ON THE ABSTRACT PROPERTIES OF LINEAR DEPENDENCE.

By Hassler Whitney.

1. Introduction. Let $C_1, C_2, \ldots, C_n$ be the columns of a matrix $M$. Any subset of these columns is either linearly independent or linearly dependent; the subsets thus fall into two classes. These classes are not arbitrary; for instance, the two following theorems must hold:

(a) Any subset of an independent set is independent.

(b) If $N_p$ and $N_{p+1}$ are independent sets of $p$ and $p + 1$ columns respectively, then $N_p$ together with some column of $N_{p+1}$ forms an independent set of $p + 1$ columns.

There are other theorems not deducible from these; for in §16 we give an example of a system satisfying these two theorems but not representing any matrix. Further theorems seem, however, to be quite difficult to find. Let us call a system obeying (a) and (b) a "matroid." The present paper is devoted to a study of the elementary properties of matroids. The fundamental question of completely characterizing systems which represent matrices is left unsolved. In place of the columns of a matrix we may equally well consider points or vectors in a Euclidean space, or polynomials, etc.

This paper has a close connection with a paper by the author on linear graphs; we say a subgraph of a graph is independent if it contains no circuit. Although graphs are, abstractly, a very small subclass of the class of matroids, (see the appendix), many of the simpler theorems on graphs, especially on non-separable and dual graphs, apply also to matroids. For this reason, we carry over various terms in the theory of graphs to the present theory. Remarkably enough, for matroids representing matrices, dual matroids have a simple geometrical interpretation quite different from that in the case of graphs (see §13).

The contents of the paper are as follows: In Part I, definitions of matroids in terms of the concepts rank, independence, bases, and circuits are considered, and their equivalence shown. Some common theorems are deduced (for instance Theorem 8). Non-separable and dual matroids are studied in

---

1 Presented to the American Mathematical Society, September, 1934.
2 "Non-separable and planar graphs," Transactions of the American Mathematical Society, vol. 34 (1932), pp. 339-362. We refer to this paper as B.
Part II; this section might replace much of the author's paper G. The subject of Part III is the relation between matroids and matrices. In the appendix, we completely solve the problem of characterizing matrices of integers modulo 2, of interest in topology.

I. Matroids.

2. Definitions in terms of rank. Let a set $M$ of elements $e_1, e_2, \ldots, e_n$ be given. Corresponding to each subset $N$ of these elements let there be a number $r(N)$, the rank of $N$. If the three following postulates are satisfied, we shall call this system a matroid.

(R$_1$) The rank of the null subset is zero.

(R$_2$) For any subset $N$ and any element $e$ not in $N$,

$$r(N + e) = r(N) + k,$$

where $(k = 0$ or $1)$.

(R$_3$) For any subset $N$ and elements $e_1, e_2$ not in $N$, if $r(N + e_1) = r(N + e_2) = r(N)$, then $r(N + e_1 + e_2) = r(N)$.

Evidently any subset of a matroid is a matroid. In what follows, $M$ is a fixed matroid. We make the following definitions:

$$\rho(N) = \text{number of elements in } N.$$

$$n(N) = \rho(N) - r(N) = \text{nullity of } N.$$

$N$ is independent, or, the elements of $N$ are independent, if $n(N) = 0$; otherwise, $N$, and its set of elements, are dependent.

Lemma 1. For any $N$, $r(N) \geq 0$ and $n(N) \geq 0$. If $N \subseteq M$, then $r(N) \leq r(M)$, $n(N) \leq n(M)$.

Lemma 2. Any subset of an independent set is independent.

$e$ is dependent on $N$ if $r(N + e) = r(N)$; otherwise $e$ is independent of $N$.

A base is a maximal independent submatroid of $M$, i.e. a matroid $B$ in $M$ such that $n(B) = 0$, while $B \subseteq N, B \neq N$ implies $n(N) > 0$. See also Theorem 7. A base complement $A = M - B$ is the complement in $M$ of a base $B$. A circuit is a minimal dependent matroid, i.e. a matroid $P$ such that $n(P) > 0$, while $N \subseteq P, N \neq P$ implies $n(N) = 0.$

Theorem 1. $N$ is independent if and only if it is contained in a base, or, if and only if it contains no circuit.