for every $n$.*

In order to show the independence of condition (vii) from the other conditions we construct an *example of a primary ring $E$ not all of whose ideals are two-sided.*

Let $F$ be a commutative field which possesses an isomorphism $v$ upon a proper subfield $F^v < F$. Consider the set $E$ of all the (ordered) pairs $(f, g)$ for $f$

([19]) See, for example, R. Baer, Compositio Mathematica, vol. 1 (1934), pp. 274–275. Note that this Theorem A is a special case of Theorem I.5.1 above.

([20]) See R. Baer, Bulletin of the American Mathematical Society, vol. 46 (1940), pp. 800–806.

([21]) H. Prüfer has introduced subgroups of this type into the study of primary abelian groups; in analogy to Prüfer's terminology they may be called "groups of type $P^\infty$" or "cycles of order $\infty$."

and $g$ in $F$. Two such pairs $(f, g)$ and $(f', g')$ define the same element in $E$ if, and only if, $f=f'$, $g=g'$; their sum is defined by $(f, g)+(f', g')=(f+f', g+g')$ and their product by $(f, g)(f', g')=(ff', f^v g'+gf')$. One verifies readily that $E$ is a ring with identity $1=(1, 0)$ and $0=(0, 0)$, that $(f, g)$ possesses an inverse in $E$ if, and only if, $f\neq 0$, and that therefore the only right-ideal different from 0 and $E$ is the set of all the elements $(0, f)$ for $f$ in $F$, since $(0, f)(g, 0)=(0, fg)$. This ideal $(0, F)$ is clearly a two-sided ideal whose square is 0 so that $E$ is a primary ring. A left-ideal is formed by all the elements $(0, f^v)$ for $f$ in $F$, as follows from the above formulas and the multiplicativity of $v$. Since $0<F^v<F$, this left-ideal is different from all the right-ideals(22).

If in the preceding construction we would choose $F$ as a finite field possessing an automorphism $v\neq 1$ (so that $F=F^v$), then $E$ would be *a finite, primary, noncommutative ring all of whose ideals are two-sided.*

**Application to the principles of projective geometry.** If $L$ is a primary ring of subgroups of the abelian group $G$ such that the orders of the cycles in $L$ do not exceed 1 (so that cycles not 0 are *points*) and such that there exist at least three independent cycles of order 1 in $L$, then it is a consequence of Theorem II.1.2 that $L$ is the ring of all the $E$-admissible subgroups of $G$ where $E$ is the ring of all the $L$-admissible endomorphisms of $G$; and it is a consequence of Theorem II.2.2 that the ring $E$ is a primary ring of endomorphisms of $G$. Since the maximum order of the cycles in $L$ is 1, it follows from Theorem II.2.1 and (iv) that $E$ is a (not necessarily commutative) field. But this implies immediately that Desargues' theorem is valid in the projective geometry represented by $L$. Since the possibility of representing the linear subspaces of a projective geometry by means of a ring of subgroups of an abelian group may be considered to be the essence of representations by means of homogeneous coordinates, we may state this result somewhat loosely as follows.

*A projective plane admits of a representation by means of homogeneous coordinates if, and only if, Desargues' theorem holds true in it.*

3. **The fundamental theorem of projectivity.** If $E$ is a ring of endomorphisms of the abelian group $G$, and if $\boldsymbol{f}$ is an isomorphism of $G$ upon the (whole) abelian group $H$, then there exists the inverse isomorphism $\boldsymbol{f}^{-1}$ of $\boldsymbol{f}$ which maps $H$ upon $G$; and mapping the endomorphism $e$ in $E$ upon $e^{\boldsymbol{f}}=\boldsymbol{f}^{-1}e\,\boldsymbol{f}$ constitutes an isomorphism of $E$ upon a ring of endomorphisms of $H$ which we call the isomorphism of $E$ induced by $\boldsymbol{f}$.

THEOREM II.3.1(23). *If $E^i$ is a primary ring of endomorphisms of the abelian group $G^i$ $(i=1, 2)$, if the ring $D(G^i, E^i)$ of the $E^i$-admissible subgroups of $G^i$ is primary and contains either no cycles of order $n$ or at least three independent ones,*

(22) There are many possibilities of generalizing this construction.

(23) This theorem asserts—in the terminology of projective geometry—that every projectivity is induced by a semi-linear transformation.

*if $E^i$ contains every $D(G^i, E^i)$-admissible endomorphism of $G^i$, and if $\mathfrak{p}$ is a projectivity of $D(G^1, E^1)$ upon $D(G^2, E^2)$, then there exists an isomorphism $\mathfrak{q}$ of $G^1$ upon $G^2$ which induces $\mathfrak{p}$ in $D(G^1, E^1)$ and which induces an isomorphism of $E^1$ upon $E^2$.*

The existence of an isomorphism $\mathfrak{q}$ of $G^1$ upon $G^2$ which induces $\mathfrak{p}$ in $D(G^1, E^1)$ is an immediate consequence of Theorem II.1.3. Furthermore we know that such an isomorphism $\mathfrak{q}$ induces an isomorphism of $E^1$ upon a ring $F$ of endomorphisms of $G^2$; and for reasons of symmetry it suffices to show that $F \leqq E^2$. Thus if $e$ is an endomorphism of $G^1$, $S$ an $E^2$-admissible subgroup, then $Se^{\mathfrak{q}} = (S^{\mathfrak{q}^{-1}}e)^{\mathfrak{q}} = (S^{\mathfrak{p}^{-1}}e)^{\mathfrak{p}} \leqq (S^{\mathfrak{p}^{-1}})^{\mathfrak{p}} = S$ so that $e^{\mathfrak{q}}$ is $D(G^2, E^2)$-admissible and therefore in $E^2$.

If in particular $G = G^1 = G^2$, $E = E^1 = E^2$, then $\mathfrak{p}$ is a projectivity of $D(G; E)$ (upon itself), $\mathfrak{q}$ an automorphism of $G$ and $\mathfrak{q}$ induces an automorphism in $E$. If $g$ is an element in $G$, $e$ an endomorphism in $E$, then $(ge)^{\mathfrak{q}} = ((g^{\mathfrak{q}})^{\mathfrak{q}^{-1}}e)^{\mathfrak{q}} = g^{\mathfrak{q}}e^{\mathfrak{q}}$; and it is easily verified that exactly those automorphisms of $G$ which induce an automorphism in $E$ induce a projectivity of $D(G; E)$ (upon itself). In analogy to the distinction between linear and quasi-linear transformations we say that the automorphism $\mathfrak{q}$ of $G$ is a *proper $E$-automorphism*[24], if $\mathfrak{q}$ induces the identity in $E$, that is, if $\mathfrak{q}$ commutes with all the endomorphisms in $E$.

We consider now—throughout this section—an abelian group $G$, a primary ring $E$ of endomorphisms of $G$ such that every left-ideal (as well as right-ideal) in $E$ is two-sided and such that the primary ring $D(G; E)$ of subgroups of $G$ is the sum of a finite number of cycles in $D(G; E)$. It is then a consequence of Theorem II.2.1, Theorem II.2.4—using the additional hypothesis that $G$ contains at least two independent cycles of maximum order $m = m(E)$—and Theorem I.3.7 that $G$ splits completely and is primary in the Dedekind set $D(G; E)$. Consequently $G$ is the direct sum of a finite number of cycles $Z_1, \cdots, Z_k$ in $D(G; E)$; and it follows from Lemma I.3.8 that there exists a cycle $Z$ in $D(G; E)$ which is not part of any proper partial sum of the $Z_i$; it is readily verified that this is equivalent to saying that $G = Z + \sum_{j \neq i} Z_j$ for every $i$.

If $G$ is the direct sum of the cycles $Z_{1i}$ and of the cycles $Z_{2i}$ in $D(G; E)$, then it follows from Corollary I.3.4 that the numbering may be effected in such a way that $n(Z_{1i}) = n(Z_{2i})$ for every $i$. If furthermore $Z_i$ is a cycle such that $G = Z_i + \sum_{j \neq h} Z_{ih}$ for every $j$, then our generalization of the fundamental theorem of projectivity may be stated as follows[25].

THEOREM II.3.2. *There exists one and only one projectivity $\mathfrak{p}$ of $D(G; E)$ which is induced by a proper $E$-automorphism of $G$ and which satisfies: $Z_{1j}^{\mathfrak{p}} = Z_{2j}$, $Z_1^{\mathfrak{p}} = Z_2$.*

---

[24] It is customary in the theory of abelian operator groups to admit only these "proper $E$-automorphisms" as automorphisms.

[25] If one takes into account Theorem II.3.3. below.

**Proof.** To prove the unicity of $\mathfrak{p}$ we consider a proper $E$-automorphism $\mathfrak{f}$ of $G$ which leaves $Z_1$ and every $Z_{1i}$ invariant. Since the $Z$'s are cycles in $D(G; E)$, there exists an element $z$ in $Z_1$ such that $Z_1 = zE$; and since $G$ is the direct sum of the $Z_{1i}$, there exist uniquely determined elements $z_i$ in $Z_{1i}$ such that $z = z_1 + \cdots + z_k$. From the choice of $z$ and $Z_1$ it follows immediately that $Z_{1i} = z_iE$. From the choice of $\mathfrak{f}$ it follows $Z_1 = z^fE$, $Z_{1i} = z_i^fE$; and there exist therefore elements $e$, $e_i$ in $E$ (though not in the prime ideal $P$ of $E$) such that $ze = z^f$, $z_ie_i = z_i^f$. But now it follows immediately that $z_ie = z_ie_i$ so that $g^f = ge$ for every $g$ in $G$, that is, $\mathfrak{f}$ induces the identity in $D(G; E)$; and this proves the unicity of the required projectivity.

To prove the existence of some projectivity meeting the requirements we note first that there exist elements $z_{ij}$ such that $Z_{ij} = z_{ij}E$ and such that $Z_i = (z_{i1} + \cdots + z_{ik})E$. Since $n(z_{1j}) = n(z_{2j})$ for every $j$, there exists one and only one proper $E$-automorphism $\mathfrak{q}$ such that $z_{1j}^q = z_{2j}$; and $\mathfrak{q}$ clearly induces a projectivity $\mathfrak{p}$ of $D(G; E)$ (upon itself) such that $Z_{1j}^p = Z_{2j}$, $Z_1^p = Z_2$.

The proper $E$-automorphism $\mathfrak{f}$ of $G$ shall be termed a *perspectivity of* $G$, if there exists an $E$-admissible direct summand $F$ of $G$ such that $G/F$ is a cycle and such that every element in $F$ is left invariant by $\mathfrak{f}$. That this definition[26] is not too narrow may be seen from the following fact.

*The projectivity $\mathfrak{p}$ of $D(G; E)$ (upon itself) is induced by a perspectivity of $G$, if there exists an $E$-admissible direct summand $T$ of $G$ such that $G/T$ is a cycle and such that every $E$-admissible subgroup of $T$ is left invariant by $\mathfrak{p}$, provided $G$ contains at least three independent elements of maximum order.*

**Proof.** It is a consequence of Theorem II.3.1 that $\mathfrak{p}$ is induced in $D(G; E)$ by some automorphism $\mathfrak{q}$ of $G$ which induces an automorphism of $E$. It is a consequence from our general hypotheses that $T$ possesses a basis $B$ and $B$ contains certainly two different elements of maximum order $m$ in $G$. If $t$ is an element of order $m$ in $B$, and if $b$ is an element not $t$ in $B$, then $t^q = te$ for $e$ in $E$ though not in $P$, $b^q = be'$, $(b+t)^q = (b+t)e''$ for $e'$, $e''$ in $E$. Consequently $te = te''$, $be' = be''$. Since $t$ is of order $m$, $P^m = 0$, we have $e = e''$, $b^q = be' = be'' = be$; and this implies $x^q = xe$ for every $x$ in $T$. Since $e$ is not in $P$, there exists an inverse $e^{-1}$ of $e$ in $E$. If we put $y^f = y^qe^{-1}$ for every $y$ in $G$, then $\mathfrak{f}$ and $\mathfrak{q}$ induce the same projectivity $\mathfrak{p}$ in $D(G; E)$, but $\mathfrak{f}$ is a perspectivity, since it leaves every element in $T$ invariant, and since $tv = t^{f^{-1}}v = (t^{f^{-1}}v)^f = tv^f$ and $P^m = 0$ imply $v = v^f$ for $v$ in $E$.

THEOREM II.3.3. *The group of proper $E$-automorphisms of $G$ is generated by the perspectivities of $G$.*

---

[26] It is readily verified that this definition and the customary definition—postulating a center apart from the "axis" we postulated—coincide in the case of ordinary projective geometry, provided one is able, as we are, to use Desargues' theorem.

**Proof**([27]). The proper $E$-automorphism $f$ of $G$ shall be termed *irreducible* (in the course of this proof), if there exists an $E$-admissible direct summand $T$ of $G$ with the following properties:

(i) Every element in $T$ is left invariant by $f$.

(ii) If $f$ is the product of the proper $E$-automorphisms $u$ and $v$, if the $E$-admissible direct summands $U$ and $V$ of $G$ both contain $T$, and if $u$ leaves the elements in $U$, $v$ the elements in $V$ invariant, then $U=T$ or $V=T$.

It is an obvious consequence of the maximum condition for $E$-admissible subgroups, that every proper $E$-automorphism of $G$ is the product of irreducible proper $E$-automorphisms of $G$; and thus all we have to prove is the following statement.

*A proper E-automorphism of G is a perspectivity if, and only if, it is irreducible.*

The irreducibility of perspectivities is a consequence of the fact that $S=G$, if $S$ is an $E$-admissible direct summand of $G$ such that there exists an $E$-admissible direct summand $T$ of $G$ satisfying $T<S$ and $G/T$ is a cycle.

Thus let us assume now that the proper $E$-automorphism $f$ of $G$ is irreducible. Then there exists an $E$-admissible direct summand $T$ of $G$ such that $f$, $T$ satisfy the above conditions (i), (ii). Since $T$ is a direct summand of $G$, there exists an element $b$ and an $E$-admissible subgroup $U$ of $G$ such that $G$ is the direct sum of $T$, $U$ and $bE$ and such that the orders of the elements in $U$ do not exceed $n(b)$.—If the elements $b$ and $b^f$ were independent modulo $T$, then there would exist an $E$-admissible subgroup $V$ of $G$ such that $G$ would be the direct sum of $T$, $V$, $bE$ and $b^fE$. Since $b$ and $b^f$ are of equal order, there exists one and only one proper $E$-automorphism $v$ of $G$ which leaves every element in $T+V$ invariant and which interchanges $b$ and $b^f$. This is impossible, since $v$ leaves every element in the direct summand $T+V+(b+b^f)E$ invariant, and since $fv^{-1}$ leaves every element in the direct summand $T+V+bE$ invariant. Thus it follows that $b$ and $b^f$ are dependent modulo $T$; and this implies that $G$ is the direct sum of $T$, $U$ and $b^fE$ too. Consequently there exists one and only one proper $E$-automorphism $u$ of $G$ which leaves every element in $T+U$ invariant and which maps $b$ upon $b^f$. Since $f$ is irreducible, and since $fu^{-1}$ leaves every element in $T+bE$ invariant, it follows that $T=T+U$ or $U=0$; and this implies that $f$ is a perspectivity.

If $D(G; E)$ contains at least three independent cycles of maximum order, then it follows from Theorem II.3.1 that every projectivity of $D(G; E)$ upon itself is induced by a proper $E$-automorphism of $G$ if, and only if, every automorphism of $E$ is an inner automorphism. Thus we see that projective geometry over the field of real numbers has—as far as the behaviour of projectivities is concerned—more in common with abelian groups of order a power of a prime than with projective geometry over the field of complex

([27]) It should be noted that this proof is slightly simpler and proves more than the customary proofs of the projective special case of this theorem.

numbers, since both the field of real numbers and the ring of integers modulo a power of a prime admit of the identity-automorphism only, whereas the field of complex numbers possesses an infinity of automorphisms.

4. **Duality and the theory of characters.** Throughout this section we make the following *assumptions*. $E$ is a primary ring of endomorphisms of the abelian group $G$; every ideal in $E$ is a two-sided ideal in $E$; $G$ is in the ring $D(G; E)$ of the $E$-admissible subgroups of $G$ the sum of a finite number of cycles; $D(G; E)$ contains[28] at least two independent cycles of maximum order $m$. We note the following consequences of these hypotheses (and Theorems II.2.1, II.2.4 and I.3.7): if $P$ is the prime ideal in $E$ (unless $E$ is a field and $P=0$), then $0=P^m<P^{m-1}$; if $S$ is an $E$-admissible subgroup of $G$, then $S$ is the direct sum of a finite number of cycles in $D(G; E)$ and $G/S$ is the direct sum of a finite number of cycles in $D(G/S; E)$.

*A character*[29] *of $G$ in $E$* is a single-valued function $f$ of the elements in $G$ with values in $E$ such that $f(ge+g'e')=f(g)e+f(g')e'$ for $g$, $g'$ in $G$ and $e$, $e'$ in $E$. If $f$ and $v$ are characters of $G$ in $E$, and if $e$ is an element in $E$, then $f(g)+v(g)$ and $ef(g)$ are characters of $G$ in $E$; and thus it follows that the set $Ch(G; E)$ of all the characters of $G$ in $E$ is an abelian group, admitting the elements in $E$ as left-operators. Characters and character group of $Ch(G; E)$ in $E$ are defined in a like manner, apart from certain obvious interchanges of right and left.

THEOREM II.4.1. (a) *$G$ is essentially the same as the group of characters of $Ch(G; E)$ in $E$.* (b) *$D(G; E)$ and $D(Ch(G; E); E)$ are duals of each other.*

**Proof.** If $g$ is an element in $G$, $f$ an element in $Ch(G; E)$, then we put $Q_g(f)=f(g)$. It is readily verified that $Q_g$ is for every $g$ in $G$ a character of $Ch(G; E)$ in $E$, that $Q_{x+y}=Q_x+Q_y$, $Q_{xe}=Q_xe$ for $x$, $y$ in $G$, $e$ in $E$. To prove that $Q_g=0$ implies $g=0$; suppose that $g\neq 0$ and that $B$ is a basis of $G$ over $E$. Then $g=\sum_{b \text{ in } B} be(b)$ for $e(b)$ in $E$; and $g\neq 0$ implies that at least one $be(b)\neq 0$. If $p$ is a prime in $E$, then there exists one and only one character $s=s_b$ of $G$ in $E$ which maps $b$ upon $p^{m-n(b)}$ and all the other elements in $B$ upon 0. Thus $s(g)=p^{m-n(b)}e(b)$; and this is not 0, since $e(b)$ would otherwise be an element in $P^{n(b)}$ so that $be(b)$ would be 0.—Thus we have proved that an isomorphism of $G$ upon a group of characters of $Ch(G; E)$ in $E$ is established by mapping the element $g$ in $G$ upon the character $Q_g$ of $Ch(G; E)$. To prove that this isomorphism exhausts the character group of $Ch(G; E)$ we consider again the characters $s_b$ of $Ch(G; E)$ (for $b$ in some basis $B$ of $G$ over $E$). From the fact that every right- and every left-ideal in $E$ is of the form $Ep^i=p^iE=P^i$ we infer readily that the $s_b$ for $b$ in $B$ form a basis of $Ch(G; E)$ over $E$. If $v$ is a

(28) This last hypothesis is only needed in order to be able to apply Theorem II.2.4. After this one application has been effected, this hypothesis may be dropped.

(29) For generalizations of the concept of character, see P. Lewis, *Characters of abelian groups*, American Journal of Mathematics, vol. 64 (1942), pp. 81–105.

character of $Ch(G; E)$ in $E$, then $p^{n(b)}s_b = 0$ implies that $v(s_b) = p^{m-n(b)}d(b)$ for $d(b)$ in $E$. If $g = \sum_{b \text{ in } B} bd(b)$, then $Q_g(s_b) = s_b(g) = p^{m-n(b)}d(b) = v(s_b)$ so that $Q_g = v$; and this completes the proof of (a).

If $S$ is an $E$-admissible subgroup of $G$, then we denote by $(f(S) = 0)$ the set of all the characters of $G$ in $E$ which map $S$ upon 0; and the analogous definition may be used for $E$-admissible subgroups $S$ of $Ch(G; E)$.—If $S$ is an $E$-admissible subgroup of $G$, then every character of $G/S$ in $E$ is induced by one and only one character in $(f(S) = 0)$; and since we showed in the first part of the proof that 0 is the only element in $G/S$ mapped upon 0 by all the characters of $G/S$ in $E$, it follows that[30] $(f((f(S) = 0)) = 0) = S$. Since—by (a)—$G$ is the character group of $Ch(G; E)$, the same formula holds true for $E$-admissible subgroups of $Ch(G; E)$. But now it is readily verified that mapping the $E$-admissible subgroup $S$ of $G$ upon the $E$-admissible subgroup $(f(S) = 0)$ of $Ch(G; E)$ constitutes a biunivoque and monotonically decreasing correspondence (that is, a duality) between $D(G; E)$ and $D(Ch(G; E); E)$.

THEOREM II.4.2. *If $D(G; E)$ contains at least three independent cycles of maximum order, then the existence of an anti-automorphism of $E$ is a necessary and sufficient condition for the existence of an auto-duality of $D(G; E)$.*

REMARK. We note that consequently not every primary abelian operator group is self-dual.—Since there exists an auto-duality of $D(G; E)$ whenever $G$ is the direct sum of two cycles of order 1 in $D(G; E)$, the assumption of the existence of at least three independent cycles of maximum order is indispensable[31].

**Proof.** Every element $e$ in $E$ induces an endomorphism $e'$ of $Ch(G; E)$; since $Ch(G, E)$ contains elements of order $m$ (if $n(b) = m$, then the character $s_b$ constructed in the proof of Theorem II.4.1 is of order $m$) $e' = 0$ implies $e = 0$; since $(e+d)' = e'+d'$, $(ed)' = d'e'$ for $d$, $e$ in $E$, it follows that mapping $e$ upon $e'$ constitutes an anti-isomorphism of $E$ upon a ring $E'$ of endomorphisms of $Ch(G; E)$. It is a consequence of Theorems II.4.1, (b), II.2.1 and II.2.2 that $E'$ contains every $D(Ch(G; E); E)$-admissible endomorphism of $Ch(G; E)$.

If there exists an anti-automorphism of $E$, then there exists an isomorphism $f$ of $E$ upon $E'$ and there exists one and only one isomorphism $v$ of $G$ upon $Ch(G; E)$ which satisfies $b^v = s_b$ for $b$ in a basis $B$ of $G$ and $s_b$ defined as in the proof of Theorem II.4.1 and which satisfies furthermore $(ge)^v = g^v e^f$ for $g$ in $G$ and $e$ in $E$. Thus there exists a projectivity of $D(G; E)$ upon its—by Theorem II.4.1, (b)—dual $D(Ch(G; E); E)$, proving the self-duality of $D(G; E)$.

If there exists an auto-duality of $D(G; E)$, then there exists by Theorem

---

[30] This identity is in the projective special case essentially the content of the theory of linear equations.

[31] That the existence of a duality cannot be expected, unless $G$ is the sum of a finite number of cycles in $D(G; E)$, has been pointed out before; cf. R. Baer, Duke Mathematical Journal, vol. 5 (1939), pp. 824–838.

II.4.1, (b) a projectivity of $D(G; E)$ upon $D(Ch(G; E); E)$; and hence it follows from Theorem II.3.1 that $E$ and $E'$ are isomorphic. Since $E$ and $E'$ have been shown to be anti-isomorphic in the first paragraph of the proof, this implies the existence of an anti-automorphism of $E$.

5. **The theorem of Pappus.** Throughout this section we shall assume that $E$ is a primary ring of endomorphisms of the abelian group $G$, that $P$ is the greatest two-sided ideal different from $E$ in $E$, that the ring $D(G; E)$ of all the $E$-admissible subgroups of $G$ is primary and contains either no subcycles of order $n$ or at least three independent ones, and that $E$ contains every $D(G; E)$-admissible endomorphism of $G$.

The seven cycles $U_1, U_2, U_3 / Z / V_1, V_2, V_3$ in $D(G; E)$ are in *Pappus order*[32], if they are of equal order $n$, if $Z, U_1, V_1$ are independent, and if

$$U_1 + Z = U_2 + Z = U_3 + Z = U_1 + U_2 = U_2 + U_3,$$
$$V_1 + Z = V_2 + Z = V_3 + Z = V_2 + V_1 = V_1 + V_3.$$

Before stating the extension of Pappus' theorem whose proof is the goal of this section, we establish a useful normal form for cycles in Pappus order.

LEMMA II.5.1. *If the seven cycles $U_1, U_2, U_3 / Z / V_1, V_2, V_3$ of order $n$ in $D(G; E)$ are in Pappus order, if $W(i, j) = W(j, i)$ for $i \neq j$ is the cross-cut of $U_i + V_j$ and $U_j + V_i$, then the $W(i, j)$ are cycles of order $n$; and there exist three independent elements $z, u, v$ of order $n$ in $G$ and elements $1+x, y$ in $E$ though not in $P$ such that*

$$U_1 = uE, \quad U_2 = (u - z)E, \quad U_3 = (u(1 + x) - zx)E,$$
$$Z = zE,$$
$$V_1 = vE, \quad V_2 = (v - z)E, \quad V_3 = (vy + z)E,$$
$$W(1, 2) = (u + v - z)E, \; W(2, 3) = ((v - z)y + (u(1 + x) - zx)(1 + y))E,$$
$$W(3, 1) = (u(1 + x) - (vy + z)x)E.$$

(N)

**Proof.** There exist elements $z$, $b$ in $G$ such that $Z = zE$, $U_1 = bE$. Then $U_2 = (zr + bs)E$ for $r$, $s$ in $E$. Since $U_2$ is part of $U_1 + Z$, but of no proper partial sum of this direct sum, neither $r$ nor $s$ can be in $P$—by Theorem II.2.1—so that $r^{-1}$ exists in $E$. Hence $U_1 = uE$ for $u = -bsr^{-1}$ and $U_2 = (z - u)E$. Likewise we find an element $v$ such that $V_1 = vE$, $V_2 = (z - v)E$. The independence of $z, u, v$ is a consequence of the independence of $Z, U_1, V_1$.—Since $U_3$ is part of the direct sum $Z + U_2$, but of no proper partial sum of $Z + U_2$, there exist ele-

[32] This arrangement of the cycles is necessitated by typesetting limitations. The more suggestive form is used in (N) below. Note the asymmetry in the treatment of 1 and 2, though it is possible to interchange 1 and 2, provided one interchanges at the same time $U$ and $V$. The customary form of stating the theorem of Pappus is so wide that there exists hardly a geometry in which it holds true and it will become apparent from the proof of Theorem II.5.2 below that the restrictions we imposed upon the cycles $Z, U_i, V_i$ are unavoidable.

ments $r$, $s$ in $E$, though not in $P$, such that $U_3=(zr+(z-u)s)E$. Let $x=-sr^{-1}-1$. Then $1+x$ is not in $P$ and $U_3=(u(1+x)-zx)E$.—Since $V_3$ is part of the direct sum $Z+V_1$, but of no proper partial sum of $Z+V_1$, there exist elements $d$, $t$ in $E$, though not in $P$ such that $V_3=(zd+vt)E$. Then $y=td^{-1}$ is not in $P$ and $V_3=(vy+z)E$.

The elements in $W(1, 2)$ are of the form $ur+(v-z)s=vh+(u-z)k$; since this equation implies $ur=uk$, $zk=zs$, $vs=vh$, it follows that $W(1, 2)=(u+v-z)E$.

The elements in $W(2, 3)$ are of the form $(u-z)r+(vy+z)s=(v-z)h+(u(1+x)-xz)k$; this equation implies that $r\equiv(1+x)k$, $ys\equiv h$, $r-s\equiv h+xk \bmod P^n$, as follows from the independence of $z$, $u$, $v$ and of Theorem II.2.1; but these congruences imply $h\equiv ys$, $k\equiv r-xk\equiv h+s\equiv(y+1)s \bmod P^n$ so that $W(2, 3)=((v-z)y+(u(1+x)-zx)(1+y))E$.

The elements in $W(3, 1)$ are of the form $ur+(vy+z)s=vh+(u(1+x)-zx)k$ and this implies $ur=u(1+x)k$, $vys=vh$, $zs=-zxk$ or $r\equiv(1+x)k$, $ys\equiv h$, $s\equiv -xk \bmod P^n$ so that $W(3, 1)=(u(1+x)-(vy+z)x)E$.

Since $z$, $u$, $v$ are three independent elements of order $n$, it is now clear that the $W(i, j)$ are cycles of order $n$.

THEOREM II.5.2. *If $D(G; E)$ contains three independent cycles of order $n$, then the commutativity of $E/P^n$ is equivalent to the validity of the nth property of Pappus: If the cycles $U_1$, $U_2$, $U_3$ / $Z$ / $V_1$, $V_2$, $V_3$ of order $n$ in $D(G; E)$ are in Pappus order, if $W(i, j)=W(j, i)$ is for $i\neq j$ the cross-cut of $U_i+V_j$ and $U_j+V_i$, then*

$$W(1, 2)+W(2, 3)=W(2, 3)+W(3, 1)=W(3, 1)+W(1, 2).$$

**Proof.** Suppose first that the $n$th property of Pappus be satisfied by the cycles in $D(G; E)$, and suppose that $x$ and $y$ are two elements in $E$ such that neither $1+x$ nor $y$ is in $P$. There exist in $G$ three independent elements $z$, $u$, $v$ of order $n$; and the seven cycles

$$\begin{array}{rlll} & U_1=uE, & U_2=(u-z)E, & U_3=(u(1+x)-zx)E, \\ Z=zE, & & & \\ & V_1=vE, & V_2=(v-z)E, & V_3=(vy+z)E \end{array}$$

are easily seen to be in Pappus order. Since consequently $W(2, 3)\leqq W(2, 1)+W(1, 3)$, we infer from Lemma II.5.1 the existence of elements $r$, $s$ in $E$ such that

$$'v-z)y+(u(1+x)-zx)(1+y)=(u+v-z)r+(u(1+x)-(vy+z)x)s;$$

and these elements $r$, $s$ must clearly satisfy the congruences

$$(1+x)(1+y)\equiv r+(1+x)s,\ y\equiv r-yxs,\ y+x(1+y)\equiv r+xs \bmod P^n.$$

Subtracting the third from the first congruence, we find $s\equiv 1 \bmod P^n$, and

hence it follows by subtracting the second from the third congruence that $xy \equiv yx \bmod P^n$.

If $1+x$ is in $P$, but $y$ is not in $P$, then $x$ is not in $P$; and $x = 1+(x-1)$ together with the results already obtained imply that $(x-1)y \equiv y(x-1) \bmod P^n$ so that $xy \equiv yx \bmod P^n$, if at least one of the two elements $x$ and $y$ is not in $P$. If both are in $P$, then $1+x$ is not in $P$, so that $(1+x)y \equiv y(1+x) \bmod P^n$ and hence $xy \equiv yx \bmod P^n$; and this proves that $E/P^n$ is a commutative ring.

If conversely $E/P^n$ is a commutative ring, then any seven cycles of order $n$ in Pappus order may be assumed to be in the normal form (N) of Lemma II.5.1. Since $y(1+x)$ is not in $P$ and possesses therefore an inverse in $E$, and since we derive from the commutativity of multiplication the identity

$$u(1+x)(1+y) + vy - z(y + x(1+y)) - (u(1+x) - vyx - zx)$$
$$= u(1+x)y + vy(1+x) - zy(1+x) = (u+v-z)y(1+x),$$

we find immediately that $W(1, 2)+W(2, 3) = W(2, 3)+W(3, 1) = W(3, 1) + W(1, 2)$, that is, the $n$th property of Pappus is satisfied in $D(G; E)$.

COROLLARY II.5.3. *If the nth property of Pappus is satisfied in $D(G; E)$ (and if $D(G; E)$ contains cycles of order $n$), then the $(n-1)$st property of Pappus is satisfied in $D(G; E)$.*

For $E/P^{n-1}$ is commutative, if $E/P^n$ is commutative.

COROLLARY II.5.4. *The nth property of Pappus is satisfied in $D(G; E)$ for every $n$ if, and only if, $E$ is commutative.*

For $E$ is commutative, if every $E/P^n$ is commutative, since 0 is the crosscut of the $P^n$.

6. **The ordinary primary abelian groups.** We assume throughout this section that $L$ is a primary ring of subgroups of the abelian group $G$ which either does not contain any cycles of order $n$ or at least three independent ones. It is the object of this section to find conditions on the (abstract) Dedekind set $L$ which assure that $L$ contains *every* subgroup of $G$.

If we denote by $E$ the ring of all the $L$-admissible endomorphisms of $G$, then it is a consequence of Theorem II.1.2 that $L$ is exactly the set $D(G; E)$ of all the $E$-admissible subgroups of $G$; and it is a consequence of Theorems II.2.2 and II.2.3 that $E$ is a primary ring of endomorphisms. Thus there exists in $E$ a uniquely determined greatest two-sided ideal $P$ different from $E$; and all the elements in $E$ that are not in $P$ possess inverses in $E$.

The integral multiples of the unit in $E$—which we denote by $0, \pm 1, \pm 2, \cdots$—form a subring $E_0$ of $E$. Clearly $E_0$ is part of the central of $E$; and the crosscut of $E_0$ and $P$ is either 0—in which case $E$ is said to be of characteristic(33)

(33) The characteristic of the ring $E$ is exactly the characteristic of the field $E/P$ in the customary terminology.

0—or consists of all the multiples of a certain rational prime number $r$—in which case $E$ is said to be of characteristic(33) $r$.

If the set of all the subgroups of the abelian group $C$ is a cycle of order $n$, then $C$ is a cyclic group containing $c^n$ elements for $c$ a rational prime number. If the primary ring $L$ of subgroups of $G$ contains every subgroup of $G$, then the characteristic of $E$ is a rational prime number $r$, cycles of order $n$ in $L$ are cyclic groups of order $r^n$; and(34) $E$ is the ring of all the $r$-adic integers, provided the orders of the cycles in $L$ are not bounded; whereas $E$ is the ring of the rational integers modulo $r^m$, if $m$ is the maximum order of the cycles in $L$; in short: $G$ is a primary abelian group of characteristic $r$.

The six cycles $W$, $Z_1$, $Z_2$; $W_1$, $W_2$, $Z$ form *a complete triangle of order n* with *vertex* $W$ [and basis $Z_1+Z_2$], if

(a) $W$, $Z_1$, $Z_2$ are three independent cycles of order $n$ in $L$,

(b) $Z_1+Z_2=Z_2+Z=Z+Z_1$, $W_1+W_2=W_2+Z=Z+W_1$, $W+Z_i=Z_i+W_i=W_i+W$.

A normal form for complete triangles is established by the following lemma.

LEMMA II.6.1. *The six cycles $W$, $Z_1$, $Z_2$; $W_1$, $W_2$, $Z$ form a complete triangle of order $n$ if, and only if, there exist in $G$ three independent elements $w$, $z_1$, $z_2$ of order $n$ such that $W=wE$, $Z_i=z_iE$, $W_i=(w+z_i)E$, $Z=(z_1-z_2)E$.*

**Proof.** The sufficiency of the condition is readily verified.—Thus we assume that the six cycles form a complete triangle. There exists an element $w$ such that $W=wE$. Since $W$ is part of $Z_i+W_i$, but of no proper part of this sum, there exist elements $z_i$, $w_i$ such that $w=w_i-z_i$, $W_i=w_iE$, $Z_i=z_iE$. Since $w$, $z_1$, $z_2$ are independent elements of order $n$, and since $Z$ is part of $Z_1+Z_2$ and $W_1+W_2$, but of no proper part of these sums, one may readily verify that $Z=(z_1-z_2)E$.

If the six cycles $W$, $Z_1$, $Z_2$; $W_1$, $W_2$, $Z$ form a complete triangle of order $n$ in $L$, then we define derived elements $W^{(j)}$, $W_i^{(j)}$ inductively for $j=-1, 0, 1, 2, \cdots$ by the following rules.

$$(-1)\qquad W = W^{(-1)}, \qquad W_i = W_i^{(-1)}.$$

$$(j+1)\begin{cases} W^{(j+1)} \text{ is the cross-cut of } W \text{ and } W_1 + W_1^{(j)}; \\ V^{(j+1)} \text{ is the cross-cut of } W^{(j+1)} + Z \text{ and } W_1^{(j)} + W_2; \\ W_1^{(j+1)} \text{ is the cross-cut of } V^{(j+1)} + Z_2 \text{ and } Z_1 + W^{(j+1)}; \\ W_2^{(j+1)} \text{ is the cross-cut of } W_1^{(j+1)} + Z \text{ and } Z_2 + W^{(j+1)}. \end{cases}$$

In particular we call $W^{(j)}$ the $j$th *derivative of the vertex of the complete triangle.*

LEMMA II.6.2. *If the six cycles $W$, $Z_1$, $Z_2$; $W_1$, $W_2$, $Z$ form a complete triangle*

(34) Cf. R. Baer, American Journal of Mathematics, vol. 59 (1937), p. 110, Theorem 5.2.

*of order $n$ in $L$, and if $w$, $z_i$ are elements in $G$ such that $W=wE$, $Z_i=z_iE$, $W_i=(w+z_i)E$, $Z=(z_1-z_2)E$, then the derived elements satisfy: $W^{(j)}=(wj)E$, $W_i^{(j)}=(z_i-wj)E$.*

**Proof** (by induction). Our contention is obvious for $j=-1$ and thus we assume it to be true for $j$ in order to prove it for $j+1$. Using the fact that $w$, $z_1$, $z_2$ are three independent elements of order $n$, one verifies:

$W^{(j+1)}$ is the cross-cut of $wE$ and $(w+z_1)E+(z_1-wj)E$ and hence equals $w(j+1)E$;

$V^{(j+1)}$ is the cross-cut of $w(j+1)E+(z_1-z_2)E$ and $(z_1-wj)E+(w+z_2)E$ and hence equals $(z_1-z_2-w(j+1))E$;

$W_1^{(j+1)}$ is the cross-cut of $(z_1-z_2-w(j+1))E+z_2E$ and $z_1E+w(j+1)E$ and hence equals $(z_1-w(j+1))E$;

$W_2^{(j+1)}$ is the cross-cut of $(z_1-w(j+1))E+(z_1-z_2)E$ and $z_2E+w(j+1)E$ and hence equals $(z_2-w(j+1))E$;

and this completes the proof of the lemma.

THEOREM II.6.3. *If the primary ring $L$ of subgroups of the abelian group $G$ contains either no cycle of order $n$ or at least three independent ones, then the following conditions are necessary and sufficient for $L$ to contain every subgroup of $G$.*

(i) *If the subgroup $S$ in $L$ is the direct sum of two cycles of order 1 in $L$, then the number of subgroups in $L$ that are part of $S$ is $r+3$ for $r$ a rational prime number.*

(ii) *If $W$ is the vertex of some complete triangle of order $n$ in $L$, then there exists a superscript $j$ such that the $j$th derivative $W^{(j)}$ of $W$ is the subcycle of order $n-1$ of $W$.*

*If* (i) *and* (ii) *are satisfied, then $G$ is a primary abelian group of characteristic $r$.*

**Proof.** The necessity of condition (i) is an obvious consequence of the fact that $G$ is a primary abelian group of characteristic $r$, if $L$ contains every subgroup; and the necessity of (ii) is immediately derived from Lemmas II.6.1 and II.6.2.—Assume conversely that conditions (i) and (ii) are satisfied by $L$. If $L$ contains cycles of order $n$ different from 0, then $L$ contains three independent elements $w$, $z_1$, $z_2$ of order $n$. The six cycles $W=wE$, $Z_1=z_1E$, $Z_2=z_2E$; $W_1=(w+z_1)E$, $W_2=(w+z_2)E$, $Z=(z_1-z_2)E$ form a complete triangle of order $n$. Since the subcycle of order $n-1$ of $W$ is—by Theorem II.2.1—just $WP$, it follows from condition (ii) and from Lemma II.6.2 that there exists an integer $j$ such that $WP=wjE$; and this implies that $P=jE$ for $j$ in $E_0$.

It is a consequence of condition (i) that $E/P$ is a prime field of prime number characteristic $r$ so that $E/P^n$ consists of exactly $r^n$ elements, provided there exist—as we assume just now—cycles of order $n$ in $L$. If we denote by $P_0$

the cross-cut of $P$ and $E_0$, then it follows from $P=jE$ for $j$ in $E_0$, that $E_0/P_0^n$ consists of $r^n$ elements too so that $E/P^n$ and $E_0/P_0^n$ are essentially the same. If $G_n$ is the sum of all the cycles of an order not exceeding $n$ in $L$, then it follows from the fact that $L$ contains every $E$-admissible subgroup of $G$, that every subgroup of $G_n$ belongs to $L$, since every subgroup of $G_n$ is $E_0$-admissible, therefore $E/P^n$-admissible, therefore $E$-admissible. Since every element in $G$ is contained in some $G_n$, it follows finally that every subgroup of $G$ belongs to $L$ and that $G$ is a primary abelian group of characteristic $r$.

We add some remarks. If $S$ is any subset of the ring $L$ of subgroups of $G$, then we denote by $N(S)$ the *net* determined by $S$, that is, the smallest subset of $L$ which contains $S$ and which contains with any two elements their sum and their cross-cut. If, for example, $S$ consists of the six cycles of a complete triangle, then one may prove in a similar fashion as Theorem II.6.3 that $N(S)$ contains every part of the sum of the cycles of the triangle, provided $L$ contains every subgroup of $G$.

Applying Lemmas II.6.1 and II.6.2 one verifies immediately the following *characterization of the characteristic of E.*

Suppose that $W$ is the vertex of a complete triangle of order $n\neq 0$ in $L$. Then the characteristic of $E$ is 0 if, and only if, every derivative of the vertex $W$ is equal to $W$; and the characteristic of $E$ is the rational prime number $r$ if, and only if, the $r$th derivative $W^{(r)}$ of $W$ is a proper subcycle of $W$ (possibly 0).

## Part III. Construction of the underlying group

In the first part a class of Dedekind sets was determined which exhibited the salient features of both projective spaces and finite abelian groups. In the second part we introduced the primary abelian operator groups as those operator groups whose sets of admissible subgroups just met the requirements postulated in the first part. In this part we are going to prove that the (abstract) Dedekind sets with these properties may always be realized as the sets of admissible subgroups of a primary abelian operator group, provided they are "big enough." This last restriction is not surprising, considering the impossibility of obtaining a complete theory in the projective plane—there does not exist a planar proof of Desargues' theorem. The problem of determining the minimum number of parameters necessary for the validity of our theorem is still an open one; it is clear that it cannot be less than four and we prove that it is at most six.

The discussion in this part is based on the results of the two preceding parts. The method used is rather different from those customarily employed in dealing with similar problems of projective geometry, though an extension of Desargues' theorem is of central importance—and this part has some intrinsic interest apart from its applications. But in projective geometry it is customary to construct first the field of coordinates and then to introduce the linear subspaces by means of linear equations. Considering that the coordi-

nates are just the operators operating on the underlying group, this amounts to constructing the operators first and the group on which they operate only afterward. We invert this order of procedure, construct first the group with a set of distinguished subgroups representing the given Dedekind set and obtain operators as well as primarity as an application of theorems in Part II. Apart from this difference in the order of procedure one may say that the main difference consists of the true projectivity of our method and of the complete avoidance of affine means—the affine method consisting in first finding a representation for all the elements outside a certain distinguished hyperplane, a representation which is extended afterwards over the whole space, the projective method avoiding this preferential treatment of some element and thus finding representations of all the elements (as subgroups) at the same time.

1. **Collinearity.** The three elements $u, v, w$ in the Dedekind set $D$ are said to be *collinear*, if $u+v=v+w=w+u$.

LEMMA III.1.1. *If $u+w=w+v$, then $u$, $v$ and $w(u+v)$ are collinear.*

For it follows from Dedekind's law that

$$u + v = (u + v + w)(u + v) = (u + w)(u + v) = u + w(u + v)$$
$$= (v + w)(u + v) = v + w(u + v).$$

LEMMA III.1.2. *If there exists an element $e$ such that $a$, $c$, $e$ and $b$, $d$, $e$ are triplets of collinear elements, then both $(a+b)(c+d)$, $c$, $d$ and $(a+b)(c+d)$, $a$, $b$ are triplets of collinear elements.*

This follows from Lemma III.1.1, since for example,

$$a + (c + d) = a + c + d = e + c + d = b + c + d = (c + d) + b.$$

2. **The theorem of Desargues.** The elements $w(i, j)=w(j, i)$ for $i\neq j$ are termed *connecting links of the two triplets $u(i)$ and $v(i)$—$i=1, 2, 3$*—of elements in the Dedekind set $D$, if $u(i)$, $w(i, j)$, $u(j)$ and $v(i)$, $w(i, j)$, $v(j)$ are two triplets of collinear elements for every $i\neq j$.

THEOREM III.2.1. *If the elements $w(i, j)$ are connecting links of the two triplets $u(i)$ and $v(i)$, and if $v(3)(u(1)+u(2)+u(3))=0$, then the $w(i, j)$ are collinear.*

**Proof.** If $i, j, h$ is any permutation of the three numbers 1, 2, 3, then it follows from the definition of connecting links that

$$u(1) + u(2) + u(3) = w(i, j) + w(j, h) + u(3),$$
$$v(1) + v(2) + v(3) = w(i, j) + w(j, h) + v(3);$$

and hence it follows from the hypothesis and Dedekind's law that

$$w(i,j) + w(j,h) = w(i,j) + w(j,h) + v(3)(u(1) + u(2) + u(3))$$
$$= (w(i,j) + w(j,h) + v(3))(u(1) + u(2) + u(3))$$
$$= (v(1) + v(2) + v(3))(u(1) + u(2) + u(3)),$$

proving the collinearity of the connecting links $w(i, j)$.

The seven cycles $u(1)$, $u(2)$, $u(3)$ / $z$ / $v(1)$, $v(2)$, $v(3)$ are in *Desargues order*, if

(a) $z \neq 0$, $n(u(i)) \leqq n(z)$, $n(v(i)) \leqq n(z)$ for $i = 1, 2, 3$,

(b) $u(i), v(i), z$ are collinear for $i = 1, 2, 3$,

(c) $z(u(i)+u(j))(v(i)+v(j)) = 0$ for $i \neq j$([35]).

Since a cycle $c \neq 0$ contains one and only one subcycle $c^*$ of order 1—a notation we shall use throughout—condition (c) is equivalent to the following handier condition

(c′) $z(u(i)+u(j)) = 0$ or $z(v(i)+v(j)) = 0$ for $i \neq j$.

From these conditions we derive the following helpful statement

(d) $u(i)v(i) = 0$; and if $z(u(i)+u(j)) = 0$, then $n(v(i)) = n(z)$ and $v(i)(u(i) + u(j)) = 0$.

If $zu(i) = 0$, then $z$, $(z+u(i))/u(i) = (u(i)+v(i))/u(i)$—by (b)—and $v(i)/(u(i)v(i))$ are isomorphic cycles; and hence it follows from (a) that $u(i)v(i) = 0$ and $n(v(i)) = n(z)$.—If $z(u(i)+u(j)) = 0$, though $v(i)(u(i)+u(j)) \neq 0$, then $v(i) \neq 0$ and $v(i)^* \leqq u(i)+u(j)$. If $u(i) \neq 0$, then it follows from $u(i)v(i) = 0$ and Theorem I.2.2 that $z^* \leqq u(i)^* + v(i)^* \leqq u(i)+u(j)$, contradicting our assumption. Thus $u(i) = 0$; and this implies $v(i)^* = u(j)^*$ and $v(i) = z$—by (b)—so that $z^* = u(j)^*$, an impossibility which proves (d).

(e) The elements $w(i, j) = (u(i)+u(j))(v(i)+v(j))$ are the *only* connecting links of the two triples $u(i)$ and $v(i)$.

That the $w(i, j)$ are connecting links is an immediate consequence of Lemma III.1.2.—If the elements $x(i, j)$ are connecting links too, and if, for example, $z(u(i)+u(j)) = 0$, then $v(i)(u(i)+u(j)) = 0$ and hence

$$x(i,j) = x(i,j) + v(i)(u(i) + u(j)) = (x(i,j) + v(i))(u(i) + u(j))$$
$$= (v(j) + v(i))(u(i) + u(j)) = w(i,j)$$

by Dedekind's law.

(f) If $z+u(1)+u(2)+u(3)$ splits completely, then the connecting links $w(i, j)$ are cycles.

If $w(i, j)$ would not be a cycle, then it would follow from Theorem I.3.6 that $w(i, j)$ contains at least two different subcycles of order 1. Hence $u(i) \neq 0$, $u(i)^* \leqq v(i)+v(j)$ and $v(i) \neq 0$, $v(i)^* \leqq u(i)+u(j)$, contradicting (c′) and (d).

DESARGUES' PROPERTY. *If the seven cycles* $u(1), u(2), u(3) / z / v(1), v(2), v(3)$

([35]) It may be seen from trivial examples that this last condition is indispensable, though it seems to be fairly common to omit it.

*are in Desargues order, then their connecting links* $w(2, 3)$, $w(3, 1)$, $w(1, 2)$ *are collinear.*

We note that this property refers to all cycles in a certain Dedekind set.

THEOREM III.2.2. *If the element* $w$ *splits completely, is primary and contains at least five independent cycles of maximum order, then Desargues' property is satisfied by the cycles in the Dedekind set* $w/u$ *for every part* $u$ *of* $w$.

**Proof** ([36]). We show first that Desargues' property is satisfied by the subcycles of $w$; and we shall derive the general property from the special case.

Thus let us assume that the seven subcycles $z$, $u(i)$, $v(i)$ of $w$ are in Desargues order; and put $n(z)=m$. Since $z$, $u(i)$, $v(i)$ are collinear for every $i$, we find that $s=z+u(1)+u(2)+u(3)=z+v(1)+v(2)+v(3)$. Since there exist at least five independent subcycles of order $m$ of $w$, and since $s$ is a sum of four cycles only, it follows that there exists a subcycle $p$ of $w$ whose order is $m$ and which is independent of $s$.

Since $pz=0$, and since $p$ and $z$ are cycles of equal order $m$, it follows from Theorem I.3.7 and Lemma I.3.8 that there exists a subcycle $q$ of $p+z$ which is not part of any proper partial sum of $p+z$ and that $p+z$ is the direct sum of $p$ and $z$, of $z$ and $q$, of $q$ and $p$, $n(q)=m$.

We prove next that the elements $r(i)=(p+u(i))(q+v(i))$ are cycles.

For if this would not be true, then $r(i)$ would contain by Theorem I.3.6 two different subcycles of order 1; and since both $p+u(i)$ and $q+v(i)$ are sums of two cycles, this would imply that $q^*\leqq p+u(i)$, $p^*\leqq q+v(i)$ and $(p+u(i))^*=(q+v(i))^*$—where we denote by $r^*$ the sum of all the subcycles of order 1 of the element $r$, a notation which we shall use throughout. As a consequence of (c′) we have $zu(i)=0$ or $zv(i)=0$. In the first case we obtain: $(p+u(i))^*=p^*+q^*=p^*+z^*=z^*+u(i)^*$, an inference contradicting $sp=0$; and in the same way we obtain a contradiction from $zv(i)=0$ so that the $r(i)$ have to be cycles.

Since $z$, $p$, $q$ and $z$, $u(i)$, $v(i)$ and $z$, $u(j)$, $v(j)$ are three triplets of collinear elements, it follows from Lemma III.1.2 that the elements $w(i,j)$, $r(j)$, $r(i)$ are connecting links of the two triplets $p$, $u(i)$, $u(j)$ and $q$, $v(i)$, $v(j)$—note that the elements $w(i, j)=(u(i)+u(j))(v(i)+v(j))$ are *the* connecting links of the triplets $u(i)$ and $v(i)$. From (c′) it follows that not both $z(u(i)+u(j))$ and $z(v(i)+v(j))$ can be different from 0. If $z(u(i)+u(j))=0$, then it follows from $p(z+u(i)+u(j))=0$ and from Dedekind's law that $0=(p+z)(u(i)+u(j))=(p+q)(u(i)+u(j))$; and this together with $pq=0$ implies $0=q(p+u(i)+u(j))$; and if $z(v(i)+v(j))=0$, then we prove likewise that $0=q(p+v(i)+v(j))$. Thus it follows in either case from Theorem III.2.1 that $w(i, j)$, $r(i)$ and $r(j)$ are collinear.

---

([36]) This is an adaptation of the proofs of Desargues' theorem as given in projective geometry; cf., for example, Veblen and Young, *Projective Geometry*, Boston, 1910, p. 41.

From $ps=0$, $r(i)\leqq p+u(i)$ and Dedekind's law we infer that

$$r(i)(u(1)+u(2)+u(3)) = r(i)(p+u(i))(u(1)+u(2)+u(3))$$
$$= r(i)(u(i)+p(u(1)+u(2)+u(3))) = r(i)u(i)$$

and likewise it follows that

$$r(i)(v(1)+v(2)+v(3)) = r(i)v(i).$$

Since $r(i)$ is a cycle, and since $u(i)v(i)=0$—by (d)—it is impossible that both $r(i)(u(1)+u(2)+u(3))$ and $r(i)(v(1)+v(2)+v(3))$ are different from 0. If $r(i)(u(1)+u(2)+u(3))=0$, then the connecting links $w(i, j)$ of the triplets $u(i)$ and $r(i)$ are collinear by Theorem III.2.1; and if $r(i)(v(1)+v(2)+v(3))=0$, then the connecting links $w(i, j)$ of the triplets $v(i)$ and $r(i)$ are collinear by Theorem III.2.1 so that the connecting links $w(i, j)$ of the triplets $u(i)$ and $v(i)$ are collinear in any case.

If $u$ is a part of $w$, and if $u(1)$, $u(2)$, $u(3)$ / $z$ / $v(1)$, $v(2)$, $v(3)$ are cycles in Desargues order in the Dedekind set $w/u$ of all the elements between $u$ and $w$ (whose null-element is $u$), then $s=z+u(1)+u(2)+u(3)=z+v(1)+v(2)+v(3)$. Since the parts of $w$ are sums of cycles by Theorem I.3.7 there exist subcycles $c, c(i)$ of $w$ (in $D$) such that $z=u+c$ and $u(i)=u+c(i)$. If $t=c+c(1)+c(2)+c(3)$, then $s=u+t$ and $s/u$ and $t/(tu)$ are isomorphic. Thus it suffices to prove that the cycles in the Dedekind set $t/(tu)$ satisfy Desargues' property. Since $t$ is a sum of four cycles, and since there exist at least five independent cycles of maximum order in $w$, there exists a subcycle $p$ of $w$ such that $pt=0$ and such that $n(p)=n(z/u)$. Now it is clear that the system $(p+t)/(tu)$ meets—as far as the subcycles of $t/(tu)$ are concerned—all the requirements we needed in the first part of the proof; and this completes the proof of our theorem.

3. **The vectors.** *A complete $n-m$-simplex $S=S_n^m$* consists of $n$ independent cycles $c(1), \cdots, c(n)$ of order $m$—the *vertices* of $S$—together with cycles $c(i, j)=c(j, i)$ for $i\neq j$—the *links* of $S$—subject to the following conditions.

(i) $c(i)$, $c(j)$ and $c(i, j)$ are collinear.

(ii) $c(i, j)$, $c(j, k)$ and $c(k, i)$ are collinear, if $i, j, k$ are three different integers.

Since $c(i)$ and $c(j)$ are for $i\neq j$ independent cycles of the same order $m$, and since $c(i, j)$ is a cycle, the order of $c(i, j)$ must be $m$ too and $c(i, j)c(k)=0$ for every $k$.

LEMMA III.3.1. *If the cycles $c(1), \cdots, c(n)$ of order $m$ are independent, if $\sum_{i=1}^{n} c(i)$ splits completely and is primary, and if $4<n$, then the $c(i)$ are the vertices of some complete $n-m$-simplex.*

**Proof.** Since $c(1)+c(i)$ is for $1<i$ the direct sum of two cycles of equal order $m$, and is at the same time primary, it follows from Lemma I.3.8 that there exists a cycle $c(1, i)=c(i, 1)$ of order $m$ such that $c(1)$, $c(i)$ and $c(1, i)$ are collinear.

If $i, j, k$ are three different integers which are all different from 1, then $c(1)(c(i)+c(j)+c(k))=0$ so that the seven cycles

$$c(1, i),\ c(1, j),\ c(1, k)\ /\ c(1)\ /\ c(i),\ c(j),\ c(k)$$

are in Desargues order; and their connecting links $c(j, k)$, $c(i, k)$, $c(i, j)$ are collinear by Theorem III.2.2 where $c(i, j)=(c(i)+c(j))(c(1, i)+c(1, j))$ is by (e), (f) of the preceding section a cycle (of order $m$); and hence a complete $n-m$-simplex is formed by the vertices $c(i)$ and the links $c(i, j)$.

If the cycles $c(i)$ are the vertices and the cycles $c(i, j)$ the links of a complete $n-m$-simplex $S$, then a *vector $V$ over $S$* determines—and is itself determined by—the *cycle $c(V)$ generated by $V$* and the *coordinates* $(i, V)$ for $i=1, \cdots, n$ subject to the following rules.

(a) $(i, V)=\infty$ *if, and only if,* $c(i)\ c(V)\neq 0$.

(b) $n(c(V))\leqq m$.

(c) *If* $c(i)\ c(V)=0$, *then* $(i, V)$ *is a cycle and* $c(i)$, $c(V)$, $(i, V)$ *are collinear.*

(d) *If* $c(i)\ c(V)=c(j)\ c(V)=0$, $i\neq j$, *then* $(i, V)$, $(j, V)$, $c(i, j)$ *are collinear.*

An immediate consequence of $n(c(V))\leqq n(c(i))$ and (c) is the following statement.

(e) $(i, V)\ c(V)=0$; $n((i, V))=m$.

THEOREM III.3.2. *If $S$ is an $n-m$-simplex with vertices $c(i)$ and links $c(i, j)$, if $4<n$, if $c$ is a cycle and $n(c)\leqq m$, if $c+\sum_{i=1}^{n}c(i)$ is primary and splits completely, if $c\ c(k)=0$, if $d$ is a cycle such that $c$, $d$, $c(k)$ are collinear, then there exists one and only one vector $V$ over $S$ such that $c=c(V)$ and $d=(k, V)$.*

**Proof.** We may assume without loss in generality that $k=1$.—Suppose first that $V$ and $U$ are vectors over $S$ such that $c(V)=c=c(U)$ and $(1, V)=d=(1, U)$. There exists at most one $i$ such that $c(1)(c+c(i))$ is not 0. If $c(1)(c+c(j))=0=c(1)(c+c(k))$ for $j\neq k$, then the seven cycles $c$, $c(j)$, $c(k)\ /\ c(1)\ /\ d$, $c(1, j)$, $c(1, k)$ are in Desargues order; and it follows from (e), (f) of the preceding section that their connecting links are uniquely determined and are $c(j, k)$, $(j, *)$, $(k, *)$; and hence it follows from (c) in the definition of a vector that $(j, *)=(j, U)=(j, V)$, $(k, *)=(k, V)=(k, U)$.—If finally $cc(i)=0$, but $c(1)(c+c(i))=0$, then it follows from similar reasoning that for some $j$ different from 1 and $i$

$$\begin{aligned}(i, V) &= (c+c(i))((j, V)+c(j, i))\\ &= (c+c(i))((j, U)+c(j, i))=(i, U)\end{aligned}$$

so that $U=V$.

In order to prove the existence of a vector $V$ over $S$ meeting all the requirements we proceed in a similar fashion. There exists at most one $i\neq 1$ such that $c(1)(c+c(i))\neq 0$. If $j\neq 1$ and $c(1)(c+c(j))=0$, then we put $(j, V)=(c+c(j))(d+c(1, j))$. If $j\neq k$ and $c(1)(c+c(j))=0=c(1)(c+c(k))$, then the seven cycles $d$, $c(1, j)$, $c(1, k)\ /\ c(1)\ /\ c$, $c(j)$, $c(k)$ are in Desargues order and

their connecting links are $c(i, k)$, $(k, V)$, $(j, V)$. Hence it follows from (f) of the preceding section that $(j, V)$, $(k, V)$ are cycles, meeting the requirements (c) and (d)of the definition of a vector, as follows from (e) of the preceding section and from Theorem III.2.2. If we put $c=c(V)$, $d=(1, V)$, then the definition of the desired vector $V$ has been completed, if either $c(1)(c+c(i))=0$ for every $i\neq 1$ or $c(1)(c+c(i))\neq 0$ for an $i\neq 1$ such that $c(i)c\neq 0$, as we have to put $(i, V)=\infty$ in this case.

In order to complete the proof we assume now that $cc(n)=0$ and $c(1)(c+c(n))\neq 0$. But then $c(i)(c+c(n))=0$ for $1<i<n$; we put $(n, V)_i=(c+c(n))((i, V)+c(i, n))$. Then we may prove as before that $(n, V)_i$ is a cycle, that $c$, $c(n)$, $(n, V)_i$ as well as $(i, V)$, $c(i, n)$, $(n, V)_i$ are collinear. If furthermore, $1\leqq j<n$, $j\neq i$, then the seven cycles $c(i, n)$, $c(i, j)$, $(i, V)$ / $c(i)$ / $c(n)$, $c(j)$, $c=c(V)$ are in Desargues order; their connecting links $(j, V)$, $(n, V)_i$, $c(n, j)$ are collinear by Theorem III.2.2. But this implies $(n, V)_i\leqq(n, V)_j$ so that $(n, V)_i=(n, V)_j$ for reasons of symmetry. If we put now $(n, V)=(n, V)_2=\cdots=(n, V)_{n-1}$, then this completes again the definition of the required vector.

If $S$ is a complete $n-m$-simplex, $4<n$, if $c$ is a cycle such that $n(c)\leqq m$ and the sum of $c$ and of the vertices is primary and splits completely, then there exists a vertex $c(k)$ of $S$ such that $cc(k)=0$; and it follows from the primarity by Lemma I.3.8 that there exists a cycle $d$ such that $c$, $d$, $c(k)$ are collinear; and hence we have proved the following corollary to Theorem III.3.2.

*There exists a vector $V$ over $S$ which generates the cycle $c$.*

4. **Subtraction of vectors.** Throughout this section we shall assume that the element $g$ (in the Dedekind set $D$) is primary and splits completely, that $S$ is a complete $n-m$-simplex whose vertices $c(i)$ and whose links $c(i, j)$ are parts of $g$ and that $5<n$, though for some of the following results it would suffice to assume $4<n$.

LEMMA III.4.1. *If $A$ and $B$ are vectors over $S$ such that $c(A)$ and $c(B)$ are parts of $g$, and if $c(h)(c(A)+c(B))=0=(c(A)+c(B))c(k)$, then $(c(A)+c(B))((h, A)+(h, B))$ and $(c(A)+c(B))((k, A)+(k, B))$ are equal cycles and $c(A)$, $c(B)$, $(c(A)+c(B))((h, A)+(h, B))$ as well as $(h, A)$, $(h, B)$, $(c(A)+c(B))((h, A)+(h, B))$ are collinear triplets.*

**Proof.** We note first the existence of a $j$ such that $c(j)(c(A)+c(B)+c(h)+c(k))=0$, and that it suffices clearly to prove our statement for the couple $h, j$ instead of proving it for the couple $h, k$. Since $c(h)(c(A)+c(B))=0$, it follows that $c(j)+c(h)+c(A)+c(B)$ is the direct sum of $c(A)+c(B)$, $c(h)$, $c(j)$. Since $c(i)$, $c(X)$, $(i, X)$ are collinear whenever $c(i)c(X)=0$, it follows that the cycles $(h, A)$, $(h, B)$, $c(j, h)$ / $c(h)$ / $c(A)$, $c(B)$, $c(j)$ are in Desargues order; and their connecting links are the—by (e), (f) of §III. 2—uniquely determined cycles $(j, B)$, $(j, A)$, $((h, A)+(h, B))(c(A)+c(B))$ which are collinear by Theorem III.2.2.

On account of this lemma we *define*:

If $A$ and $B$ are vectors over $S$ such that $c(A)$ and $c(B)$ are parts of $g$, then $(A, B)=(c(A)+c(B))((i, A)+(i, B))$ for every $i$ such that $c(i)(c(A)+c(B))=0$.

We note that $(A, B)=(B, A)$ is a cycle such that both $c(A)$, $c(B)$, $(A, B)$ and $(i, A)$, $(i, B)$, $(A, B)$ are collinear triplets. This cycle $(A, B)$ shall serve later as the cycle generated by the difference of $A$ and $B$. For the definition of the coordinates of the difference vector we need two auxiliary functions.

LEMMA III.4.2. *If $A$ and $B$ are vectors over $S$ such that $c(A)$ and $c(B)$ are parts of $g$, then*

(a) $(c(A)+c(B))(c(i)+c(j))=0$ *and* $i\neq j$ *imply*

*that* $w(i/j; A, B)=(c(i, j)+(A, B))((i, A)+(j, B))$ *is a cycle of order* $m$,

*that* $(i, A)$, $(j, B)$, $w(i/j; A, B)$ *are collinear and their sum is the direct sum of any two of them,*

*that* $c(i, j)$, $(A, B)$, $w(i/j; A, B)$ *are collinear and that their sum is both the direct sum of* $c(i, j)$ *and* $(A, B)$ *and the direct sum of* $(A, B)$ *and* $w(i/j; A, B)$;

(b) $(c(A)+c(B))(c(i)+c(j))$ $(c(A)+c(B))(c(j)+c(h))=(c(A)+c(B))(c(h)+c(i))=0$ *for three different integers* $i, j, h$ *implies the collinearity of* $w(i/j; A, B)$, $w(h/j; A, B)$ *and* $c(i, h)$.

The formula defining $w(i/j; A, B)$ is meaningful if, and only if, $c(i)c(A)=c(B)c(j)=0$. But we shall consider this function only, if

$$(c(A)+c(B))(c(i)+c(j))=0.$$

**Proof.** If $(c(A)+c(B))(c(i)+c(j))=0$ and $i\neq j$, then it follows from property (d) of the vector definition and from Lemma III.4.1 that the two triplets $c(i, j)$, $(i, A)$, $(j, A)$ and $(A, B)$, $(j, B)$, $(j, A)$ are collinear; and hence it follows from Lemma III.1.2 that the triplets $(i, A)$, $(j, B)$, $w(i/j; A, B)$ and $c(i, j)$, $(A, B)$, $w(i/j; A, B)$ are collinear too.

Since it follows from our hypothesis and Lemma III.4.1 that $0=(c(A)+c(B))(c(i)+c(j))=((A, B)+c(A))(c(i)+c(i, j))$, and since $c(A)(i, A)=0$ by (e) of the preceding section, it follows from Lemma I.1.1 that

$$\begin{aligned}(i, A)w(i/j; A, B) &= (i, A)(c(i)+c(A))(c(i, j)+(A, B))w(i/j; A, B)\\ &= (i, A)(c(i)c(i, j)+c(A)(A, B))w(i/j; A, B)\\ &= (i, A)c(A)(A, B)w(i/j; A, B)=0;\end{aligned}$$

and likewise it follows that

$$\begin{aligned}(i, A)(j, B) &= (i, A)(c(i)+c(A))(c(j)+c(B))(j, B)\\ &= (i, A)(c(i)c(j)+c(A)c(B))(j, B)\\ &= (i, A)c(A)c(B)(j, B)=0.\end{aligned}$$

The sum of the collinear triplet $(i, A)$, $(j, B)$, $w(i/j; A, B)$ is therefore the direct sum of the two cycles $(i, A)$ and $(j, B)$ of order $m$; and $(i, A)\ w(i/j; A, B) = 0$ implies therefore that $w(i/j; A, B)$ cannot contain more than one subcycle of order 1. Thus it follows from Theorem I.3.7 that $w(i/j; A, B)$ is a cycle; and the remainder of (a) is readily proved.

In order to prove (b) we assume first in addition to the special hypotheses of (b) that $0 = c(A)(c(i)+c(j)+c(h))$. Then it follows from Lemma I.1.1 and $(c(A)+(A, B))(c(j)+c(i, j)) = 0$ that

$$\begin{aligned}(j, A)(c(i, j) + (A, B)) &= (j, A)(c(j) + c(A))(c(i, j) + (A, B)) \\ &= (j, A)(c(j)c(i, j) + c(A)(A, B)) \\ &= (j, A)c(A)(A, B) = 0\end{aligned}$$

and likewise that $(j, A)(c(h, j)+(A, B)) = 0$; and it follows from Dedekind's law and $c(j)(c(i, j)+c(j, h)) = 0$ that

$$\begin{aligned}&(j, A)(c(i, j) + c(j, h)) \\ &\quad = (j, A)(c(j) + c(A))(c(i) + c(j) + c(h))(c(i, j) + c(j, h)) \\ &\quad = (j, A)(c(j) + c(A)(c(i) + c(j) + c(h)))(c(i, j) + c(j, h)) \\ &\quad = (j, A)c(j)(c(i, j) + c(j, h)) = 0.\end{aligned}$$

Hence we have shown that the seven cycles $c(i,j)$, $c(h,j)$, $(A, B) / (j, A) / (i, A)$, $(h, A)$, $(j, B)$ are in Desargues order; and it follows from part (a) of this lemma that their uniquely determined connecting links are the cycles $w(h/j; A, B)$, $w(i/j; A, B)$, $c(i, h)$ and that their collinearitv is a consequence of Theorem III.2.2.

To derive the general case of (b) from the special case already proved we note that $c(A)+c(B)+c(i)+c(j)+c(h)$ is a sum of five cycles; and hence it follows from $5 < n$ and from Corollary I.3.4 that there exists an integer $k$, different from $i, j, h$, such that

$$c(k)(c(A) + c(B) + c(i) + c(j) + c(h)) = 0.$$

Thus it follows from $(c(A)+c(B))(c(i)+c(j)) = 0$ that

$$(c(A) + c(B))(c(i) + c(j) + c(k)) = 0;$$

and likewise that

$$\begin{aligned}(c(A) + c(B))(c(j) + c(h) + c(k)) &= 0, \\ (c(A) + c(B))(c(h) + c(i) + c(k)) &= 0;\end{aligned}$$

and hence it follows from what we have shown in the preceding paragraph that $w(i/j; A, B)$, $w(k/j; A, B)$, $c(i, k)$ and $w(k/j; A, B)$, $w(h/j; A, B)$, $c(k, h)$ are collinear triplets.

Using (a) and Lemma I.1.1 it follows that

$$(k, A)(w(k/j; A, B) + c(k, h))$$
$$= (k, A)(c(k) + c(A))((A, B) + c(k, j) + c(k, h))(w(k/j; A, B) + c(k, h))$$
$$= (k, A)(c(A)(A, B) + c(k)(c(k, j) + c(k, h)))(w(k/j; A, B) + c(k, h))$$
$$= (k, A)c(A)(A, B)(w(k/j; A, B) + c(k, h)) = 0$$

and likewise that

$$(k, A)(w(k/j; A, B) + c(k, i)) = 0;$$

and since $(k, A)(c(k, h)+c(k, i)) = 0$ may be shown as before, it follows that the seven cycles $w(k/j; A, B)$, $c(k, h)$, $c(k, i)$ / $(k, A)$ / $(j, B)$, $(h, A)$, $(i, A)$ are in Desargues order; and hence it follows from Theorem III.2.2 that their uniquely determined connecting links $c(i, h)$, $w(i/j; A; B)$, $w(h/j; A, B)$ are collinear, completing the proof of (b).

The following two remarks will simplify the handling of the function $w(i/j; A, B)$. It is a consequence of its defining equation and of $(A, B) = (B, A)$ that

$$w(i/j; A, B) = w(j/i; B, A);$$

and hence it follows under the hypotheses of Lemma III.4.2, (b) that $w(i/j; A, B)$, $w(i/h; A, B)$, $c(j, h)$ *are collinear.*

LEMMA III.4.3. *If $A$ and $B$ are vectors over $S$ such that $c(A)$ and $c(B)$ are parts of $g$, then*

(a) $(c(A)+c(B))(c(i)+c(j)) = 0$ *and* $i \neq j$ *imply that* $z(i/j; A, B) = (w(i/j; A, B)+c(j))(c(i)+(A, B))$ *is a cycle of order* $m$,

*that $z(i/j; A, B)$, $w(i/j; A, B)$, $c(j)$ are collinear and their sum is the direct sum of any two of them,*

*that $z(i/j; A, B)$, $(A, B)$, $c(i)$ are collinear and their sum is both the direct sum of $z(i/j; A, B)$ and $(A, B)$ and the direct sum of $(A, B)$ and $c(i)$,*

*that $z(i/j; A, B)$, $(i, A)$, $c(B)$ are collinear;*

(b) $(c(A)+c(B))(c(i)+c(j)) = (c(A)+c(B))(c(i)+c(h)) = 0$ *for three different integers $i, j, h$ imply $z(i/j; A, B) = z(i/h; A, B)$.*

**Proof.** Since it follows from Lemma III.4.2 and the definition of a complete simplex that the triplets $w(i/j; A, B)$, $(A, B)$, $c(i, j)$ and $c(j)$, $c(i)$, $c(i, j)$ are collinear, we may infer from Lemma III.1.2 that the triplets $z(i/j; A, B)$, $w(i/j; A, B)$, $c(j)$ and $z(i/j; A, B)$, $c(i)$, $(A, B)$ are collinear. Since $c(A)+c(B)+c(i)+c(j)$ is the direct sum of $c(A)+c(B)$, $c(i)$ and $c(j)$, it follows from $(A, B) \leqq c(A)+c(B)$ and $z(i/j; A, B) \leqq c(i)+(A, B)$ that $z(i/j; A, B)c(j) = 0$; and similarly we see that $w(i/j; A, B)c(j) = 0$. From these facts one derives as usual all the statements of (a) except the last one. This last statement is a consequence of Theorem III.2.1, since $z(i/j; A, B)$, $(i, A)$, $c(B)$ are connecting links of the two triplets $c(A)$, $(A, B)$, $c(i)$ and $(j,B)$, $c(j)$, $w(i/j; A, B)$, and since $c(j)(c(A)+(A, B)+c(i)) = 0$, as has been pointed out before.

In order to prove (b) we assume first that—in addition to the other hypotheses—$(c(A)+c(B))(c(i)+c(j)+c(h))=0$. Then $c(i, h)((A, B)+c(j, i))=0$ $=c(i, h)((A, B)+c(i))$; and thus the seven cycles $c(j, i)$, $c(i)$, $(A, B)$ / $c(i, h)$/ $c(j, h)$, $c(h)$, $w(i/h; A, B)$ are in Desargues order, as follows from Lemma III.4.2 and the properties of a complete simplex. Thus their connecting links are uniquely determined; they are—by Lemma III.4.2—the cycles $z(i/h; A, B)$, $w(i/j; A, B)$, $c(j)$; and the collinearity of these cycles is a consequence of Theorem III.2.2. Thus

$$z(i/h; A, B) \leqq (w(i/j; A, B) + c(j))(c(i) + (A, B)) = z(i/j; A, B);$$

and this inequality implies equality, since every $z(\cdots)$ has been shown to be a cycle of order $m$.

To derive the general case of (b) from the special case we have proved just now, we note first that there exists an integer $k$ such that $c(k)(c(i)+c(j)$ $+c(h)+c(A)+c(B))=0$, since $5<n$, since $c(i)+c(j)+c(h)+c(A)+c(B)$ is a sum of five cycles and therefore by Corollary I.3.4 a direct sum of at most five cycles. Hence it follows from our hypothesis that $(c(A)+c(B))(c(i)+c(j)$ $+c(k))=0=(c(A)+c(B))(c(i)+c(h)+c(k))$; and from what has been shown already it follows that

$$z(i/j; A, B) = z(i/k; A, B) = z(i/h; A, B),$$

as was to be shown.

If $A$ and $B$ are vectors over $S$ such that $c(A)$ and $c(B)$ are parts of $g$, then there exist integers $i$ such that $c(i)(c(A)+c(B))=0$; and to every $i$ satisfying this condition there exist integers $j\neq i$ such that $(c(i)+c(j))(c(A)+c(B))=0$. It is a consequence of Lemma III.4.3, (b) that the cycle $z(i/j; A, B)$ is independent of the choice of $j$; and thus the following *definition* is well determined.

DEFINITION. *If* $c(i)(c(A)+c(B))=0$, *then* $z(i; A, B)=z(i/j; A, B)$ *for every* $j\neq i$ *such that* $(c(i)+c(j))(c(A)+c(B))=0$.

LEMMA III.4.4. *If* $A$ *and* $B$ *are vectors over* $S$ *such that* $c(A)+c(B)\leqq g$, *and if* $c(i)(c(A)+c(B))=c(j)(c(A)+c(B))=0$ *for* $i\neq j$, *then* $z(i; A, B)$, $z(j; A, B)$ *and* $c(i, j)$ *are collinear.*

**Proof.** From $5<n$ we infer as usual the existence of an integer $h$ such that $c(h)(c(i)+c(j)+c(A)+c(B))=0$. From the hypothesis of this lemma it follows now that $(c(i)+c(h))(c(A)+c(B))=0=(c(j)+c(h))(c(A)+c(B))$ so that $z(i; A, B)=z(i/h; A, B)$, $z(j; A, B)=z(j/h; A, B)$. The three cycles $z(i; A, B)$, $z(j; A, B)$, $c(i, j)$ are therefore connecting links of the two triplets $c(j)$, $c(i)$, $(A, B)$ and $w(j/h; A, B)$, $w(i/h; A, B)$, $c(h)$, as follows from Lemma III.4.2, (b) and Lemma III.4.3, (a); and the collinearity of these connecting links is a consequence of Theorem III.2.1, since $c(h)(c(i)+c(j)+(A, B))=0$.

If $A$ and $B$ are any two vectors over $S$ such that $c(A)+c(B)\leqq g$, then there exist integers $i\neq j$ such that $(c(A)+c(B))(c(i)+c(j))=0$. Thus $(A, B)$ is a

well determined cycle (contained in $c(A)+c(B)$ so that $n((A, B)) \leqq m$ by Theorem I.2.1) by Lemma III.4.1 and the cycles $z(i; A, B)$ and $z(j; A, B)$ are well determined by Lemma III.4.3, (b). It follows finally from Lemma III.4.4 and Theorem III.3.2 that there exists one and only one vector $D$ over $S$ such that $c(D) = (A, B)$ and such that $(i, D) = z(i; A, B)$ for every $i$ such that $c(i)(c(A)+c(B)) = 0$; and this vector $D$ over $S$ which is uniquely determined by $A$ and $B$ shall be termed *the difference $A - B$ of $A$ and $B$.*

There exists one and only one vector 0 over $S$ satisfying $c(0) = 0$ and $(i, 0) = c(i)$ for every $i$; and one verifies readily that 0 is the only vector $V$ over $S$ such that $c(V) = 0$.

LEMMA III.4.5. *If $A$ is a vector over $S$ such that $c(A) \leqq g$, then*

(i) $A - A = 0$,

(ii) $A = A - 0$,

(iii) $A = 0 - (0 - A)$.

**Proof.** There exist integers $i \neq j$ such that $c(A)(c(i)+c(j)) = 0$. Thus it follows from Lemma III.4.1 that $c(A - A) = (A, A) = c(A)(i, A) = 0$ by (e) of §3 of this part and this implies $A - A = 0$ by Lemma III.4.3. It follows furthermore from Lemma III.4.1 and (c) of §3 that

$$c(A - 0) = (A, 0) = (c(A) + 0)((i, A) + c(i)) = c(A)((i, A) + c(i)) = c(A);$$

and hence it follows from Lemma III.4.3 that

$$\begin{aligned}(i, A - 0) &= z(i; A, 0) = z(i/j; A, 0) = (c(i) + c(A))(c(j) + w(i/j; A, 0)) \\ &= (c(i) + c(A))(c(j) + (c(i, j) + c(A))((i, A) + c(j))) \\ &= (c(i) + c(A))(c(j) + c(i, j) + c(A))((i, A) + c(j)) \\ &= (c(i) + c(A))((i, A) + c(j)) = (i, A) \quad \text{or} \quad A - 0 = A.\end{aligned}$$

To prove (iii) we note that $c(0 - A) = (0, A) = (A, 0) = c(A - 0) = c(A)$ and that therefore $w(i/j; 0, A) = (c(i, j)+c(A))(c(i)+(j, A))$, $c(A) \leqq c(i, j)+c(A) = c(i, j)+w(i/j; 0, A)$ by Lemma III.4.2, (a) and $(i, 0 - A) = z(i/j; 0, A) = (c(i)+c(A))(c(j)+w(i/j; 0, A))$ so that

$$\begin{aligned}c(0 - (0 - A)) &= (0, 0 - A) = (0 + c(A))(c(i) + (i, 0 - A)) \\ &= c(A)(c(i) + (c(i) + c(A))(c(j) + w(i/j; 0, A))) \\ &= c(A)(c(i) + c(j) + w(i/j; 0, A))(c(i) + c(A)) = c(A)\end{aligned}$$

by Dedekind's law and Lemma III.4.1; and consequently it follows from Lemmas III.4.1, III.4.3 and III.4.4 that

$$\begin{aligned}w(i/j; 0, 0 - A) &= (c(i, j) + c(A))(c(i) + (j, 0 - A)) \\ &= (c(i, j) + c(A))(c(i) + z(j/i; 0, A)) \\ &= (c(i, j) + c(A))(c(i) + w(j/i; 0, A)) \\ &= (c(i, j) + (A, 0))(c(i) + w(i/j; A, 0)) = w(i/j; A, 0)\end{aligned}$$

and

$$(i, 0-(0-A)) = (c(i)+c(A))(c(j)+w(i/j; 0, 0-A))$$
$$= (c(i)+c(A))(c(j)+w(i/j; A, 0)) = z(i/j; A, 0) = (i, A)$$

by (ii); and hence $0-(0-A)=A$.

LEMMA III.4.6. *If $A, B, C$ are vectors over $S$ such that $s=c(A)+c(B)+c(C)$ is contained in $g$, then $(A-B)-C=(A-C)-B$.*

The proof of this associative law of subtraction will be effected in a number of steps.

(1) *$c(A-B)$, $c(B-C)$, $c(C-A)$ are collinear.*

There exists an integer $i$ such that $sc(i)=0$. Then the seven cycles $(i, A)$, $(i, B)$, $(i, C)$ / $c(i)$ / $c(A)$, $c(B)$, $c(C)$ are in Desargues order and their uniquely determined connecting links $c(B-C)$, $c(C-A)$, $c(A-B)$—by Lemma III.4.1—are collinear by Theorem III.2.2.

(2) *If $(c(i)+c(j))s=0$ for $i\neq j$, then the two triplets $c(B-C)$, $w(i/j; A, C)$, $w(i/j; A, B)$ and $c(A-B)$, $w(i/j; A, C)$, $w(i/j; B, C)$ are collinear.*

The seven cycles $c(A-B)$, $c(A-C)$, $c(i, j)$ / $(j, A)$ / $(j, B)$, $(j, C)$, $(i, A)$ are in Desargues order by Lemma III.4.1 and the definition of vectors, since

$$(j, A)(c(A-B)+c(A-C)+c(i, j)) \leqq (j, A)(c(j)+c(A))(c(i, j)+s)$$
$$\leqq (j, A)(c(A)+c(j)(s+c(i, j)))$$
$$= (j, A)c(A) = 0;$$

their connecting links are by (1) and Lemma III.4.2 the cycles $w(i/j; A, C)$, $w(i/j; A, B)$, $c(B-C)$ and their collinearity is a consequence of Theorem III.2.2.—The collinearity of the second triplet is immediately inferred from the collinearity of the first triplet, if one remembers that $w(i/j; X, Y) = w(j/i; Y, X)$.

(3) *If $c(i)s=0$, then the two triplets $(i, A-B)$, $(i, A-C)$, $c(B-C)$ and $(i, A-C)$, $(i, B-C)$, $c(A-B)$ are collinear.*

There exists some $j\neq i$ such that $s(c(i)+c(j))=0$. Then the cycles of the first triplet are connecting links of the two triplets $c(A-C)$, $c(A-B)$, $c(i)$ and $w(i/j; A, C)$, $w(i/j; A, B)$, $c(j)$, as follows from (1), (2), Lemma III.4.3; and thus the collinearity of the first triplet is a consequence of Theorem III.2.1, since $c(j)(c(i)+c(A-C)+c(A-B)) \leqq c(j)(c(i)+s)=0$.—The cycles of the second triplet are likewise connecting links of the triplets $(i, B)$, $(i, A)$, $c(C)$ and $w(i/j; B, C)$, $w(i/j; A, C)$, $c(j)$; and the collinearity of the second triplet follows from Theorem III.2.1, since $c(j)(c(C)+(i, A)+(i, B)) \leqq c(j)(c(i)+s)=0$.

Since $5<n$, there exist three different integers $i, j, h$ such that $(c(i)+c(j)+c(h))s=0$; and these three integers shall be kept fixed throughout the remainder of the proof.

(4) *$w(i/j; B, C)$, $w(j/h; C, A)$, $w(h/i; A, B)$ are collinear.*

One verifies readily that $c(A-B)(j, C)=(c(A-B)+(j, C))(i, B)=(c(A-B)+(j, C)+(i, B))(h, A)=0$. It follows from (2) and Lemma III.4.2 that $w(i/j; B, C)$, $w(j/h; C, A)$, $w(h/i; A, B)$ are connecting links of the two triplets $(h, A)$, $(i, B)$, $(j, C)$ and $c(h, i)$, $c(A-B)$, $w(i/j; A, C)$; and (4) is now a consequence of Theorem III.2.1, since the above equations imply $c(A-B)((h, A)+(i, B)+(j, C))=0$.

We introduce now three auxiliary vectors. If $X$ is any of the vectors $A$, $B$, $C$ under consideration, then $X_h$ is the—by Theorem III.3.2 uniquely determined—vector satisfying $c(X_h)=(h, 0-X)$, $(i, X_h)=w(h/i; 0, X)$. It is an immediate consequence of Lemmas III.4.2 and III.4.3 that $(j, X_h)=w(h/j; 0, X)$. We are not able to say anything concerning the $h$-coordinate of this vector $X_h$.

We note furthermore that $(c(i)+c(j))(c(A_h)+c(B_h)+c(C_h))=(c(i)+c(j))((h, 0-A)+(h, 0-B)+(h, 0-C))\leqq(c(i)+c(j))(c(h)+s)=0$ so that the statements (2) and (3) may be applied upon $A_h$, $B_h$, $C_h$ too.

(5) *If $X$ and $Y$ are two of the vectors $A$, $B$, $C$, then $X-Y=X_h-Y_h$.*

It is a consequence of $s(c(i)+c(j)+c(h))=0$ and of (2), (3) that the two triplets $c(X-Y)$, $(h, 0-X)$, $(h, 0-Y)$ and $c(X-Y)$, $w(h/i; 0, X)$, $w(h/i; 0, Y)$ are collinear triplets. Since furthermore

$$\begin{aligned}(h, 0-X)(w(h/i; 0, X)+w(h/i; 0, Y)) &\leqq (h, 0-X)(c(h)+c(X))(c(h, i)+c(X)+c(Y))\\ &\leqq (h, 0-X)c(X)=0,\end{aligned}$$

it follows from Dedekind's law and the definition of the cycle generated by the difference of vectors (cf. Lemma III.4.1) that

$$\begin{aligned}c(X_h-Y_h) &= ((h, 0-X)+(h, 0-Y))(w(h/i; 0, Y)+w(h/i; 0, X))\\ &= c(X-Y)+(h, 0-X)(w(h/i; 0, Y)+w(h/i; 0, X))\\ &= c(X-Y).\end{aligned}$$

It is a consequence of (4) that the cycles $w(i/j; X, Y)$, $w(j/h; Y, 0)$, $w(h/i; 0, X)$ are collinear; and it is a consequence of Lemma III.4.2 that the cycles $c(i, j)$, $c(X-Y)$, $w(i/j; X, Y)$ are collinear. Thus it follows that $w(i/j; X, Y)\leqq(c(i, j)+c(X-Y))(w(h/i; 0, X)+w(h/j; 0, Y))=(c(i, j)+c(X_h-Y_h))((i, X_h)+(i, Y_h))=w(i/j; X_h, Y_h)$; and this inequality implies equality, since the cycles $w(i/j; \cdots)$ are of order $m$. From the equalities thus obtained, it follows that $z(i/j; X, Y)=z(i/j; X_h, Y_h)$ (cf. Lemma III.4.3); and hence $(i, X-Y)=(i, X_h-Y_h)$ and $X-Y=X_h-Y_h$ is now a consequence of Theorem III.3.2.

(6) *$(i, A-C)$, $(j, A-B)$, $w(i/j; B, C)$ are collinear.*

It follows from (2) that $w(i/j; B_h, 0)$, $c(C_h)=c(C_h-0)$—by Lemma III.4.5, (ii)—and $w(i/j; B_h, C_h)$ are collinear; and from (3) that $(i, A_h-B_h)$, $c(B_h-C_h)$,

$(i, A_h - C_h)$ are collinear. The three cycles $(i, A_h)$, $(j, A_h - B_h)$, $w(i/j; B_h, 0)$ are collinear, since they are—by Lemmas III.4.1 to III.4.3—connecting links of the two triplets $c(B_h)$, $c(i, j)$, $(j, A_h)$ and $c(j)$, $(i, B_h)$, $c(A_h - B_h)$, and since Theorem III.2.1 may be applied as a consequence of

$$\begin{aligned} c(B_h)(c(j) + (i, B_h) + c(A_h - B_h)) \\ &= (h, 0 - B)(c(j) + w(h/i; 0, B) + c(A - B)) \\ &\leqq (h, 0 - B)(c(h) + c(B))(c(j) + c(h, i) + c(A) + c(B)) \\ &= (h, 0 - B)c(B) = 0. \end{aligned}$$

Since $c(B_h) = (h, 0 - B)$ is a cycle of order $m$, and since $c(B_h)(c(i, j) + c(B_h - C_h) + (i, A_h - B_h)) = (h, 0 - B)(c(i, j) + c(B - C) + (i, A - B)) \leqq (h, 0 - B)(c(i) + c(j) + c(A) + c(B) + c(C)) = 0$, it follows that the seven cycles $w(i/j; B_h, 0)$, $c(C_h)$, $(i, A_h) / c(B_h) / c(i, j)$, $c(B_h - C_h)$, $(i, A_h - B_h)$ are in Desargues order, that $(i, A_h - C_h)$, $(j, A_h - B_h)$, $w(i/j; B_h, C_h)$ are their uniquely determined connecting links; and (6) is now a consequence of Theorem III.2.2 and of (5).

(7) $c((A - B) - C) = c((A - C) - B)$.

The three cycles $c((A - B) - C)$, $(i, A - C)$, $(i, B)$ are collinear, since they are—by (b)—connecting links of the two triplets $(i, A)$, $c(A - B)$, $c(C)$ and $w(i/j; B, C)$, $(j, C)$, $(j, A - B)$, and since Theorem III.2.1 may be applied as a consequence of $(j, C)((i, A) + c(A - B) + c(C)) \leqq (j, C)(c(i) + s)) = 0$.

$c(i)s = 0$ implies that the seven cycles $(i, A)$, $(i, A - B)$, $(i, C) / c(i) / c(A)$, $c(A - B)$, $c(C)$ are in Desargues order; and it follows from Theorem III.2.2 that their connecting links $c((A - B) - C)$, $c(A - C)$, $c(B)$ are collinear. Consequently we find that

$$c((A - B) - C) \leqq (c(A - C) + c(B))((i, A - C) + (i, B)) = c((A - C) - B)$$

and the symmetry of our hypotheses on $B$ and $C$ implies the opposite inequality, proving the desired equation (7).

(8) $c(h) = c(A - A_h)$.

Since $c(h) \leqq ((h, 0 - A) + c(A))(w(h/i; 0, A) + (i, A)) = c(A_h - A)$ as a consequence of Lemmas III.4.1 to III.4.4, the equation (8) may be inferred from the fact that $n(c(A - A_h)) \leqq m = n(c(h))$.

(9) *$c(h)$, $c(A_h - X)$, $c(A - X)$ and $c(h)$, $(k, A_h - X)$, $(k, A - X)$ are collinear triplets for $X = B$, $C$ and $k = i, j$.*

This is an immediate consequence of (8), (4) and (1)

(10) *$c(h)$, $c((A_h - B) - C)$, $c((A - B) - C)$ are collinear.*

For they are connecting links of the seven cycles $(i, C)$, $(i, A_h - B)$, $(i, A - B) / c(i) / c(C)$, $c(A_h - B)$, $c(A - B)$ which are in Desargues order, since $c(i)(c(A - B) + c(A_h - B) + c(C)) \leqq c(i)(c(h) + s) = 0$, and since therefore Theorem III.2.2 may be applied.

(11) *$c(h)$, $w(i/j; A_h - B, C)$, $w(i/j; A - B, C)$ are collinear.*

Since $(i, C)$ is a cycle of order $m$, since $(i, C)(c(i, j)+c((A-B)-C)+c((A_h-B)-C)) \leqq (i, C)(c(i,j)+c(h)+s)=0$, it follows that the seven cycles $c(i, j)$, $c((A-B)-C)$, $c((A_h-B)-C)$ / $(i, C)$ / $(j, C)$, $(i, A-B)$, $(i, B_h-B)$ are in Desargues order so that their connecting links—by (10) and (9)—$c(h)$, $w(i/j; A_h-B, C)$, $w(i/j; A-B, C)$ are collinear as a consequence of Theorem III.2.2.

(12) $(j, B)$, $(i, A-C)$, $w(i/j; A-B, C)$ *are collinear.*

The seven cycles $c(B-C)$, $(j, C)$, $(i, A_h-B)$ / $(i, C)$ / $(i, B)$, $c(i, j)$, $c((A_h-B)-C)$ are in Desargues order, since $(i, C)$ is a cycle of order $m$, and since $(i, C)(c(B-C)+(j, C)+(i, A_h-B)) \leqq (i, C)(s+c(j)+(i, A_h)) \leqq (i, C)(s+c(j)+w(h/i; 0, A))=(i, C)(s+c(j)+c(h, i))=0$. Since the cycles $w(i/j; A_h-B, C)$, $(i, A_h-C)$, $(j, B)$ are by (3) and (7) their connecting links, it follows from Theorem III.2.2 that they are collinear. Using this fact and (9), (11) we find that

$$\begin{aligned} c(h)+w(i/j; A-B, C)+(j, B) &= c(h)+w(i/j; A_h-B, C)+(j, B) \\ &= c(h)+(j, B)+(i, A_h-C) \\ &= c(h)+(i, A-C)+w(i/j; A-B, C) \\ &= c(h)+(i, A_h-C)+w(i/j; A_h-B, C). \end{aligned}$$

Since $c(h)((j, B)+(i, A-C)+w(i/j; A-B, C)) \leqq c(h)(s+c(j)+c(i))=0$, these identities imply that

$$\begin{aligned} &(j, B)+(i, A-C)+w(i/j; A-B, C) \\ &\quad = (j, B)+(i, A-C) \\ &\quad = (i, A-C)+w(i/j; A-B, C) = (j, B)+w(i/j; A-B, C), \end{aligned}$$

as was to be shown.

It follows now from (12) and (7) and Lemmas III.4.1 to III.4.4 that $w(i/j; A-B, C) \leqq ((j, B)+(i, A-C))(c(i, j)+c((A-C)-B))=w(i/j; A-C, B)$; thus $w(i/j; A-B, C)=w(i/j; A-C, B)$, since they are both cycles of order $m$. But now it follows from (7) that $z(i/j; A-B, C)=z(i/j; A-C, B)$ and that consequently $z(i; A-B, C)=z(i; A-C, B)$ or $(i, (A-B)-C)=(i, (A-C)-B)$; and $(A-B)-C=(A-C)-B$ is now a consequence of (7) and Theorem III.3.2.

LEMMA III.4.7. *If $t \leqq g$, then the set $(S; t)$ of all the vectors $V$ over $S$ which satisfy $c(V) \leqq t$ is an abelian group (under the definition of subtraction introduced in connection with Lemma* III.4.4).

**Proof.** If the vectors $A$ and $B$ over $S$ belong to $(S; t)$, then it follows from Lemmas III.4.4 and III.4.1 that $A-B$ is a uniquely determined vector over $S$ which satisfies: $c(A-B) \leqq c(A)+c(B) \leqq t$; and thus $(S; t)$ contains with any two vectors over $S$ their uniquely determined difference. It is a consequence

of Lemmas III.4.5 and III.4.6 that this subtraction in $(S; t)$ satisfies furthermore the following rules.

(A) There exists one and only one element 0 in $(S; t)$ satisfying $0=A-A$, $A=A-0=0-(0-A)$ for every $A$ in $(S; t)$.

(B) If $A$, $B$, $C$ are elements in $(S; t)$, then $(A-B)-C=(A-C)-B$.

To prove that $(S; t)$ is an abelian group, we define *addition*[37]:

$$A+B=0-((0-A)-B)$$

for $A$ and $B$ in $(S; t)$.

It is obvious that the sum of two elements in $(S; t)$ is a uniquely determined element in $(S; t)$; and the commutativity of addition is a consequence of (B). Next one infers from these rules that

$$\begin{aligned} A+(B-A) &= 0-((0-A)-(B-A)) = 0-((0-(B-A))-A) \\ &= 0-(((B-B)-(B-A))-A) \\ &= 0-(((B-(B-A))-B)-A) \\ &= 0-(((B-(B-A))-A)-B) \\ &= 0-(((B-A)-(B-A))-B) = 0-(0-B) = B, \end{aligned}$$

so that $B-A$ is a solution of the equation $A+X=B$. Finally one verifies the associative law of addition as follows

$$\begin{aligned} &A+(B+C) \\ &\quad = 0-((0-A)-(B+C)) = 0-((0-A)-(0-((0-B)-C))) \\ &\quad = 0-((0-(0-((0-B)-C)))-A) = 0-(((0-B)-C)-A) \\ &\quad = 0-(((0-B)-A)-C) = 0-(((0-A)-B)-C) \\ &\quad = 0-((0-(0-((0-A)-B)))-C) = 0-((0-(A+B))-C) \\ &\quad = (A+B)+C; \end{aligned}$$

and this completes the proof of Lemma III.4.7.

LEMMA III.4.8. *If $t<u\leqq g$, and if the maximum order of the subcycles of $u$ does not exceed $m$, then there exists a vector $V$ over $S$ such that $c(V)\leqq u$, though $c(V)$ is not part of $t$.*

**Proof.** Since the parts of $g$ are sums of cycles, there exists a cycle $z$ such that $z\leqq u$, though $z$ is not part of $t$. From our hypothesis it follows that

---

(37) See in this context the following treatments of the postulates of subtraction in abelian groups: M. Ward, these Transactions, vol. 32 (1930), pp. 520–526; D. G. Rabinow, American Journal of Mathematics, vol. 59 (1937), pp. 211–224, 385–392; B. A. Bernstein, these Transactions, vol. 43 (1938), pp. 1–6.

$n(z) \leqq m$. But we proved as a corollary to Theorem III.3.2 the existence of a vector $V$ over $S$ such that $c(V) = z$; and this is just the statement to be proved.

LEMMA III.4.9. *If $z_1, \cdots, z_k$ are subcycles of $g$, and if $V$ is a vector over $S$ such that $c(V) \leqq z_1 + \cdots + z_k$, then there exist vectors $V_i$ over $S$ such that $c(V_i) \leqq z_i$ and $V = V_1 + \cdots + V_k$ (using addition as in Lemma* III.4.7).

For the proof of this theorem we shall need the following lemma.

LEMMA III.4.10. *If $u$ and $v$ are cycles such that $uv = 0$ and such that $u+v$ is primary and splits completely, and if the elements $u, v, t$ are collinear, then there exists a subcycle $d$ of $t$ such that $u, v, d$ are collinear.*

**Proof of Lemma** III.4.10. If $t = u+v$, then follows from Lemma I.3.8 the existence of a cycle $d \leqq t$ which is not a subcycle of any proper partial sum of $u+v$ and $u, v, d$ are clearly collinear.

Thus we assume now that $t < u+v$; and we may assume without loss in generality that $0 < n(u) \leqq n(v) = k$. Since $(u+v)/u$ is a cycle of order $k$, there exists between $u$ and $u+v$ an element $r$ such that $(u+v)/r$ is a cycle of order 1. Since $t+u = u+v$, it follows that $t \leqq r$ does not hold; and since $t$ is a sum of cycles, there exists a subcycle $d$ of $t$ which is not part of $r$. Thus $d+u \leqq r$ does not hold and this implies $d+u = u+v$. Since the orders of the subcycles of $u+v$ do not exceed $k$—by Theorem I.2.1—and since $(u+v)/u$ is a cycle of order $k$, it follows that $n(d) = k$ and $du = 0$. Since $t$ splits as a part of $u+v$, and since $d$ is a subcycle of maximum order of $t$ (and $u+v$), $t$ is the direct sum of $d$ and of a cycle $e$ of order $j$; and $t < u+v = u+d$ implies $j < n(u)$. The cross-cut $dv$ is a cycle of order $i$; and $d+v$ is—as before—the direct sum of $v$ and of a cycle $z$ of order $k-i$. Since $u+v = e+d+v = e+z+v$, and since $n(e) < n(u)$, it follows from Corollary I.3.4 that $k-i = n(z) \not< n(u)$ or $n(u) \leqq n(z)$ and hence $d+v = z+v = u+v$ is a consequence of Corollary I.3.4 so that $u, v, d$ are collinear.

**Proof of Lemma** III.4.9. Since Lemma III.4.9 is certainly true for $k = 1$, we may assume that it holds true for vectors $W$ such that $c(W) \leqq \sum_{i=1}^{k-1} z_i = s$. Since $z_k$ is a cycle, there exists a uniquely determined subcycle $z$ of $z_k$ such that $s + c(V) = s + z$—note $c(V) \leqq s + z_k$. It follows from Lemma III.1.1 that $c(V), z$ and $s(c(V)+z) = t$ are collinear. From $5 < n$ we infer the existence of an integer $i$ such that $c(i)(z + c(V)) = 0$. The $i$th coordinate $(i, V)$ of the vector $V$ is therefore a well determined cycle. If $r = (c(i)+z)(t+(i, V))$, then it follows from Lemma III.1.2 that the triplets $r$, $c(i)$, $z$ and $r$, $t$, $(i, V)$ are collinear, since the triplets $c(i)$, $(i, V)$, $c(V)$ and $z$, $t$, $c(V)$ are collinear. Since $c(i)z = 0$, it follows from Lemma III.4.10 that there exists a subcycle $d$ of $r$ such that $d, c(i), z$ are collinear. By Theorem III.3.2 there exists one and only one vector $B$ such that $c(B) = z$, $(i, B) = d$.

We note $c(B) \leqq z_k$. Since furthermore

$$c(V - B) = (c(V) + c(B))((i, V) + (i, B)) = (c(V) + z)((i, V) + d)$$
$$\leqq (c(V) + z)((i, V) + r) = (c(V) + t)((i, V) + t)$$
$$= t + (i, V)(c(V) + z) = t,$$

$V-B$ is a vector such that $c(V-B) \leqq z_1 + \cdots + z_{k-1}$; and hence there exist by our induction hypothesis vectors $V_i$ such that $c(V_i) \leqq z_i$ for $i=1, \cdots, k-1$ and such that $V-B = V_1 + \cdots + V_{k-1}$ or

$$V = V_1 + \cdots + V_{k-1} + B,$$

as was to be shown.

5. **The existence of primary abelian operator groups.** The term *primary abelian operator group* shall signify an abelian group $G$ and a ring $E$ of endomorphisms of $G$ satisfying the following conditions.

(a) Every right-ideal and every left-ideal in $E$ is two-sided.

(b) There exists an ideal $P$ different from $E$ in $E$ such that every ideal different from 0 and $E$ in $E$ is a power of $P$.

(c) $E$ contains every $D(G; E)$-admissible endomorphism of $G$ (where $D(G; E)$ denotes the Dedekind set of all the $E$-admissible subgroups of $G$).

(d) To every element $x$ in $G$ there exists a positive integer $i$ such that $xP^i = 0$.

Suppose now that the element $g$ of some partially ordered set has the property.

(D, 6) If $g$ contains one subcycle of order $n$, then $g$ contains at least six independent subcycles of order $n$.

It is an immediate consequence of Theorem II.3.1 that the parts of such an element $g$ form the system of admissible subgroups of essentially at most one primary abelian operator group.

THEOREM III.5.1. *If the element $g$ in a partially ordered set satisfies* (D, 6), *then the following conditions are necessary and sufficient for the parts of $g$ to be the admissible subgroups of some primary abelian operator group.*

(A) *The parts of $g$ form a Dedekind set.*

(B) *Sums of a finite number of subcycles of $g$ split completely and are primary.*

(C) *If $M$ is a nonvacuous set of subcycles of $g$ and contains every cycle $z$ which is contained in the sum of a finite number of cycles in $M$, then there exists one and only one part $s(M)$ of $g$ such that $M$ is exactly the set of subcycles of $s(M)$.*

**Proof.** The necessity of (A) is a well known fact in the theory of abelian operator groups, the necessity of (B) is a consequence of Theorems II.2.1, II.2.4 and I.3.7, and the necessity of (C) is a consequence of the fact that by Theorem II.2.1 every element in a primary abelian operator group generates a cycle.

To prove the sufficiency of (A), (B), (C) we show first that:

(+) *The validity of* (A), (B), (C) (*and* (D, 6)) *implies the existence of a primary ring* $D_0$ *of subgroups of an abelian group* $G$ *and of a projectivity of the set of parts of* $g$ *upon* $D_0$.

*Case* 1. The orders of the subcycles of $g$ are bounded.

Then we denote by $m$ the maximum order of the subcycles of $g$. By (D, 6) there exist 6 independent subcycles of order $m$ of $g$; and hence it follows from (A), (B) and Lemma III.3.1 that there exists a complete 6-$m$-simplex $S$ with vertices and links parts of $g$. If $x \leqq g$, then we denote by $(S; x)$ the set of all those vectors $V$ over $S$ which satisfy $c(V) \leqq x$. It is a consequence of Lemma III.4.7 that $(S; x)$ is an abelian group (with regard to the subtraction and addition introduced in (III.4.4)) whenever $x$ is the sum of a finite number of cycles. From this fact one infers immediately that every $(S; x)$ for $x \leqq g$ is an abelian group and moreover a subgroup of the abelian group $G = (S; g)$. If $x$ and $y$ are different parts of $g$, then it follows from (C) that one of them, say $x$, contains a cycle which the other one does not contain; and thus follows from Lemma III.4.8 the existence of a vector $V$ such that $c(V) \leqq x$ though $c(V) \leqq y$ does not hold, that is, $(S; x) \neq (S; y)$ is a consequence of $x \neq y$. But this fact puts into evidence that mapping the part $x$ of $g$ upon the subgroup $(S; x)$ of $G$ constitutes a projectivity of the Dedekind set of the parts of $g$ upon the system $D_0$ of subgroups $(S; x)$ of the abelian group $G$.—If $x \leqq g$, then denote by $M(x)$ the set of all the subcycles of $x$. It follows from (C) that $x = s(M(x))$; and if $M$ is a set of subcycles of $g$, meeting the requirements of (C), then $M = M(s(M))$. If $J$ is any set of parts of $g$, then let $H$ be the cross-cut of all the sets $M(x)$ for $x$ in $J$. Clearly $s(J)$ is the greatest part of $g$ which is contained in all the $x$ in $J$; and $(S; s(J))$ is the cross-cut of all the $(S; x)$ for $x$ in $J$. Denote furthermore by $K$ the set of all the cycles which are contained in the sum of a finite number of cycles from the set $M(x)$ for $x$ in $J$. This set $K$ meets the requirements of (C) and thus $s(K)$ is a well determined part of $g$. Clearly $(S; s(K))$ contains all the subgroups $(S; x)$ for $x$ in $J$; and it follows from the construction of $K$ and from Lemma III.4.9 that $(S; s(K))$ is exactly the subgroup of $G$ which is generated by all the subgroups $(S; x)$ for $x$ in $J$. Thus $D_0$ has been shown to be a ring of subgroups of $G$. If $V$ is any vector over $S$, then the smallest subgroup of $G$ in $D$ containing $V$ is just $(S; c(V))$; and this is a cycle in the set $D_0$, since the map of $x$ upon $(S; x)$ has been shown to be a projectivity. Thus $D_0$ is a primary ring of subgroups; and this completes the proof of (+) in Case 1.

*Case* 2. The orders of the subcycles of $g$ are not bounded.

Then denote by $M(i)$ the set of all the subcycles of $g$ whose order does not exceed $i$. It is a consequence of Theorem I.2.1 that $M(i)$ meets the requirements of (C); and thus there exists a well determined part $g(i) = s(M(i))$ of $g$ which contains every subcycle of order not exceeding $i$ and none of higher order. Since the orders of the subcycles of $g$ are not bounded, it follows from (D, 6) that $g(i)$ contains at least six independent subcycles of order $i$ (the

maximum order in $g(i)$). Since $g(i) \leqq g$ satisfies (with $g$) the conditions (A), (B), (C) it follows from Case 1 that there exists an abelian group $Q(i)$, a primary ring $D(i)$ of subgroups of $Q(i)$ and a projectivity $\boldsymbol{q}(i)$ of the Dedekind set of the parts of $g(i)$ upon the system $D(i)$ of subgroups. Then $\boldsymbol{q}(i)^{-1}\boldsymbol{q}(i+1)$ is a projectivity of $D(i)$ upon the subgroups of $g(i)^{q(i+1)}$ in $D(i+1)$; and it is a consequence of Theorem II.1.3 that this projectivity is induced by an isomorphism of $Q(i)$ upon the subgroup $g(i)^{q(i+1)}$ of $Q(i+1)$ (in $D(i+1)$). Using these facts one immediately constructs an abelian group $G$, subgroups $G_i$ of $G$, a primary ring $T_i$ of subgroups of $G_i$ and a projectivity $\boldsymbol{p}_i$ of the Dedekind set of the parts of $g(i)$ upon the ring $T_i$ of subgroups, meeting the following requirements.

(i) $G_i \leqq G_{i+1}$, $T_i \leqq T_{i+1}$, $\boldsymbol{p}_i$ and $\boldsymbol{p}_{i+1}$ coincide on the parts of $g(i)$.

(ii) Every element in $G$ is contained in some $G_i$.

If $S_i$ is a subgroup of $T_i$, and if $S_i \leqq S_{i+1}$, then there exists one and only one subgroup $S$ of $G$ which contains all the elements in the $S_i$ and no further elements; and the set $D_0$ of all these subgroups of $G$ is clearly a primary ring, the smallest primary ring containing all the $T_i$.—If $x$ is any part of $g$, then it follows from (C) that $x$ is completely determined by the products $xg(i)$; and if $x(i) \leqq g(i)$, $x(i) \leqq x(i+1)$, then the existence of a smallest part $x$ of $g$, containing all the $x(i)$, is readily inferred from (C). Thus it follows easily that there exists one and only one projectivity $\boldsymbol{p}$ of the set of parts of $g$ upon $D_0$ which coincides with $\boldsymbol{p}_i$ on the parts of $g(i)$; and this completes the proof of (+) in Case 2.

If $G$ is an abelian group and $D_0$ a primary ring of subgroups of $G$ such that there exists a projectivity of the parts of $g$ upon $D_0$, then it follows from (D, 6) and Theorem II.1.2 that $D_0$ is the ring $D(G; E)$ of all the $E$-admissible subgroups of $G$ where $E$ is the ring of all the $D_0$-admissible endomorphisms of $G$; and it is a consequence of Theorems II.2.2 and II.2.3 together with the statements (ii), (v) in §II.2, that the right-ideals in $E$ are two-sided; and that every two-sided ideal different from 0 in $E$ is a power of the uniquely determined prime ideal $P$ in $E$. It is a consequence of (B), (C), Theorems I.3.7 and II.2.4 that every left-ideal in $E$ is two-sided; and thus we have shown that $D_0$ is the set of all the admissible subgroups of the primary abelian operator group $G$ over $E$; and this completes the proof.

REMARK. The condition (D, 6) entering into our formulation of the Theorem III.5.1 is patently not necessary for the existence of the primary abelian operator group $G$ over $E$. If we substitute for (D, 6) the condition

(D) *$g$ is contained in an element which satisfies* (A), (B), (C), (D, 6),

then it is readily verified that (D) is necessary and sufficient for the existence of the primary abelian operator group $G$ over $E$.

It is finally an obvious consequence of Theorem II.6.3 that one has to add the conditions (i), (ii) of Theorem II.6.3 to these conditions (A), (B),

(C), (D, 6) (or (D)), in order to assure that the Dedekind set of the parts of $g$ is essentially the same as the set of *all* the subgroups of a suitable primary abelian group.

UNIVERSITY OF ILLINOIS,
URBANA, ILL.