PACIFIC JOURNAL OF MATHEMATICS
Vol. 45, No. 2, 1973

THE CONSTRUCTIVE THEORY OF COUNTABLE ABELIAN P-GROUPS

FRED RICHMAN

The purpose of this paper is to develop the theory of abelian p-groups along constructive lines. To this end a constructive theory of ordinal numbers and an axiomatic treatment of the notion of height are presented. The classical theorems of Zippin and Ulm concerning existence and uniqueness of countable p-groups with prescribed invariants are proved in a finitistic setting.

1. Introduction. Throughout this paper the letter p will denote a fixed prime, and we shall use the word *group* to mean an abelian p-group. The idea of a p-group illustrates how the constructive point of view directs our attention to the manner in which a mathematical object is presented, and not merely to its absolute structure. When we say that an element x of a group has order a power of p, we mean that we *can find* an integer n such that $p^n x = 0$. The interpretation of this is that we possess an algorithm that will produce, in a finite number of steps (bounded in advance), such an integer n.

Decision problems play an important role in this approach. It is easy to come up with an algorithm that produces a sequence of 0's and 1's so that no one knows whether it will ever produce a 1. The nth output of one such algorithm is 1 if and only if 100 consecutive 7's appear in the first n digits of the decimal expansion of π. However, the idea of a decision problem does not depend upon the existence of such algorithms. It is a question of what information is at your disposal; we could just as well imagine that we were examining the output of an algorithm, possibly a completely transparent one, of whose nature we were ignorant. One such problem is deciding whether two elements of a set are equal or not. A set is called *discrete* if we can settle this question for any two of its elements. The set of sequences of 0's and 1's is not discrete, for we cannot necessarily tell whether a given sequence is equal to a sequence of all 0's.

Countability, in the constructive setting, carries a different connotation from the classical one of "not too big." Here the significance is that we can call for the elements one by one, and given an element we can compute its place in that sequence. A subset of a countable set need not be countable. The set of exponents n for which Fermat's conjecture is true is such a subset. The dif-

ficulty is that we cannot necessarily decide whether a given n is in the subset or not. Here again the reliance on a specific problem is unnecessary. The idea of not having enough information to decide whether an element is in a subset or not is clear.

A set is *subfinite* if you can list its elements $x_1, \cdots, x_n$. A *finite* set is a discrete subfinite set. A function is to be thought of as a finite algorithm, or as a black box that behaves like one.

The relevant invariants for countable p-groups are defined in terms of ordinal numbers. Section 2 is devoted to developing a constructive theory of ordinals. In § 3 the notion of a height function is developed. This function provides the information necessary to construct the Ulm invariants, and to construct the isomorphism in Ulm's theorem on the uniqueness of groups with prescribed invariants. In § 5 we provide a method for constructing groups with prescribed Ulm invariants ("Zippin's theorem," see [3; Theorem 36.1]) that differs, even in classical terms, from the usual treatments.

2. **A constructive theory of ordinal numbers.** In this section we define the notion of an ordinal number, establish a few properties, and give a few examples.

DEFINITION. An *oridinal number* is a set λ with a binary relation $<$ such that:

1. If $a < b$ and $b < c$, then $a < c$.
2. Precisely one of $a < b$, $a = b$, and $b < a$, holds for each pair a, b in λ.
3. If S is a subset of λ, with the property that $b \in S$ whenever $b \in \lambda$ and $a \in S$ for all a in λ such that $a < b$, then $S = \lambda$.

A few comments on this definition. We have defined a well ordered set rather than an ordinal number. Two well ordered sets represent the same ordinal number if there is an order preserving correspondence between them. Following Bishop [1] we identify equivalence classes with their representatives, and define equality to be equivalence. Property 2, interpreted constructively, implies that we can decide which of the three alternatives holds. In particular, an ordinal is discrete. Note that the empty set is an ordinal.

THEOREM 1. *If λ is an ordinal, and μ is a subset of λ, then μ is an ordinal (under the induced order).*

Proof. The first two properties are clearly inherited by μ. To prove the third, suppose that T is a subset of μ with the property that $b \in T$ whenever $b \in \mu$ and $a \in T$ for all a in μ such that $a < b$. Let

$S = \{x \in \lambda$: if $m \in \mu$ and $m \leqslant x$, then $m \in T\}$. It is easily seen that S satisfies the hypothesis of Property 3. Hence $S = \lambda$, and so $T = \mu$.

If $a \in \lambda$, and $a \leqslant b$ for all b in λ, we say that a is the *first element of* λ. Classically, each nonempty ordinal has a first element; constructively, we may not be able to find it. For example, let λ be either the set of positive integers or the set of nonnegative integers, but we do not know which. By Theorem 1, since the nonnegative integers constitute an ordinal, so does λ. However, we cannot exhibit the first element. Although we could strengthen the definition of ordinal number by requiring a first element, we cannot hope to find the first element of every nonempty subset of an ordinal, even for very well specified subsets. Consider the subset S of $\omega + 1$ consisting of ω together with those integers n such that 100 consecutive 7's appear in the first n places of the decimal expansion of π. Although we know an algorithm for checking whether any given element of $\omega + 1$ is in S or not, there is no known finite procedure that will produce the first element of S. In particular, if we demand that ordinals come equipped with first elements, we lose Theorem 1.

If λ is an ordinal and a is an element of λ such that $b \leqslant a$ for all b in λ, then we say that a is the *last element* of λ. If for a in λ there is a b in λ such that $a < b$, and whenever $a < c$ for c in λ, then $b \leqslant c$, then we write $b = a + 1$ and say that b is the *successor* of a. Thus, $a + 1$ is the first element of the subset $\{c \in \lambda$: $a < c\}$. As with first elements, if we wish to be able to find the successor of each element other than the last, we must strengthen the definition of ordinal. Let λ be the subset of $\omega + 1$ consisting of 0, ω, and the odd perfect numbers. We know of no algorithm that will produce the successor of 0.

Even if we know the first element, and are able to find successors (and will recognize the last element should we chance upon it), we still cannot necessarily determine whether we are dealing with a limit ordinal or not. For example, let λ be the set of positive integers n such that there are no odd perfect numbers less than n. Since we will never have all the information we might want about an ordinal, it seems best to build as little information into the definition of ordinal as possible. Properties 1, 2, and 3 will suffice for our purposes here.

Brouwer [2] defines ordinals as sets that are built up from nonempty finite sets by finite and countable addition. One disadvantage to this approach is that it admits only countable ordinals, and does

not even allow ordinals such as the example in the preceding paragraph. The definition suggested here has the virtue of being equivalent to the classical definition (classically). The difference between the approach adopted here and those of Brouwer and others is that we are developing a constructive theory of ordinals rather than a theory of constructive ordinals.

Although we cannot necessarily find the first element of a nonempty ordinal λ, it would be absurd to deny that one existed, in the sense of asserting that for any a in λ there is a b in λ such that $b < a$. This would entail the existence of an infinite descending sequence of elements of λ, which is impossible, just as in the classical setting. In fact we can prove a little more.

THEOREM 2. *Let λ be an ordinal and let $a_1 \geqq a_2 \geqq \cdots$ be a sequence of elements of λ. Then we can find a positive integer n such that $a_n = a_{n+1}$.*

Proof. Let S be the set of all elements of λ such that the conclusion is true for any such sequence with a_1 in S. Suppose $b \in \lambda$, and $a \in S$ whenever $a < b$. Then, given a sequence $a_1 \geqq a_2 \geqq \cdots$ with $a_1 = b$, either $a_1 = a_2$ and we choose $n = 1$, or $a_1 > a_2$ in which case $a_2 \in S$ and we find the required n by considering the sequence

$$a_2 \geqq a_3 \geqq \cdots .$$

So $b \in S$ and hence $S = \lambda$ and the theorem is proved.

We cannot necessarily find a positive integer n such that $a_m = a_n$ for all $m \geqq n$ although classically such an n exists. To see this, define $a_i = 0$ if 100 consecutive 7's appear in the first i places of the decimal expansion of π, and $a_i = 1$ otherwise. Using Theorem 2 we can clarify what it means to be able to find the successor of an element. If $a < b$ then, given $a + 1$, we can compare b with $a + 1$, and either find an element strictly between a and b or verify that no such element exists. This property is equivalent to having $a + 1$.

COROLLARY. *Let a be an element of an ordinal λ such that if $a < b$ we can either find an element c in λ such that $a < c < b$, or ascertain that no such element c exists. Then, given an element b_0 of λ such that $a < b_0$, we can find $a + 1$.*

Proof. Consider the sequence $b_0 \geqq b_1 \geqq \cdots$ where $a < b_{i+1} < b_i$ unless $b_i = a + 1$, in which case $b_{i+1} = b_i$ By Theorem 2 we can find an n such that $b_{n+1} = b_n$, and hence $b_n = a + 1$.

If λ is an ordinal and a and b are in λ, then we use the notations $[0, a) = \{b \in \lambda\colon b < a\}$, and $[0, a] = \{b \in \lambda\colon b \leqslant a\}$. Notice that $[0, a)$ is an ordinal, which we may identify with a. Two ordinals λ and μ are said to be *equal* if there is an invertible order preserving function ρ from λ to μ. We write $\rho\colon \lambda = \mu$. More generally, an *injection* of λ into μ is a function ρ from λ to μ such that if $a < b$ then $\rho a < \rho b$, and if $c < \rho b$, then there is an a in λ such that $\rho a = c$.

THEOREM 3. *If ρ and σ are injections of λ into μ, then $\rho a = \sigma a$ for all a in λ.*

Proof. Let $S = \{a \in \lambda\colon \rho a = \sigma a\}$. Suppose $a \in S$ for all $a < c$. If $\sigma c < \rho c$, then there is an a in λ such that $\rho a = \sigma c < \rho c$, so $a < c$, so $\rho a = \sigma a$; but $\rho a = \sigma c > \sigma a$, a contradiction. Similarly we cannot have $\rho c < \sigma c$. Hence $\rho c = \sigma c$, so $S = \lambda$.

COROLLARY. *If λ is an ordinal and a and b are in λ, then $a = b$ if and only if $[0, a) = [0, b)$ as ordinals.*

Proof. If $a \leqslant b$ and $\rho\colon [0, a) = [0, b)$, then $\rho = \sigma$, where σ is the inclusion $[0, a) \subseteqq [0, b)$. Hence $a = b$.

If λ and μ are ordinals, we write $\lambda \leqslant \mu$ if there is an injection $\rho\colon \lambda \to \mu$. Since the product of injections is an injection, the ordinals are partially ordered by $\leqslant$. However, we cannot always compare ordinals. Let $\lambda = \{n$: the first n decimal places of π contain no sequence of 100 consecutive 7's$\}$, and let $\mu = \{n$: the first n decimal places of π contain no sequence of 100 consecutive 8's$\}$. There is no way to compare ordinals like λ and μ. We could rule out λ and μ by changing the definition of ordinal to include more information, but other incomparable ordinals would arise to take their place. No one has yet succeeded in developing a theory of ordinal numbers in which any two ordinals are constructively comparable.

Obvious examples of ordinals are $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, and $\omega = \{0, 1, 2, \cdots\}$. We can construct more complicated ordinals in the usual ways.

DEFINITION. Let μ be an ordinal and let λ_a be an ordinal for each a in μ.

(1) $\sum_\mu \lambda_a$ is the disjoint union of the λ_a, where $x < y$ if $x \in \lambda_a$ and $y \in \lambda_b$ for $a < b$, or if $x < y$ in λ_a.

(2) $\prod_\mu \lambda_a$ is the set of functions f in the cartesian product of the λ_a such that $f(a)$ is the first element of λ_a for each a in μ outside of some finite subset (depending on f). The order is given by

$f < g$ if for some a in μ, we have $f(a) < g(a)$ and $f(b) = g(b)$ for all $b > a$.

If $\mu = \{0, 1\}$ we write $\sum_\mu \lambda_a$ as $\lambda_0 + \lambda_1$ and $\prod_\mu \lambda_a$ as $\lambda_0\lambda_1$. We write α^β for $\prod_\beta \alpha$. Note that $\alpha\beta = \sum_\beta \alpha$. Before verifying that these definitions give ordinals, we observe that the union of any set of comparable ordinals is an ordinal under the natural definitions of $x = y$ and $x < y$.

THEOREM 4. *If μ is an ordinal, and λ_a is an ordinal for each a in μ, then $\sum_\mu \lambda_a$ and $\prod_\mu \lambda_a$ are ordinals.*

Proof. The only problem is in verifying Property (3), the induction property. If α and β are ordinals it is clear that $\alpha + \beta$ is an ordinal. Let $S = \{b \in \mu\colon \sum_{[0,b]} \lambda_a$ is an ordinal$\}$, and suppose that $c \in S$ for all $c < b$. Then $\sum_{[0,b]} \lambda_a = \sum_{[0,b)} \lambda_a + \lambda_b$ is an ordinal because $\sum_{[0,b)} \lambda_a$ is the union of the chain of comparable ordinals $\sum_{[0,c)} \lambda_a$ for $c < b$. Hence $S = \mu$, so $\sum_\mu \lambda_a$ is an ordinal, being the union of the ordinals $\sum_{[0,b]} \lambda_a$ for $b \in \mu$. Similarly we can let $S = \{b \in \mu\colon \prod_{[0,b]} \lambda_a$ is an ordinal$\}$. The argument proceeds as above except we use the equation $\prod_{[0,b]} \lambda_a = (\prod_{[0,b)} \lambda_a)\lambda_b$ and the fact that $\alpha\beta = \sum_\beta \alpha$ is an ordinal if α and β are.

As an illustration, let us examine a representation of the ordinal ε_0. If β is an ordinal, then an element f in ω^β can be considered to be a list $(b_1, \cdots, b_n)$ of elements of β, where $f(a)$ is the number of indices j such that $a = b_j$. Thus ω^ω consists of lists of integers, ω^{ω^ω} consists of lists of lists of integers, and so on. There are natural inclusions $\omega \subseteqq \omega^\omega \subseteqq \omega^{\omega^\omega} \cdots$ and the union is ε_0. The elements of ε_0 are thus lists of lists of $\cdots$ of lists of integers. The first few elements are

$$0, 1, 2, \cdots (1), (1, 0), (1, 0, 0), \cdots (1, 1), (1, 1, 0), \cdots (2), \cdots (3), \cdots ((1)) .$$

A typical element is $(((1, 0), (1, 0), 0), (2), (2), 2, 0, 0)$.

3. **The height function.** Having said what ordinals are, and given a number of examples, we turn to the question of heights of elements in a group. The height of an element x in a group G is defined classically by defining subgroups $p^\alpha G$ of G for all ordinals α. This is done by induction, setting $p^{\alpha+1}G = p(p^\alpha G)$ and $p^\alpha G = \bigcap_{\beta<\alpha} p^\beta G$ for limit ordinals α. If $x \in p^\alpha G \backslash p^{\alpha+1}G$, then x is said to have height α; if $x \in p^\alpha G$ for all α, then x is said to have height ∞. The *length* of G is the least ordinal λ such that $p^\lambda G = p^{\lambda+1}G$.

Constructively, there are several drawbacks to this approach. To

make use of the inductive definition we have to know whether our ordinals are limit ordinals or not, and what the predecessors of their elements are, if any. Since ordinal numbers need not be comparable, we may have elements x and y whose heights are incomparable. Also we may have an element x whose height is both α and β, but we cannot show that $\alpha = \beta$. The length of a group, defined in this way, makes no sense constructively. Finally, we will certainly want to be able to decide whether an element x is in $p^\alpha G$ or not. In fact, given an x, we will want to know exactly what its height is. Such information is not included in this definition.

What we really want is a function h that assigns to each element of the group G its height. To make these heights comparable we take the range of h to be a fixed ordinal λ together with the symbol ∞. It is natural that λ be the length of G, and we achieve this by demanding that h be surjective. We denote $\lambda \cup \{\infty\}$ by λ_∞ and write $a < \infty$ for all a in λ_∞.

DEFINITION. Let G be a group and λ an ordinal. A *height function* on G with values in λ is a surjection $h\colon G \to \lambda_\infty$ such that:

1. $hpx > hx$.
2. If $hx > a$, then we can find a y such that $hy \geqq a$ and $py = x$.

We call λ the *length* of G.

Note that (1) implies that $h0 = \infty$. It is clear that the classical height function satisfies this definition in the classical sense. It is not completely clear that this definition is a classical characterization of the height function. This will be a consequence of the more incisive result that h and λ are isomorphism invariants of G, in the constructive sense. We first show that h is a valuation.

THEOREM 5. *If $h\colon G \to \lambda_\infty$ is a height function, then*

$$h(x - y) \geqq \min(hx, hy)$$

for any pair x, y in G, with equality holding if $hx \neq hy$.

Proof. It suffices to prove the theorem when $hy \leqslant hx$, for then $h(-y) = hy$ upon setting $x = 0$. Let S be the set of b in λ for which $h(x - y) \geqq hy$ whenever $b = hy \leqslant hx$. We shall show that if $a \in S$ for all $a < b$, then $b \in S$. Suppose, on the contrary, that

$$h(x - y) < hy = b \leqslant hx\,.$$

Then $y = pz$ and $x = pw$, where $hz \geqq h(x - y)$ and $hw \geqq h(x - y)$, so $h(x - y) = h(pz - pw) > h(z - w) \geqq \min(hz, hw) \geqq h(x - y)$, a con-

tradiction. Thus $S = \lambda$, so the claim is true if $hy \neq \infty$. If $hy = \infty$, then $h(x - y) = \infty$, lest $hx = h(y + (x - y)) \neq \infty$. Finally, if $hx \neq hy$, then $hy = h(x - (x - y)) \geqq \min(hx, h(x - y))$, so $hy \geqq h(x - y)$.

THEOREM 6. *If f is an isomorphism of G onto H, and h and h_0 are height functions on G and H with values in λ and μ respectively, then we can find a ρ: $\lambda = \mu$ such that $h_0 f = \rho h$, where we set $\rho\infty = \infty$.*

Proof. Let h^{-1} be any right inverse of h, set $\rho = h_0 f h^{-1}$, and let $S = \{a \in \lambda$: $hx = a$ implies $h_0 fx = \rho a$, and ρ is an injection on $[0, a]\}$. We wish to show that $S = \lambda$. Suppose $a \in S$ for all $a < b$. If $hx = b$ we shall show: (i) if $a < b$, then $h_0 fx > \rho a$, and (ii) if $c < h_0 fx$ then we can find an $a < b$ such that $\rho a = c$. In particular, if $x = h^{-1}b$, then $h_0 fx = \rho b$, and (i) and (ii) show that ρ is an injection on $[0, b]$.

If $a < b$, then there is a z such that $a \leqslant hz < b$ and $pz = x$. So $pfz = fx$ and $h_0 fz = \rho hz \geqq \rho a$. Thus $h_0 fx > \rho a$. If $c < h_0 fx$, then we can find a z such that $h_0 z \geqq c$ and $pz = fx$. Then $pf^{-1}z = x$, so $hf^{-1}z = d < b = hx$. So $h_0 z = h_0 f f^{-1} z = \rho d$, and ρ is an injection on $[0, d]$. Hence there is an $a \leqslant d < b$ such that $\rho a = c$.

Since $S = \lambda$, the function ρ is an injection of λ into μ. Similarly we get an injection from μ into λ. Their composition is an injection of λ (or μ) into itself, and hence is the identity by Theorem 3. Finally, if $hx = \infty$ then $h_0 fx = \infty$ lest $hx = hf^{-1}fx \neq \infty$.

Since the height function is unique, it should behave like the classical height function. For example, homomorphisms increase heights, provided that you can make sense of this statement. If two ordinals are comparable, then we can compare their elements in a well-defined manner.

THEOREM 7. *Let G and H be groups, h and h_0 height functions on G and H with values in λ and μ respectively. If λ and μ are comparable, and if f is a homomorphism from G to H, then*

$$h_0 fx \geqq hx \qquad \text{for all } x \text{ in } G .$$

Proof. Let $S = \{a \in \lambda$: $hx = a$ implies $h_0 fx \geqq a\}$. Suppose that $a \in S$ for all $a < b$. If $hx = b$ and $h_0 fx < b$, then $x = py$, where $hy \geqq h_0 fx$. Since $b = hx = hpy > hy$, we have $h_0 fy \geqq hy$. But

$$h_0 fx = h_0 pfy > h_0 fy ,$$

so $h_0 fx > hy$, a contradiction. Thus $S = \lambda$. If $hx = \infty$, then $x = px_1$

and $hx_1 = \infty$, so $x_1 = px_2$ and $hx_2 = \infty$, etc., and we get a descending chain $h_0fx > h_0fx_1 > h_0fx_2 > \cdots$. Hence $h_0fx = \infty$ by Theorem 2.

Heights computed in summands are the same as heights computed in the original group.

THEOREM 8. *Let G be a group, h: $G \to \lambda_\infty$ a height function, e an idempotent endomorphism of G, and $H = \{x \in G: ex = x\}$. Let $\mu = \{a \in \lambda$: there is an x in H such that $hx = a\}$. Then $\mu \subseteqq \lambda$ is an injection, and h: $H \to \mu_\infty$ is a height function on H.*

Proof. To show that $\mu \subseteqq \lambda$ is an injection, let $S = \{b \in \mu$: if $a \in \lambda$ and $a < b$ then $a \in \mu\}$. We show that $S = \lambda$. Suppose that $c \in S$ for all $c < b$ in λ. If $a < b$, then there is an x in H and a y in G such that $hx = b$ and $x = py$, and $hy \geqq a$. Now $ey \in H$ and $hey \geqq hy \geqq a$. So $hx = hex = hpey > hey \geqq a$. If $hey = a$ we are done. If $hey > a$, then, letting $c = hey$ we are done. In any case, the element ey demonstrates that h is a height function.

Recall that a group G is *divisible* if $pG = G$ and *reduced* if $\{0\}$ is its only divisible subgroup. If G has a height function h, it is evident that G is divisible if and only if $h(G) = \{\infty\}$, and G is reduced if and only if $h^{-1}(\infty) = \{0\}$. In any case, the set $h^{-1}(\infty)$ is a divisible subgroup that contains every divisible subgroup. If G is countable, we can find a complementary summand to this maximum divisible subgroup; in fact we can find a complementary summand to any divisible subgroup D for which the question "is x in D?" is decidable for each x in G.

THEOREM 9. *Let G be a countable group and let D be divisible subgroup of G such that it is decidable whether $x \in D$ for each x in G. Then we can construct a countable subgroup K of G such that $G = K \oplus D$.*

Proof. Let $x_1, x_2, \cdots$ be an enumeration of the elements of G such that px_{i+1} is in the subgroup generated by $x_1, \cdots, x_i$ for each i. We shall construct subfinite subgroups $K_1 \subseteqq K_2 \subseteqq \cdots$ of G such that $x_i \in K_i + D$ and $K_i \cap D = \{0\}$. Then $K = \bigcup K_i$ is as desired. Given K_i we construct K_{i+1} as follows. If $x_{i+1} \in K_i + D$ (a decidable question) we set $K_{i+1} = K_i$. If $x_{i+1} \notin K_i + D$ we write $px_{i+1} = k_i + d$, where $k_i \in K_i$ and $d \in D$. Since D is divisible, we can find d' in D such that $d = pd'$. Let $y = x_{i+1} - d'$. Then $py = k_i$, and we let K_{i+1} be the subgroup generated by K_i and y. Certainly $x_{i+1} \in K_i + D$; we must show that $K_{i+1} \cap D = \{0\}$. If w is an element of $K_{i+1} \cap D$,

then we way write $w = ny + z$, where $z \in K_i$. So $ny = w - z$, where $w \in D$ and $z \in K_i$. If p does not divide n, then $y \in K_i + D$, so

$$x_{i+1} \in K_i + D ,$$

a contradiction. Thus p divides n, so $ny \in K_i$ and $w = 0$.

COROLLARY. *If G is a countable group with height function, then we can construct countable subgroups R and D of G such that R is reduced, D is divisible, and $G = R \oplus D$.*

Either directly or by using Theorem 9 we can prove the classical result that a countable discrete divisible group is a countable direct sum of copies of $Z(p^\infty)$ and the trivial group. For example we can follow the proof of [4; Theorem 4], using countability instead of Zorn's lemma. In the nondiscrete case, the best you can get is a homomorphic image of such a direct sum. However, there seems to be no good reason to deny discreteness to these groups.

Thus our attention is drawn to countable groups with height functions that are reduced. We call such groups *Ulm groups*. Note that any Ulm group is discrete. An elegant idea of E. A. Walker allows us to construct reduced groups of any length.

THEOREM 10. *If λ is an ordinal, then there is a reduced group G with height function h and length λ.*

Proof. Let F be the free abelian group on strings $\langle a_1, \cdots, a_n \rangle$ where $a_i \in \lambda$ for $1 \leqslant i \leqslant n$, and $a_1 < a_2 < \cdots < a_n$. We identify the empty string with the zero element of F. Let M be the subgroup of F generated by elements of the form

$$p \langle a_1, a_2, \cdots, a_n \rangle - \langle a_2, \cdots, a_n \rangle ,$$

and let G be the quotient group F/M, that is, G is F with equality defined by $g_1 = g_2$ if $g_1 - g_2 \in M$. Then any element of G is equal to a unique element of the form $\sum n_i\theta_i$, where the θ_i are distinct free generators of F, and $0 \leqslant n_i < p$. That such an element can be found is clear from the nature of the generators of M. That such an element is unique follows from the fact that every nonzero element $\sum m_i\theta_i$ of M has nonzero coordinate m_i that is divisible by p. This unique element is said to be in *standard form*. Define h: $G \to \lambda_\infty$ by $hg = a$, where a is the least element of λ occuring in a string that has a nonzero coefficient in the standard form of g, and $hg = \infty$ if all the coefficients are zero (and so $g = 0$). It is readily seen that h is a reduced height function on G under which G has length λ.

COROLLARY. *If λ is a countable ordinal, then there is an Ulm group of length λ.*

By a countable ordinal λ we mean one for which λ_∞ is countable. This allows the empty set to be countable, and gives every Ulm group a countable length.

4. **Ulm invariants.** A complete set of invariants for Ulm groups is provided by certain countable discrete vector spaces over the p-element field, called Ulm invariants. It will be convenient to define these invariants in a more general setting, suggested by subgroups of Ulm groups.

DEFINITION. Let S a group, λ an ordinal, and h a function from S to λ_∞. We say that h is a *subheight function* on S with values in λ if

1. $hpx > hx$.
2. $h(x - y) \geqq \min(hx, hy)$.

We say that h (or S) is *reduced* if $h^{-1}(\infty) = \{0\}$

We write $a \ll b$ if we can find c such that $a < c < b$.

DEFINITION. Let S be a group and h a subheight function on S with values in λ. For each a in λ define $F_S(a) = \{x \in S: hx \geqq a\}$, where equality in $F_S(a)$ is defined by $x = y$ if $h(x - y) > a$. The ath *Ulm invariant* of S is the subspace of $F_S(a)$ defined by

$$f_S(a) = \{x \in F_S(a): hpx \gg a\} .$$

The function f_S is called the *Ulm function* of S.

Both $F_S(a)$ and $f_S(a)$ are discrete vector spaces over the p-element field. The classical definition of Ulm invariant is the dimension of the subspace of $f_S(a)$ defined by $V = \{x \in S: hx \geqq a$ and $px = 0\}$. If h is a height function then $V = f_S(a)$, for if $x \in f_S(a)$ then $hpx > b > a$, so $px = pz$ where $hz \geqq b$. Hence $x - z \in V$, but $x - z = x$ in $f_S(a)$. Since V is countable if S is, this makes $f_S(a)$ countable when S is an Ulm group. The equality of V and $f_S(a)$ is well known and lies at the heart of the proof of Ulm's theorem. The advantage of our definition is that $f_S(a)$ is the relevant space when S is a subgroup of an Ulm group. We let the space itself be the invariant because, constructively, the dimension of $f_S(a)$ need not be an integer or ∞ since we may never be able to decide exactly what the dimension is.

There is one thing to watch out for concerning the space $f_S(a)$. Given an element x in S, we cannot necessarily decide whether

$hpx \gg hx$. Hence we cannot in general decide whether a given element of $F_S(a)$ is in $f_S(a)$. In particular, if S is finite, then $f_S(a)$ need not be finite or even subfinite.

Let f be a function that assigns to each element a in a countable ordinal λ a countable discrete vector space $f(a)$ over the p-element field. When is $f = f_G$ for some Ulm group G? Classically, necessary and sufficient condition on f may be stated: if $a \in \lambda$ then $f(a + n)$ is nonzero for some nonnegative integer n. This is too strong a condition from the constructive point of view, for by Theorem 10 we can construct an Ulm group of length λ for any countable ordinal λ, but given an element a in λ we cannot in general even find $a + n$. We want to determine the precise conditions that f must satisfy for f to be isomorphic to the Ulm function of some Ulm group. The fact that given two elements $a < b$ in λ, we cannot necessarily decide whether $a \ll b$, introduces complications.

THEOREM 11. *Let G be an Ulm group of length λ. Then*

1. *If $a < b$ for $a \in \lambda$ and $b \in \lambda_\infty$, then we can find an element c in λ such that $a \leqslant c < b$, and such that if $c \ll b$ then we can find a nonzero element of $f_G(c)$.*

2. *If $x \in F_G(a)$, then we can find an element $b > a$ in λ_∞ such that $a \ll b$ if and only if $x \in f_G(a)$.*

3. *If U is a finite subspace of $f_G(a)$ and V is a finite subspace of $F_G(b)$, where $a < b$, then either $a \ll b$ or we can find a subspace W of $F_G(a)$, disjoint from U and isomorphic to V, such that $a \ll b$ if and only if $W \subseteqq f_G(a)$.*

Proof. To prove statement (1) when $b = \infty$, find x in G such that $hx = a$ and set $c = hp^{n-1}x$, where p^n is the order of x. Then $p^{n-1}x$ is a nonzero element of $f_G(c)$. If $b \in \lambda$, find x in G such that $hx = b$, and find y in G such that $py = x$ and $hy \geqq a$. Set $c = hy$. If $c \ll b$ then y is a nonzero element of $f_G(c)$. To prove statement (2) set $b = hpx$. Then $a \ll b$ if and only if $x \in f_G(a)$ by definition. To prove statement (3) let $v_1, \cdots, v_n$ be a basis for V, and find $w_1, \cdots, w_n$ such that $pw_i = v_i$ and $hw_i \geqq a$. Let W be the finite subspace of $F_G(a)$ generated by the w_i. Map W into V by taking $\sum m_i w_i$ to $\sum m_i v_i$. Either $a \ll b$ or this map is well defined (and therefore is an isomorphism), for if $h(\sum m_i w_i) > a$, then $h(\sum m_i v_i) \gg a$, so either $a \ll b$ or $h(\sum m_i v_i) > b$. (Note that we need consider only a finite number of values of m_i in this argument.) Moreover, if $u \in U$, then $hpu \gg a$, while if w is a nonzero element of W, then $hpw = b$. So if $u = w$ in $F_G(a)$, then $h(w - u) > a$, and hence $h(pw - pu) \gg a$, so $b \gg a$. Finally, $a \ll b$ if and only if $W \subseteqq f_G(a)$ by definition.

DEFINITION. Let λ be a countable ordinal and f a function assigning to each element a in λ a countable discrete vector space over the p-element field. We say that f is a *U-function* if, for each a in λ, we can imbed $f(a)$ in a countable discrete vector space $F(a)$ over the p-element field so that

1. If $a<b$ for $a\in\lambda$ and $b\in\lambda_\infty$, then we can find an element c in λ such that $a\leqslant c<b$, and such that if $c\ll b$ then we can find a nonzero element of $f(c)$.

2. If $x\in F(a)$, then we can find an element $b>a$ in λ_∞ such that $a\ll b$ if and only if $x\in f(a)$.

3. If U is a finite subspace of $f(a)$ and V is a finite subspace of $F(b)$, where $a<b$, then either $a\ll b$ or we can find a subspace W of $F(a)$, disjoint from U and isomorphic to V, such that $a\ll b$ if and only if $W\subseteqq f(a)$.

Theorem 11 then says that every Ulm function is a U-function. As a constructive Zippin's theorem we shall show that, conversely, if f is a U-function, then we can construct an Ulm group whose Ulm function is isomorphic to f. The space $F(a)$ plays no overt role in the classical treatment, and we could dispense with it here if we had successors. If, given $a<b$ in λ, we can find $a+1$, then we can satisfy properties (2) and (3) in the definition of a U-function by simply taking $F(a)=f(a)\oplus K$, where K is any infinite dimensional countable discrete vector space over the p-element field. The space $F(a)$ only plays a role as a buffer against the appearance of embarrassing elements of λ. An example of a reasonable looking function f that is not a U-function is provided by letting λ be a countable ordinal such that $\{0,2\}\subseteqq\lambda\subseteqq\{0,1,2\}$, and letting $f(a)$ be one-dimensional for every a in λ. If f were a U-function, then we could decide whether 1 was in λ or not. In fact we let $U=f(0)$ and $V=f(2)$ and appeal to Property (3) in the definition of U-function. Either $1\in\lambda$, or we get a one-dimensional space W, disjoint from U, such that if $1\in\lambda$, then $W\subseteqq f(0)$, a contradiction.

5. Existence of Ulm groups. Our plan is to construct an Ulm group whose Ulm function is isomorphic to a given U-function f. We will construct this group element by element, giving us at each stage a finite group S with a subheight function defined on it. If S is to end up as a subgroup of an Ulm group with Ulm function f, we will have to put restrictions on the Ulm invariants of S.

DEFINITION. Let S be a group and h a reduced subheight function on S with values in λ. Let f be a U-function on λ. Then S is *f-admissible* if, for each a in λ, we have an imbedding φ of $F_S(a)$

in $F(a)$ such that $x \in f_S(a)$ if and only if $\varphi(x) \in f(a)$.

If S is a subgroup of an Ulm group with Ulm function f, then S is clearly f-admissible. The existence theorem for Ulm groups is proved by verifying the converse of this statement for finite groups S. The key construction involves enlarging an f-admissible finite group to an f-admissible finite group in which a given instance of Property (2) of a height function is satisfied.

LEMMA. *Let S be a finite group and h a reduced subheight function on S with values in λ. Let f be a U-function on λ. If S is f-admissible, $x \in S$, and $a < hx = b$, then we can construct a finite group T containing S, and we can extend h to T so that T is f-admissible and $py = x$ for some y in T such that $hy \geqq a$.*

Proof. Let $U = \{s \in S: hs \geqq a \text{ and } hps > b\}$ and let $V = F_S(b)$. By increasing a, if necessary, we can assume that there is no element s in S such that $a < hs < b$. By Property (3) of a U-function, either $a \ll b$, in which case by increasing a we can assume that $a \notin h(S)$, or we can find a subspace W of $F(a)$ disjoint from (the image of) U, and isomorphic to V, such that $a \ll b$ if and only if $W \subseteqq f(a)$.

Adjoin y to S subject only to the relation $py = x$, and set

$$h(s + ky) = \min(hs, a)$$

for $s \in S$ and $0 < k < p$. We shall show that this defines an f-admissible group T. It is immediate that h is a subheight function on T. To show that T is f-admissible we must, for each e in λ, imbed $F_T(e)$ in $F(e)$ in the appropriate way. If $e \neq a$, or if $e = a \notin h(S)$, then $F_T(e)$ is naturally isomorphic to $F_S(e)$ which is already properly imbedded in $F(e)$. So we need only consider the case where $e = a$ and we have the subspace W of $F(a)$ described above. Since upon discovering that $a \ll b$ we can start again and assume that $a \notin h(S)$, which is the easy case, we may proceed on the assumption that we will not run across anything strictly between a and b while we imbed $F_T(a)$ in $F(a)$.

It is clear that $F_T(a) = F_S(a) \oplus \langle y \rangle$ so all we need is to find an element y_0 in $F(a)$ that is not in the image of $F_S(a)$, and that is in $f(a)$ if and only if $a \ll b$. We can assume that x has maximal height among elements of the form $x + ps$ where $s \in S$ and $hs \geqq a$, since if $py = x$ then $p(y + s) = x + ps$. Then $f_T(a)$ is equal to $f_S(a) \oplus \langle y \rangle$ or $f_S(a)$ depending on whether $a \ll b$ or not. Multiplication by p gives a map from $F_S(a)$ to $F_S(b)$ whose kernel is U. Now x is not in the image of this map by our assumption on x. Hence

$$\dim U + \dim F_S(b) > \dim F_S(a) ,$$

so the finite space W must contain an element y_0 not in $F_S(a)$.

THEOREM 12. *Let λ be a countable ordinal and f a U-function defined on λ. Let S be a finite group and h a subheight function on S with values in λ. If S is f-admissible, then S can be imbedded in an Ulm group G such that $f_G(a) \cong f(a)$ for each a in λ, and so that the height function on G agrees with h.*

Proof. If μ is a finite subset of λ, then by repeated applications of the lemma, we can imbed S in a finite group $E(S, \mu)$, and extend h so that $E(S, \mu)$ is f-admissible, and so that if $a \in \mu$ and $x \in S$ with $a < hx$, then there is a y in $E(S, \mu)$ satisfying $py = x$ and $hy \geqq a$. We shall construct a chain of finite f-admissible groups $S = S_0 \subseteq S_1 \subseteq \cdots$ with a common height function h. Let $x_1, x_2, \cdots$ be an enumeration of $\bigcup_i f(a)$, and let $a_1, a_2, \cdots$ be an enumeration of λ. Let

$$\mu_n = \{a_1, \cdots, a_n\}$$

and set $S_{2n} = E(S_{2n-1}, \mu_n)$. For $x_n \in f(a)$, set $S_{2n-1} = S_{2n-2}$ if x_n is in the image of $F_{S_{2n-2}}(a)$; otherwise set $S_{2n-1} = S_{2n-2} \oplus \langle y \rangle$ where y is a new element defined by $py = 0$ and $hy = a$. Then $G = \bigcup S_j$ is clearly a countable group with subheight function h taking values in λ. That h is in fact a height function follows easily from the construction $S_{2n} = E(S_{2n-1}, \mu_n)$, provided that we can show that $h(G) = \lambda_\infty$. This follows from property (1) of a U-function. For suppose $a \in \lambda$. Then there is a c in λ such that $a \leqslant c$ and $f(c) \neq \{0\}$. By the construction of S_{2n-1} we can find an element x_1 in G such that $hx_1 = c$. If $a = c$ we are through. Otherwise, by the construction of S_{2n}, we can find an element x_2 of G such that $a \leqslant hx_2 < hx_1$. Continuing in this way we find an element x_n in G such that $a = hx_n$ by Theorem 2. The isomorphism between $f_G(a)$ an $f(a)$ is provided by the construction of S_{2n-1}.

6. **Ulm's theorem.** We now know how to construct a group with prescribed Ulm invariants. That this group is unique up to isomorphism is the content of Ulm's theorem. The construction of the required isomorphism follows Kaplansky [4], with a few modifications to overcome the undecidability of $a \ll b$. If S is a subgroup of an Ulm group G, and $x \in G$, we say that x is *S-proper* if x is of maximum height among the elements of $x + S$.

THEOREM 13. *Let G and K be Ulm groups with isomorphic Ulm invariants. Then we can construct an isomorphism between G and K.*

Proof. Let h denote the height function of either G or K, and let λ denote their common length. We may assume an enumeration $x_1, x_2, \cdots$ of the elements of G such that px_i is in the subgroup generated by $x_1, \cdots, x_{i-1}$, and a similar enumeration $y_1, y_2, \cdots$ of the elements of K. We shall construct sequences of finite subgroups $S_1 \subseteqq S_2 \subseteqq \cdots \subseteqq G$, and $T_1 \subseteqq T_2 \subseteqq \cdots \subseteqq K$, and height preserving isomorphisms $\varphi_n: S_n \to T_n$, so that $x_n \in S_{2n-1}$ and $y_n \in T_{2n}$, and so that φ_{n+1} extends φ_n. It will suffice to show that if φ is a height preserving isomorphism between a finite subgroup $S \subseteqq G$ and a finite subgroup $T \subseteqq K$, and if $x \in G$ and $px \in S$, then φ can be extended to a height preserving isomorphism of the subgroup generated by S and x.

If $x \in S$ we are done. Otherwise, by choosing an element of maximum height in the finite set $x + S$, we may assume that x is S-proper. Among such x we may pick one which maximizes hpx. Note that $h(x + s) = \min(hx, hs)$ for all s in S because x is S-proper. Let $hx = a$. We must define φx.

Since $h\varphi px = hpx > a$, we can find y in K such that $hy \geqq a$ and $py = \varphi px$. If $hy = a$ and y is T-proper (note that these questions are decidable), then we can extend φ by setting $\varphi x = y$. If $hy = a$ and y is not T-proper, then there is an s in S such that

$$h(y + \varphi s) > a ,$$

so $h(py + \varphi ps) \gg a$, and so $h(px + ps) \gg a$. But $h(x + s) \geqq a$, since $hs = h\varphi s = a$, so $x + s$ is S-proper. Hence, by our choice of x, we have $hpx \geqq h(px + ps)$, so $hpx \gg a$. Again, if $hy > a$, then $hpx \gg a$.

So we turn our attention to the case when $hpx \gg a$ and hence $x \in f_G(a)$ but, since x is S-proper, $x \notin f_S(a)$. We need to find an element y_0 in $f_K(a)$ that is not in $f_T(a)$. Let σ be the given isomorphism of $f_G(a)$ with $f_K(a)$. Note that it is decidable whether an element of $f_K(a)$ is in $f_T(a)$ or not. If $\sigma x \notin f_T(a)$ we are done. If not, then by repeated application of φ^{-1} and σ we can find a finite subgroup V of $f_S(a)$ such that $\sigma x \in \varphi V = \sigma V$, or find a y_0 along the way. But if $\sigma x \in \sigma V$, then $x \in V$ which contradicts the fact that $x \notin f_S(a)$. Thus we get our y_0.

We can choose y_0 so that $py_0 = 0$. Moreover y_0 is T-proper, for if $h(y_0 + t) > a$, and hence $ht = a$, then $hpt = hp(y_0 + t) \gg a$, so $t \in f_T(a)$, and $y_0 = -t \in f_T(a)$, a contradiction. Set $\varphi x = y_0 + y$, where $py = \varphi px$ and $hy \geqq a$, noting that $y_0 + y$ is T-proper since y_0 is.

A theorem of Prüfer characterizes the Ulm groups that are direct sums of cyclic groups as those Ulm groups that have no nonzero elements of infinite height [3; Theorem 11.3]. This theorem can be

proven directly, or flogged to death with Ulm's theorem. We shall do the latter. The interest here is in the constructive interpretation of an Ulm group without elements of infinite height, and in the distinction between possessing a sequence of independent generators of a group, and knowing that the group could not fail to be a direct sum of cyclic groups.

An example will illustrate the problem. Let λ be a countable ordinal such that $\{1\} \subseteqq \lambda \subseteqq \{0, 1\}$. Let G be the Ulm group specified by the U-function f, where $f(1)$ is one-dimensional and $f(a) = \{0\}$ if $a \neq 1$. Then G cannot be other than cyclic of order p or cyclic of order p^2. But possession of a generator of G would decide the question of whether $0 \in \lambda$ or not. Certainly in no sense does G have elements of infinite height. Note that G is even bounded, yet we cannot necessarily write it as a direct sum of cyclic groups.

The trouble is with λ. An *initial segment* of ω is a subset λ of ω such that it $n \in \lambda$, then $m \in \lambda$ for all $m \leqq n$. This amounts to saying that $\lambda \leqq \omega$.

THEOREM 14. *Let G be an Ulm group of length λ. Then G is a direct sum of cyclic groups if and only if $\lambda \leqslant \omega$.*

Proof. If G is a direct sum of cyclic groups, then it is easy to define a height function on G that makes the length of G equal to an initial segment of ω. Since length is an isomorphism invariant, we have $\lambda \leqslant \omega$. On the other hand, if $\lambda \leqslant \omega$ then we can construct a group H of length λ, that is a direct sum of cyclic groups, such that $f_G = f_H$. By Ulm's theorem G is isomorphic to H, so G is a direct sum of cyclic groups.

REFERENCES

1. E. Bishop, *Foundations of Constructive Analysis*, McGraw-Hill, 1967.
2. L. E. J. Brouwer, *Zur Begründen der intuitionistischen Mathematik. III*, Math. Annalen, **96** (1927), 451--488.
3. L. Fuchs, *Abelian Groups*, Pergamon, 1960.
4. I. Kaplansky, *Infinite Abelian Groups*, Univ. of Mich. Press, 1969.

Received December 2, 1971 and in revised form January 18, 1973. This research was supported by NSF Grant GP-28379.

NEW MEXICO STATE UNIVERSITY