COUNTABLE TORSION-FREE ABELIAN GROUPS

By M. O'N. CAMPBELL

[Received 27 January 1959.—Read 19 February 1959]

Introduction

IN this paper we present a new classification of the countable torsion-free abelian groups. Since any abelian group G may be regarded as an extension of a periodic group (namely the torsion part of G) by a torsion-free group, and since there exists the well-known complete classification of the countable periodic abelian groups due to Ulm, it is clear that the classification problem studied here is of great interest.

By a group we shall always mean an abelian group, and the additive notation will be employed throughout. It is well known that all the maximal linearly independent sets of elements of a given group are cardinally equivalent; the corresponding cardinal number is the *rank* of the group. Derry (**2**) and Mal'cev (**4**) have studied the torsion-free groups of finite rank only, and have given classifications of these groups in terms of certain equivalence classes of systems of matrices with p-adic elements. Szekeres (**5**) attempted to abolish the finiteness restriction on rank; he extracted certain invariants, but did not derive a complete classification.

By a *basis* of a torsion-free group G we mean any maximal linearly independent subset of G. A subgroup generated by a basis of G will be called a *basal subgroup* or described as basal in G. Thus U is a basal subgroup of G if and only if (i) U is free abelian, and (ii) the factor group G/U is periodic. Of prime importance for our theory is the concept of divisibility of group elements. An element x of a group G is said to be *divisible in G by an integer n* if $x = ny$ for some element y of G; nG denotes the subgroup consisting of the elements divisible in G by n. The motivation for our theory lies in the fact that a torsion-free group is completely determined once we know the divisibility properties of the elements of one of its basal subgroups. Thus arises the notion of a *D-system*, which is central in the discussion. D-systems are certain systems of sequences of integral vector modules (that is, additive groups of suitable ordered sets of integers) which we associate with the countable torsion-free groups in a many-to-one correspondence. An equivalence relation is set up between D-systems; the corresponding equivalence classes, called *D-types*, are in a one-to-one correspondence with the groups.

One of the most important concepts employed is that of a *quotient*, which

enters both into the definition of D-systems and also into that of the equivalence relation that separates them into D-types. The notion of a quotient is new to the theory of abelian groups.

The first part of the paper deals with the general theory, and Part II with the practical problems arising therefrom. In Part III the theory is applied to yield a characterization of the countable free groups in terms of their D-systems.

I

1. Auxiliary material

We denote by $\mathscr{F}$ the set of all matrices (finite or infinite) over the rational field having at most a finite number of non-zero elements in each row. By a matrix we shall mean always a matrix in $\mathscr{F}$. A square matrix with an inverse in $\mathscr{F}$ will be said to be *regular*. An *integral* matrix is one that has only integral elements. If $A = (a_{ij})$ is such a matrix, having n columns, and $\mathbf{u} = (u_1, u_2, \ldots)$ is an ordered set of n elements of a group, then $A\mathbf{u}$ will denote the ordered set $(w_1, w_2, \ldots)$ given by $w_i = \sum_j a_{ij} u_j$ $(i = 1, 2, \ldots)$; in other words, $\mathbf{u}$ is treated as a column matrix admitting left multiplication by integral matrices only.

A one-rowed matrix $\mathbf{c} = (c_1\ c_2\ \ldots\ c_i\ \ldots)$ will be called a *vector* with *coordinates* c_i. The least common multiple of the denominators of the c_i, when these are expressed in their lowest terms, is the *denominator* of $\mathbf{c}$.

By a *vector module* we mean an additive group of vectors. If A is a matrix the vector module generated by the rows of A will be denoted by (A).

(1.1) If A, B are matrices with equal numbers of columns, then $(A) \subseteq (B)$ if and only if $A = CB$ for some integral matrix C.

(1.2) Let A, B, C be matrices such that AC, BC exist. Then $(A) \subseteq (B)$ implies $(AC) \subseteq (BC)$.

These two propositions are almost immediate consequences of the notation.

From this point onwards r will denote an arbitrary finite or countable cardinal number. The module that consists of all the vectors with r coordinates will be denoted by R, and the submodule formed by the integral vectors of R by J.

Let M be a submodule of J, and let P be an integral square matrix of order r. The set of integral vectors $\mathbf{c}$ such that $\mathbf{c}P \in M$ is a submodule of J; for if $\mathbf{a}P$, $\mathbf{b}P \in M$, then $(\mathbf{a}-\mathbf{b})P = \mathbf{a}P - \mathbf{b}P \in M$. We denote this submodule by $M:P$ and call it the *quotient* of M by P. If A is an integral matrix with r columns and P is regular, then $(A):P$ may be described as the integral part of (AP^{-1}), that is to say $(AP^{-1}) \cap J$. If P is scalar, say mI,

where I is the unit matrix, we write $M:m$ for $M:mI$. For any sequence $\mathbf{M} = (M_0, M_1, M_2,...)$ of submodules of J, $\mathbf{M}:P$ will have the obvious meaning $(M_0:P, M_1:P, M_2:P,...)$.

The following simple properties of quotients will be used in the sequel. We suppose that M, N are submodules of J and that P, Q are integral square matrices of order r.

(1.3) $$M \subseteq N \text{ implies } M:P \subseteq N:P.$$

(1.4) $$M:P:Q = M:QP.$$

(1.5) If A is an integral matrix having r columns, and Q is regular, then

$$(AQ):PQ = (A):P.$$

For if $\mathbf{c}PQ \in (AQ)$, then $\mathbf{c}P = \mathbf{c}PQQ^{-1} \in (AQQ^{-1}) = (A)$; and the converse is obvious.

Quotients of the form $mJ:P$, where m is an integer, are of special importance in view of later applications, since all the quotients that we shall encounter will be reducible to this form. Clearly $mJ:P$ is the set of all integral solutions $\mathbf{c} = (c_1\ c_2\ ...)$ of the system of linear congruences

$$\mathbf{c}P \equiv 0 \pmod{m},$$

and is therefore calculable.

2. D-systems and torsion-free groups

Let G denote a torsion-free group of finite or countable rank r, and let $\mathbf{u} = (u_1, u_2,...)$ be an ordered basis of G, generating the basal subgroup U. For each positive integer m, let $f(m)$ denote the set of all integral vectors $\mathbf{c}$ such that $\mathbf{cu}$ is divisible in G by m. $f(m)$ is the image of $U \cap mG$ under the isomorphism $(\mathbf{cu} \to \mathbf{c})$ of U onto J, and hence $f(m)$ is a submodule of J. The function f defined by $(m \to f(m))$ completely describes the divisibility properties in G of the elements of U, and will be called, appropriately, the *divisibility function* of G with respect to $\mathbf{u}$.

(1.6) Uniqueness Theorem. *The group G is completely determined by the function f to within isomorphism.*

Proof. Let x be an arbitrary element of G. Since $\mathbf{u}$ is a basis of G, we have $mx = \mathbf{cu}$ for some positive integer m and some integral vector $\mathbf{c}$ in $f(m)$. Consider the mapping θ of G into R given by $x\theta = m^{-1}\mathbf{c}$, and let K denote the image of G under θ. We shall show that K is a submodule of R and that θ is an isomorphism of G onto K. We begin by proving a

(1.7) Lemma. *Let h, k be positive integers, $\mathbf{a}$, $\mathbf{b}$ members of J, $hx = \mathbf{au}$, $ky = \mathbf{bu}$, where $x, y \in G$. Then $x = y$ if and only if $h^{-1}\mathbf{a} = k^{-1}\mathbf{b}$.*

Proof. We have $(k\mathbf{a}-h\mathbf{b})\mathbf{u} = k\mathbf{au}-h\mathbf{bu} = hk(x-y)$. Since G is

torsion-free, $x-y = 0$ if and only if $hk(x-y) = 0$, that is if and only if $(k\mathbf{a}-h\mathbf{b})\mathbf{u} = 0$. Now the set $\mathbf{u}$ is linearly independent; hence the latter equation holds if and only if $k\mathbf{a}-h\mathbf{b} = 0$, or $h^{-1}\mathbf{a} = k^{-1}\mathbf{b}$. This proves the lemma.

The mapping θ is therefore one to one. Also we have, with the notation of the lemma,

$$(x-y)\theta = (hk)^{-1}(k\mathbf{a}-h\mathbf{b}) = h^{-1}\mathbf{a}-k^{-1}\mathbf{b} = x\theta-y\theta;$$

and thus θ is a homomorphism. Hence K is a submodule of R, and G is isomorphic to K. Finally, since by definition K is completely determined by f, G also is completely determined to within isomorphism by f. This completes the proof of the Uniqueness Theorem.

Obviously $f(1) = J$, and $f(m) \subseteq f(n)$ if n divides m. We have also the following

(1.8) THEOREM. *For any finite set of positive integers $n_1, n_2, \ldots, n_k$, coprime in pairs,*

$$f(n_1 n_2 \ldots n_k) = f(n_1) \cap f(n_2) \cap \ldots \cap f(n_k).$$

Proof. Let n_i' denote $(n_1 n_2 \ldots n_k)/n_i$ $(i = 1, 2, \ldots, k)$. Then

$$(n_1', n_2', \ldots, n_k') = 1,$$

and hence there exist integers $s_1, s_2, \ldots, s_k$ such that

$$s_1 n_1' + s_2 n_2' + \ldots + s_k n_k' = 1.$$

Now suppose that an element x of G is divisible in G by each n_i. Then for suitable elements y_i of G we have

$$x = \sum_i s_i n_i' x = \sum_i s_i n_i' n_i y_i = n_1 n_2 \ldots n_k \sum_i s_i y_i.$$

Hence $\mathbf{cu}$ is divisible in G by $n_1 n_2 \ldots n_k$ if and only if $\mathbf{cu}$ is divisible by each n_i. This completes the proof.

It follows that $f(m)$ is the intersection of all $f(q)$, where q ranges over the prime power factors of m, and thus f is completely determined by its values at the prime powers and the condition $f(1) = J$. For each prime p we have a sequence

$$f(p^0) = J \supseteq f(p) \supseteq f(p^2) \supseteq \ldots \supseteq f(p^n) \supseteq \ldots .$$

The system of these sequences, one for each prime p, will be called the *divisibility system* of G with respect to $\mathbf{u}$. By the Uniqueness Theorem, groups with a divisibility system in common are isomorphic.

It is natural now to attempt to characterize divisibility systems intrinsically, that is to say, in terms not involving the groups to which they belong. Consider the sequence $[f(p^n)]$ for any fixed prime p, and suppose that $\mathbf{c} \in f(p^n)$. Then $\mathbf{cu} \in p^n G$, and hence $p\mathbf{cu} \in p^{n+1}G$; therefore $\mathbf{c} \in f(p^{n+1}):p$.

But since G is torsion-free, this chain of reasoning is reversible, and thus

$$f(p^{n+1}):p = f(p^n) \quad (n = 0, 1, 2,...)$$

for every prime p. These relations together with the condition $f(1) = J$ are sufficient for the characterization of the divisibility systems, as will be shown in the next theorem. First, we put the relations into a formal definition:

If p is a prime and $\mathbf{M} = (M_0, M_1, M_2,..., M_n,...)$ is an infinite sequence of submodules of J, then $\mathbf{M}$ will be called a D_p-*sequence* if the following conditions are satisfied:

(D_p) $$M_0 = J; \qquad M_{n+1}:p = M_n \quad (n = 0, 1, 2,...).$$

A system $[\mathbf{M}(p)]$, containing precisely one D_p-sequence

$$\mathbf{M}(p) = (M_0(p), M_1(p), M_2(p),...)$$

for each prime p, will be called a *D-system*. The individual sequences $\mathbf{M}(p)$ are the *components* of the D-system.

We observe that the second part of (D_p) is expressible in the following alternative form:

$$M_{n+1} \cap pJ = pM_n \quad (n = 0, 1, 2,...).$$

Every divisibility system is thus a D-system. In order to prove the converse, we shall require the following simple properties of an arbitrary D_p-sequence $\mathbf{M}$, where m, n denote arbitrary non-negative integers. A simple induction argument yields the result:

(1.9) $$M_{m+n}:p^m = M_n,$$

and an immediate consequence of this is that

(1.10) $$p^m M_n \subseteq M_{m+n}.$$

Now suppose that h is an integer prime to p. Then $sh+tp^n = 1$ for suitable integers s, t. Hence if $\mathbf{c} \in M_n:h$, then $\mathbf{c} = sh\mathbf{c}+tp^n\mathbf{c} \in M_n$, since $p^n\mathbf{c} \in M_n$ by (1.10). Therefore $M_n:h \subseteq M_n$. But it is obvious that $M_n \subseteq M_n:h$, and therefore we have

(1.11) $$M_n:h = M_n \text{ if } (h,p) = 1.$$

We shall now prove the following

(1.12) EXISTENCE THEOREM. *Every D-system is a divisibility system of a suitable group.*

Proof. Let $[\mathbf{M}(p)]$ be any given D-system. We shall construct a submodule of R of which it is a divisibility system.

We denote by L_p, for each prime p, the set of all vectors of the form $p^{-n}\mathbf{c}$, where n is a non-negative integer and $\mathbf{c} \in M_n(p)$. If

$$\mathbf{a} \in M_m(p) \quad \text{and} \quad \mathbf{b} \in M_n(p),$$

then $p^n\mathbf{a}$ and $p^m\mathbf{b}$ are members of $M_{m+n}(p)$, by (1.10), and hence

$$p^{-m}\mathbf{a}-p^{-n}\mathbf{b} = p^{-(m+n)}(p^n\mathbf{a}-p^m\mathbf{b}) \in L_p.$$

L_p is therefore a submodule of R. Also since $M_0(p) = J$, $J \subseteq L_p$.

Let $L = \sum_p L_p$, where p ranges over all the primes. J is a free submodule of L, and for any vector $\mathbf{c}$ in R we have $d\mathbf{c} \in J$, where d is the denominator of $\mathbf{c}$; hence J is basal in L. Also, the rows of the unit matrix of order r form a linearly independent set of generators of J; they therefore constitute a basis of L. Consider the divisibility function g of L with respect to this basis, ordered according to the order in which the vectors occur in the unit matrix. $g(p^n)$ consists of the integral vectors of p^nL. It is clear from the definition of L_p that $M_n(p) \subseteq p^nL$; hence it remains to show that

$$g(p^n) \subseteq M_n(p).$$

Let $L'_p = \sum_q L_q$, where q ranges over all the primes other than p. Then we have $L = L_p + L'_p$. Now every element of L'_p is expressible in the form $s^{-1}\mathbf{b}$, where s is a positive integer prime to p and $\mathbf{b} \in J$. Hence if $\mathbf{c} \in g(p^n)$, then we have $\mathbf{c} = p^n(p^{-m}\mathbf{a}+s^{-1}\mathbf{b})$, where s, $\mathbf{b}$ satisfy the conditions above and $\mathbf{a} \in M_m(p)$ for some non-negative integer m. Hence

$$sp^m\mathbf{c} = sp^n\mathbf{a}+p^{m+n}\mathbf{b} \in M_{m+n}(p),$$

by (1.10), and therefore $\mathbf{c} \in M_{m+n}(p) : s : p^m = M_n(p)$, by (1.9) and (1.11).

It follows that $g(p^n) = M_n(p)$ for every prime p and every non-negative integer n, and the Existence Theorem is established.

A D-system which is a divisibility system of a group G will be said to *belong to* G. Our main results above can thus be summarized in the statement that any given D-system belongs to a unique abstract group.

3. The isomorphism problem

The divisibility system assigned to the group G in Section 2 depended on the choice of the ordered basis $\mathbf{u}$. Hence it is to be expected that distinct D-systems may belong to isomorphic groups. The theme of this section is the determination of conditions under which this situation obtains.

As before, let G be a torsion-free group of rank r, and let

$$\mathbf{u} = (u_1, u_2, \ldots, u_i, \ldots)$$

be an ordered basis of G, generating the subgroup U. We shall first consider a transition to a new ordered basis contained in U. Obviously such a basis is expressible in the form $P\mathbf{u}$, where P is an integral square matrix of order r.

(1.13) LEMMA. *$P\mathbf{u}$ is a basis of G if and only if P is regular.*

Proof. Let x be an arbitrary element of G. Then $mx = \mathbf{cu}$ for some positive integer m and some integral vector $\mathbf{c}$. Now suppose that P is

regular; then $\mathbf{c} = \mathbf{c}P^{-1}P = k^{-1}\mathbf{a}P$, where k is the denominator of $\mathbf{c}P^{-1}$ and $\mathbf{a}$ is integral. Hence $kmx = \mathbf{a}P\mathbf{u}$, and thus every element of G is linearly dependent on the set $P\mathbf{u}$. Also $P\mathbf{u}$ is linearly independent; for $\mathbf{b}P\mathbf{u} = 0$, where $\mathbf{b}$ is an integral vector, implies $\mathbf{b}P = 0$, and thus $\mathbf{b} = \mathbf{b}PP^{-1} = 0$. Therefore $P\mathbf{u}$ is a basis of G.

Suppose now that $P\mathbf{u}$ is a basis. Then there exist positive integers t_i such that $t_i u_i = \mathbf{b}^i P\mathbf{u}$ for each i, where the $\mathbf{b}^i$ are suitable integral vectors. Denoting by T the regular diagonal matrix whose ith diagonal element is t_i, and denoting by B the matrix whose ith row is $\mathbf{b}^i$, for each i, we have $T\mathbf{u} = BP\mathbf{u}$, and hence $T = BP$, since $\mathbf{u}$ is linearly independent. P therefore possesses a left inverse $T^{-1}B$ in $\mathfrak{F}$. Now if P has a non-zero left annihilator in $\mathfrak{F}$, then there is an integral vector $\mathbf{c} \neq 0$ such that $\mathbf{c}P = 0$, and hence $\mathbf{c}P\mathbf{u} = 0$. But the latter equation is inconsistent with the linear independence of the basis $P\mathbf{u}$. Hence P is regular.

This completes the proof of the lemma.

Now if f is the divisibility function of G with respect to $\mathbf{u}$, then

$$\mathbf{c}P\mathbf{u} \in p^n G$$

if and only if $\mathbf{c}P \in f(p^n)$, in other words if and only if $\mathbf{c} \in f(p^n)\colon P$. We have therefore the following:

(1.14) LEMMA. *If* $[\mathbf{M}(p)]$ *is the divisibility system of* G *with respect to* $\mathbf{u}$, *then the divisibility system of* G *with respect to* $P\mathbf{u}$, *where* P *is regular, is* $[\mathbf{M}(p)\colon P]$.

Thus for *any* regular integral matrix P of order r, $[\mathbf{M}(p)\colon P]$ is a D-system and belongs to G.

We shall now establish a connexion between the divisibility systems of G with respect to arbitrary ordered bases with the aid of the next

(1.15) LEMMA. *If* U, V *are basal subgroups of* G, *then so is* $U \cap V$.

Proof. $U \cap V$, a subgroup of the free group U, is free. Also for any element x of G there exist positive integers m, n such that $mx \in U$, $nx \in V$, and hence $mnx \in U \cap V$. These results show that $U \cap V$ is basal in G.

If $\mathbf{u}$, $\mathbf{v}$ are ordered bases of G, and U, V denote the subgroups that they generate, we can select a basis $\mathbf{w}$ of G in $U \cap V$, by the preceding lemma, and by Lemma 1.13 we have $P\mathbf{u} = \mathbf{w} = Q\mathbf{v}$ for suitable regular matrices P, Q. If $[\mathbf{M}(p)]$, $[\mathbf{N}(p)]$ are the divisibility systems of G with respect to $\mathbf{u}$, $\mathbf{v}$, respectively, then by Lemma 1.14,

$$\mathbf{M}(p)\colon P = \mathbf{N}(p)\colon Q$$

for all primes p. This relation provides the key to the solution of the isomorphism problem. We shall say that the D-systems $[\mathbf{M}(p)]$, $[\mathbf{N}(p)]$ are

associated if, for all primes p, and for suitable regular integral matrices P, Q, independent of p,

$$\mathbf{M}(p):P = \mathbf{N}(p):Q.$$

We now proceed to prove the

(1.16) ISOMORPHISM THEOREM. *Two D-systems* $[\mathbf{M}(p)]$, $[\mathbf{N}(p)]$ *belong to isomorphic groups if and only if they are associated.*

Proof. Suppose that the D-systems belong to G, H, respectively. From the manner in which D-systems are assigned to groups in our theory, it is clear that isomorphic groups possess identical sets of D-systems. Hence if G, H are isomorphic, then both the D-systems of the theorem belong to G, and therefore they are associated.

Conversely, suppose that $[\mathbf{M}(p)]$, $[\mathbf{N}(p)]$ are associated by means of P, Q. By Lemmas 1.13 and 1.14, $[\mathbf{M}(p):P]$ is a D-system belonging to G, and $[\mathbf{N}(p):Q]$ is a D-system belonging to H. Thus G, H have a common D-system, and are therefore isomorphic, by the Uniqueness Theorem.

It is now clear that the relation of association between D-systems is an equivalence relation. The equivalence classes that it defines will be called *D-types*. The set of D-systems belonging to a given group is a D-type; every D-type corresponds to some group; and two groups are isomorphic if and only if their D-types are the same. Here we have the complete classification of the countable torsion-free groups.

Groups of finite rank. We shall now examine further the association relation for the D-systems that belong to groups of finite rank, and we shall show that the relation can be simplified considerably for such systems.

Let the D-systems $[\mathbf{M}(p)]$, $[\mathbf{N}(p)]$ be associated by means of P, Q. Since Q is of finite order, the elements of Q^{-1} can all be expressed with a common denominator, m say, and hence $Q^{-1} = m^{-1}T$, where T is a regular integral matrix. Hence $TQ = mI$, and we have

$$\mathbf{N}(p):m = \mathbf{N}(p):TQ = \mathbf{N}(p):Q:T = \mathbf{M}(p):P:T = \mathbf{M}(p):TP$$

for each prime p, where TP is regular. Thus the association condition is expressible in the form:

$$[\mathbf{N}(p):m] = [\mathbf{M}(p):P]$$

for some positive integer m and some regular integral matrix P.

The determination of $[\mathbf{N}(p):m]$ is simple because of (1.9) and (1.11). If $(m,p) = 1$, then $\mathbf{N}(p):m = \mathbf{N}(p)$. If m is divisible by p, then let $m = p^h m'$, where $(m', p) = 1$. We have

$$\mathbf{N}(p):m = \mathbf{N}(p):m':p^h = \mathbf{N}(p):p^h.$$

Now if $(M_0, M_1, M_2,\ldots)$ is a D_p-sequence, then $M_n:p^h = M_{n-h}$ if $n \geqslant h$, and $M_n:p^h = M_n:p^n:p^{h-n} = J:p^{h-n} = J$ if $n < h$. Hence $\mathbf{N}(p):p^h$ can be

obtained by adjoining to $\mathbf{N}(p)$ an initial run of J's, h in number. For example:

$$(M_0, M_1, M_2, \ldots) : p^3 = (J, J, J, M_0, M_1, M_2, \ldots).$$

It follows that every D-system of the form $[\mathbf{N}(p) : m]$ can be obtained from $[\mathbf{N}(p)]$ by augmenting each of at most a finite number of the components of $[\mathbf{N}(p)]$ (i.e. those components that correspond to the primes that divide m) with an initial finite run of J's, and leaving all the remaining components unaltered. Thus *all* the D-systems associated with $[\mathbf{M}(p)]$ can be derived as follows:

(i) Obtain $[\mathbf{M}(p) : P]$ for an arbitrary regular matrix P.

(ii) Delete at most a finite number of J's from the new system, leaving at least one J in each component.

This concludes the special remarks for finite r.

II

Our next main task will be to evolve a method for constructing D-systems. We observe that the components of a D-system are independent of one another, and hence it is sufficient to study the D_p-sequences for a fixed prime p. It is first necessary to obtain certain additional auxiliary results.

1. Auxiliary material

The *length* of a vector $\mathbf{c} = (c_1 c_2 \ldots c_i \ldots)$ is defined to be 0 if $\mathbf{c} = 0$ and k if $c_k \neq 0$ while $c_i = 0$ for every $i > k$. A square matrix having only zeros above its main diagonal while each diagonal element is non-zero will be said to be *triangular*. For any vector module M and any positive integer k, $M^{(k)}$ will denote the submodule that consists of all the vectors in M whose lengths do not exceed k—the kth 'segment' of M. Obviously M is the union of its segments. If A is a triangular matrix, then for each k, the first k rows of A generate the whole of $(A)^{(k)}$.

We shall be concerned here with submodules M of J such that M contains vectors of all lengths possible in J. (The members of any D_p-sequence $\mathbf{M}$ have this property, since $p^n J \subseteq M_n$. It can be easily proved that the class of modules with the property mentioned is the class of basal submodules of J). Throughout the remainder of this section M will denote such a module.

For each k, the kth coordinates of the vectors in $M^{(k)}$ clearly form a non-trivial additive group of integers—an infinite cyclic group. Let

$$m_k = m_k(M)$$

denote the positive generator of this group. Then we have the following

(2.1) THEOREM. *Let* $[\mathbf{a}^i]$ *be any selection of* r *vectors in* M *such that for each* i, *the length of* $\mathbf{a}^i$ *is* i *and the* i*-th coordinate of* $\mathbf{a}^i$ *is* m_i *or* $-m_i$. *Then* $[\mathbf{a}^i]$ *generates* M.

Proof. The proof is by induction. Obviously $\mathbf{a}^1$ generates $M^{(1)}$. Now suppose that $\mathbf{a}^1, \mathbf{a}^2, \ldots, \mathbf{a}^n$ generate $M^{(n)}$, and that $\mathbf{c}$ is any vector in $M^{(n+1)}$. Then there exists an integer t such that the $(n+1)$th coordinate of $\mathbf{c}-t\mathbf{a}^{n+1}$ is 0, and thus $\mathbf{c}-t\mathbf{a}^{n+1} \in M^{(n)}$; hence $\mathbf{c}$ belongs to the vector module generated by $\mathbf{a}^1, \mathbf{a}^2, \ldots, \mathbf{a}^{n+1}$. It follows that for each k, $M^{(k)}$ is generated by $\mathbf{a}^1, \mathbf{a}^2, \ldots, \mathbf{a}^k$, and since M is the union of the $M^{(k)}$ the set $[\mathbf{a}^i]$ generates M.

On arranging the vectors $\mathbf{a}^i$ in order of increasing length we obtain a triangular matrix A which represents M in the sense that $M = (A)$; but A is not uniquely defined, since we have in general an infinity of choices for each $\mathbf{a}^i$. We shall discuss next a method for the selection of the $\mathbf{a}^i$ which will yield a unique result. A vector $\mathbf{c} = (c_1\ c_2\ \ldots)$ in M of length k, say, will be said to be *reduced with respect to* M if $c_k = m_k$ and $0 \leqslant c_i < m_i$ for each $i < k$.

(2.2) THEOREM. *For each* k, M *contains one and only one vector of length* k *that is reduced with respect to* M.

Proof. There cannot be more than one such vector; for let us suppose that $\mathbf{a} = (a_1\ a_2\ \ldots)$ and $\mathbf{b} = (b_1\ b_2\ \ldots)$ are both of length k and reduced with respect to M, and let j be the length of $\mathbf{a}-\mathbf{b}$. If $j \neq 0$, then $a_j - b_j$ is a multiple of m_j. But $0 \leqslant a_j < m_j$ and $0 \leqslant b_j < m_j$; hence $a_j - b_j = 0$, and thus the length of $\mathbf{a}-\mathbf{b}$ is less than j. From this contradiction it follows that

$$\mathbf{a}-\mathbf{b} = 0.$$

We shall now establish the existence of the vector of the theorem. Let $[\mathbf{a}^i]$ be a selection of r vectors in M, such that for each i the length of $\mathbf{a}^i$ is i and the ith coordinate of $\mathbf{a}^i$ is m_i. Clearly $\mathbf{a}^1$ satisfies the conditions of the theorem for the case $k = 1$. If $k > 1$, and $\mathbf{a}^k$ is not reduced with respect to M, we can obtain a vector of length k that is reduced with respect to M by means of the following transformations on $\mathbf{a}^k$: Add to $\mathbf{a}^k$ a suitable multiple of $\mathbf{a}^{k-1}$ to obtain a vector whose length is k, whose kth coordinate is m_k, and whose $(k-1)$th coordinate is non-negative and less than m_{k-1}. If the new vector is not reduced with respect to M, add to this vector a suitable multiple of $\mathbf{a}^{k-2}$ to obtain a vector whose length is k, whose kth coordinate is m_k, and whose $(k-1)$th, $(k-2)$th coordinates are non-negative and less than m_{k-1}, m_{k-2}, respectively; and so on. By this procedure we obtain in a finite number of steps a vector of length k reduced with respect to M.

This completes the proof of the theorem.

The triangular matrix whose rows are the vectors reduced with respect to M will be called the *canonical representative* of M.

p-elementary matrices. Of vital importance for the construction of D_p-sequences in the next section are the canonical representatives of submodules M of J such that $pJ \subseteq M$ (or equivalently $M:p = J$). Such matrices will be said to be *p-elementary*, and we proceed to determine them explicitly.

If $pJ \subseteq M$, then for each k, the vector $(0\ 0\ \ldots\ 0\ p\ 0\ \ldots)$ of length k belongs to M, and hence m_k divides p; hence $m_k = 1$ or p. If $m_k = p$, then clearly the vector above is the vector of length k reduced with respect to M. Hence the p-elementary matrices $E = (e_{ij})$ satisfy the following conditions:

(2.3) (i) E is integral and triangular;
(ii) $e_{ii} = 1$ or p, for each i;
(iii) if $e_{ii} = 1$, then all the remaining elements of the ith column are zero;
(iv) if $e_{ii} = p$, then all the remaining elements of the ith row are zero;
(v) $0 \leqslant e_{ij} < p$ if $e_{ii} = 1$, $e_{jj} = p$ $(i > j)$.

It will now be shown that every matrix E that satisfies (2.3) is p-elementary. We define another triangular matrix $\bar{E} = (\bar{e}_{ij})$ as follows:

$$\bar{e}_{ii} = p/e_{ii}; \qquad \bar{e}_{ij} = -e_{ij} \quad (i \neq j).$$

(2.4) THEOREM. $\bar{E}E = pI = E\bar{E}$.

Proof. Since E, $\bar{E}$ are triangular, so also is $\bar{E}E$, and each diagonal element of $\bar{E}E$ is equal to the product of the corresponding elements of $\bar{E}$, E, and hence is equal to p. Let us consider the elements below the main diagonal of $\bar{E}E = (f_{ij})$. These elements are given by the equations

$$f_{ij} = \sum_k \bar{e}_{ik} e_{kj} \quad (i > j).$$

Suppose that $k \neq i$, $k \neq j$. Then $\bar{e}_{ik} e_{kj} = 0$; for if $e_{kj} \neq 0$, then $e_{kk} = 1$ and hence $\bar{e}_{ik} = -e_{ik} = 0$. We have therefore

$$f_{ij} = \bar{e}_{ij} e_{jj} + \bar{e}_{ii} e_{ij} = -e_{ij} e_{jj} + (p/e_{ii}) e_{ij}$$
$$= e_{ij}(p - e_{ii} e_{jj})/e_{ii}.$$

Now if $e_{ij} \neq 0$, then $e_{ii} = 1$ and $e_{jj} = p$; hence $p - e_{ii} e_{jj} = 0$. Thus $f_{ij} = 0$ if $i > j$. Hence $\bar{E}E = pI$.

It follows that $p^{-1}\bar{E}$ is the inverse of E, and therefore

$$E\bar{E} = pEE^{-1} = pI.$$

This completes the proof.

With the aid of the result above we can prove the following

(2.5) THEOREM. *Any matrix E that satisfies the conditions* (2.3) *is p-elementary.*

Proof. $pJ = (pI) = (\bar{E}E) \subseteq (E)$. Since E is triangular, the first k rows of E generate $(E)^{(k)}$, and hence $m_k((E)) = e_{kk}$ for each k. It can now be easily verified that the rows of E are reduced with respect to (E), and hence the theorem is established.

Examples

I and pI are p-elementary.

The p-elementary matrices of order 2 are

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \quad \begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}, \quad \begin{pmatrix}p & 0\\ h & 1\end{pmatrix} \ (0 \leqslant h < p), \quad \begin{pmatrix}p & 0\\ 0 & p\end{pmatrix}.$$

An example of order 3 is

$$\begin{pmatrix}p & 0 & 0\\ h & 1 & 0\\ 0 & 0 & p\end{pmatrix} \quad (0 \leqslant h < p).$$

2. The construction of D_p-sequences

Throughout this section **M** will denote a D_p-sequence $(M_0, M_1, M_2, \ldots)$. Our first theorem, supported by the following lemma, shows that **M** can be represented by a sequence of p-elementary matrices.

(2.6) LEMMA. *Let A be a given regular integral matrix of order r, and let M be a given submodule of J such that $M:p = (A)$. Then $M = (EA)$ for some unique p-elementary matrix E.*

Proof. $M \subseteq M:p = (A)$, and therefore $M = (BA)$ for some integral matrix B. Now $(B):p = (BA):pA = M:p:A = (A):A = J$. Consequently, there is a p-elementary matrix E such that $(B) = (E)$, and we have $M = (BA) = (EA)$.

We now show that E is unique. Suppose that $(FA) = (EA)$, where F also is p-elementary. Then

$$(F) = (FAA^{-1}) = (EAA^{-1}) = (E),$$

and hence $F = E$.

This completes the proof of the lemma.

(2.7) THEOREM. *Let* **M** *be a given D_p-sequence. Then there is a unique sequence $(E_1, E_2, \ldots)$ of p-elementary matrices such that*

$$M_1 = (E_1), \qquad M_n = (E_n E_{n-1} \ldots E_1) \quad (n = 2, 3, \ldots).$$

Proof. The proof is by induction on n. There is a unique p-elementary matrix E_1 such that $M_1 = (E_1)$, since $M_1:p = M_0 = J$. Let us assume the

existence and the uniqueness of each of the first k members of the sequence $[E_n]$, and apply the lemma above with $A = E_k E_{k-1} \dots E_1$ and $M = M_{k+1}$. Then the existence and uniqueness of E_{k+1} follow, and the theorem is established.

Those sequences of p-elementary matrices that determine D_p-sequences in the manner indicated in the last theorem will be said to be *admissible*. Our task now is to characterize the admissible sequences.

If E, F are p-elementary matrices we say that F is *adherent* to E if $(FE):p = (E)$. A sequence of p-elementary matrices will be called a *chain* if each member of the sequence after the first is adherent to its immediate predecessor in the sequence. It will be shown that the class of admissible sequences consists exclusively of the chains. We begin with an auxiliary

(2.8) LEMMA. *Let A, E, F be square matrices of order r, where A is integral and regular, E, F are p-elementary, and $(EA):p = (A)$. Then*

$$(FEA):p = (EA)$$

if and only if F is adherent to E.

Proof. If $(FEA):p = (EA)$, then

$$(FE):p = (FEA):pA = (FEA):p:A = (EA):A = (E).$$

Conversely, suppose that F is adherent to E. We have $(FEA) \subseteq (EA)$, and therefore $(FEA):p \subseteq (EA):p = (A)$; hence $(FEA):p = (BA)$ for a suitable matrix B. We have

$$(B) = (BA):A = (FEA):p:A = (FEA):A:p = (FE):p = (E).$$

Hence $(BA) = (EA)$.

This completes the proof of the lemma.

We are now in a position to prove the following

(2.9) THEOREM. *A sequence $[E_n] = (E_1, E_2, \dots)$ of p-elementary matrices is admissible if and only if it is a chain.*

Proof. We write $A_0 = I$, $A_n = E_n A_{n-1}$ $(n = 1, 2, \dots)$, $M_n = (A_n)$ $(n = 0, 1, 2, \dots)$, and $\mathbf{M} = (M_0, M_1, M_2, \dots)$. If $\mathbf{M}$ is a D_p-sequence, then on applying the lemma with $A = A_{n-1}$, $E = E_n$, $F = E_{n+1}$, we deduce that E_{n+1} is adherent to E_n $(n = 1, 2, \dots)$.

$M_0 = J$, and since E_1 is p-elementary we have $M_1:p = J = M_0$. If we assume that $[E_n]$ is a chain and that $M_{k+1}:p = M_k$, then on applying the lemma with $A = A_k$, $E = E_{k+1}$, $F = E_{k+2}$, we have $M_{k+2}:p = M_{k+1}$. Hence $\mathbf{M}$ is a D_p-sequence, and the proof of the theorem is now complete.

It will be our next object to determine practical criteria for adherence. With these criteria we shall have a method for the explicit construction of all the D_p-sequences.

We shall reason in terms of the linear algebra of $J \pmod p$, that is to say the algebra of the elementary group J/pJ treated as a linear space over the Galois field $GF(p)$ of the integers $\pmod p$. A set of vectors in J will be said to be *linearly dependent* $(mod\, p)$ if for some finite subset $\mathbf{c}^1, \mathbf{c}^2, \ldots$, we have $(n_1\mathbf{c}^1+n_2\mathbf{c}^2+\ldots) \in pJ$ for suitable integers $n_1, n_2, \ldots$, not all of which are divisible by p; otherwise the set will be said to be *linearly independent* $(mod\, p)$. For any submodule M of J the dimension of the linear space $M \pmod p$ or $M/M \cap pJ$ will be denoted by $\dim M$.

A criterion for the linear independence $\pmod p$ of a subset S of J is familiar from linear algebra. Let the vectors in S be ordered in any manner to form a matrix C. If S consists of a finite number n of vectors, then S is linearly independent $\pmod p$ if and only if C possesses at least one minor of order n that is not divisible by p. If S is infinite, then S is linearly independent $\pmod p$ if and only if each of its finite subsets has this property, and it is sufficient to apply the test to the first m rows of C for every finite m.

The main diagonals of p-elementary matrices will play an important part in the analysis that follows; hence we introduce the following notation for any such matrix $E = (e_{ij})$: $\mathscr{I}(E)$ denotes the set of suffixes i such that $e_{ii} = 1$, and $\rho_k(E)$ denotes the number of suffixes $i \leqslant k$ in $\mathscr{I}(E)$ for each k.

The adherence criteria are contained in the next theorem, to which the following notation applies: F is a p-elementary matrix and $A = (a_{ij})$ any integral triangular matrix, both of order r; $FA = (b_{ij})$; $\mathbf{a}^i$, $\mathbf{b}^i$ denote the ith rows of A, FA, respectively.

(2.10) THEOREM. *$(FA):p = (A)$ if and only if one of the following conditions holds*:

(1) *The set $\mathscr{I}(F)$ is empty, or equivalently $F = pI$.*

(2) *$\mathscr{I}(F)$ is not empty, and the set $[\mathbf{b}^i;\ i \in \mathscr{I}(F)]$ is linearly independent* $\pmod p$.

Proof. (1) obviously implies $(FA):p = (A)$. In the remainder of the proof we shall assume that $\mathscr{I}(F)$ is not empty. Suppose that (2) does not hold. Then there is a least suffix j in $\mathscr{I}(F)$ such that the set

$$[\mathbf{b}^i;\ i \in \mathscr{I}(F),\ i \leqslant j]$$

is linearly dependent $\pmod p$, and we have $\sum n_i \mathbf{b}^i + n_j \mathbf{b}^j = p\mathbf{c}$, where the summation extends over all i such that $j > i \in \mathscr{I}(F)$, $\mathbf{c} = (c_1\ c_2\ \ldots)$ is a suitable integral vector, and the n_i are suitable integers, where $n_j \not\equiv 0 \pmod p$. On equating the jth coordinates of the two sides of the equation above we have $pc_j = n_j b_{jj} = n_j a_{jj}$. Hence c_j is not a multiple of a_{jj}. But since A is triangular the jth coordinate of every vector in (A) of length j is a multiple of a_{jj}. Hence $\mathbf{c} \notin (A)$. On the other hand $p\mathbf{c} \in (FA)$, and hence $\mathbf{c} \in (FA):p$. We conclude therefore that $(FA):p \neq (A)$.

Suppose now that (2) does hold, and that $\mathbf{c}$ is an arbitrary vector of length k in $(FA):p$. Then $p\mathbf{c} = s_1\mathbf{b}^1+s_2\mathbf{b}^2+\ldots+s_k\mathbf{b}^k$ for suitable integers s_i, where $s_k \neq 0$. On equating the kth coordinates of the two sides of the latter equation we have $pc_k = s_k b_{kk}$. We shall consider separately the cases (i) $k \notin \mathscr{I}(F)$, and (ii) $k \in \mathscr{I}(F)$.

Case (i). Here $b_{kk} = pa_{kk}$, and hence $c_k = s_k a_{kk}$.

Case (ii). We have $b_{kk} = a_{kk}$; hence $pc_k = s_k a_{kk}$. Now

$$s_1\mathbf{b}^1+s_2\mathbf{b}^2+\ldots+s_k\mathbf{b}^k \in pJ,$$

and $\mathbf{b}^i = p\mathbf{a}^i \in pJ$ for each i that is not in $\mathscr{I}(F)$; hence if $s_k \not\equiv 0 \pmod{p}$, then the set $[\mathbf{b}^i;\ i \in \mathscr{I}(F),\ i \leqslant k]$ is linearly dependent $(\mathrm{mod}\, p)$, contrary to the assumption that (2) holds. Therefore $s_k \equiv 0 \pmod{p}$, and hence c_k is a multiple of a_{kk}.

Thus, for each k, the kth coordinate of every vector of length k in $(FA):p$ is a multiple of a_{kk}. Now $(pA) \subseteq (FA)$, since $(pI) \subseteq (F)$, and therefore $(A) \subseteq (FA):p$; hence there is a vector in $(FA):p$, namely $\mathbf{a}^k$, whose length is k and whose kth coordinate is a_{kk}. We conclude that, with the notation of section 1, $m_k((FA):p) = |a_{kk}|$ for each k, and hence by Theorem 2.1 we have $(FA):p = (A)$.

This completes the proof of the theorem.

Now FA is triangular, and hence the vectors $\mathbf{b}^i$ $(i \leqslant k)$ generate $(FA)^{(k)}$. Also, if $i \notin \mathscr{I}(F)$, then $\mathbf{b}^i = p\mathbf{a}^i \in pJ$. Hence the vectors $\mathbf{b}^i$ $(i \in \mathscr{I}(F),\ i \leqslant k)$ generate $(FA)^{(k)}$ $(\mathrm{mod}\, p)$. But these vectors are $\rho_k(F)$ in number; hence they form a linearly independent set $(\mathrm{mod}\, p)$ if and only if

$$\dim(FA)^{(k)} = \rho_k(F).$$

It follows that the conditions that $(FA):p = (A)$ can be expressed in the following form:

$$\rho_k(F) = \dim(FA)^{(k)} \text{ for each } k. \tag{2.10.1}$$

Let E, F be p-elementary matrices of order r. If F is adherent to E, then $\rho_k(F) = \dim(FE)^{(k)}$. Also $\rho_k(E) = \dim(E)^{(k)}$ since $(EI):p = (I)$. But $(FE)^{(k)} \subseteq (E)^{(k)}$, and hence we have $\dim(FE)^{(k)} \leqslant \dim(E)^{(k)}$. Thus it follows that the following conditions are *necessary* (though not sufficient) for F to be adherent to E:

$$\rho_k(F) \leqslant \rho_k(E) \text{ for each } k. \tag{2.10.2}$$

These conditions involve only the main diagonals of the matrices. We now give a set of *sufficient* (though not necessary) conditions for adherence which also involve only diagonal elements:

(2.10.3) $F = (f_{ij})$ is adherent to $E = (e_{ij})$ if $e_{ii} = 1$ for every suffix i in

$\mathscr{I}(F)$, or equivalently if $f_{ii} = p$ for each i such that $e_{ii} = p$. (In particular, p-elementary matrices with identical main diagonals are mutually adherent.)

For if $e_{ii} = 1$ for every i in $\mathscr{I}(F)$, then for each such i, the ith coordinate of the ith row of FE is 1, and it is easy to deduce that the rows of FE that correspond to the suffixes in $\mathscr{I}(F)$ form a linearly independent set (mod p).

An interesting consequence of the necessary conditions (2.10.2) for adherence is the following:

Let $[E_n]$ be a chain. For each fixed k, the sequence $[\rho_k(E_n)]$ is a descending sequence of non-negative integers, and hence $\rho_k(E_{n+1}) = \rho_k(E_n)$ for all sufficiently large n. It follows that for each fixed i, the ith diagonal element of E_n is constant for all sufficiently large n. Hence if r is finite we can assert also that all the members of the chain from some point onwards have the same disposition of 1's and p's on their main diagonals.

We shall conclude the present section with a number of illustrative examples and a survey of the chains for the simplest cases $r = 1, r = 2$.

Examples

pI is adherent to every p-elementary matrix of order r. Every p-elementary matrix of order r is adherent to I. pI is the only matrix that is adherent to pI. I is adherent to no matrix other than I.

In the two examples that follow, the question of adherence cannot be decided merely by the comparison of main diagonals, since in these examples the conditions (2.10.2) are satisfied, but the stronger conditions (2.10.3) do not hold.

(i) $\begin{pmatrix} p & 0 \\ h & 1 \end{pmatrix}$ is adherent to $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ if and only if $h \neq 0$;

for $(h \quad p)$ is linearly independent (mod p) if and only if that condition holds.

(ii) $\begin{pmatrix} p & 0 & 0 & 0 \\ h & 1 & 0 & 0 \\ 0 & 0 & p & 0 \\ m & 0 & k & 1 \end{pmatrix}$ is adherent to $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & n & 1 & 0 \\ 0 & 0 & 0 & p \end{pmatrix}$

if and only if the set

$$\begin{matrix} (h & p & 0 & 0) \\ (m & kn & k & p) \end{matrix}$$

is linearly independent (mod p), that is if and only if $h \neq 0$, $k \neq 0$.

The following tables summarize the adherence situation for the cases $r = 1, r = 2$. In each table the figure 1 or 0 stands at the intersection of the

row marked F and the column marked E according as F is or is not adherent to E.

$r = 1$.

	1	p
1	1	0
p	1	1

$r = 2$. (The letters ϵ, η_h denote the matrices

$$\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}, \quad \begin{pmatrix}p & 0\\ h & 1\end{pmatrix} \quad (0 \leqslant h < p),$$

respectively.)

	I	ϵ	η_0	η_k	pI	
I	1	0	0	0	0	
ϵ	1	1	0	0	0	
η_0	1	0	1	1	0	$(k, m \neq 0)$.
η_m	1	1	1	1	0	
pI	1	1	1	1	1	

The chains for $r = 1$ are as follows:

$$(1, 1, \ldots, 1, 1, \ldots),$$

$$(p, p, \ldots, p, p, \ldots),$$

$$(1, 1, \ldots, 1, p, p, \ldots),$$

where the number of 1's in the last sequence is arbitrary.

For the case $r = 2$ each chain may be represented in the form

$$(S_1, S_2, S_3, S_4),$$

where S_1 is a sequence of I's, S_2 a sequence of ϵ's, S_3 a sequence of matrices of the type η_h with arbitrary values of h, and S_4 a sequence of pI's, subject to the following conditions:

(i) precisely one S_i is infinite, and the subsequent S_i are all empty;

(ii) η_0 is not the immediate successor of ϵ.

3. Quotient transformations of D_p-sequences

In the cases $r > 1$ the determination of the D-systems associated with a given D-system involves quotients by non-scalar matrices. It is therefore appropriate to discuss the nature of the calculations implicit in a quotient transformation $(\mathbf{M} \to \mathbf{M}: P)$ of a given D_p-sequence

$$\mathbf{M} = (M_0, M_1, M_2, \ldots).$$

Let $[E_n]$ be the corresponding chain, and let us write

$$A_0 = I, \qquad A_n = E_n A_{n-1},$$

so that $M_n = (A_n)$ $(n = 0, 1, 2,...)$. Let A_n^* denote the product $\bar{E}_1 \bar{E}_2 ... \bar{E}_n$. Then, by Theorem 2.4,

$$A_n A_n^* = E_n E_{n-1} ... E_1 \bar{E}_1 \bar{E}_2 ... \bar{E}_n = p^n I,$$

and hence

$$M_n : P = (A_n) : P = (A_n A_n^*) : PA_n^* = p^n J : PA_n^*.$$

$M_n : P$ is therefore the set of integral solutions $\mathbf{c}$ of the system of linear congruences

$$\mathbf{c} PA_n^* \equiv 0 \pmod{p^n}.$$

The procedure described in Theorem 2.1 for the construction of a system of generators for M can be applied to $M_n : P$ as follows:

For each k, find a solution $\mathbf{a}^k$ of the above system of congruences, such that the length of $\mathbf{a}^k$ is k and the kth coordinate of $\mathbf{a}^k$ is m_k, where m_k is positive and as small as possible. Then the set $[\mathbf{a}^i]$ generates $M_n : P$, and the triangular matrix whose rows are the $\mathbf{a}^i$ provides a representation of $M_n : P$.

Example

Let $A_n = \begin{pmatrix} p^n & 0 \\ 0 & 1 \end{pmatrix}$, i.e. $E_n = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ $(n = 1, 2,...)$,

$$M_n = (A_n), \quad \text{and } P = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Then clearly $A_n^* = \begin{pmatrix} 1 & 0 \\ 0 & p^n \end{pmatrix}$, and hence

$$\mathbf{c} PA_n^* = (c_1 \quad c_2) \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & p^n \end{pmatrix}$$

$$= (ac_1 + bc_2 \quad p^n(cc_1 + dc_2)).$$

We have therefore to determine the solution module of the congruence

$$ac_1 + bc_2 \equiv 0 \pmod{p^n}$$

for each n. This module is generated by $(m_1\ 0)$ and $(s\ m_2)$, where these are solutions of the congruence, and m_1, m_2 are positive and as small as possible.

Let $a = p^h a'$, $b = p^k b'$, where a', b' are prime to p. Then

$$p^h a' m_1 \equiv 0 \pmod{p^n},$$

and we have

$$m_1 = \begin{cases} 1 & \text{if } n \leqslant h, \\ p^{n-h} & \text{if } n > h. \end{cases}$$

In considering the solution $(s\ m_2)$ we have two cases:

(i) $h \leqslant k$.

$$p^h a' s + p^k b' m_2 \equiv 0 \pmod{p^n};$$

hence

$$p^k m_2 \equiv 0 \pmod{(p^n, p^h)}.$$

If $n \leqslant h$, then $(p^n, p^h) = p^n$, and hence $m_2 = 1$. If $n > h$, then

$$(p^n, p^h) = p^h,$$

and again $m_2 = 1$.

For s we can take any solution of the congruence

$$p^h a's + p^k b' \equiv 0 \pmod{p^n};$$

for example, $s = 0$ if $n \leqslant k$, and $s = \alpha_{n-k}$ if $n > k$, where α_n is the nth convergent of the p-adic expansion of the rational number

$$(-p^{k-h}b'/a') = (-b/a).$$

(ii) $h > k$.

Reasoning as we began in (i), we have

$$m_2 = \begin{cases} 1 & \text{if } n \leqslant k, \\ p^{n-k} & \text{if } k < n \leqslant h, \\ p^{h-k} & \text{if } n > h. \end{cases}$$

We can take s to be 0 if $n \leqslant h$. If $n > h$, then $a's + b' \equiv 0 \pmod{p^{n-h}}$, and hence a possible value for s is the $(n-h)$th convergent of the p-adic expansion of $(-b'/a')$.

So far we have assumed that $a \neq 0$, $b \neq 0$. The cases $a = 0$ and $b = 0$ are easily dealt with.

(iii) $a = 0$.

$$M_n\colon P = (B_n), \text{ where } B_n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 0 \\ 0 & p^{n-k} \end{pmatrix}$$

according as $n \leqslant k$ or $n > k$, where $b = p^k b'$, $(b', p) = 1$.

(iv) $b = 0$.

$$M_n\colon P = (C_n), \text{ where } C_n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} p^{n-h} & 0 \\ 0 & 1 \end{pmatrix}$$

according as $n \leqslant h$ or $n > h$, where $a = p^h a'$, $(a', p) = 1$.

III

Free Abelian Groups

A source of interesting problems is the following question: What are necessary and sufficient conditions that a D-system $[\mathbf{M}(p)]$ belongs to a group that possesses some specified structural property X? Examples are the cases where X is the property of being a free group, or a compietely decomposable group (that is a direct sum of groups of rank 1). In this section we shall answer the question in the former of these two cases.

It will be recalled that in the Existence Theorem (1.12) it was shown that $[\mathbf{M}(p)]$ belongs to a submodule $L = \sum_p L_p$ of R, where for each prime p,

L_p consists of all vectors of the form $p^{-n}\mathbf{c}$ ($\mathbf{c} \in M_n(p)$). Our task then is to determine conditions for L to be free.

The known result that every subgroup of a free group is free will be assumed, and the following concept will be central in the discussion: A set of vectors will be said to be *bounded* if there is a positive integer m such that the denominators of all the vectors in the set divide m.

(3.1) LEMMA. *A submodule M of R is free if and only if each segment $M^{(k)}$ is bounded.*

Proof. Consider any fixed segment $M^{(k)}$, and suppose that M is free. Then $M^{(k)}$ is free, and therefore $M^{(k)}$ has finite sets of generators, since clearly its rank is finite. Choose a definite finite set of generators, and let all the members of the set be expressed in the form $d^{-1}\mathbf{c}$ ($\mathbf{c} \in J$), where d is the least common multiple of their denominators. Then obviously every vector in $M^{(k)}$ is of this form, and hence $M^{(k)}$ is bounded.

Denote by $k_1, k_2, \ldots, k_i, \ldots$ the non-zero lengths that occur in M, in ascending order of magnitude, and suppose now that for each i the denominators of all the vectors in $M^{(k_i)}$ divide some positive integer d_i. Consider the k_ith coordinates of all the vectors in $M^{(k_i)}$. These coordinates clearly form a non-trivial subgroup of the additive group generated by the number $1/d_i$; let t_i be a generator of this subgroup, and let $\mathbf{a}^i$ be a vector in $M^{(k_i)}$ such that the k_ith coordinate of $\mathbf{a}^i$ is t_i. We shall show that the set $[\mathbf{a}^i]$ is linearly independent and generates M.

If there is a non-trivial relation

$$s_1\mathbf{a}^1 + s_2\mathbf{a}^2 + \ldots + s_j\mathbf{a}^j = 0,$$

where the s_i are integers, and we assume without loss of generality that $s_j \neq 0$, then by considering the k_jth coordinate of the left-hand side of the above equation we have $s_j = 0$. This contradiction shows that the set $[\mathbf{a}^i]$ is linearly independent.

Let $\mathbf{c}$ be a vector in M. If $\mathbf{c} \in M^{(k_1)}$, then the k_1th coordinate of $\mathbf{c}$ is mt_1 for some integer m; hence the length of $\mathbf{c} - m\mathbf{a}^1$ is less than k_1, and thus $\mathbf{c} - m\mathbf{a}^1 = 0$. Hence $\mathbf{a}^1$ generates $M^{(k_1)}$. Now suppose that $\mathbf{a}^1, \mathbf{a}^2, \ldots, \mathbf{a}^j$ generate $M^{(k_j)}$, and that $\mathbf{c} \in M^{(k_{j+1})}$. The k_{j+1}th coordinate of $\mathbf{c}$ is of the form nt_{j+1}, where n is an integer, and therefore $\mathbf{c} - n\mathbf{a}^{j+1} \in M^{(k_j)}$, since the length of that vector is less than k_{j+1}. Hence $\mathbf{c}$ belongs to the module generated by $\mathbf{a}^1, \mathbf{a}^2, \ldots, \mathbf{a}^{j+1}$, and therefore these vectors generate $M^{(k_{j+1})}$. We have thus shown by induction that M is generated by the $\mathbf{a}^i$; hence M has a linearly independent set of generators, and is therefore free.

This completes the proof of the lemma.

We now return to L. It will be shown that the boundedness of $L^{(k)}$

depends on certain simple conditions on the $L_p^{(k)}$, where p ranges over all the primes. These conditions will be derived from the next

(3.2) LEMMA. $$L^{(k)} = \sum_p L_p^{(k)}.$$

Proof. It was shown in the proof of the Existence Theorem that

$$J \cap p^n L = M_n(p).$$

Hence if $p^{-n}\mathbf{b} \in L$ ($\mathbf{b} \in J$), then $\mathbf{b} \in M_n(p)$, since $\mathbf{b} \in p^n L$. Therefore $p^{-n}\mathbf{b} \in L_p$, and hence L_p contains all those vectors in L whose denominators are powers of p.

Consider an arbitrary vector $\mathbf{c}$ in $L^{(k)}$. If $\mathbf{c}$ is not integral let its denominator d be expressed as a product $q_1 q_2 \ldots$ of powers of distinct primes, and let $(1/d)$ be expressed in the form $\sum_i (n_i/q_i)$, where the n_i are integers. Then we have $\mathbf{c} = \sum_i (n_i/q_i)d\mathbf{c}$. Each of these summands is a multiple of $\mathbf{c}$, and hence belongs to $L^{(k)}$; also each summand has a prime power denominator, and therefore belongs to one of the L_p. From these results we conclude that $L^{(k)} \subseteq \sum_p L_p^{(k)}$. On the other hand it is obvious that

$$\sum_p L_p^{(k)} \subseteq L^{(k)}.$$

This proves the lemma.

Now if a vector module M is bounded, then obviously at most a finite number of distinct prime powers occur as denominators of vectors in M. Hence necessary conditions for $L^{(k)}$ to be bounded are the following:

(i) $L_p^{(k)}$ is bounded for every prime p;

(ii) $L_p^{(k)}$ consists entirely of integral vectors for all primes p with at most a finite number of exceptions.

We assert that these conditions are also sufficient. For suppose that there is a finite set of primes $p_1, p_2, \ldots, p_h$, and non-negative integers $n_1, n_2, \ldots, n_h$, such that the denominators of all the vectors in $L_{p_i}^{(k)}$ divide $p_i^{n_i}$ ($i = 1, 2, \ldots, h$), and suppose also that $L_p^{(k)} \subseteq J$ for all the remaining primes p. Then clearly the denominator of every vector in $\sum_p L_p^{(k)}$ divides $p_1^{n_1} p_2^{n_2} \ldots p_h^{n_h}$, and hence $L^{(k)}$ is bounded.

There now remains only the problem of expressing the conditions (i) and (ii) above in terms of the modules $M_n(p)$. In the next lemma we shall consider an arbitrary but definite prime p, and we shall, for the sake of convenience, write M_n for $M_n(p)$.

(3.3) LEMMA. *Let h be an arbitrary non-negative integer. Then the following propositions are equivalent*:

(1) $M_{h+1}^{(k)} \subseteq pJ$.
(2) $M_{n+1}^{(k)} = pM_n^{(k)}$ $(n = h, h+1, h+2,\ldots)$.
(3) *The denominators of all the vectors in $L_p^{(k)}$ divide p^h.*

Proof. (2) obviously implies (1). If (1) holds, then since the sequence $[M_n]$ is descending, we have $M_{n+1}^{(k)} \subseteq pJ$ $(n = h+1, h+2,\ldots)$. But

$$M_{n+1}^{(k)} \cap pJ = pM_n^{(k)},$$

by the conditions (D_p); hence $M_{n+1}^{(k)} = pM_n^{(k)}$ $(n = h, h+1,\ldots)$. Thus (1) and (2) are equivalent.

Now let us assume (2). Then by induction we have $M_n^{(k)} = p^{n-h}M_h^{(k)}$ if $n > h$. Hence if $\mathbf{c} \in M_n^{(k)}$ $(n > h)$, then we can write $p^{-n}\mathbf{c} = p^{-h}\mathbf{b}$, where $\mathbf{b}$ is a suitable integral vector. Hence the denominator of every vector in $L_p^{(k)}$ divides p^h.

Finally, if (3) holds, then the denominator of every vector of the form $p^{-(h+1)}\mathbf{c}$ $(\mathbf{c} \in M_{h+1}^{(k)})$ divides p^h, and hence $\mathbf{c} \in pJ$. Thus $M_{h+1}^{(k)} \subseteq pJ$, and therefore (3) implies (1).

This completes the proof of the lemma.

By considering in turn an arbitrary h and $h = 0$ we have:

(i) $L_p^{(k)}$ is bounded if and only if $M_{n+1}^{(k)} = pM_n^{(k)}$ for all sufficiently large n.
(ii) $L_p^{(k)} \subseteq J$ if and only if $M_{n+1}^{(k)} = pM_n^{(k)}$ $(n = 0, 1, 2,\ldots)$.

The conditions for $[\mathbf{M}(p)]$ to belong to a free group can now be stated.

(3.4) THEOREM. $[\mathbf{M}(p)]$ *belongs to a free group if and only if the following conditions hold for each k*:

(i) *for each prime p, $M_{n+1}(p)^{(k)} = pM_n(p)^{(k)}$ for all sufficiently large n;*
(ii) *for all primes p, with at most a finite number of exceptions,*

$$M_{n+1}(p)^{(k)} = pM_n(p)^{(k)} \quad (n = 0, 1, 2,\ldots).$$

A more concise statement of the conditions above is that

$$M_{n+1}(p)^{(k)} = pM_n(p)^{(k)}$$

for all pairs (p, n) with at most a finite number of exceptions.

Denoting by $[E_n(p)]$ the chain corresponding to $\mathbf{M}(p)$, we can express the conditions in the following alternative form:

For each k, $\rho_k(E_n(p)) = 0$ for all pairs (p, n) with at most a finite number of exceptions.

We observe, finally, that if r is finite, then L coincides with one of its segments, and hence the conditions can be simplified by the omission of all references to k as follows:

$M_{n+1}(p) = pM_n(p)$ for all but at most a finite number of pairs (p, n), or equivalently,

$E_n(p) = pI$ for all but at most a finite number of pairs (p, n).

This paper is based on a thesis for the Ph.D. degree of the University of London.

I wish to thank Professor K. A. Hirsch and the referee for their encouragement and advice.

REFERENCES

1. A. KUROSH, *The theory of groups* (Vol. I; New York, 1955).
2. D. DERRY, 'Uber eine Klasse von abelschen Gruppen', *Proc. London Math. Soc.* (2) 43 (1937) 490–56.
3. A. KUROSCH, 'Primitive torsionsfreie abelsche Gruppen von endlichem Range', *Ann. Math.* (2) 38 (1937) 175–203.
4. A. MAL'CEV, 'Torsion-free abelian groups of finite rank', *Mat. Sbornik* 4 (1938) 45–68.
5. G. SZEKERES, 'Countable abelian groups without torsion', *Duke Math. J.* 15 (1948) 293–306.

Department of Mathematics
University College of Ghana