GROUPS WITH PREASSIGNED CENTRAL AND CENTRAL QUOTIENT GROUP*

BY

REINHOLD BAER

Every group G determines two important structural invariants, namely its central $C(G)$ and its central quotient group $Q(G)=G/C(G)$. Concerning these two invariants the following two problems seem to be most elementary. If A and B are two groups, to find necessary and sufficient conditions for the existence of a group G such that A and $C(G)$, B and $Q(G)$ are isomorphic (existence problem) and to find necessary and sufficient conditions for the existence of an isomorphism between any two groups G' and G'' such that the groups A, $C(G')$ and $C(G'')$ as well as the groups B, $Q(G')$ and $Q(G'')$ are isomorphic (uniqueness problem). This paper presents a solution of the existence problem under the hypothesis that B (the presumptive central quotient group) is a direct product of (a finite or infinite number of finite or infinite) cyclic groups whereas a solution of the uniqueness problem is given only under the hypothesis that B is an abelian group with a finite number of generators.

There is hardly any previous work concerning these problems. Only those abelian groups with a finite number of generators which are central quotient groups of suitable groups have been characterized before.†

1. Before enunciating our principal results (in §2) some notation and concepts concerning abelian groups will have to be recorded for future reference.

If G is any abelian group, then the composition of the elements in G is denoted as addition: $x+y$. If n is any positive integer, then nG consists of all the elements nx for x in G, and G_n consists of all the elements x in G such that $nx=0$. $F(G)$ is the subgroup of all the elements of finite order in G, that is, the join of the groups G_n, and $F(G, p)$ is the subgroup of all those elements in $F(G)$ whose order is a power of the prime number p; in other words, $F(G, p)$ is the join of all the groups G_{p^n}. It is well known that $F(G)$ is the direct sum of the groups $F(G, p)$.

A set B of elements in G is termed *independent*, if all the elements in B are non-zero, if none of the elements in B is a multiple of another element in B, and if the group, generated by the elements in B, is the direct sum of the cyclic groups which are generated by the elements in B. If G is generated by

* Presented to the Society, September 10, 1937; received by the editors September 20, 1937.

† R. Baer, Mathematische Zeitschrift, vol. 38 (1934), p. 406.

B, and if B is independent, then B is called a *basis* of G. It may be mentioned that the elements u and v (neither zero) are dependent if there exist integers i and k such that $iu = kv \neq 0$.

If G is an abelian group, then there need not exist a basis of G, but there always exists a greatest independent subset of G. Each greatest independent subset of G contains a certain (finite or infinite) number of elements, and the least of these numbers is called the *rank* $r(G)$ of G. If either every non-zero element in G is of infinite order or every non-zero element in G is of order p, then every greatest independent subset of G contains exactly $r(G)$ elements.

Numerical invariants:

$$r(G, 0) = r(G \pmod{F(G)}), \qquad r(G, p^i) = r((p^{i-1}G)_p \pmod{(p^iG)_p}).$$

If G is a direct sum of cyclic groups, then in every decomposition of G into indecomposable direct summands there are exactly $r(G, 0)$ cyclic direct summands of infinite order and exactly $r(G, p^i)$ cyclic direct summands of order p^i. It is a consequence of this fact that the structure of direct sums of cyclic groups is completely determined by the invariants $r(G, 0)$, $r(G, p^i)$.

If S is any subgroup of the abelian group G, then G/S denotes the group of classes of residues of G (mod S), and the direct sum of the abelian groups $G, H, \cdots, K, \cdots$ is denoted by $G+H+\cdots+K+\cdots$.

2. The following theorems contain the main results of this investigation:

EXISTENCE THEOREM. *If V is an abelian group and if G is a direct sum of cyclic groups, then the following conditions are necessary and sufficient for the existence of a group whose central is V and whose central quotient group is isomorphic to G:*

(i) *If G contains elements of order p^i, then V contains elements of order p^i.*

(ii) *If G contains elements of infinite order, then V contains elements of infinite order, or the orders of the elements in $F(V)$ are not bounded.*

(iii) *If the orders of the elements in $F(G)$ are bounded, and if $r(G, 0)$ is a finite positive integer, then V contains elements of infinite order and $1 < r(G, 0)$.*

(iv) *If the orders of the elements in $F(G)$ are bounded, and if $r(G, 0)$ is an odd (finite) number, then V contains two independent elements of infinite order $(1 < r(V, 0))$.*

(v) *If $G = F(G)$, $F(G, p) \neq 0$, and the orders of the elements in $F(G, p)$ are bounded, $F(G, p)$ contains at least two independent elements of maximum order.*

(vi) *If $G = F(G)$, if the orders of the elements in $F(G, p)$ are bounded, if $r(G, p^{i+k})$ is finite for $0 \leqq k$, and if $r(G, p^i)$ is odd, then V contains two independent elements of order p^i, $(1 < r((p^{i-1}V)_p)$.*

The following corollary is easily derived from this theorem:

COROLLARY. *The direct sum G of cyclic groups is isomorphic to the central quotient group of a suitable group if, and only if,*

(a) $r(G, 0)=1$ *implies that the orders of the elements in* $F(G)$ *are not bounded*;

(b) $G=F(G)$ *and* $r(G, p^i)=1$ *imply that* G *contains elements of order* p^{i+1}.

For (a) and (b) are part of the conditions (iii) and (v), respectively, and if G satisfies the conditions (a) and (b), then it is fairly obvious how to construct a group V such that G and V satisfy the conditions (i) to (vi) of the existence theorem.

UNIQUENESS THEOREM. *If G and V are abelian groups, and if G may be generated by a finite number of its elements, then the following conditions are necessary and sufficient for the existence of one, and essentially only one, group whose central is V and whose central quotient group is isomorphic to G:*

(1) *If p is a prime number such that G contains elements of order p, then $V=pV$ and V contains elements of order p.*

(2) *If G contains elements of infinite order, then $V=nV$ for every positive integer n, and V contains elements of infinite order.*

(3) *If $r(G, 0)\neq 0$, then $1<r(G, 0)<4$.*

(4) *If $r(G, 0)=3$, then $F(G)=0$, $F(V)=0$, and $2=r(V, 0)$ $(=r(V))$.*

(5) *If $r(G, 0)=2$ and $F(G, p)\neq 0$, then $F(G, p)$ is a direct sum of an odd number of isomorphic cyclic groups, and $1=r(V_p)$.*

(6) *If $G=F(G)$ (that is, if G is a finite group), if $F(G, p)\neq 0$, and if $2<r(V_p)$, then $F(G, p)$ is a direct sum of two isomorphic cyclic groups.*

(7) *If $G=F(G)$, $F(G, p)\neq 0$, and $2=r(V_p)$, then $F(G, p)$ is a direct sum of two cyclic groups of order p^{i+j} and one cyclic group of order p^i where $0\leqq i$, $0\leqq j$, $0<i+j$.*

(8) *If $G=F(G)$, $F(G, p)\neq 0$, and $1=r(V_p)$, then $F(G, p)$ is a direct sum of two isomorphic groups.*

Remark. If V and G satisfy condition (1), then at least one of them is infinite.

The proofs of these theorems will occupy us throughout this paper. In fact we shall prove slightly more than is needed for these theorems. Thus it will be possible to derive, from the facts presented in the following sections, the following statement which shows that the hypothesis of the existence of a finite basis in G is not a necessary one (though it is needed):

If G is a direct sum of finite cyclic groups of order n, if $r(G)=\aleph_0$, and if $V=nV$ and V_n is a cyclic group of order n, then there exists one, and essentially only one, group whose central is V and whose central quotient group is isomorphic to G.

3. The proofs of the theorems enunciated in §2 are based on the following theorems which transform the "metabelian" problems into abelian problems and which have been proved by the author in an earlier paper.* The following definitions are found necessary for the statement of these transformation theorems:

If G and V are two abelian groups, then the operation xy is called a *multiplication of G in V* if it obeys the following rules:

(3.1) *If x and y are elements in G, then xy is a uniquely determined element in V.*

(3.2) $0 = xx = xy + yx$, $x(y+z) = xy + xz$.

A multiplication xy of G in V may be called a *proper multiplication of G in V*, if it satisfies the condition:

(3.3) $wx = 0$ *for every x in G if, and only if,* $w = 0$.

We define *an admissible set of functions of G in V* to consist of a proper multiplication xy of G in V and of functions $P(n, x)$ which satisfy the following conditions:

(3.4) *If G contains elements of order n, and if x is an element in G_n, then $P(n, x)$ is a uniquely determined element in V* (mod nV).

(3.5) *If G contains elements of order n, and if x and y are elements in G_n, then*

$$P(n, x + y) = n(n - 1)2^{-1}xy + P(n, x) + P(n, y).$$

(3.6) *If m is a positive integer, G contains elements of order nm, and if x is an element in G_n, then*

$$P(nm, x) = mP(n, x).$$

(3.7) *If G contains elements of order nm and if x is an element in G_{nm}, then*

$$P(n, mx) = nV + P(nm, x).$$

The following theorem constitutes a transformation of the existence theorem:

THEOREM.† *There exists a proper multiplication of the abelian group G in the abelian group V if, and only if, there exists a group whose central is isomorphic to V and whose central quotient group is isomorphic to G.*

The following is a transformation of the uniqueness theorem:

---

* R. Baer, *Groups with abelian central quotient group*, these Transactions, vol. 44 (1938), pp. 357–386.

† Baer, ibid., Corollary 2.3.

THEOREM.* *Any two groups whose centrals are isomorphic to the abelian group V and whose central quotient groups are isomorphic to the direct sum G of cyclic groups are isomorphic if, and only if, there exists for any pair*

$$xy,\ P(n, x) \text{ and } x \circ y,\ P_0(n, x)$$

of sets of admissible functions of G in V an automorphism ϕ of V and an automorphism γ of G such that

$$(xy)^\phi = x^\gamma \circ y^\gamma \text{ and } P(n, x)^\phi = P_0(n, x^\gamma).$$

4. The relations of the conditions which are involved in the definition of a multiplication xy of the abelian group G in the abelian group V may be analyzed as follows:

If $0=xy+yx$ is always satisfied, then $2xx=0$ is inferred by putting $x=y$. If $xx=0$ and $x(y+z)=xy+xz$, as well as $(y+z)x=yx+zx$ (this would be a consequence of $xy+yx=0$!), are satisfied, then $0=(x+y)(x+y)=xx+xy+yx+yy=xy+yx$.

If, finally, xy is a proper multiplication of G in V, then the hypothesis that G is an abelian group is a consequence of the other conditions.

(4.1) *If xy is a multiplication of G in V, and if u is an element in G_n, then ux and xu are elements in V_n for every x in G.*

For multiplications are associative with regard to multiplication by integers, that is, $n(xy)=(nx)y=x(ny)$.

If xy is a multiplication of G in V, then to every element g in G there corresponds the homomorphism of G into V which is defined by mapping the element x in G upon the element gx in V. To the sum of two elements in G there corresponds the sum of the corresponding homomorphisms, and to any two different elements in G there correspond different homomorphisms of G into V if, and only if, xy is a proper multiplication of G in V. Thus every multiplication of G in V defines a representation of G as a group of homomorphisms of G into V, and this representation is a true one if, and only if, the multiplication is a proper one.

5. We prove the following statement:

(5.1) *If xy is a multiplication of G in V, and if u and v are elements in G such that u and uv have the same order, then u and v are independent elements in G.*

Proof. Suppose that h and k are integers such that $hu=kv$. If neither h nor k is 0, then let d be the g.c.d. of h and k. There exist, therefore, integers

* Baer, ibid., Theorem 6.2.

h', k' such that $d=hh'+kk'$, and it follows that

$$d(uv)=hh'uv+kk'uv=h'(hu)v+k'u(kv)=h'kvv+k'huu=0.$$

Hence d is a multiple of the order of uv, and, since u and uv have the same order, this implies $du=0$ and therefore $hu=0$ provided u and uv are of finite order; whereas the above equation leads to a contradiction if u and uv are both of infinite order. Thus u and v are independent.

(5.2) *If xy is a proper multiplication of G in V, then there exists corresponding to every element u in $F(G)$ an element u' in G such that u and uu' have the same order; and if u is an element of infinite order such that ux is an element of finite order for every x in G, then the orders of the elements ux for x in G are not bounded.*

Proof. Suppose that all the elements ux for x in G are of finite order and that the orders of the elements ux for x in G are bounded. Then the l.c.m. of the orders of the elements ux is a finite positive integer m. It follows that $0=m(ux)=(mu)x$ for every x in G, consequently $mu=0$ by (3.3). Clearly m is the order of u, as follows from (4.1) and the definition of m. Since it is fairly clear how to prove the existence of an element u' in G such that m is the order of uu', this completes the proof.

(5.3) *If xy is a multiplication of G in V; and if b' and $b'b''$ have the same order p^n, then $b''\not\equiv 0 \pmod{pG}$.*

Proof. If $b''=pb$, then $b'b''=p(b'b)$; consequently $p^{n-1}(b'b'')=(p^nb')b=0$.

6. If xy is a multiplication of G in V, and if S is a subgroup of G and T is a subgroup of V, then xy induces a multiplication of S in V/T. But clearly this induced multiplication need not be a proper multiplication of S in V/T, even if the inducing multiplication is a proper one.

(6.1) *If xy is a proper multiplication of G in V, if m is a positive integer such that mG contains multiples, not zero, of every non-zero element in G, and if T is a subgroup of V such that 0 is the cross cut of T and mV, then xy induces a proper multiplication of G in V/T.*

Proof. If $w\neq 0$ is an element in G, then there exists an integer k and an element u in G such that $kw=mu\neq 0$. Since xy is a proper multiplication of G in V, there exists an element w' in G such that $0\neq kww'=muw'$. Since 0 is the only element contained in T as well as in mV, it follows that kww', and consequently ww', are not elements in T; and this implies that xy defines a proper multiplication of G in V/T.

(6.2) *If xy is a proper multiplication of G in V, if G is generated by its subgroups G_1 and G_2, and if there exists a positive integer m such that $mx_1x_2=0$ for x_i in G_i and such that mG_1 contains multiples, not zero, of every non-zero element in G_1, then xy defines a proper multiplication of G_1 in V.*

Proof. If $w\neq 0$ is an element in G_1, then there exists an integer k and an element w' in G_1 such that $kw=mw'\neq 0$. Since xy is a proper multiplication of G in V, there exists an element u in G such that $kwu\neq 0$. Since G is generated by G_1 and G_2, there exist elements u_i in G_i such that $u=u_1+u_2$. Consequently, $0\neq kwu=mw'(u_1+u_2)=kwu_1+mw'u_2=kwu_1$, since w' is an element in G_1. Hence $wu_1\neq 0$; and xy defines, therefore, a proper multiplication of G_1 in V.

Note that the hypothesis $mx_1x_2=0$, for x_i in G_1, is satisfied if $mG_2=0$.

7. If G is the direct sum of its subgroups G_v, and if, for every v, a multiplication xy of G_v in V is given, then there exists one and only one multiplication xy of G in V which induces the given multiplications in the groups G_v and satisfies $rs=0$ for elements r and s which belong to different components G_v. This multiplication xy of G in V is a proper one if, and only if, the induced multiplications of the groups G_v in V are proper multiplications.

Notation. If xy is a multiplication of G in V, then $M(G, xy)$ is the subgroup of V generated by the elements xy for x and y in G; and if B is a subgroup of G, and S is a subgroup of V, then $(B<G; S, xy)$ consists of all the elements w in G such that $wb\equiv 0 \pmod{S}$ for every b in B.

Thus a multiplication xy of G in V is also a multiplication of G in $M(G, xy)$, and a proper multiplication of G in V is a proper multiplication of G in $M(G, xy)$. (If G is generated by two elements, then $M(G, xy)$ is a cyclic group (which may be 0); and if G is generated by a finite number of elements, then so is $M(G, xy)$.) It may be noted that $(B<G; S, xy)$ is always a subgroup of the group G.

LEMMA 7.1. *If xy is a multiplication of G in V, if B is a subgroup of G generated by the elements b' and b'' such that b', b'', and $b'b''$ all have the same order, and if $M(G, xy)$ is the direct sum of $M(B, xy)$ and its subgroup S, then G is the direct sum of $(B<G; S, xy)$ and the cyclic groups, generated by b' and b''.*

Proof. It is a consequence of (5.1) that b' and b'' form a basis of B, since b', b'', and $b'b''$ all have the same order. If w is an element in the cross cut of B and $(B<G; S, xy)$, then $wb=0$ for every element b in B, since 0 is the cross cut of S and $M(B, xy)$. Since xy defines a proper multiplication of B in V, this implies that $w=0$. If finally u is any element in G, then $ub'=s'+r'(b'b'')$ and $ub''=s''+r''(b'b'')$, for s', s'' in S and r', r'' suitable integers. Hence $u-r''b'+r'b''$ is an element in $(B<G; S, xy)$, and G is therefore the direct

sum of B and $(B<G; S, xy)$. This completes the proof.

COROLLARY 7.2. *If xy is a proper multiplication of the group G with a finite number of generators in the cyclic group $M(G, xy)$, then*

(a) *G is either a direct sum of a finite number of infinite cyclic groups or a direct sum of a finite number of finite cyclic groups; and*

(b) *there exists a basis $b_1', b_1'', \cdots, b_k', b_k''$ of G with the following properties:*

(i) *b_j', b_j'', and $b_j' b_j''$ all have the same order;*

(ii) *$b_i' b_j' = b_i'' b_j'' = b_i' b_h'' = 0$ for $i \neq h$;*

(iii) *$b_j' b_j'' = r_j b_{j-1}' b_{j-1}''$ for $1 < j \leqq k$; and if G is finite, then r_j is a divisor of the order of b_{j-1}'.*

(c) *G is a direct sum of two isomorphic groups G' and G'' such that $M(G', xy) = M(G'', xy) = 0$.*

Proof. (c) is an obvious consequence of (b), and (a) follows easily from (5.2) and the fact that the non-zero elements in a cyclic group are either all of finite order or all of infinite order. Since $M(G, xy)$ is a cyclic group, there exists a pair of elements b_1', b_1'' in G such that $b_1' b_1''$ generates $M(G, xy)$. Since $b_1' b_1''$ is an element of maximum order in $M(G, xy)$, it follows from (5.2) that b_1', b_1'', and $b_1' b_1''$ all have the same order. If B is the subgroup of G, generated by b_1' and b_1'', then it follows from $M(G, xy) = M(B, xy)$ and Lemma 7.1 that G is the direct sum of $(B<G; 0, xy)$ and the cyclic groups generated by b_1' and b_1''. Since $uv = 0$ for u in $(B<G; 0, xy)$ and v in B, it follows that xy defines proper multiplications of B as well as of $(B<G; 0, xy)$. Since $M((B<G; 0, xy), xy)$ is a subgroup of the cyclic group $M(G, xy)$, it is itself cyclic and (b) of Corollary 7.2 may be applied to $(B<G; 0, xy)$ since it is generated by less elements than G. Now the proof is easily completed by complete induction.

COROLLARY 7.3. *If G is a direct sum of $\aleph_0$ cyclic groups of equal finite order, if xy is a proper multiplication of G in V, and if $M(G, xy)$ is a cyclic group, then there exists a basis b_j', b_j'' for $j = 1, 2, \cdots$ of G with the following properties:*

(i) *b_j', b_j'', and $b_j' b_j''$ all have the same order.*

(ii) *$b_i' b_j' = b_i'' b_j'' = b_k' b_k'' = 0$ for $h \neq k$.*

(iii) *$b_1' b_1'' = \cdots = b_i' b_i'' = \cdots$ generates $M(G, xy)$.*

Proof. Let $g_1, g_2, \cdots, g_i, \cdots$ be an enumeration of the elements in G. Then by complete induction elements b_j', b_j'' and groups G_j will be defined for $0 < j$ with the following properties:

(1) The group B_i which is generated by the elements b_j', b_j'' with $j < i$ has these elements as a basis.

(2) The elements b_j', b_j'' satisfy (i) to (iii).

(3) B_i contains the elements g_j with $j<i$.

(4) G is the direct sum of G_i and B_i.

(5) $uv=0$, if u in G_i and v in B_i.

(6) xy induces proper multiplications of B_i and of G_i in V.

Since $B_1=0$, $G_1=G$ is a suitable start of this construction, it may be assumed that elements b_j', b_j'', for $j<i$ and a group G_i, have been defined which meet the requirements (1) to (6). Then $g_i=c+d$ with c in B_i and d in G_i. Since G_i is by condition (4) a direct sum of $\aleph_0$ cyclic groups of equal order, d is a multiple of an element b_i' in G_i which is of maximum order in G. There exists, by (5.2) and by the fact that $M(G_i, xy)$ is a cyclic group, an element b_i'' in G_i such that b_i', b_i'', and $b_i'b_i''$ have the same order, and such that $b_i'b_i''$ generates $M(G_i, xy)$. Since the orders of the elements in G are finite, b_i'' may be chosen in such a way that $b_i'b_i''=b_1'b_1''$. Finally we may put $G_{i+1}=(C<G_i;\ 0,\ xy)$, where C is the subgroup generated by b_i', b_i''. Then it follows from Lemma 7.1 that the elements b_j', b_j'', for $j<i+1$, and the group G_{i+1} satisfy (1) to (6).

The subgroup generated by all the elements b_i', b_i'', for $i=1, 2, \cdots$, contains every element in G by (3); and the b_i', b_i'' form therefore, by (1), a basis of G which satisfies (i) to (iii) by (2).

COROLLARY 7.4. *If G is a direct sum of two infinite cyclic groups and of an odd number of cyclic groups of the same finite order n, if xy is a proper multiplication of G in V such that $F(M(G, xy))$ is a cyclic group, then there exists a basis $b, b', b'', b_1', b_1'', \cdots, b_k', b_k''$ of G with the following properties:*

(i) $bb'=b_1'b_1''=\cdots=b_k'b_k''=c$.

(ii) *c, b, b_j', and b_j'' are elements of order n.*

(iii) *b', b'', and $b'b''$ are elements of infinite order.*

(iv) $bb''=bb_j'=bb_j''=b'b_j'=b'b_j''=b''b_j'=b''b_j''=b_i'b_j'=b_i''b_j''=b_j'b_h''=0$ *for $j\neq h$.*

Proof. Denote by N the set $(F(G)<F(G);\ 0,\ xy)$ of all elements w in $F(G)$ such that $wx=0$ for every x in $F(G)$. Then xy defines a proper multiplication of $F(G)/N$ in the cyclic group $F(M(G, xy))$. Therefore there exists, by Corollary 7.2, a basis $b_1', b_1'', \cdots, b_k', b_k''$ of $F(G)$ (mod N) which satisfies the conditions (i) to (iii) of (b) of Corollary 7.2.

Denote by u_1, u_2 any pair of elements in G which forms a basis of G (mod $F(G)$), and let w_j, for $j=1, 2, 3$ be any three elements in N whose order is a prime number p (dividing n). If d is some element of order p in $M(G, xy)$, then $w_iu_i=r_{ji}d$. If h_1, h_2, and h_3 are not trivial solutions of the two congruences in three unknowns $\sum_{j=1}^{3}h_jr_{ji}\equiv 0 \pmod p$, then $w=\sum_{j=1}^{3}h_jw_j$ belongs to N and

satisfies $wu_i=0$. Thus $w=0$, since xy is a proper multiplication of G in V. Hence the rank of N_p is at most two, and this implies, together with the existence of the particular basis b_i', b_i'' of $F(G)$ (mod N) (mentioned before), that N_p is a cyclic group. N is therefore a cyclic group of order n, and it may be assumed, without loss in generality, that the b_i', b_i'' satisfy (i). If g generates N, then $gu_i=r_ic$, where c generates $F(M(G, xy))$. If r is the g.c.d. of r_1 and r_2, then there exist integers r_1' and r_2' such that $r_1r_1'+r_2r_2'=r$, and it follows from (5.2) that r and n are relatively prime. (If $r_2=0$, then r_1 is relatively prime to n, and g may be chosen in such a way that $r_1=1$.) The elements

$$u_1' = r_1'u_1 + r_2'u_2, \qquad u_2' = -r_2r^{-1}u_1 + r_1r^{-1}u_2$$

form a basis of G (mod $F(G)$) which satisfies $gu_1'=rc$, $gu_2'=0$; thus it may be assumed without loss in generality that an element b, generating N, and a basis v_1, v_2 of G (mod $F(G)$) have been chosen in such a way that $bv_1=c$, $bv_2=0$. Put finally

$$b_i = v_i + \sum_{j=1}^{k} (s_{ij}'\, b_j' + s_{ij}''\, b_j''),$$

where the numbers s are determined as solutions of the equations

$$v_ib_j' = s_{ij}''c, \qquad v_ib_j'' = -s_{ij}'c.$$

Then a basis of G has been found which meets the requirements of the Corollary 7.4.

8. We prove the following lemma:

LEMMA 8.1. *If G is a direct sum of three cyclic groups, if xy is a proper multiplication of G in V, and if $M(G, xy)$ is a direct sum of two cyclic groups, then there exists a basis b_1, b_2, b_3 of G such that $b_1b_3=0$, whereas b_1b_2 and b_2b_3 form a a basis of $M(G, xy)$.*

Proof. Denote by u, v a basis of $M(G, xy)$, by $\bar{u}$ the cyclic subgroup, generated by u, and by $\bar{v}$ the cyclic subgroup, generated by v. Then $M(G, xy)=\bar{u}+\bar{v}$. If both u and v are of finite order, it may be assumed that the order of u is a divisor of the order of v. (Then it may happen that $u=0$.) There exists a pair of elements b', b'' in G such that $v=b'b''$; and it is a consequence of (5.2) and the choice of v that b', b'', and v have the same order. If B is the subgroup of G generated by b' and b'', then it follows from Lemma 7.1 that b', b'' form a basis of B and that $G=B+(B<G; \bar{u}, xy)$. Clearly $(B<G; \bar{u}, xy)$ is a cyclic group generated by an element c. There exist in B elements b such that $bc=u$ and amongst these elements b there is one b_2 such that the homomorphism of B, induced by b_2, maps B upon $\bar{v}$. It is now clear how to complete the proof.

9. Two multiplications xy and $x \circ y$ of G in V are called *isomorphic*, if there exists an automorphism γ of G and an isomorphism μ of $M(G, xy)$ upon $M(G, x \circ y)$ such that

$$(xy)^{\mu} = x^{\gamma} \circ y^{\gamma} \text{ for } x \text{ and } y \text{ in } G.$$

If the isomorphism μ may be chosen in such a fashion that it is induced by some automorphism of V, then the two multiplications are termed *equivalent.*

The following propositions are fairly obvious consequences of the statements in §§7 and 8.

If G is a direct sum of three (but not of two) cyclic groups, then any two proper multiplications of G such that $M(G, \cdots)$ are direct sums of two cyclic groups are isomorphic.

If G is a direct sum of $\aleph_0$ isomorphic finite cyclic groups, or if G is a finite group, then any two proper multiplications with the cyclic $M(G, \cdots)$ are isomorphic.

If G is a direct sum of two infinite cyclic groups and of an odd finite number of isomorphic finite cyclic groups, then any two proper multiplications of G with cyclic $F(M(G, \cdots))$ are isomorphic.

It is a consequence of (5.2) that any two proper multiplications of a direct sum of two cyclic groups are isomorphic.

If G is a direct sum of a finite number of infinite cyclic groups, and if xy is a proper multiplication of G such that $M(G, xy)$ is a cyclic group, then the numbers r_i appearing in (iii) of (b) of Corollary 7.2 may be chosen as positive integers. Then it is possible to prove that they are invariants with regard to isomorphisms. (This proof follows from the consideration of the subgroup $(G<G; nM(G,xy), xy)$ of all elements w in G such that $wx \equiv 0 \pmod{nM(G, xy)}$ for every x in G.) It is then a consequence of Corollary 7.2 that two proper multiplications of G with cyclic $M(G, \cdots)$ are isomorphic if, and only if, they induce the same invariants r_i.

10. The object of the next three sections is to construct proper multiplications of somewhat elementary groups G. They will be combined afterwards to form proper multiplications of the more general types of groups G.

If B is a basis of the group G, then a multiplication xy of G in V is completely determined by the values of the products bb' for b and b' in B, and these values may be chosen completely at random with the two restrictions that $bb = 0$ and that $bb' = -b'b$. In enumerating the values of the products bb' it may be understood that the product bb' need not be mentioned, if the value of $b'b$ has been given, and that $bb' = 0$, if the value of neither bb' nor $b'b$ has been mentioned.

11. We prove the following proposition:

(11.1) *If G is a direct sum of finite cyclic groups, if G is a direct sum of two isomorphic groups, and if V contains elements of order n whenever G contains elements of order n, then there exists a proper multiplication of G in V.*

Proof. There exists a basis of G, consisting of pairs b_v', b_v'' such that b_v and b_v'' always have the same order. There exists in V an element c_v such that b_v', b_v'', and c_v have the same order. Then a proper multiplication of G in V is determined by the rule $b_v' b_v'' = c_v$, for every v.

(11.2) *If G is a direct sum of cyclic groups whose orders are powers of a fixed prime number p, the orders of the elements in G are not bounded, and V contains elements of every order p^i, then there exists a proper multiplication of G in V.*

Proof. $G = G' + G'' + G'''$, where G' and G'' are isomorphic groups and where G''' has a basis $b_1, b_2, \cdots, b_i, \cdots$ such that the orders of the elements b_i are not bounded and such that the order of b_{i-1} divides the order of b_i. There exists in V an element c_i whose order equals the order of b_i. A proper multiplication of G''' in V is characterized by the equations $b_i b_{i+1} = c_i$, for $i = 1, 2, \cdots$. By (11.1) there exists a proper multiplication of $G' + G''$ in V, consequently there exists a proper multiplication of G in V.

(11.3) *If G is a direct sum of two cyclic groups of order p^n and of a finite number of cyclic groups whose orders are divisors of p^n, and if V contains elements of order p^n and contains two independent elements of order p^i in case $r(G, p^i)$ is odd, then there exists a proper multiplication of G in V.*

Proof. This is a consequence of (11.1) if all the numbers $r(G, p^i)$ are even. If not all the numbers $r(G, p^i)$ are even, then there exists a greatest integer m such that $r(G, p^m)$ is odd and $0 < m \leqq n$. V contains an element u of order p^n and an element v of order p^m which is independent of u. There exists a basis $b_1, b_2, \cdots$ of G such that the order $p^{n(j)}$ of b_j satisfies the inequality $n(j) \leqq n(j-1)$ and consequently $n = n(1) = n(2)$. If $n = m$, then b_3 is of order p^n, and in this case we put $h = 3$. If $m < n$, then let h be the smallest number such that $n(h) = m$. The number h thus defined is in both cases an odd integer and $n(2j-1) = n(2j)$, for $0 < 2j < h$.

It is now easily verified that a proper multiplication xy of G in V is characterized by the equations

$$b_{2j-1} b_{2j} = p^{n-n(2j)} u, \quad \text{for} \quad 0 < 2j < h,$$
$$b_{j-1} b_j = p^{m-n(j)} v, \quad \text{for} \quad h \leqq j.$$

(11.4) *If G is a direct sum of an infinity of cyclic groups of order p^n and of cyclic groups whose orders divide p^n, and if V contains elements of order p^n, then there exists a proper multiplication of G in V.*

Proof. There exists a basis $b_1, b_2, \cdots, b_v, \cdots$ of G which is well ordered by the subscripts of its elements b_v in such a fashion that there is no last element in the basis and that the order $p^{n(v)}$ of b_v divides $p^{n(k)}$ for $v<k$. There exists an element u of order p^n in V.

A proper multiplication of G in V is characterized by the equations

$$b_v b_{v+1} = p^{n-n(v)}u.$$

(11.5) *Suppose that G is a direct sum of two cyclic groups of order p^n and of a finite number of cyclic groups whose orders divide p^n and that V contains an element of order p^n and two independent elements of order p^i, if $r(G, p^i)$ is odd. Then there exist two non-isomorphic, proper multiplications of G in V if one of the following conditions is satisfied:*

(a) $2<r(G_p), 1<r(V_p)$, *and G is a direct sum of two isomorphic groups.*

(b) $2<r(G_p), 2<r(V_p)$.

(c) $3<r(G_p)$ *and G is not a direct sum of two isomorphic groups.*

Proof. If (a) is satisfied by G and by V, then there exists a basis $b_1, b_2, \cdots, b_{2k}$ such that $1<k$ and such that b_{2i-1} and b_{2i} have the same order $p^{n(i)}$. V contains an element u of order p^n and an element w of order p which is independent of u. If $h=0$ and if $h=1$, then a proper multiplication

$$x \underset{h}{\circ} y$$

of G in V is defined by the equations

$$b_{2i-1} \underset{h}{\circ} b_{2i} = p^{n-n(i)}u, \qquad b_{2i} \underset{h}{\circ} b_{2i+1} = hw$$

and

$$x \underset{0}{\circ} y \quad \text{and} \quad x \underset{1}{\circ} y$$

are clearly non-isomorphic multiplications of G in V.

If (b) is satisfied, then it may be assumed that G is not a direct sum of two isomorphic groups, since otherwise (a) might be applied. Then there exists a greatest integer m such that $r(G, p^m)$ is odd and $0<m\leqq n$. V contains a subgroup V' which is a direct sum of a cyclic group of order p^n and of a cyclic group of order p^m; and V contains an element w of order p which is not contained in V'.

There exists by (11.3) a proper multiplication xy of G in V', and it is a consequence of Corollary 7.2 that $M(G, xy)$ is not a cyclic subgroup of V'. Denote by $x \ominus y$ the multiplication of G in V which is characterized by the equations

$$b_1 \ominus b_k = w,$$

where b_1, b_k is a pair of elements in a basis of G such that $b_1 b_k = 0$. (That it is possible to determine xy and a basis of G in such a fashion may be verified by looking over the proof of (11.3).) Then

$$x \circ y = (xy) + (x \ominus y)$$

is a proper multiplication of G in V which satisfies

$$2 = r(M(G, xy)_p) < 3 = r(M(G, x \circ y)_p);$$

consequently xy and $x \circ y$ are non-isomorphic proper multiplications of G in V.

Assume now that the conditions of (c) are satisfied. Then there exists a greatest integer m such that $r(G, p^m)$ is odd and $0 < m \leqq n$. Furthermore V contains an element u of order p^n and an element v of order p^m which is independent of u.

It is finally possible to decompose G in the form

$$G = G' + G'' + \sum_{j=1}^{k} Z(j),$$

where G' and G'' are isomorphic groups and the maximum order of the elements in G' is p^n, and where $Z(j)$ is a cyclic group of order $p^{n(j)}$, $1 \leqq k$; $0 < n(k) < \cdots < n(1) = m \leqq n$.

Two cases may be distinguished.

Case 1. G' (and therefore G'') is a cyclic group of order p^n. Since G is not a direct sum of three cyclic groups, this implies that 1 is less than k. Denote by g', g'', and $z(j)$ elements which generate G', G'', and $Z(j)$, respectively.

A proper multiplication xy of G in V is characterized by the equations

$$g'g'' = u, \qquad g''z(1) = v, \qquad z(j-1)z(j) = p^{n-n(j)}u.$$

If $x = x'g' + x''g'' + \sum_{j=1}^{k} x(j)z(j)$ is any element in G, then

$$xg' = -x''u, \qquad xg'' = x'u - x(1)v, \qquad xz(1) = x''v - x(2)p^{n-n(2)}u,$$

$$xz(j) = (x(j-1)p^{n-n(j)} - x(j+1)p^{n-n(j+1)})u, \quad \text{for} \quad 1 < j < k,$$

$$xz(k) = x(k-1)p^{n-n(k)}u.$$

Denote by $W(xy, H)$ the set of all elements w in the subgroup H of G for which *the set wG of all the elements wx for x in G is a cyclic subgroup of V.* (This notation shall be used throughout this proof.) Clearly the element w in H belongs to $W(xy, H)$ if, and only if, the elements wg', wg'', $wz(j)$, for $1 \leqq j \leqq k$, generate a cyclic subgroup of V. It may now be computed that $W(xy, G)$ consists exactly of the elements of the form

$$x'g' + p^m x''g'' + \sum_{j=2}^{k} x(j)z(j)$$

and of the elements which may be represented in the form

$$x'g' + h\sum_{j=0}^{i} p^{h(j)}z(2j+1),$$

where $k=2i+1$, $h(j)=(n(2j+2)-n(2j+3))+\cdots+(n(k-1)-n(k))$, or the elements which may be represented in the form

$$x'g' + h\sum_{j=0}^{i-1} p^{h(j)}z(2j+1),$$

where $k=2i$, $h(j)=(n(2j+2)-n(2j+3))+\cdots+(n(k-2)-n(k-1))+n(k)$.

Another proper multiplication $x \circ y$ of G in V is characterized by the equations

$$g' \circ g'' = u, \qquad g'' \circ z(1) = v, \qquad g' \circ z(k) = p^{m-n(k)}v,$$
$$z(j-1) \circ z(j) = p^{n-n(j)}u, \quad \text{for} \quad 1 < j \leqq k.$$

Suppose now that $w=w'g'+w''g''+\sum_{j=1}^{k} w(k)z(k)$ is an element of G_p. Then

$$w \circ g' = -w''u - w(k)p^{m-n(k)}v, \qquad w \circ g'' = w'u - w(1)v,$$
$$w \circ z(1) = w''v - w(2)p^{n-n(2)}u,$$
$$w \circ z(j) = -w(j+1)p^{n-n(j+1)}u, \quad \text{for} \quad 1 < j < k,$$
$$w \circ z(k) = 0,$$

since $n(k)<n(k-1)\leqq m\leqq n$. Consequently $W(x \circ y, G_p)$ consists exactly of those elements which may be represented in the form

$$p^{n-1}w'g' + p^{n-1}w''g'' + \sum_{j=2}^{k-1} p^{n(j)-1}w(j)z(j) \quad \text{or} \quad p^{n-1}w'g' + p^{m-1}w(1)z(1),$$

if $m<n$, and which may be represented in the form

$$p^{n-1}w'g' + \sum_{j=2}^{k-1} p^{n(j)-1}w(j)z(j) \quad \text{or} \quad p^{n-1}w'g' + p^{m-1}w(1)z(1),$$

if $n=m$.

Thus $W(xy, G_p)$ and $W(x \circ y, G_p)$ are of essentially different structure, and the two proper multiplications xy and $x \circ y$ of G in V are not isomorphic.

Case 2. G' (and therefore G'') is not a cyclic group. Then there exists a basis $b_1', \cdots, b_i'$ of G', $b_1'', \cdots, b_i''$ of G'' such that $1<i$, b_j' and b_j'' have

the same order $p^{m(j)}$ and $m(i) \leqq \cdots \leqq m(1) = n$. Proper multiplications xy and $x \circ y$ of G in V are characterized by the equations

$$b_j' b_j' = p^{n-m(j)}u, \qquad b_1' z(1) = v, \qquad z(j-1)z(j) = p^{n-n(j)}u,$$

for $1 < j \leqq k$ and by the equations

$$b_j' \circ b_j'' = p^{n-m(j)}u, \qquad b_1' \circ z(1) = v, \qquad z(j-1) \circ z(j) = p^{n-n(j)}u,$$

for $1 < j \leqq k$, $b_2' \circ z(1) = p^{m-q}v$, where $q = \min(m(2), n(1)) \neq 0$. (Note that $1 \leqq k$, and that $k = 1$ is a possibility.)

The elements in $W(xy, G)$ are exactly the elements contained in the following two sets A and B: A consists of the elements of the form

$$p^m w(1)'b_1' + w(1)''b_1'' + \sum_{j=2}^{i} (w(j)'b_j' + w(j)''b_j'') + \sum_{j=2}^{k} w(j)z(j),$$

and B consists of the elements of the form

$$\begin{aligned} &w(1)''b_1'' + hz(1) && \text{if } k = 1, \\ &w(1)''b_1' + hz && \text{if } 1 < k, \end{aligned}$$

where

$$z = \sum_{j=0}^{i} p^{h(j)}z(2j+1),$$

$$h(j) = (n(2j+2) - n(2j+3)) + \cdots + (n(k-1) - n(k))$$

if $k = 2i+1$; and

$$z = \sum_{j=0}^{i-1} p^{h(j)}z(j),$$

$$h(j) = (n(2j+2) - n(2j+3)) + \cdots + (n(k-2) - n(k-1)) + n(k)$$

if $k = 2i$.

In order to show that $W(x \circ y, G)$ is essentially different from $W(xy, G)$ and that consequently the two proper multiplications xy and $x \circ y$ of G in V are not isomorphic, the following remark will suffice:

$$A' \leqq W(x \circ y, G) \leqq (A', B'),$$

where (A', B') may denote the set-theoretical join of the sets A' and B'. Here A' consists of the elements

$$w(1)'p^{m-q}b_1' + (w(2)'p^q - w(1)')b_2' + w(1)''b_1'' + w(2)''b_2'' + \sum_{j=3}^{i} (w(j)'b_j' + w(j)''b_j'') + \sum_{j=2}^{k} w(j)z(j),$$

and B' consists of the elements

$$w(1)'p^{m-q}b_1' + (w(2)'p^q - w(1)')b_2' + hz(1),$$

if $k=1$, and of the elements

$$w(1)'p^{m-q}b_1' + (w(2)'p^q - w(1)')b_2' + hz,$$

if $1<k$, where z has the same meaning as in the computation of $W(xy, G)$.

12. We prove the following statement:

(12.1) *If G is a direct sum of infinitely many infinite cyclic groups, and if the orders of the elements in $F(V)$ are not bounded, then there exists a proper multiplication of G in V.*

Proof. Clearly it is sufficient to prove the statement for countable groups G. Then there exists a countable basis B of G, and the elements of such a basis B may be denoted by $(i_1, \cdots, i_n)$ where n and i_j run over all the positive integers. There exists furthermore to every positive integer i an element $c(i)$ in V whose order exceeds i. Then a proper multiplication of G in V is characterized by the equations

$$(i_1, \cdots, i_n)(i_1, \cdots, i_n, i_{n+1}) = c(i_{n+1}).$$

(12.2) *If G is a direct sum of infinite cyclic groups, if $r(G, 0) = r(G)$ is not an odd finite number, and if V contains elements of infinite order, then there exists a proper multiplication of G in V. If $2<r(G, 0)$, then there exists a proper multiplication xy of G in V such that $(G<G; 2M(G, xy), xy) = 2G$ and a proper multiplication $x \circ y$ of G in V such that $2G<(G<G; 2M(G, x \circ y), x \circ y)$; and these two proper multiplications of G in V are not isomorphic.*

Proof. There exists a basis of G which consists of pairs b_v', b_v''. There exists furthermore an element u of infinite order in V, and a proper multiplication of G in V is characterized by the equations

$$b_v' b_v'' = u$$

for every v. Clearly

$$2G = (G < G; 2M(G, xy), xy).$$

If $2<r(G, 0)$, then a proper multiplication of G in V is characterized by the equations

$$b_1' \circ b_1' = u, \qquad b_v' \circ b_v'' = 2u$$

for every $v \neq 1$. Since $(G<G; 2M(G, x \circ y), x \circ y)$ is generated by the elements $2b_1'$, $2b_1''$, b_v', b_v'', for $v \neq 1$, it follows that $2G<(G<G; 2M(G, x \circ y), x \circ y)$. This completes the proof.

(12.3) *If G is a direct sum of three infinite cyclic groups, and if V is a direct sum of two infinite cyclic groups and one cyclic group (which may be 0, finite, or infinite), then there exists a proper multiplication xy of G in V such that $M(G, xy) = V$.*

Proof. There exists a basis b', b'', b''' of G, and there exists a basis u', u'', v of V such that u' and u'' are elements of infinite order. Then a proper multiplication of G in V is characterized by the equations

$$b'b'' = u', \qquad b''b''' = u'', \qquad b'''b' = v;$$

and clearly $V = M(G, xy)$.

(12.4) *If G is a direct sum of four infinite cyclic groups, and if V is a direct sum of an infinite cyclic group and one cyclic group, then there exists a proper multiplication xy of G in V such that $M(G, xy) = V$.*

Proof. There exists a basis $b_1, \cdots, b_4$ of G and a basis u, v of V, where u may be an element of infinite order. A proper multiplication xy of G in V such that $V = M(G, xy)$ is characterized by the equations $b_1b_2 = b_3b_4 = u$, $b_2b_3 = v$.

13. We prove the following statement:

(13.1) *If G is a direct sum of cyclic groups, if $G \neq F(G)$, if the orders of the elements in $F(G)$ are not bounded, and if V contains elements of order n whenever $F(G)$ contains elements of order n, then there exists a proper multiplication of G in V.*

Proof. $G = F(G) + U' + U''$, where U' is a direct sum of a finite number (not zero) of infinite cyclic groups and where U'' is either 0 or a direct sum of an infinity of infinite cyclic groups. Since the orders of the elements in $F(V)$ are not bounded, it follows from (12.1) that there exists a proper multiplication of U'' in V. Therefore it may be assumed without loss in generality that $r(G, 0)$ is finite.

If $r(G, 0)$ is finite, then G is a direct sum of $r(G, 0)$ groups $H(i)$ such that the orders of the elements in $F(H(i))$ are not bounded and such that $r(H(i), 0) = 1$. Thus it may be assumed without loss in generality that $r(G, 0) = 1$.

$F(G)$ is a direct sum of two groups G' and G'' such that G'' is a direct sum of two isomorphic groups and such that the orders in G' are not bounded and all the numbers $r(G', p^i)$ are finite. Since there exists by (11.1) a proper multiplication of G'' in V, it is sufficient to prove the existence of a proper multiplication of $G' + \bar{u}$ in V, where u is an element in G which generates G (mod $F(G)$) and where $\bar{u}$ is the group generated by u.

If $F(G', p) \neq 0$, then there exists a basis $b_{1p}, b_{2p}, \cdots, b_{ip}, \cdots$ of $F(G', p)$

such that the order of b_{i-1p} is not greater than the order of b_{ip}. There exists, furthermore, in V an element v_{ip} of the same order as b_{ip}.

A proper multiplication of $G'+\bar{u}$ in V is characterized by the following equations

$$b_{i-1p}b_{ip} = v_{i-1p},$$
$$b_{ip}u = v_{ip}$$

for every i, if $F(G', p)$ is infinite, and

$$b_{i-1p}b_{ip} = v_{i-1p},\ b_{mp}u = v_{mp},$$

if $F(G', p)$ is finite and $m = r(F(G', p)_p)$.

(13.2) *If G is a direct sum of a finite number of cyclic groups, if $1 < r(G, 0)$, if V contains elements of the finite order n whenever $F(G)$ contains elements of order n, if V contains elements of infinite order, and if V contains two independent elements of infinite order, in case $r(G, 0)$ is odd, then the following propositions are true*:

(1) *There exists a proper multiplication xy of G in V with the properties*:

(i) *$(F(G, p) < F(G, p); 0, xy)$ is a cyclic group which is 0 if, and only if, $F(G, p)$ is a direct sum of an even number of isomorphic cyclic groups*;

(ii) *$M((F(G) < G; 0, xy), xy)$ does not contain non-zero elements of finite order.*

(2) *There exists a proper multiplication xy of G in V with the property*:

(iii) *$(F(G, p) < F(G, p); 0, xy)$ is a cyclic group, not zero, if $F(G, p)$ is a direct sum of an odd number of isomorphic cyclic groups, and it is a direct sum of two cyclic groups, not zero, otherwise, if $F(G, p) \neq 0$.*

(3) *If $F(G, p) \neq 0$, and if V contains two independent elements of order p, then there exists a proper multiplication xy of G in V such that $M(G, xy)$ contains two independent elements of order p.*

(4) *If V contains elements of finite order, and if $2 < r(G, 0)$, then there exists a proper multiplication xy of G in V such that $M((F(G) < G; 0, xy), xy)$ contains non-zero elements of finite order.*

Proof. There exists a basis $b_1, b_2, \cdots, b_h$ of G (mod $F(G)$) such that $1 < h = r(G, 0)$; and there exists a basis $b_{1p}, \cdots, b_{kp}$ of $F(G, p)$ such that $0 \leqq k = k(p)$ (that is, $k(p) = 0$, if $F(G, p) = 0$) and such that the orders $p^{n_{ip}}$ of b_{ip} satisfy the inequality $0 < n_{jp} \leqq n_{j-1p}$, for $0 < j - 1 < k$. V contains an element $v(p)$ of order $p^{n_{1p}}$ if $F(G, p) \neq 0$, an element u of infinite order, and, if $r(G, 0)$ is odd, an element v of infinite order which is independent of u.

A proper multiplication xy of G in V is characterized by the following equations:

$$b_1b_2 = b_3b_4 = \cdots = u;$$
$$b_{h-1}b_h = v$$

if, and only if, h is odd; and

$$b_2b_h = w,$$

if $2<h$, where w is an element of finite order in V which shall be kept indeterminate for the moment. If $F(G, p)\neq 0$, then

$$b_{1p}b_1 = v(p), \qquad b_{1p}b_2 = w(p),$$

where $w(p)$ is either 0 or an element of order p which is independent of $v(p)$, and

$$b_{j-1p}b_{jp} = p^{m_{jp}}v(p) \quad \text{with} \quad m_{jp} = n_{1p} - n_{jp}.$$

If $w=0$ and $w(p)\neq 0$, then xy meets the requirements of (3). If $w(p)=0$, then $(F(G)<G;\ 0,\ xy)$ is the direct sum of $(F(G)<F(G);\ 0,\ xy)$, the cyclic groups generated by the elements b_i for $1<i$, and the cyclic group generated by n_1b_1, where $n_1=\prod_p p^{n_{1p}}$. The requirements of (4) are therefore satisfied if $w\neq 0$; and condition (ii) is satisfied if $w=0$.

Suppose now that $w=w(p)=0$. Every element of $F(G, p)$ has the form $x=\sum_{j=1}^{k(p)}x_jb_{jp}$, consequently

$$xb_{1p} = -x_2p^{m_{2p}}v(p), \qquad xb_{jp} = (x_{j-1}p^{m_{jp}} - x_{j+1}p^{m_{j+1p}})v(p)$$

for $1<j<k(p)$, and

$$xb_{k(p)p} = x_{k(p)-1}p^{m_{kp}}v(p)$$

Thus x belongs to $(F(G, p)<F(G, p);\ 0,\ xy)$ if, and only if,

$$0 = x_2b_{2p} = x_4b_{4p} = \cdots, \quad x_{j-1} = x'_{j-1}p^{n_{jp}-n_{j+1p}},$$
$$x'_{j-1} \equiv x_{j+1} \pmod{p^{n_{j+1p}}}, \qquad x_{k(p)-1} \equiv 0 \pmod{p^{n_{kp}}}.$$

Consequently $(F(G, p)<F(G, p);\ 0,\ xy)$ is the cyclic group generated by

$$\sum_{j=0}^{i-1} p^{h_{jp}}b_{2(i-j)-1p}$$

with

$$h_{0p} = n_{2ip}, \cdots, h_{jp} = n_{2ip} + (n_{2i-2p} - n_{2i-1p}) + \cdots + (n_{2(i-j)p} - n_{2(i-j)+1p})$$

if $k(p)=2i$, and by

$$\sum_{j=0}^{i} p^{h_{jp}}b_{2(i-j)+1p}$$

with

$$h_{ip} = [n_{2(i-j)p} - n_{2(i-j)+1p}] + \cdots + [n_{2ip} - n_{2i+1p}]$$

if $k(p) = 2i+1$. It is now obvious that this multiplication xy satisfies (i).

In order to prove (2) we will consider the multiplication $x \circ y$ of G in V which is characterized by the equations

$$b_1 \circ b_2 = b_3 \circ b_4 = \cdots = u,$$
$$b_{h-1} \circ b_h = v,$$

if and only if h is odd; if $F(G, p) \neq 0$, then

$$b_{1p} \circ b_1 = v(p), \qquad b_{j-1p} \circ b_{jp} = p^{m_{jp}} v(p), \quad \text{for} \quad j < k(p),$$
$$b_{k(p)p} \circ b_2 = p^{m_{k(p)p}} v(p), \quad \text{if} \quad 1 < k(p).$$

If $k(p) = 1$, then $(F(G, p) < F(G, p);\ 0, x \circ y)$ is the cyclic group generated by b_{1p}. If $1 < k(p)$, then $(F(G, p) < F(G, p);\ 0, x \circ y)$ is the direct sum of the cyclic group, generated by $b_{k(p)p}$, and the group $W(p)$, consisting of all the elements w in the group B, generated by the b_{jp} with $j < k(p)$, which satisfy $wx = 0$ for every x in $F(G, p)$. But $W(p) = (B < B;\ 0, x \circ y)$, and in the group, generated by B and the b_j for $j < k(p)$, the multiplication is of the same type as considered in the first part of the proof. Thus $W(p)$ is a cyclic group, and $W(p) = 0$ if, and only if, B is a direct sum of an even number of isomorphic cyclic groups. This completes the proof.

14. **Proof of the existence theorem.** If G is a direct sum of cyclic groups, and if V is an abelian group, then it follows from the transformation of the existence theorem (§3) that the existence theorem is equivalent to the following proposition:

There exists a proper multiplication of G in V if, and only if, the conditions (i) *to* (vi) *of the existence theorem are satisfied.*

Suppose first that there exists a proper multiplication xy of G in V. Then (i) and (ii) are consequences of (5.2). Suppose now that the orders of the elements in $F(G)$ are bounded and that $r(G, 0)$ is a finite positive integer. Then $G = F(G) + U$, where $U \neq 0$ is a direct sum of a finite number of infinite cyclic groups. If m is the finite maximum order of the elements in $F(G)$, then $muv = 0$ for u in $F(G)$ and v in U, and it is now a consequence of (6.2) that xy induces a proper multiplication of U in V. Since U is generated by a finite number of elements, $M(U, xy)$ is also generated by a finite number of elements, and $F(M(U, xy))$ is therefore a finite group. Hence xy induces by (6.1) a proper multiplication of U in $M(U, xy)/F(M(U, xy)) = V^*$, and all the non-zero elements in V^* are of infinite order. Now it follows from (5.2) that $V^* \neq 0$, that is, that V contains elements of infinite order, and it follows from (5.1) that U contains at least two independent elements, that is, $1 < r(G, 0)$. If

furthermore $r(G, 0)$ is an odd finite number, then it follows from Corollary 7.2 that V^* is not a cyclic group, and consequently that V contains at least two independent elements of infinite order. Thus the necessity of the conditions (iii) and (iv) has been verified.

If $G=F(G)$, then $G=F(G, p)+F'(G, p)$, where $F'(G, p)$ is the direct sum of all the $F(G, q)$ for $q\neq p$, and $uv=0$ for u in $F(G, p)$ and v in $F'(G, p)$. Thus a multiplication xy of G in V is a proper multiplication if, and only if, xy induces a proper multiplication of every $F(G, p)$ in V.

Suppose now that xy is a proper multiplication of $F(G, p)$ in V and that the orders of the elements in $F(G, p)$ are bounded. Then (v) is a consequence of (5.2) and (5.1). Suppose now that $F(G, p)=F'+F''$, where $p^{i-1}F'=0$, whereas F'' is a direct sum of cyclic groups whose orders are multiples of p^i. Then xy induces by (6.2) a proper multiplication of F'' in V. Clearly $M(F'', xy)\leqq F(V, p)$. If $F(V, p)=V'+V''$, where $p^{i-1}V'=0$, V'' contains exactly one cyclic subgroup of order p^i, then it follows from (6.1) that xy induces a proper multiplication of F'' in $F(V, p)/V'\sim V''$. If F'' is a finite group, it follows from Corollary 7.2 that F'' is a direct sum of two isomorphic groups. This shows the necessity of condition (vi).

Assume now that the direct sum G of cyclic groups and the abelian group V satisfies the conditions (i) to (vi) of the existence theorem.

Case 1. $F(G)\neq G$. If the orders of the elements in $F(G)$ are not bounded, there exists, by (13.1) and (i), a proper multiplication of G in V. If the orders of elements in $F(G)$ are bounded, then $G=F'+F''+U$, where F' is a finite group, F'' is a direct sum of two isomorphic groups without elements of infinite order, and U is a direct sum of infinite cyclic groups. If V does not contain elements of infinite order, then U is, by (iii), a direct sum of an infinity of infinite cyclic groups, and the orders of the elements in $F(V)$ are not bounded, by (ii). There exists, by (12.1), a proper multiplication xy of U in V and there exists, by (11.1), a proper multiplication xy of F'' in V. Consequently there exists a proper multiplication of $F''+U$ in V. F' has, as a finite group, a basis of the form $b_1, \cdots, b_k$, where the order of b_{i-1} is a divisor of the order of b_i. Denote by v_i an element in V whose order equals the order of b_i and by $u_0, u_1, \cdots$ a basis of U. Then the proper multiplication of $F''+U$ in V is extended to a proper multiplication of G in V by the equations

$$b_{i-1}b_i = v_i, \qquad b_k u_0 = v_k, \qquad b_j u_v = 0, \quad \text{for} \quad v \neq 0,$$

$b_j f''=0$ for f'' in F''.

If the orders of the elements in $F(G)$ are bounded, then $G=F'+U'+W$, where W is a direct sum of two isomorphic groups, F' a finite group, and U' a direct sum of two or three infinite cyclic groups; and if $r(U', 0)=3$, then

$r(W, 0)$ is finite. If the orders of the elements in $F(V)$ are bounded, then V contains elements of infinite order, and if $r(U', 0) = 3$, then $r(G, 0)$ is an odd finite number and V contains, by (iv), two independent elements of infinite order. Thus there exists, by (13.2), a proper multiplication of $F' + U'$ in V; and by (11.1), (12.2) there exists a proper multiplication of W in V. Consequently there exists a proper multiplication of G in V.

Case 2. $F(G) = G$. Since $F(G)$ is the direct sum of the groups $F(G, p)$, it is sufficient to construct proper multiplications of $F(G, p)$ in V. If the orders of the elements in $F(G, p)$ are not bounded, there exists by (11.2) a proper multiplication of G in V. If the orders of the elements in $F(G, p)$ are bounded, either $F(G, p)$ is a finite group and the existence of a proper multiplication of $F(G, p)$ in V is a consequence of (11. 3), or $F(G, p)$ is a direct sum of an infinity of cyclic groups of order p^n and some cyclic groups of lower order and the existence of a proper multiplication of $F(G, p)$ in V is a consequence of (11.4), or finally $F(G, p)$ is a direct sum of a group F' and a group F'', where F' is a direct sum of a finite number of cyclic groups whose orders are multiples of p^n whereas F'' is a direct sum of an infinity of cyclic groups of order p^{n-1} and cyclic groups of lower order. In this last case there exists a proper multiplication of $F(G, p)$ in V, since there exists by (11.3) a proper multiplication of F' in V and by (11.4) a proper multiplication of F'' in V.

15. **Theorem 15.1.** We prove the following theorem:

THEOREM 15.1. *Assume that V is an abelian group, and that G is a direct sum of a finite number of cyclic groups. Then there exists one and, apart from isomorphic ones, only one proper multiplication of G in V if the following conditions are satisfied:*

(A) *If $r(G, 0) \neq 0$, then $1 < r(G, 0) < 4$.*

(B) *If $r(G, 0) = 3$, then $F(G) = F(V) = 0$ and $2 = r(V, 0)$ $(= r(V))$.*

(C) *If $r(G, 0) = 2$ and $F(G, p) \neq 0$, then $F(G, p)$ is a direct sum of an odd number of isomorphic cyclic groups, and V contains elements of infinite order and exactly one cyclic subgroup of order p^k, where p^k is the order of the cyclic direct summands of $F(G, p)$.*

(D) *If $G = F(G)$ (that is, if G is a finite group), if $F(G, p) \neq 0$ and if $2 < r(V_p)$, then $F(G, p)$ is a direct sum of two isomorphic cyclic groups.*

(E) *If $G = F(G)$, $F(G, p) \neq 0$, and $2 = r(V_p)$, then $F(G, p)$ is a direct sum of two cyclic groups of order p^n and one cyclic group of order p^m with $0 \leqq m \leqq n$, $0 < n$, and V contains two independent elements of order p^m.*

(F) *If $G = F(G)$, $F(G, p) \neq 0$, and $1 = r(V_p)$, then $F(G, p)$ is a direct sum of two isomorphic groups.*

(G) *If $F(G)$ contains elements of order n, then V contains elements of order n.*

Proof. If the conditions (A) to (G) are satisfied, then it follows from the existence theorem and its "transformation" that there exists a proper multiplication of G in V. That any two proper multiplications of G in V are isomorphic, if the conditions (A) to (G) are satisfied, is a consequence of the following propositions:

(1) Lemma 8.1 if $r(G, 0)=3$.

(2) Corollary 7.4 if $r(G, 0)=2$.

(3) Corollary 7.2 if $G=F(G)$ is a direct sum of two isomorphic groups and $r(V_p)=1$ for every prime number p such that elements of order p are contained in G.

(4) Lemma 8.1 if $G=F(G)$ and $F(G, p)$ is a direct sum of at most three cyclic groups and $r(V_p)=2$, provided $F(G, p)\neq 0$.

(5) (5.1) and (5.2) if $G=F(G)$ and if $F(G, p)$ is a direct sum of two isomorphic cyclic groups.

Suppose now that there exists one, and apart from isomorphic multiplications, only one proper multiplication of G in V. Assume first that $F(G)\neq G$. Then $1<r(G, 0)$ since $F(G)$ and $r(G, 0)$ are finite, as follows from condition (iii) of the existence theorem. Since furthermore $G=F(G)+U+U'$, where U is a direct sum of an even number of infinite cyclic groups and U' is either 0 or an infinite cyclic group, and since every proper multiplication of U in an infinite cyclic subgroup of V may be extended to a proper multiplication of G in V, it follows from (12.2) that $r(G, 0)\leqq 3$. If $r(G, 0)=3$, then it follows from (13.2), (1) and (4), that $F(V)=0$, and it is a consequence of condition (i) of the existence theorem that $F(G)=0$. Now condition (B) is a consequence of (12.3). If $r(G, 0)=2$, then it follows from (13.2), (1) and (2), that $F(G, p)$ is either 0 or a direct sum of an odd number of isomorphic cyclic groups and that $r(V_p)=1$ is a consequence of (13.2), (3). Thus conditions (A) to (C) are proved to be necessary.

Assume secondly that $G=F(G)$ is a finite group. Then the conditions (D), (E), (F) are consequences of (11.4) and of the conditions (i), (v), and (vi) of the existence theorem which imply also condition (G).

16. **Proof of the uniqueness theorem.** If G is a direct sum of a finite number of cyclic groups, if V is an abelian group, and if G and V satisfy the conditions (1) to (8) of the uniqueness theorem, then it is a consequence of Theorem 15.1 that any two proper multiplications of G in V are isomorphic and that proper multiplications of G in V exist. If G contains elements of infinite order, then V is a direct sum of groups of type* p^∞ and of groups of the type of the additive group of all the rational numbers, and if $G=F(G)$, but

* Groups of type p^∞ contain only elements whose orders are powers of p, and contain, for every positive integer i, exactly one cyclic subgroup of order p^i.

$F(G, p) \neq 0$, then $F(V, p)$ is a direct summand of V which is itself a direct sum of groups of type p^∞.* Thus the isomorphisms of relevant subgroups of finite rank of V may be induced by automorphisms of V. Since finally all the functions $P(n, x)$ appearing in the transformation of the uniqueness theorem satisfy $P(n, x) = 0$ (because $V = nV$ for every relevant n), it follows from the transformation of the uniqueness theorem that the conditions (1) to (8) are sufficient.

In order to prove the necessity of the conditions (1) to (8) it is sufficient to prove the necessity of the conditions (1) and (2), as may be inferred from Theorem 15.1 and the transformation of the uniqueness theorem. V contains a subgroup of the form $F(V) + U$, where U is a direct sum of $r(G, 0)$ infinite cyclic groups, and where U may contain any preassigned element of infinite order as a basis element. If $F(G) \neq G$, then there exist proper multiplications xy of G in $F(V) + U$ such that a given basis element of U appears in $M(G, xy)$. If $V \neq nV$ for some positive n, then it is always possible to find a proper multiplication xy of G in V such that all elements of infinite order in $M(G, xy)$ are elements in nV and to find another one where this is not the case. Thus condition (2) is also necessary.

In order to prove (1) we will have to consider the functions $P(n, x)$. For every proper multiplication xy of G in V there exist admissible functions $P(n, x)$ which have, on a basis of $F(G)$, preassigned values. If $P(n, x) = 0$ for every x of a basis of $F(G)$, then $P(n, x) = 0$ for every odd n and every x in G_n, and the $P(2^i, x)$ are elements in $M(G, xy)_2$. Thus $V = pV$ for every odd prime number such that $F(G, p) \neq 0$; and if V contains elements of order 4 and if $F(G, 2) \neq 0$, then $V = 2V$. By condition (2) and condition (i) of the existence theorem only the following case has to be discussed in order to complete the proof of the necessity of condition (1): *$F(G, 2)$ is a direct sum of groups of order 2 and so is $F(V, 2)$.*

It follows from (6) to (8) that only the following cases are possible:

I. $r(F(G, 2)) = 3$ and $r(F(V, 2)) = 2$.
II. $2 < r(F(G, 2)) = 2i$ and $r(F(V, 2)) = 1$.
III. $2 = r(F(G, 2))$.

Case I. There exists, by Lemma 8.1, for the given proper multiplication xy of G in V a basis b', b'', b of $F(G, 2)$ such that bb' and $b'b''$ form a basis of $F(G, 2)$ and such that $bb'' = 0$. If $P(2, b) = P(2, b') = P(2, p'') = 0$, then

$$P(2, b + b') = bb', \qquad P(2, b' + b'') = b'b'', \qquad P(2, b'' + b) = 0,$$
$$P(2, b + b' + b'') = bb' + b'b''.$$

* Cf. R. Baer, Annals of Mathematics, vol. 37 (1936), pp. 766–781.

If on the other hand $P'(2, b) = P'(2, b') = P'(2, b'') = bb'$, then

$$P'(2, b + b') = bb', \qquad P'(2, b' + b'') = b'b'', \qquad P'(2, b'' + b) = 0,$$
$$P'(2, b + b' + b'') = b'b'';$$

and these two sets of admissible functions are clearly essentially different, unless $V = 2V$.

Case II. There exists, by Corollary 7.2, a basis b_i', b_i'' of $F(G, 2)$ such that $b_1' b_1'' = \cdots = b_k' b_k'' = c$ and such that all the other products of basis elements are 0. The admissible function $P(2, x)$, characterized by $P(2, b_i') = P(2, b_i'') = 0$, has the property that $P(2, x) \neq 0$ for exactly 2^{k-1} elements x in $F(G, 2)$. The admissible functions $P'(2, x)$, on the other hand, which are characterized by

$$P'(2, b_1') = P'(2, b_1'') = c, \qquad P'(2, b_j') = P'(2, b_j'') = 0,$$

for $1 < j$, have the property that $P'(2, x) \neq 0$ for exactly $2^{k-1}(3 \cdot 2^{k-1} - 1)$ (for 3, if $k = 1$) elements x in $F(G, 2)$. This completes the proof of the necessity of condition (1) since this treatment of Case II covers Case III too.

THE UNIVERSITY OF ILLINOIS,
URBANA, ILL.