A GENERAL BASIS THEOREM

by A. P. ROBERTSON and J. D. WESTON
(Received 2nd November 1957 ; Revised MS. received 19th September 1958)

THE well-known " basis theorem " of elementary algebra states that in a finite-dimensional vector space, any two bases have the same number of elements ; or, equivalently, that a vector space is n-dimensional if it has a basis consisting of n vectors (where the dimension of a vector space is defined to be the least upper bound of the numbers k for which there exist k linearly independent vectors, and a basis is defined to be a maximal set of linearly independent vectors). This theorem has an analogue in the theory of groups : if an Abelian group has a finite maximal set of independent non-cyclic elements, the number of elements in one such set being n, then no set of independent non-cyclic elements can have more than n members.

There are other theorems which are essentially of the same type. For example, consider a collection of paths in a given space, each path having distinct end-points. Let a finite system of these paths be called an " even network " if the number of paths in the system that terminate at a particular point is always even (thus an even network is characterised by the property that a complete circuit of it can be made by traversing each of its paths once only). Let a system of paths be called " singular " if it does not contain an even network. Now suppose that the given collection of paths contains a maximal singular system, the number of paths in one such system being n. Then any system containing more than n of the given paths contains an even network.

These three theorems remain valid when n is infinite under a suitable interpretation. Thus, in an infinite-dimensional vector space, any two bases have the same cardinal number, and the same holds for any two maximal sets of independent non-cyclic elements of an Abelian group, or for any two maximal singular systems of paths.

We shall show that, by suitably generalising the notion of an equivalence relation, it is possible to isolate an abstract principle which underlies these theorems. The principle we establish is in fact an extension of the " pigeon-hole " principle, which asserts that if a given set is partitioned, by an equivalence relation, into n classes which are disjoint from one another, then any subset having more than n elements contains at least two equivalent elements.

We consider an abstract set X, and a class $\mathscr{R}$ of finite subsets of X satisfying the following elimination axiom :

If E and F are distinct members of $\mathscr{R}$ and $x \in E \cap F$, then $E \cup F$ has a subset belonging to $\mathscr{R}$ but not containing x.

There is a considerable range of possibilities for $\mathscr{R}$, as the following examples indicate.

(1) $\mathscr{R}$ could consist of all the finite subsets of X which have more than a certain number of elements.

(2) If an equivalence relation is defined over X, $\mathscr{R}$ could consist of all two-element subsets of the corresponding equivalence classes.

(3) If X is a vector space, $\mathscr{R}$ could consist of those finite sets of vectors $x_1, \ldots, x_k$ for which there exist non-zero scalars $\lambda_1, \ldots, \lambda_k$ such that

$$\lambda_1 x_1 + \ldots + \lambda_k x_k = 0.$$

(4) If X is an Abelian group, $\mathscr{R}$ could consist of those finite sets of elements $x_1, \ldots, x_k$ for which there exist non-zero integers $n_1, \ldots, n_k$ such that

$$x_1^{n_1} x_2^{n_2} \ldots x_k^{n_k} = e,$$

where e is the unit element of the group.

(5) If X is a collection of paths with distinct end-points, $\mathscr{R}$ could consist of all the even networks contained in X.

It is obvious that the axiom is satisfied in cases (1) and (2). To verify that it is satisfied in cases (3) and (4) one has only to eliminate a common "unknown" from a pair of simple equations. In case (5), it is enough to observe that if E and F are distinct even networks, then their symmetric difference $E \Delta F = (E \cup F) \setminus (E \cap F)$ is an even network.

Supposing X and $\mathscr{R}$ to be given, and the elimination axiom to be satisfied, we shall call the subsets of $\mathscr{R}$ *impurities*. We say that a non-empty subset of X is a *pure set* if it contains no member of $\mathscr{R}$; otherwise it is an *impure set*.

Pure sets need not exist: for example, $\mathscr{R}$ might consist of all the non-empty subsets of X which have fewer than a certain number of elements. We are concerned, however, with those instances in which pure sets exist, and then maximal pure sets also exist. For, since $\mathscr{R}$ consists of finite sets, purity is an inductive property; hence, by Zorn's lemma, every pure set is contained in a maximal pure set. In example (1) it is obvious that pure sets exist and that all the maximal pure sets have the same number of elements; that this is true generally is our main result:

Any two maximal pure sets have the same (cardinal) number of elements.

This clearly implies the various theorems we have mentioned. In particular, if it is applied to case (2), where $\mathscr{R}$ is effectively an equivalence relation, it gives the pigeon-hole principle; and if it is applied to case (3), where purity means linear independence, it gives the basis theorem.

Before proving our main theorem, we observe that any maximal pure set M can be regarded as a "basis" for X, in the following sense: *corresponding to each element x of $X \setminus M$ there is a unique subset E of M such that $E \cup (x) \in \mathscr{R}$.* For there is certainly one such set E, since M is a maximal pure set; if there were another, say F, we could apply the elimination axiom to $E \cup (x)$ and $F \cup (x)$ to obtain a subset of $E \cup F$, and so of M, belonging to $\mathscr{R}$, which would contradict the purity of M.

Further, *if* $y \in E$, *then* $M' = (M \cup (x)) \setminus (y)$ *is also a maximal pure set.* For any impurity F in M' would either be a subset of M or contain x; in the latter case we could use the axiom to eliminate x from F and $E \cup (x)$, obtaining an impurity contained in M. Since M is pure, so is M'. Also M' is maximal. For otherwise there would exist a strictly larger pure set M''; if $z \in M'' \setminus M'$, then $z \notin M$, since M is maximal, and so there would be a set $G \subseteq M$ with $G \cup (z) \in \mathscr{R}$. Then either $G \cup (z)$ itself or an impurity obtained by eliminating y from $G \cup (z)$ and $E \cup (x)$ would be a subset of M'', contrary to the hypothesis that M'' was pure.

We can now prove the main result. Let M and N be two maximal pure sets, and write $M' = M \setminus N$ and $N' = N \setminus M$. First suppose that N' is finite, consisting of the n elements $x_1, x_2, \ldots, x_n$. Then elements $y_1, y_2, \ldots, y_n$ of M' can be found so that each of the sets M_r defined by

$$M_0 = M, \quad M_{r+1} = (M_r \cup (x_{r+1})) \setminus (y_{r+1}) \quad (0 \leqslant r < n)$$

is maximal pure. The proof of this is by induction; suppose $y_1, y_2, \ldots y_r$ so found. Then, since x_{r+1} does not belong to the maximal pure set M_r, there is a subset E_r of M_r with $E_r \cup (x_{r+1}) \in \mathscr{R}$. Since N is pure, E_r is not a subset of N and so y_{r+1} can be chosen from $E_r \cap M'$. With the definition already given, M_{r+1} is then maximal pure. The sets $M_0, M_1, \ldots, M_n$ so constructed have the same cardinal number, and M_n is a pure set containing N, and so identical with N. Hence M and N have the same cardinal number.

Finally, suppose that N' is infinite. For each $x \in N'$ let $E(x)$ be the (unique) subset of M such that $E(x) \cup (x) \in \mathscr{R}$. We show that $M' \subseteq \bigcup_{x \in N'} E(x)$. Suppose not, and let z be an element of M' excluded from the union of the sets $E(x)$. There is a finite subset F of N with $F \cup (z) \in \mathscr{R}$; suppose that $F \setminus M$ has n elements and let y be any one of them. Then $z \notin E(y)$ and so we can apply the axiom to eliminate y from the sets $F \cup (z)$ and $E(y) \cup (y)$, obtaining an impurity consisting of elements of M together with at most $n-1$ elements of N'. This process can clearly be repeated sufficiently often to remove all the elements of N'. The result is an impurity contained in M, contradicting the purity of M. Hence $M' \subseteq \bigcup_{x \in N'} E(x)$. Now this last set has the same cardinal as N', since N' is infinite and each $E(x)$ is finite, and so the cardinal of M' is at most equal to that of N'. But the positions of M and N can be reversed and so M' and N' must have the same cardinal. Hence M and N have the same cardinal, and the proof of the main result is completed.

Department of Mathematics
The University
Glasgow, W.2

Department of Mathematics
King's College
Newcastle upon Tyne, 2