COMPOSITIO MATHEMATICA

N. J. S. HUGHES

Steinitz' exchange theorem for infinite bases

Compositio Mathematica, tome 15 (1962-1964), p. 113-118

<http://www.numdam.org/item?id=CM_1962-1964__15__113_0>

Steinitz' Exchange Theorem for Infinite Bases

by

N. J. S. Hughes

Given a system in which a suitable relation of dependence is defined, we give a construction (assuming well ordering), by which some of the elements of any basis may be replaced, in a one-one manner, by all the elements of any independent subset to give a new basis.

1. Definitions and notation

We call the set S a *dependence space* if there is defined a set Δ, whose members are finite subsets of S, each containing at least 2 elements, and if the Transitivity Axiom (below) is satisfied.

We shall use a, b, c, x, y (with or without suffixes) to denote elements of S and A, B, C, X for subsets of S and also i, j for suffixes and I, J for sets of suffixes and n will always be a positive integer.

$A+B$ will denote the union of the *disjoint* sets A and B and $A-B$ the set of those elements of A which are not in B.

We call A *directly dependent* if $A \in \Delta$.

If either $x \in A$ or there exist distinct $x_0, x_1, \ldots, x_n$, such that

$$(x_0, x_1, \ldots, x_n) \in \Delta, \tag{1}$$

where $x_0 = x$ and $x_1, \ldots, x_n \in A$, we call x *dependent* on A, denoted by $x \sim \sum A$, and *directly dependent* on (x) or $(x_1, \ldots, x_n)$ respectively.

We say that A is *dependent* if (1) is satisfied for some distinct $x_0, x_1, \ldots, x_n \in A$, and otherwise that A is *independent*.

If A is independent and, for any $x \in S$, $x \sim \sum A$, then A is a *basis* of S.

If $A = (a_i)_{i \in I}$ then $\sum A$ and $\sum_{i \in I} a_i$ are equivalent symbols. Also $\sum A + \sum B$ and $\sum (A \cup B)$ are equivalent symbols.

If either $x = a$ or (1) is satisfied for some $n \geqq 1$, with $x_0 = x$, $x_1 = a$, and, for $2 \leqq m \leqq n$, $x_m \in C$, we write

$$x \sim (a) + \sum C. \tag{2}$$

Clearly, (2) implies $a \sim (x)+\sum C$.

We assume the following Transitivity Axiom:
if $x \sim \sum A$ *and, for all* $a \in A$, $a \sim \sum B$, *then* $x \sim \sum B$.

In particular, we may take S to be the set of all non-zero elements of a vector space over a field F, and have (1) if and only if

$$\xi_0 x_0 + \ldots + \xi_n x_n = 0$$

for some non-zero $\xi_0, \ldots, \xi_n$ in F.

2. Well ordered subsets

We now assume that $A = (a_i)_{i \in I}$ is well ordered, I being also well ordered, and assume the Principle of Transfinite Induction in the form:

$(i \in I)$, $P(i)$, (i.e. $P(i)$ is true for all $i \in I$), if

$$(i \in I), (j < i) \Rightarrow P(j) \cdot \Rightarrow P(i).$$

Lemma 1

If $(i \in I)$, $a_i \sim \sum_{j<i} a_j + \sum C$, then $(i \in I)$, $a_i \sim \sum C$.
This is easily proved by Transfinite Induction.

Lemma 2

If $A+C$ is a basis of S and

$$(i \in I), x_i \sim (a_i)+\sum_{j<i} a_j + \sum C, \tag{1}$$

then the x_i are distinct and not in C, $X+C$ is a basis of S, where $X = (x_i)_{i \in I}$, and

$$(i \in I), a_i \sim (x_i) + \sum_{j<i} x_j + \sum C. \tag{2}$$

Also, if

$$y \sim (a_i) + \sum_{j<i} a_j + \sum C, \tag{3}$$

then

$$y \sim (x_i) + \sum_{j<i} x_j + \sum C. \tag{4}$$

From (1), we have

$$(i \in I), a_i \sim (x_i) + \sum_{j<i} a_j + \sum C, \tag{5}$$

and hence, by Transfinite Induction,

$$(i \in I), a_i \sim \sum_{j \leq i} x_j + \sum C. \tag{6}$$

From (3) and (6), we have

$$y \sim \sum_{j \leq i} x_j + \sum C. \tag{7}$$

If

$$y \sim \sum_{j<i} x_j + \sum C, \tag{8}$$

then, by (1),

$$y \sim \sum_{j<i} a_j + \sum C,$$

and hence, since, by (3),

$$a_i \sim (y) + \sum_{j<i} a_j + \sum C,$$

$$a_i \sim \sum_{j<i} a_j + \sum C, \tag{9}$$

which is a contradiction, since $A+C$ is independent.

From (7) and the falsity of (8), we have (4), and then, putting $y = a_i$, also (2).

If 2 of the x_i were equal, or if an x_i were in C, or if $X+C$ were dependent, we would have (since C is independent) a relation of the form:

$$x_i \sim \sum_{j<i} x_j + \sum C.$$

Then, by (1), we would have

$$x_i \sim \sum_{j<i} a_j + \sum C,$$

and, by (5), again (9).

Thus $X+C$ is independent and, by (6), is a basis of S.

3. Proof of Steinitz' exchange theorem

THEOREM

If A is a basis and B an independent subset (both being well ordered) of the dependence space S, then there is a definite subset A' of A, such that $B+(A-A')$ is also a basis of S, and a definite one-one correspondence between A' and B.

If B is a basis of S, then $A' = A$.

We shall suppose that $A = (a_i)_{i \in I}$ where I is well ordered and shall define successively disjoint subsets $I(1), I(2), \ldots$ and, for all i in their union, distinct elements b_i of B.

We suppose that $I(1), \ldots, I(p)$ have been defined and also, for all $i \in I(1)+ \ldots +I(p)$, distinct $b_i \in B$.

We let

$$J(p) = I-(I(1)+ \ldots +I(p)), \tag{1}$$

$$A^p = (a_i^p)_{i \in J(p)}, \text{ where, } (i \in J(p)),\ a_i^p = a_i, \tag{2}$$

$$(q = 1, \ldots, p),\ B^q = (b_i)_{i \in I(q)}. \tag{3}$$

We shall further suppose that A_p, defined by

$$A_p = A^p+B^1+ \ldots +B^p \tag{4}$$

is a basis of S.

If $p = 0$, we define $J(0) = I$, $A^0 = A_0 = A$.

If $b \in B-(B^1+ \ldots +B^p)$, since A_p is a basis of S and B is independent, we have a relation of the form:

$$b \sim (a_i^p) + \sum_{j<i} a_j^p + \sum B^1 + \ldots + \sum B^p. \tag{5}$$

In (5), $i = i(p+1, b)$ may, by the well ordering of $J(p)$, be supposed the least possible, but it follows easily from the independence of A_p that the set of elements, on which b is directly dependent, is in fact unique.

We now define $I(p+1)$ to be the set of all i in $J(p)$, such that $i = i(p+1, b)$, for some $b \in B-(B^1+ \ldots +B^p)$, and b_i to be the first such b (in the well ordering of B) and may replace p by $p+1$ in the definitions (1) to (4).

We then have

$$(i \in I(p+1)), \quad b_i \sim (a_i^p)+ \sum_{j<i} a_j^p + \sum B^1 + \ldots + \sum B^p. \tag{6}$$

By Lemma 2, with A^p for A, $B^1+ \ldots +B^p$ for C and

$$(i \in I(p+1)),\ x_i = b_i,\ (i \in J(p+1)),\ x_i = a_i, \tag{7}$$

A_{p+1} is a basis of S.

By the last part of Lemma 2, (with $i = i(p+1, b)$), and (7), we have

$$(b \in B-(B^1+ \ldots +B^{p+1}),\ i(p+2, b) < i(p+1, b). \tag{8}$$

The process of successively defining the subsets $I(1), I(2), \ldots$ of I and the corresponding disjoint subsets $B^1. B^2, \ldots$ of B may be continued either until, for some p, $B^1+ \ldots +B^p = B$ or to give an infinite sequence of subsets.

In the latter case $B = B^1+B^2+\dots$, for, by (8), if $b \in B-(B^1+B^2+\dots)$,

$$i(1, b), i(2, b), \dots$$

would be an infinite, strictly descending sequence of members of I.

In each case we take $A' = (a_i)_{i\in I(1)+I(2)+\dots}$ and the correspondence $a_i \leftrightarrow b_i$ is one-one between A' and B.

In the former case, $A-A' = A^p$ and, by (4), $B+(A-A') = A_p$ and is therefore a basis of S.

In the latter case, $A-A' \subseteqq A^p$, for all $p \geqq 0$, and we see, by (4), that any finite subset of $B+(A-A')$ is contained in A_p for sufficiently large p. Thus $B+(A-A')$ is independent.

Since

$$a_i \sim \sum_{j<i} a_j + \sum(A-A') + \sum B$$

is trivial if $i \in I-(I(1)+I(2)+\dots)$ and follows from (6) if $i \in I(p+1)$, for any $p \geqq 0$, by Lemma 1,

$$(i \in I),\ a_i \sim \sum(A-A') + \sum B.$$

Thus, being independent, $B+(A-A')$ is a basis of S.

Finally, since a basis is a maximal independent subset, if B is a basis of S, $A-A'$ is empty and $A' = A$.

4. Rank

Since the bases of S coincide with its maximal independent subsets, S, assumed to be well ordered, has at least one basis, and by the last part of the Theorem, any 2 bases have the same cardinal number, which may be called the rank of S (with respect to Δ).

From the example at the end of § 1, we see that a vector space over a field has a unique rank.

If G is an additive Abelian group, we let S be the set of elements of infinite order and $(x_0, \dots, x_n) \in \Delta$ if and only if, for some non-zero integers $N_0, \dots, N_n$,

$$N_0x_0 + \dots + N_nx_n = 0.$$

It now follows that the rank of G is unique (Kurosh, p. 140).

Now let G be a p-primary additive Abelian group and r be a positive integer. Let H be the subset of G generated by the union of the set of all $g \in G$, such that $p^{r-1}g = 0$ and the set of all g, such that $g = pg'$, for some $g' \in G$.

We take S to be the set of all elements of G, whose orders are exactly p^r and which are not in H, and $(x_0, \ldots, x_n) \in \Delta$, if and only if, for some integers $N_0, \ldots, N_n$ prime to p,

$$N_0 x_0 + \ldots + N_n x_n \in H.$$

If G can be expressed as a direct sum of cyclic groups, we see easily that the set of generators of the cyclic groups of order p^r is a basis of S and hence that the cardinal number of such summands is a group invariant (Kurosh, p. 174).

REFERENCE

A. G. Kurosh
Theory of Groups, Vol. 1, Chelsea Publishing Co., New York, 1955.

University College,
Cathays Park, Cardiff

(Oblatum 30-3-62).