ORDERING BY DIVISIBILITY IN ABSTRACT ALGEBRAS

By GRAHAM HIGMAN

[Received 24 December 1951.—Read 17 January 1952]

1. Introduction

We shall be concerned in this note with abstract algebras which carry a relation of quasi-order.

We recall first that a relation $a \leqslant b$ on a set A is a *quasi-order* if (i) $a \leqslant a$ for all $a \in A$, and (ii) $a \leqslant b$ and $b \leqslant c$ imply $a \leqslant c$. If also $a \leqslant b$ and $b \leqslant a$ imply $a = b$, the relation is an *order*; and if in addition for all a, b either $a \leqslant b$ or $b \leqslant a$, it is a *linear order*. We shall use the same notation $a \leqslant b$ for all quasi-orders that occur; in the rare cases where we consider two different quasi-orders on the same set, we shall give different names, say P, Q, to the set in its two quasi-orders, and distinguish '$a \leqslant b$ in P' from '$a \leqslant b$ in Q'.

If B is a subset of the quasi-ordered set A, the *closure* of B, written $\mathrm{cl}(B)$, is the set of all elements a in A such that for some b in B, $b \leqslant a$; and a *closed* subset is one that is its own closure. An *open* subset of A is one whose complement is closed. The quasi-ordered set A will be said to have the *finite basis property* (often abbreviated to f.b.p.) if every closed subset of A is the closure of a finite set. We give below (Theorem 2.1) a number of alternative definitions of this property; in particular it is equivalent to the defining condition of the *partial well-orders* considered by P. Erdős and R. Rado (3).†

By an *abstract algebra* (A, M) we mean a set A of elements and a set M of operations; each operation μ in M is an r-ary operator for some non-negative integer r, and maps each sequence $a_1, a_2, \ldots, a_r$ of r elements of A on a unique element $\mu a_1 a_2 \ldots a_r$ of A. We shall denote by M_r the subset of M containing all r-ary operations; and we shall suppose that there is an integer n such that M_r is empty for $r > n$. As a convention of notation we shall use the early letters of the alphabet, a, b,... to denote elements of A, and the late letters, x, y,... to denote finite (possibly empty) sequences of elements of A. Moreover, we shall suppose that the lengths of these sequences are such that our formulae make sense; e.g. if μ is an r-ary operation, the occurrence of the expression μxay will imply that the lengths

† I have to thank Dr. Erdős and Dr. Rado for their courtesy in letting me see this manuscript. The use of their methods has noticeably simplified my proofs in one or two places.

s and t of x and y satisfy $s+t+1 = r$. Elements of M will be denoted by Greek letters.

As usual, by an *M-subalgebra* of (A, M) we mean an algebra (B, M), where B is a subset of A such that $\mu x \in B$ for $\mu \in M$ and x a sequence of elements of B, and where the operations in M are not distinguished from those obtained from them by restricting them to sequences of elements of B. (A, M) will be called *minimal* if it has no subalgebra distinct from itself. Notice that since we admit the possibility that M contains 0-ary operations, a minimal algebra is not necessarily empty. In fact, if $\mu \in M_0$, μx is defined only if x is the empty sequence, and is then a certain element a of A. Plainly a belongs to every subalgebra of (A, M), and if A_0 is the set of all such elements a, (A, M) is minimal if and only if A_0 is a generating set of the algebra (A, M'), where $M' = M - M_0$. Thus the fact that below we consider only minimal algebras is no real restriction. It would, of course, have been possible to work with sets of generators and avoid the use of 0-ary operations; but the present set-up has the advantages first of increasing the uniformity of the treatment, and secondly of being more flexible, since the correspondence of 0-ary operations to elements of A is not necessarily one to one.

A quasi-order on the element set A of the algebra (A, M) makes it into an *ordered algebra* provided that, for all μ in M,

(i) $a \leqslant b$ implies $\mu x a y \leqslant \mu x b y$.

We shall call the quasi-order a *divisibility order* if also for all μ in M, and all relevant a, x, y, we have

(ii) $a \leqslant \mu x a y$.

Suppose next that we are given quasi-orders on M_r, $r = 0, 1, \ldots, n$. Then we shall say that a quasi-order on A is *compatible* with these quasi-orders if for λ, μ in M_r

(iii) $\lambda \leqslant \mu$ implies $\lambda x \leqslant \mu x$.

The main object of this note is to prove the following theorem:

THEOREM 1.1. *Suppose that (A, M) is a minimal algebra, and that M_r, the set of r-ary operations in M, is a quasi-ordered set with finite basis property for $r = 0, 1, \ldots, n$, and is empty for $r > n$. Then A has the finite basis property in any divisibility order of (A, M) compatible with the quasi-orders of M_r.*

An important special case of the theorem occurs when the sets M_r are finite for $r > 0$. In this case we can assume that the order on M_r is trivial ($a \leqslant b$ only if $a = b$); and the compatibility condition then amounts to saying that $(A, M - M_0)$ has a set of generators with f.b.p. If we observe that the conditions that make a quasi-order of A a divisibility order of

(A, M) are unaffected by the removal of 0-ary operations from M, we can rewrite this case of the theorem as follows:

THEOREM 1.2. *An abstract algebra with a finite set of operations has the finite basis property in a divisibility order if any generating set has.*

Particular cases of this theorem have been proved by P. Erdős and R. Rado (**3**); and the theorem was obtained independently by B. H. Neumann in the case when all the orders are linear. We give below applications of these theorems to combinatorial problems, to a known theorem on power-series rings over an ordered quasi-group, and to the study of fully invariant subgroups of a free group. It is the variety of these applications, rather than any depth in the results obtained, that suggests that the theorems may be interesting.

2. Finite basis property

We begin by listing some properties equivalent to the f.b.p.

THEOREM 2.1. *The following conditions on a quasi-ordered set A are equivalent*:

(i) *every closed subset of A is the closure of a finite subset*;
(ii) *the ascending chain condition holds for the closed subsets of A*;
(iii) *if B is any subset of A, there is a finite set B_0 such that $B_0 \subset B \subset \mathrm{cl}(B_0)$*;
(iv) *every infinite sequence of elements of A has an infinite ascending subsequence*;
(v) *if $a_1, a_2, \ldots$ is an infinite sequence of elements of A, there exist integers i, j, such that $i < j$ and $a_i \leqslant a_j$*;
(vi) *there exists neither an infinite strictly descending sequence in A, nor an infinity of mutually incomparable elements of A.*

(i) is, of course the f.b.p.; (v) is the partial well-order of Erdős and Rado (**3**), who note its equivalence with (iv). In connexion with (vi) it should be said that $a_1, a_2, \ldots$ is strictly descending if for all i, $a_{i+1} \leqslant a_i$, but not $a_i \leqslant a_{i+1}$. In an ordered set this would be written $a_{i+1} < a_i$, but this notation is ambiguous in a quasi-ordered set.

The equivalence of conditions (i), (ii), and (iii) is a well-known phenomenon, which occurs whenever a closure operation satisfies, in addition to the usual axioms (cf., for example, Birkhoff **1**, 49), the condition: $a \in \mathrm{cl}(B)$ implies $a \in \mathrm{cl}(B_0)$ for some finite subset B_0 of B (possibly depending on a). The classical instance is the equivalence of the ascending chain and finite basis conditions for ideals in a ring; the proof for that case (cf., for example, van der Waerden **8**, 23–27) can easily be adapted to ours, and we leave this to the reader.

The equivalence of (iv) and (vi), at least in the case of an order, is due to

I. Kaplansky, and is set as an exercise in Birkhoff (**1**, ex. 8, p. 39); the proof for quasi-orders is scarcely harder, so this, too, we leave to the reader. Obviously (v) is implied by (iv) and implies (vi), so it is equivalent to either of them.

Thus the first three, and the last three, of our conditions are equivalent. To complete the proof we show that (iii) implies (v), and that (v) implies (ii). Assume (iii), then, and let B be the set of elements of the sequence $a_1, a_2, \ldots$. Since B_0 is finite, there is an integer j such that every element of B_0 is an a_i with $i < j$; and since $B \subset \mathrm{cl}(B_0)$, for some a_i in B_0 we have $a_i \leqslant a_j$. So (v) also holds. On the other hand, if (v) holds, there cannot exist an infinite properly ascending sequence $A_1, A_2, \ldots$ of closed sets in A. For if there were we should only need to choose a_i in $A_{i+1} - A_i$ to falsify (v). Thus (v) implies (ii), completing the proof of the theorem.

THEOREM 2.2. *If the quasi-ordered set A has f.b.p., so has every subset and every homomorphic image of A.*

For subsets, condition (v) of Theorem 2.1 makes this obvious. For homomorphic images, remark that the inverse image of a closed set under a homomorphism is closed; condition (ii) of Theorem 2.1 then makes the preservation of f.b.p. under homomorphism obvious.

The *cardinal product* of two quasi-ordered sets A and B is the set of couples (a, b) with $a \in A$ and $b \in B$, ordered by $(a_1, b_1) \leqslant (a_2, b_2)$ if and only if $a_1 \leqslant a_2$ and $b_1 \leqslant b_2$.

THEOREM 2.3. *If two quasi-ordered sets have f.b.p., so does their cardinal product.*

This is almost obvious using condition (iv) of Theorem 2.1. For from an infinite sequence (a_i, b_i) $i = 1, 2, \ldots$, we can first select a subsequence on which the a's are ascending, and from this again a subsequence on which the b's also are ascending.

It is clear from Theorem 2.1 that a set with a linear order has f.b.p. if and only if it is well ordered. Our next theorem is the analogue for quasi-ordered sets of the principle of transfinite induction.

THEOREM 2.4. *A proposition concerning a quasi-ordered set M which is true of M if it is true of every proper open subset of M is true of every quasi-ordered set M with f.b.p.*

For if the proposition is false of M, it is also false of some proper open subset M_1 of M, and so of some proper open subset M_2 of M_1, and so on. The complements in M of $M_1, M_2, \ldots$ form an infinite properly ascending chain of closed sets in M. By Theorem 2.1, condition (ii), M has not the f.b.p.

Conversely, this induction property characterizes quasi-ordered sets with f.b.p. For if every proper open subset of M has f.b.p., then so has M. In fact we have the following slightly stronger result.

THEOREM 2.5. *If M is a quasi-ordered set such that for all a in M, $M-\mathrm{cl}(a)$ has f.b.p., then M has f.b.p.*

For if E is a non-empty closed set of M, let a be an element of it. $E-\mathrm{cl}(a)$ is a closed set of $M-\mathrm{cl}(a)$ and is therefore the closure in $M-\mathrm{cl}(a)$ of a finite set E_0. E is plainly the closure in M of $E_0 \cup a$, also a finite set. Thus M has f.b.p.

We next formulate a multiple induction principle. If $(M_0, M_1, \ldots, M_n)$, or (M_i) for short, is a sequence of quasi-ordered sets with f.b.p., then a second such sequence (M_i') is said to be obtained from the first *by descent* if for some integer r, $0 \leqslant r \leqslant n$, we have (i) for $i > r$, $M_i' = M_i$, (ii) M_r' is a proper open subset of M_r, (iii) for $i < r$, M_i' is any quasi-ordered set with f.b.p.

LEMMA. *There exists no infinite chain of sequences $(M_i^{(r)})$, $r = 1, 2, \ldots$, such that for all r, $(M_i^{(r+1)})$ is obtained from $(M_i^{(r)})$ by descent.*

The proof is by induction on n, the case $n = 0$ being simply the ascending chain condition for closed subsets of M_0. In the general case the ascending chain condition for closed subsets of $M_n^{(1)}$ makes it clear that, if such a chain exists, $M_n^{(r)}$ is constant for large r. But then an inductive hypothesis, applied to the chain consisting of the original sequences without their last terms, and starting with sufficiently large r, gives a contradiction.

The multiple induction principle, in the following 'reverse' form, is an immediate corollary of the lemma.

THEOREM 2.6. *Let $P(M_i)$ be a proposition concerning the sequence*

$$(M_i) = (M_0, M_1, \ldots, M_n)$$

of quasi-ordered sets. If the falsity of $P(M_i)$ for any sequence of sets with f.b.p. implies the falsity of $P(M_i')$ for some sequence (M_i') obtained from (M_i) by descent, then $P(M_i)$ is true whenever all sets of the sequence (M_i) have f.b.p.

3. Proof of Theorem 1.1

We begin by proving a lemma.

LEMMA. *Let (A, M) be an abstract algebra with a divisibility ordering. If X is a closed subset of A, and (A_0, M) is a subalgebra, then $(A_0 \cup X, M)$ is a subalgebra.*

Let μ be an r-ary operation in M, let $a_1, a_2, \ldots, a_r$ belong to $A_0 \cup X$, and put $b = \mu a_1 a_2 \ldots a_r$. Then either $a_1, a_2, \ldots, a_r$ all belong to A_0, in which case b belongs to A_0 because (A_0, M) is a subalgebra; or at least one, say a_i, belongs to X, in which case b belongs to X since $a_i \leqslant b$ in any divisibility ordering, and X is closed. Thus in either case b belongs to $A_0 \cup X$, which proves the lemma.

We now prove Theorem 1.1 by induction on the sequence $(M_0, M_1, \ldots, M_n)$ according to Theorem 2.6. That is, we assume the existence of a minimal algebra (A, M) which has a divisibility ordering in which A has not the f.b.p., though the ordering is compatible with quasi-orders on $M_0, \ldots, M_n$ in which these sets have the f.b.p.; and we deduce the existence of an algebra (A', M') with precisely similar properties, but in which the sequence (M'_i) is obtained from (M_i) by descent (M'_i being the set of i-ary operations in M').

First we note that since A has not the f.b.p., by Theorem 2.5 the set X of all a such that $A - \mathrm{cl}(a)$ has f.b.p. is not the whole of A. Since (A, M) is minimal, X is not closed under M. We can therefore choose μ in M_r for some r in $0 \leqslant r \leqslant n$, and a sequence $z = a_1 \ldots a_r$ of elements of X such that $\mu z = b$ does not belong to X. We next define M' in terms of this choice. If $i \neq r-1, r$, we take $M'_i = M_i$. We take M'_r to be $M_r - \mathrm{cl}(\mu)$. If $r \geqslant 1$, and λ is any r-ary operation, we denote by $\lambda(a, s)$ ($a \in A$, $s = 1, \ldots, r$) the $(r-1)$-ary operation defined by $\lambda(a,s).xy = \lambda xay$, where x has length $s-1$; we let $M^{(s)}_{r-1}$ denote the set of operations $\lambda(a, s)$ for $\lambda \in \mathrm{cl}(\mu)$ and $a \in A - \mathrm{cl}(a_s)$, ordered as the cardinal product of $\mathrm{cl}(\mu)$ and $A - \mathrm{cl}(a_s)$; and we take M'_{r-1} to be the union of M_{r-1} and $M^{(s)}_{r-1}$ for $s = 1, \ldots, r$, no order relations being assumed between elements of different terms of this union. Finally we take (A', M') to be the unique minimal subalgebra of (A, M').

We have next to show that (A', M') has the properties required of it. We give A' its quasi-order as a subset of A; this is obviously a divisibility order of (A', M'), and is compatible with the quasi-orders of $M'_0, M'_1, \ldots, M'_n$. Moreover, these latter sets have the f.b.p. This is obvious except for M'_{r-1}, which is the union of the finite collection of sets M_{r-1} and $M^{(s)}_{r-1}$. But M_{r-1} has the f.b.p. by assumption and $M^{(s)}_{r-1}$ by Theorem 2.3 and the choice of b. Since a union of a finite number of sets with f.b.p. obviously has f.b.p., M'_{r-1} has f.b.p. On the other hand, A' has not the f.b.p. We prove this by showing that it contains $A - \mathrm{cl}(b)$, which by assumption has not the f.b.p. That is, we prove that $A' \cup \mathrm{cl}(b) = A$. By the minimal property of (A, M) it is sufficient to prove that $(A' \cup \mathrm{cl}(b), M)$ is an M-subalgebra. By the lemma above, $A' \cup \mathrm{cl}(b)$ is closed under the operations of M', and so we have only to prove that it is closed under the operations of M not in M'; i.e., under λ for $\lambda \in \mathrm{cl}(\mu)$. Suppose then that c_i, $i = 1, \ldots, r$, belong to $A' \cup \mathrm{cl}(b)$, and put $d = \lambda c_1 \ldots c_r$. If $a_i \leqslant c_i$ for all i, then $\mu a_1 \ldots a_r \leqslant \lambda c_1 \ldots c_r$ or $d \in \mathrm{cl}(b)$. But if (as can happen only if $r \geqslant 1$) for some s, $c_s \in A - \mathrm{cl}(a_s)$, then $d = \lambda(c_s, s)x$, where x is a sequence of elements of $A' \cup \mathrm{cl}(b)$. Since $\lambda(c_s, s) \in M^{(s)}_{r-1} \subset M'$, and $A' \cup \mathrm{cl}(b)$ is closed under M', it again follows that $d \in A' \cup \mathrm{cl}(b)$. It follows that $A' \cup \mathrm{cl}(b)$ is closed under M and is therefore the whole of A. Finally the sequence (M'_i) is obtained from (M_i) by descent. Thus (A', M') has all the properties required of it and the theorem follows.

4. Some combinatorial applications

P. Erdős (2) proposed as a problem the proof of the following theorem.

THEOREM 4.1. *If a set X of positive integers does not contain any infinite subset no element of which divides any other element, then neither does $P(X)$, the set of integers which can be written as products of elements of X.*

This is a special case of Theorem 1.2. For the condition imposed on X is precisely that it shall have f.b.p. when $a \leqslant b$ is interpreted as a divides b, as follows from (vi) of Theorem 2.1 and the obvious fact that there exists no infinite sequence of integers that is properly descending in this order. But if the positive integers are regarded as an algebra under multiplication, this is a divisibility order. Thus by Theorem 1.2 if X has the f.b.p., so has the subalgebra generated by X, and this is Theorem 4.1.

Now let A be a quasi-ordered set. Let $S(A)$ be the set of finite subsets of A, and make it into a quasi-ordered set by the rule $P \leqslant Q$ if there is a one-to-one increasing map of P into Q. Then Erdős and Rado (3) prove the following result, and use it to prove Theorem 4.1.

THEOREM 4.2. *If A has the f.b.p., so has $S(A)$.*

Here we prove this as a corollary of another result. Let $V(A)$ be the set of finite sequences of elements of A, quasi-ordered by the rule: $x \leqslant y$ if x is majorized by a subsequence of y. That is, if $x = a_1 \ldots a_r$ and $y = b_1 \ldots b_s$, $x \leqslant y$ if there is a function $f(i)$, $i = 1,\ldots, r$, such that $1 \leqslant f(i) \leqslant s$, $f(i) < f(j)$ if $i < j$, and $a_i \leqslant b_{f(i)}$ for all i.

THEOREM 4.3. *If A has the f.b.p., so has $V(A)$.*

The elements of $V(A)$ form a semigroup under juxtaposition, and the quasi-order of $V(A)$ is a divisibility order of this semigroup. The one-element sequences form a set of generators of the semigroup, and as they obviously form a set order-isomorphic to A, Theorem 4.3 follows from Theorem 1.2.

Now let $S'(A)$ be the subset of $V(A)$ consisting of those sequences in which no element of A occurs twice. There is a natural mapping of $S'(A)$ on $S(A)$, and this is easily seen to be an order homomorphism. Thus Theorem 4.2 follows from Theorem 4.3 and Theorem 2.2.

It seems worth while to give explicitly the result of taking A to be a finite set in a trivial order.

THEOREM 4.4. *If X is any set of words formed from a finite alphabet, it is possible to find a finite subset X_0 of X such that, given a word w in X, it is possible to find w_0 in X_0 such that the letters of w_0 occur in w in their right order, though not necessarily consecutively.*

5. Power-series rings

In this section we apply our theorems to obtain results, mostly well known, about power-series rings of an ordered groupoid. Here we shall have to do with ordered sets only, not with quasi-ordered sets. We require a preliminary lemma. A homomorphism ρ of an ordered set A into an ordered set B is called *strict* if $a < b$ implies $\rho(a) < \rho(b)$.

LEMMA. *If ρ is a strict homomorphism of A into B, and A has f.b.p., then for any element b of B, $\rho^{-1}(b)$ is a finite set.*

By the definition of a strict homomorphism elements of $\rho^{-1}(b)$ are incomparable, so that this is an immediate consequence of (vi) of Theorem 2.1.

Now let G be a groupoid (i.e. an algebra with a single binary operation, which we denote by juxtaposition) and let C be an abelian group (written additively). A ring R is called a *groupoid-ring* of G over C if it contains elements $\alpha . g$, $\alpha \in C$, $g \in G$, such that

(i) $\alpha . g + \beta . g = (\alpha+\beta) . g$;

(ii) every element of R is a finite sum $\sum \alpha_i . g_i$, where the g_i are distinct, and this expression is unique up to order of terms and omission of terms with $\alpha_i = 0$;

(iii) $(\alpha . g)(\beta . h) = \rho . gh$, where ρ is a function of α, β, g, h, which we do not restrict for the moment, beyond noting that the distributive laws and (i) impose some conditions on it.

Under certain conditions it is possible to embed a groupoid-ring in a larger ring whose elements are infinite formal sums $\sum \alpha_i . g_i$, with the natural definitions of addition and multiplication. But while the sum of two such formal sums always exists, their product only exists under conditions. In fact, if for any formal sum x we denote by $D(x)$ the set of elements of G that occur in it with non-zero coefficients, then the product xy exists only if for all elements g of G the number of solutions of $g = hk$ with h in $D(x)$ and k in $D(y)$ is finite. Thus to obtain a ring we have to restrict the infinite formal sums to be considered. If G is an ordered groupoid, and, moreover, is a groupoid with cancellation, then we may do this by considering only the *power-series* of G, i.e. the formal sums x for which $D(x)$ has the f.b.p.

THEOREM 5.1. *The power-series of an ordered groupoid with cancellation form a ring.*

Let x, y be two power-series. Then $D(x+y)$ is contained in $D(x) \cup D(y)$ and so has f.b.p., which is to say that $x+y$ is a power-series. Consider the mapping $(g, h) \rightarrow gh$ of the cardinal product of $D(x)$ and $D(y)$ into G. The fact that G is an ordered groupoid says that this is an order homomorphism; the fact that G is a groupoid with cancellation is easily seen to imply that it is strict. By the lemma the number of counter-images of a fixed element of G is finite, which shows that the product xy exists. Also $D(xy)$ is contained in the image of the homomorphism, and so by Theorems 2.3 and 2.2, xy is a power-series. The ring axioms are easy to verify, and the theorem follows.

We say that the power-series x has the initial term $\alpha.g$ if $x = \alpha.g+x'$, where $\alpha \neq 0$ and $h \in D(x')$ implies $g < h$. We wish to prove next that division by a power-series with an initial term is always possible and unique. For this, however, we must make further assumptions. First, we must ensure that division by a monomial $\alpha.g$ is always possible and unique. This requires that G is a quasi-group (i.e. that for all g, h in G the equations $gk = h$ and $kg = h$ for k have each a unique solution in G) and that for fixed g, h, the non-zero elements of C form a quasi-group under the operation $\alpha \circ \beta = \rho$ defined by (iii) above. The last condition is satisfied for instance if C is a not necessarily associative ring, and $\rho = (\alpha\beta')\delta$, where $\beta \to \beta'$ is an additive isomorphism and δ depends only on g, h. We shall also need to assume that the order of G is invariant under division (i.e. that $gk \leqslant hk$ or $kg \leqslant kh$ implies $g \leqslant h$; this is not a consequence of the converse implication in general).

THEOREM 5.2. *Under the above conditions, if x_0 is a power-series with an initial term and x is any power-series, the equations $x_0 y = x$ and $yx_0 = x$ for y have each a unique solution.*

We shall deal only with the equation $x_0 y = x$, as the proofs are entirely similar. We have to show that the mapping $L_{x_0}: y \to x_0 y$ is a permutation of the set of power-series; i.e. that it has a two-sided inverse. Let $\alpha.g_0$ be the initial term of x_0, and let $x_0 = \alpha.g_0+x_0'$. Then the left multiplication $L_{\alpha.g_0}$ has an inverse by assumption, and we can write $L_{x_0} = L_{\alpha.g_0}(1+M)$, where 1 is the identity permutation, $M = L_{\alpha.g_0}^{-1} L_{x_0'}$, and mappings of the set of power-series into itself are added in the obvious way. Thus it is sufficient to prove that $(1+M)$ has an inverse, for which again it is sufficient to show that $(1-M+M^2-\dots)$ has a meaning as a mapping of the set of power-series into itself. This in turn requires that, for any power-series y, no element of G occurs in more than a finite number of the sets

$$D(y),\ D(My),\ D(M^2y),\ \dots,$$

and that the union of these sets has the f.b.p. Now if we write $Q_g = L_{g_0}^{-1} L_g$, where L_g and L_{g_0} are left multiplications in G, then the elements of $D(M^r y)$ are among the elements $Q_{g_1} Q_{g_2} \dots Q_{g_r} h$, $g_i \in D(x_0')$, $h \in D(y)$. Denote by X the set of these expressions, $r = 0, 1, 2, \dots$, ordered as the cardinal product of $V(D(x_0'))$ and $D(y)$, where $V(A)$ has the same meaning as in Theorem 4.3.

By Theorem 4.3 and Theorem 2.3 X has the f.b.p. But it is easy to see that the mapping of X into G which maps each expression $Q_{g_1} Q_{g_2} \ldots Q_{g_r} h$ on the element of G it denotes is a strict homomorphism. That no element of G belongs to an infinity of the sets $D(y), D(My), D(M^2y), \ldots$ follows from the lemma above, and that their union has f.b.p. from Theorem 2.2.

COROLLARY. *If G is linearly ordered, the power-series form a division ring.*

This corollary, which is the main point of the development, was proved by H. Hahn (**4**) for the case of associative and commutative systems, and by B. H. Neumann (**7**) and A. I. Malcev (**6**) for associative systems. I. Kaplansky (**5**) and D. Zelinsky (**9**) have pointed out that Hahn's proof in fact works without any restriction.

6. Fully invariant subgroups

Let G be a group, and denote the set of all normal subgroups of G by U. We shall order U by inverse inclusion; $H \leqslant K$ will mean $H \supset K$. It is possible to introduce operations into U so as to make it an algebra with this order as a divisibility order. For instance, we may take the unary operations $H \to nH$, where nH is the group generated by the nth powers of elements of H, for $n = 2, 3, \ldots$; and we may take the binary operation of commutation, which maps the pair H, K on the subgroup $[H, K]$ generated by the commutators $h^{-1}k^{-1}hk, h \in H, k \in K$. More generally, if $w(x_1, x_2, \ldots, x_r)$ is any word in generators $x_1, x_2, \ldots, x_r$ and their inverses which reduces to 1 on setting any generator equal to 1, we may define a corresponding operation in U, by putting $w(G_1, G_2, \ldots, G_r)$ equal to the subgroup generated by the elements $w(x_1, x_2, \ldots, x_r)$, $x_i \in G_i$. Now if U_0 is a subset of U which has the f.b.p., the ascending chain condition holds for subgroups which can be expressed as unions of elements of U_0. For if H is such a subgroup, it is determined by the set $S(H)$ of elements of U_0 contained in it. $S(H)$ is a closed set in U_0, and since $H_1 \subset H_2$ implies $S(H_1) \subset S(H_2)$, the ascending chain condition for closed subsets of U_0 implies the ascending chain condition for subgroups H. Thus we may apply Theorem 1.1 or Theorem 1.2 to prove that suitable sets of subgroups of G have the ascending chain condition. If, as in the case we consider, the set is a subalgebra of U generated, under certain operations, by G itself, the set will be a set of fully invariant subgroups of G. We give one example only.

THEOREM 6.1. *Let I be a set of integers containing no infinite subset of mutually indivisible integers. Let U_0 be the least set of subgroups of G such that*

(i) *U_0 contains G;*
(ii) *if $H \in U_0$ and $n \in I$, then $nH \in U_0$;*
(iii) *if $H \in U_0$ and $K \in U_0$, then $[H, K] \in U_0$.*

Then the ascending chain condition holds for subgroups of G which can be expressed as unions of elements of U_0.

This follows from Theorem 1.1; for U_0 is a minimal algebra with a 0-ary operation mapping the empty sequence on G, with unary operations $H \to nH$, $n \in I$, ordered by divisibility of the integers n, and with the binary operation of commutation; and the ordering of U_0 by inverse inclusion is a divisibility order compatible with the order given for the unary operations.

It is clear, however, that Theorem 1.1 is unlikely to give the whole truth in this direction, or even the whole accessible truth. For the closure operation on U most closely connected with the problem is not the one we have been considering, obtained from its order by inverse inclusion, but that which assigns as closure to any set of elements of U the set of all normal subgroups of G contained in their union. Since this is not obtained from a quasi-order, it is outside the scope of Theorem 1.1. It would be interesting to know whether any analogous theorem can be formulated and proved for more general closure operations.

REFERENCES

1. GARRETT BIRKHOFF, *Lattice theory*, rev. ed., Amer. Math. Soc. Colloquium Publications, vol. 25 (New York, 1948).
2. P. ERDŐS, Problem 4358, *Amer. Math. Monthly*, 56 (1949), 480.
3. —— and R. RADO, unpublished manuscript.
4. H. HAHN, 'Über die nichtarchimedischen Grössensysteme', *Sitz. Akad. Wiss. Wien*, 116 (1907), 601–55.
5. I. KAPLANSKY, review of (6), *Math. Rev.* 10 (1949), 8.
6. A. I. MALCEV, 'On the embedding of group algebras in division algebras', *Doklady Akad. Nauk SSSR* (N.S.), 60 (1948), 1409–1501.
7. B. H. NEUMANN, 'On ordered division rings', *Trans. Amer. Math. Soc.* 66 (1949), 202–52.
8. B. L. VAN DER WAERDEN, *Moderne Algebra*, 2 (Berlin, 1931).
9. D. ZELINSKY, 'Non-associative valuations', *Bull. Amer. Math. Soc.* 54 (1948), 175–83.

The University,
Manchester.