chapter I  Vector spaces

In this chapter we introduce the concepts of a vector space and a basis for that vector space. We assume that there is at least one basis with a finite number of elements, and this assumption enables us to prove that the vector space has a vast variety of different bases but that they all have the same number of elements. This common number is called the dimension of the vector space.

For each choice of a basis there is a one-to-one correspondence between the elements of the vector space and a set of objects we shall call n-tuples. A different choice for a basis will lead to a different correspondence between the vectors and the n-tuples. We regard the vectors as the fundamental objects under consideration and the n-tuples a representations of the vectors. Thus, how a particular vector is represented depends on the choice of the basis, and these representations are non-invariant. We call the n-tuple the coordinates of the vector it represents; each basis determines a coordinate system.

We then introduce the concept of subspace of a vector space and develop the algebra of subspaces. Under the assumption that the vector space is finite dimensional, we prove that each subspace has a basis and that for each basis of the subspace there is a basis of the vector space which includes the basis of the subspace as a subset.

1 1 Definitions

To deal with the concepts that are introduced we adopt some notational conventions that are commonly used. We usually use sans-serif italic letter to denote sets. 

w e S means is an element of the set S.

 means is not an element of the set S.

5

 T means S is a subset of the set T.

 denotes the intersection of the sets S and T, the set of elements in both S and T.

denotes the union of the sets S and T, the set of elements in S or T. denotes the set of elements in T but not in S. In case T is the set of all objects under consideration, we shall call T — S the complement of S and denote it by CS.

Sg•./l e M denotes a collection of sets indexed so that one set sg is specified for each element e M. M is called the index set. denotes the intersection of all sets s g •.11 e M.

denotes the union of all sets : g e M.

0 denotes the set with no elements, the empty set.

A set will often be specified by listing the elements in the set or by giving a property which characterizes the elements of the set. In such cases we use braces: {u, F} is the set containing just the elements and 18, {0' | P} is the set of all oc with property P, {up 1 8.1 e M} denotes the set of all corresponding to in the index set M. We have such frequent use for the set of all integers or a subset of the set of all integers as an index set that we adopt a special convention for these cases. denotes a set of elements indexed by a subset of the set of integers. Usually the same index set is used over and over. In such cases it is not necessary to repeat the specifications of the index set and often designation of the index set will be omitted. Where clarity requires it, the index set will be specified. We are careful to distinguish between the set {0%} and an element oq of that set.

Definition. By afield F we mean a non-empty set of elements with two laws of combination, which we call addition and multiplication, satisfying the following conditions :

Fl. To every pair of elements a, b e F there is associated a unique element, called their sum, which we denote by a + b.

F2. Addition is associative; (a + b) + c = a + (b + c).

F3. There exists an element, which we denote by O, such that a + O = a for all a e F.

F4. For each a e F there exists an element, which we denote by —a, such that a + ( —a) = 0. Following usual practice we write b + (—a) = b — a. F5. Addition is commutative; a + b = b + a.

F6. To every pair of element a, b e F there is associated a unique element, called their product, which we denote by ab, or a • b.

F7. Multiplication is associative; (ab)c = a(bc).

F8. There exists an element different from O, which we denote by l, such that a • 1 = a for all a e F.

1 Definitions

F9. For each a e F, a 0, there exists an element which we denote by a—I , such that a • a

FIO. Multiplicatiön is commutative: ab = ba.

Fl l. Multiplication is distributive with respect to addition:



The elements of F are called scalars, and will generally be denoted by lower case Latin italic letters.

The rational numbers, real numbers, and complex numbers are familiar and important examples of fields, but they do not exhaust the possibilities. As a less familiar example, consider the set {0, l} where addition is defined by the rules: O 1 + 1 = 0, + 1 = l ; and multiplication is defined by the rules: 0 • 0 = 0 • I — 0 1 • I = I. This field has but two elements, and there are other fields with finitely many elements.

We do not develop the various properties of abstract fields and we are not concerned with any specific field other than the rational numbers, the real numbers, and the complex numbers. We find it convenient and desirable at the moment to leave the exact nature of the field of scalars unspecified because much of the theory of vector spaces and matrices is valid for arbitrary fields.

The student unacquainted with the theory of abstract fields will not be handicapped for it will be suffcient to think of F as being one of the familiar fields. All that matters is that we can perform the operations of addition and subtraction, multiplication and division, in the usual way. Later we have to restrict F to either the field of real numbers or the field of complex numbers in order to obtain certain classical results; but we postpone that moment as long as we can. At another point we have to make a very mild assumption, that is, I + I 0, a condition that happens to be false in the example given above. The student interested mainly in the properties of matrices with real

or complex coemcients should consider this to be no restriction.

Definition. A vector space V over F is a non-empty set of elements, called vectors, with two laws of combination, called vector addition (or addition) and scalar multiplication, satisfying the following conditions:

Al. To every pair of vectors 0', e V there is associated a unique vector in V called their sum, which we denote by + p.

A2. Addition is associative; (u + F) + = + (F + y).

A3. There exists a vector, which we denote by 0, such that + 0 for all e V.

A4. For each e V there exists an element, which we denote by —u, such that + = O.

AS. Addition is commutative; -F = + u.

Bl. To every scalar a e F and vector e V, there is associated a unique vector, called the product of a and u, which we denote by am.

B2. Scalar multiplication is associative: a(boc) = (ab)u.

B3. Scalar multiplication "is distributive with respect to vector addition;



B4. Scalar multiplication is distributive with respect to scalar addition; (a + = + bot.

B5. I • = (where I e F).

We generally use lower case Greek letters to denote vectors. An exception is the zero vector of A3. From a logical point of view we should not use the same symbol "0 ' for both the zero scalar and the zero vector, but this practice is rooted in a long tradition and it is not as confusing as it may seem at first.

The vector space axioms concerning addition alone have already appeared in the definition of a field. A set of elements satisfying the first four axioms is called a group. If the set of elements also satisfies A5 it is called a commutative group or abelian group. Thus both fields and vector spaces are abelian groups under addition. The theory of groups is well developed and our subsequent discussion would be greatly simplified if we were to assume a prior knowledge of the theory of groups. We do not assume a prior knowledge of the theory of groups; therefore, we have to develop some of their elementary properties as we go along, although we do not stop to point out that what was proved is properly a part of group theory. Except for specific applications in Chapter VI we do no more than use the term "group"  to denote a set of elements satisfying these conditions.

First, we give some examples of vector spaces. Any notation other than F for a field and "V" for a vector space is used consistently in the same way throughout the rest of the book, and these examples serve as definitions for these notations:

 (l) Let F be any field and let V = P be the set of all polynomials in an indeterminate x with coefficients in F. Vector addition is defined to be the ordinary addition of polynomials, and multiplication is defined to be the ordinary multiplication of a polynomial by an element of F.

(2) For any positive integer n, let Pn be the set of all polynomials in c with coeffcients in F of degree n — l, together with the zero polynomial. The operations are defined as in Example (l).

 (3) Let F = R, the field of real numbers, and take V to be the set of all real-valued functions of a real variable. Iff and g are functions we define vector addition and scalar multiplication by the rules

(f + = f (x) -F g(x),

(1.1)

1 Definitions

1. Let F = R, and let V be the set of continuous real-valued functions of a real variable. The operations are defined as in Example (3). The point of this example is that it requires a theorem to show that Al and Bl are satisfied.



1. Let F = R, and let V be the set of real-valued functions defined on the interval [0, 1] and integrable over that interval. The operations are defined as in Example (3). Again, the main point is to show that Al and Bl are satisfied.
2. Let F = R, and let V be the set of all real-valued functions of a real variable differentiable at least m times (m a positive integer). The operations are defined as in Example (3).
3. Let F = R, and let V be the set of all real-valued functions differentiable d2y

at least twice and "tisfying the differential equation --æ + y = 0.

1. Let F = R, and let V = R.n be the set of all real ordered n-tuples, 

= (al, a a ) with ai e F. Vector addition and scalar multiplication are defined by the rules

|  |  |  |
| --- | --- | --- |
| (al, • . . , an) + (bl' | b ) = (al + bl, | (1.2) |
| a(a | a ) = (aal, , aan)• |  |

We call this vector space the n-dimensional real coordinate space or the real affine n-space. (The name "Euclidean n-space" is sometimes used, but that term should be reserved for an amne n-space in which distance is defined.) (9) Let Fn be the set of all n-tuples of elements of F. Vector addition and scalar multiplication are defined by the rules (1.2). We call this vector space an n-dimensional coordinate space.

An immediate consequence of the axioms defining a vector space is that the zero vector, whose existence is asserted in A3, and the negative vector, whose existence is asserted in A4, are unique. Specifically, suppose O satisfies A3 for all vectors in V and that for some e V there is a O' satisfying the condition + 0 = + O' = u. Then O

= (u + 0') + ( — o,) = + = 0. Notice that we have proved not merely that the zero vector satisfying A3 for all oc is unique ; we have proved that a vector satisfying the condition of A3 for some must be the zero vector, which is a much stronger statement.

Also, suppose that to a given oc there were two negatives, and satisfying the conditions of A4. Then (

Both these demonstrations used the commutative law, A5. Use of this axiom could have been avoided, but the necessary argument would then have been somewhat longer.

Uniqueness enables us to prove that Oot = 0. (Here is an example of the seemingly ambiguous use of the symbol "0." The "0" on the left side is a scalar while that on the right is a vector. However, no other interpretation could be given the symbols and it proves convenient to conform to the convention rather than introduce some other symbol for the zero vector.) For each e V, = 1 • = + O) = 1 • oc + • o' = oc Thu s

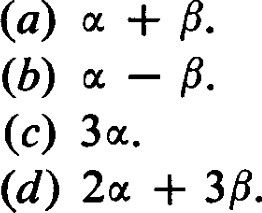
O • = O. In a similar manner we can show that (—

(1 — l)oc = 0 • oc = 0. Since the negative vector is unique we see that = —u. It also follows similarly that a • 0 = 0.

EXERCISES

1 to 4. What theorems must be proved in each of the Examples (4), (5), (6), and (7) to verify Al ? To verify Bl ? (These axioms are usually the ones which require most specific verification. For example, if we establish that the vector space described in Example (3) satisfies all the axioms of a vector space, then Al and Bl are the only ones that must be verified for Examples (4), (5), (6), and (7). Why ?)

1. Let P+ be the set of polynomials with real coeffcients and positive constant term. Is P+ a vector space? Why?
2. Show that if au = 0 and a O, then = O. (Hint: Use axiom F9 for fields.)
3. Show that if acc = O and u O, then a = O.
4. Show that the such that + = is (uniquely) = + ( —u)
5. Let = (2, —5, O, 1) and = (—3, 3, 1, —1) be vectors in the coordinate space R4. Determine



1. Show that any field can be considered to be a vector space over itself.
2. Show that the real numbers can be considered to be a vector space over the rational numbers.
3. Show that the complex numbers can be considered to be a vector space over the real numbers.
4. Prove the uniqueness of the zero vector and the uniqueness of the negative of each vector without using the commutative law, AS.

2 1 Linear Independence and Linear Dependence

Because of the associative law for vector addition, we can omit the parentheses from expressions like a10C1 + (a20(2 + = + 4 0(2) + a30C3 and write them in the simpler form aptl + a,aot2 + a.oc It is clear that this convention can be extended to a sum of any number of

2 Linear Independence and Linear Dependence

such terms provided that only a finite number of coemcients are different from zero. Thus, whenever we write an expression like Ei agi (in which we do not specify the range of summation), it will be assumed, tacitly if not explicitly, that the expression contains only a finite number of non-zero coemcients.

If = E au we say that is a linear combination of the We also say that 18 is linearly dependent on the if can be expressed as a linear combination of the occ.. An expression of the form apti = 0 is called a linear relation among the oti. A relation with all ai = O is called a trivial linear relation; a relation in which at least one coefficient is non-zero is called a non-trivial linear relation.

Definition. A set of vectors is said to be linearly dependent if there exists a n6n-trivial linear relation among them. Otherwise, the set is said to be linearly independent.

It should be noted that any set of vectors that includes the zero vector is linearly dependent. A set consisting of exactly one non-zero vector is linearly independent. For if acc = 0 with a 0, then = 1 • oc = (a—I • a)oc

= • O = 0. Notice also that the empty set is linearly independent. It is clear that the concept of linear independence of a set would be meaningless if a vector from a set could occur arbitrarily often in a possible relation. If a set of vectors is given, however, by itemizing the vectors in the set it is a definite inconvenience to insist that all the vectors listed be distinct. The burden of counting the number of times a vector can appear in a relation is transferred to the index set. For each index in the index set, we require that a linear relation contain but one term corresponding to that index. Similarly, when we specify a set by itemizing the vectors in the set, we require that one and only one vector be listed for each index in the index set. But we allow the possibility that several indices may be used to identify the same vector. Thus the set {0%, ad, where = is linearly dependent, and any set with any vector listed at least twice is linearly dependent. To be precise, the concept of linear independence is a property of indexed sets and not a property of sets. In the example given above, the relation — = 0 involves two terms in the indexed set {oti I i e {l, 2}} while the set {0%, 0"} actually contains only one vector. We should refer to the linear dependence of an indexed set rather than the linear dependence of a set. The conventional terminology, which we are adopting, is inaccurate. This usage, however, is firmly rooted in tradition and, once understood, it is a convenience and not a source of diffculty. We speak of the linear dependence of a set, but the concept always refers to an indexed set. For a linearly independent indexed set, no vector can be listed twice; so in this case the inaccuracy of referring to a set rather than an indexed set is unimportant.

The concept of linear dependence and independence is used in essentially two ways. (l) If a set {at.} of vectors is known to be linearly dependent, there exists a non-trivial linear relation of the form i = O. (This relation is not unique, but that is usually incidental.) There is at least one

non-zero coefficient; let alc be non-zero. Then oq. =  that is one of the vectors of the set {0%.} is a linear combination of the others. (2) If a set {0%.} of vectors is known to be linearly independent and a linear relation = 0 is obtained, we can conclude that all a, = O. This seemingly trivial observation is surprisingly useful.

In Example (l) the zero vector is the polynomial with all coemcients equal to zero. Thus the set of monomials {l, x, } is a linearly independent set. The set {l, x, x2 , x2 + x + l} is linearly dependent since

2 — (x2 + + 1) = 0. In Pn of Example (2), any n + 1 polynomials form a linearly dependent set.

In R3 consider the vectors ö = (l, l, l)}. These four vectors are linearly dependent since + +  — 2ö = 0, yet any three of these four vectors are linearly independent.

Theorem 2.1. If is linearly dependent on {Pi} and each is linearly dependent on then is linearly dependent on

PROOF. From bißi and = E, Cijyj it follows that  bi(E, CiD'j) = bßij)yj. 

Theorem 2.2. A set of non-zero vectors {0%, 0", . . . } is linearly dependent if and only if some is a linear combination of the with j < k.

PROOF. Suppose the vectors {11, 04, . . . } are linearly dependent. Then there is a non-trivial linear relation among them; • apti = 0. Since a positive finite number of coemcients are non-zero, there is a last non-zero coemcient a/c. Furthermore, k 2 since 0. Thus — —a? 1 Y: ( ---av l

The converse is obvious. 

For any subset A of V the set of all linear combinations of vectors in A is called the set spanned by A, and we denote it by We also say that A spans It is a part of this definition that A c (A). We also agree that the empty set O spans the set consisting of the zero vector alone. It is readily apparent that if A c B, then (A) c (B).

In this notation Theorem 2.1 is equivalent to the statement: If A c (B) and B c then A c

Theorem 2.3. The set {0%.} of non-zero vectors is linearly independent if and only iffor each k, ooc @1, . . . , otk\_l). (To follow our definitions exactly,  the set spanned by {0%, . . . , oqc 1} should be denoted by . . . , oqc—l})•

2 Linear Independence and Linear Dependence

We shall use the symbol (0%, . . . , instead since it is simpler and there is no danger of ambiguity.)

PROOF. This is merely Theorem 2.2 in contrapositive form and stated in new notation. 

Theorem 2.4. If B and C are any subsets such that% c (C), then (B) c

PROOF. Set A = (B) in Theorem 2.1. Then B c (C) implies that (B) —



Theorem 2.5. If 0th e A is dependent on the other vectors in A, then (A) — 



PROOF. The assumption that is dependent on A — {otk} means that A c (A — {01k}). It then follows from Theorem 2.4 that (A) c (A — Wk}). The equality follows from the fact that the inclusion in the other direction is evident. 

Theorem 2.6. For any set C,

PROOF. Setting B = (C) in Theorem 2.4 we obtain Again, the inclusion in the other direction is obvious. 

Theorem 2.7. If a finite set A = {0(1, , ocn} spans V, then every linearly independent set contains at most n elements.

PROOF. Let B = {F . . . } be a linearly independent set. We shall successively replace the by the L, obtaining at each step a new n-element set that spans V. Thus, suppose that Ak = {61, . . . ,  , an} is an n-element set that spans V. (Our starting point, the hypothesis of the theorem, is the case k = 0.) Since Ak spans V, is dependent on AE. Thus the set {#1, . . .  , %} is linearly dependent. In any non-trivial relation that exists the non-zero coemcients cannot be confined to the L, for they are linearly independent. Thus one of the oq(i > k) is dependent on the others, and after reindexing {4+1, • • • , oc n} if necessary we may assume that it is oqc+l. By Theorem 2.5 the set A } also spans V.

If there were more than n elements in B, we would in this manner arrive at the spanning set A {F , L}. But then the dependence of ßn+l on An would contradict the assumed linear independence of B. Thus B contains at most n elements. 

Theorem 2.7 is stated in slightly different forms in various books. The essential feature of the proof is the step-by-step replacement of the vectors in one set by the vectors in the other. The theorem is known as the Steinitz replacement theorem.

EXERCISES

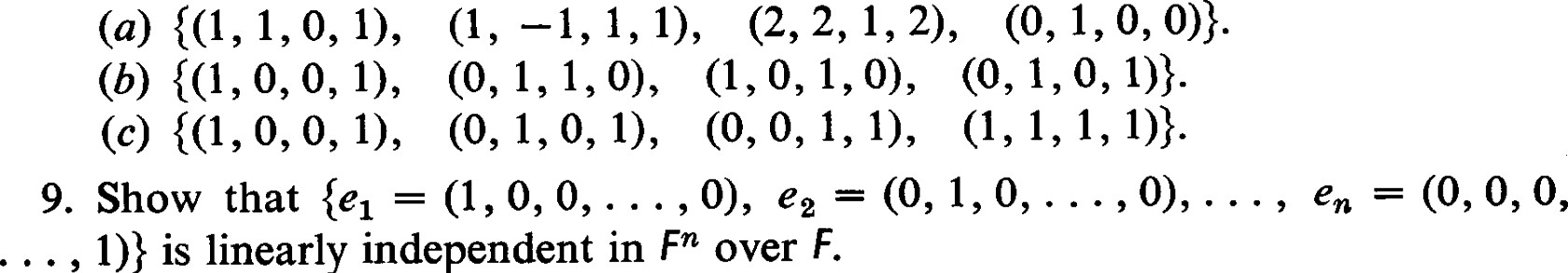
1. In the vector space P of Example (1) let PI(x) 

= x2 + — = — 1. Determine whether or not the set {Pi(æ), P2@), P3(æ), P4(x)} is linearly independent. If the set is linearly dependent, express one element as a linear combination of the others.



2

1. Determine P2(x), P3@), where the Pi(x) are the same polynomials as those defined in Exercise 1. (The set required is infinite, so that we cannot list all its elements. What is required is a description; for example, "all polynomials of a certain degree or less, all polynomials with certain kinds of coemcients," etc.)
2. A linearly independent set is said to be maximal if it is contained in no larger linearly independent set. In this definition the emphasis is on the concept of set inclusion and not on the number of elements in a set. In particular, the definition allows the possibility that two different maximal linearly independent sets might have different numbers of elements. Find all the maximal linearly independent subsets of the set given in Exercise 1. How many elements are in each of them ?
3. Show that no finite set spans P; that is, show that there is no maximal finite linearly independent subset of P. Why are these two statements equivalent ?
4. In Example (2) for n = 4, find a spanning set for P4. Find a minimal spanning set. Use Theorem 2.7 to show that no other spanning set has fewer elements.
5. In Example (1) or (2) show that {1 , x + 1, $2 + + 1, $3 + $2 + x + 1, + $3 + + + 1} is a linearly independent set.
6. In Example (1) show that the set of all polynomials divisible by x — I cannot span P.
7. Determine which of the following set in R4 are linearly independent over R.

1)} is linearly independent in Fn over F.

1. In Exercise 11 of Section 1 it was shown that we may consider the real numbers to be a vector space over the rational numbers. Show that {1, is a linearly independent set over the rationals. (This is equivalent to showing that N/ i is irrational.) Using this result show that {1, 3/1, N/S} is linearly independent.
2. Show that if one vector of a set is the zero vector, then the set is linearly dependent.
3. Show that if an indexed set of vectors has one vector listed twice, the set is linearly dependent.
4. Show that if a subset of S is linearly dependent, then S is linearly dependent.
5. Show that if a set S is linearly independent, then every subset of S is linearly independent.
6. Show that if the set A = {oc } is linearly independent and 61, , p} is linearly dependent, then is dependent on A.
7. Show that, if each of the vectors {P } is a linear combination of the vectors {ul, . . . , otn}, then {F } is linearly dependent.

3 1 Bases of Vector Spaces

Definition. A linearly independent set spanning a vector space V is called a basis or base (the plural is bases) of V.

 . . . } is a basis of V, by definition an e V can be written in the form E. a.cc.. The interesting thing aboUt a basis, as distinct from other spanning sets, is that the coeffcients are uniquely determined by oc. For suppose that we also have oc — bßi. Upon subtraction we get the linear relation (ai bi)oq = 0. Since {0%.} is a linearly independent set, ai = 0 and ai = bi for each i. A related fact is that a basis is a particularly emcient spanning set, as we shall see.

In Example (l) the vectors {oq = I i = 0, l , . . . } form a basis. We have already observed that this set is linearly independent, and it clearly spans the space of all polynomials. The space Pn has a basis with a finite number of elements; {1, c, $2 , . . . , 

The vector spaces in Examples (3), (4), (5), (6), and (7) do not have bases with a finite nurnber of elements.

In Example (8) every RTZ has a finite basis consisting of {0' ö (Here öij is the useful symbol known as the Kronecker delta.



By definition öi, = 0 if i # j and öii = I )

Theorem 3.1. If a vector space has one basis with a finite number of elements, then all other bases are finite and have the same number of elements.

PROOF. Let A be a basis with a finite number n of elements, and let B be any other basis. Since A spans V and B is linearly independent, by Theorem 2.7 the number m of element in B must be at most n. This shows that B is finite and m n. But then the roles of A and B can be interchanged to obtain the inequality in the other order so that m = n. C]

A vector space with a finite basis is called a finite dimensional vector space, and the number of elements in a basis is called the dimension of the space. Theorem 3.1 says that the dimension of a finite dimensional vector space is well defined. The vector space with just one element, the zero vector, has one linearly independent subset, the empty set. The empty set is also a spanning set and is therefore a basis of {0}. Thus {0} has dimension zero. There are very interesting vector spaces with infinite bases; for example, P of Example (l). Moreover, many of the theorems and proofs we give are also valid for infinite dimensional vector spaces. It is not our intention, however, to deal with infinite dimensional vector spaces as such, and whenever we speak of the dimension of a vector space without specifying whether it is finite or infinite dimensional we mean that the dimension is finite.

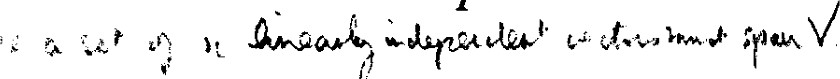
Among the examples we have discussed so far, each Pn and each Rn is n-dimensional. We have already given at least one basis for each. There are many others. The bases we have given happen to be conventional and convenient choices.

Theorem 3.2. Any n + I vectors in an n-dimensional vector space are linearly dependent.

PROOF. Their independence would contradict Theorem 2.7. 

We have already seen that the four vectors {u

 = (l, l , l)} form a linearly dependent set in R3 . Since R3 is 3-dimensional we see that this must be expected for any set containing at least four vectors from R3 . The next theorem shows that each subset of three is a basis.

Theorem 3.3. A set of n vectors in an n-dimensional vector space V is a basis if and only if it is linearly independent.

PROOF. The "only if" is part of the definition of a basis. Let A —

G} be a linearly independent set and let oc be any vector in V. Since {al, . . . , an, u} contains n + I elements it must be linearly dependent. Any non-trivial relation that exists must contain u with a non-zero coemcient, for if that coeffcient were zero the relation would amount to a relation in A. Thus is dependent on A. Hence A spans V and is a basis. C]

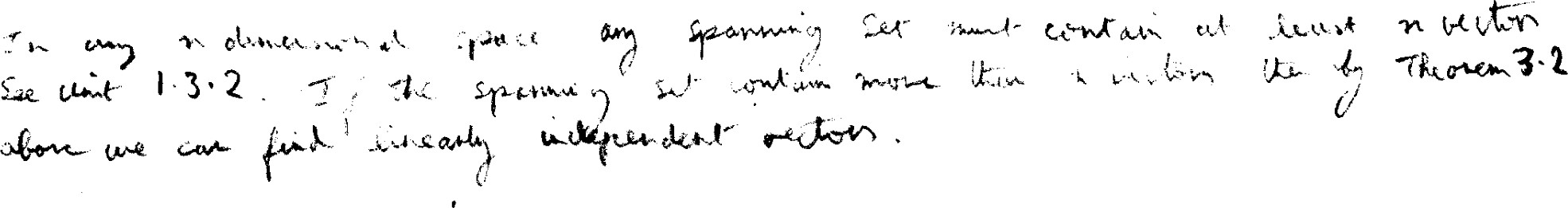
Theorem 3.4. A set of n vectors in an n-dimensional vector space V is a basis if and only if it spans V.

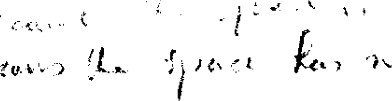
PROOF. The "only if" is part of the definition of a basis. If n vectors did span V and were linearly dependent, then (by Theorem 2.5) a proper subset would also span V, contrary to Theorem-2X-g 

We see that a basis is a maximal linearly independent set and a minimal spanning set. This idea is made explicit in the next two theorems.

Theorem 3.5. In a finite dimensional vector space, every spanning set contains a basis.

PROOF. Let B be a set spanning V. If V = {0}, then O c B is a basis of {0}. If V {0}, then B must contain at least one non-zero vector We now search for another vector in B which is not dependent on {0%}. We call this vector and search for another vector in B which is not dependent on the linearly independent set {WI, We continue in this way as long as we can, but the process must terminate as we cannot find more than n



4

linearly independent vectors in B. Thus suppose we have obtained the set WI, , m} with the property that every vector in B is linearly dependent on A. Then because of Theorem 2.1 the set A must also span V and it is a basis. 

To drop the assumption that the vector space is n-dimensional would change the complexion of Theorem 3.5 entirely. As it stands the theorem is interesting but minor, and not diffcult to prove. Without this assumption the theorem would assert that every vector space has a basis since every vector space is spanned by itself. Discussion of such a theorem is beyond the aims of this treatment of the subject of vector spaces.

Theorem 3.6. In a finite dimensional vector space any linearly independent set of vectors can be extended to a basis.

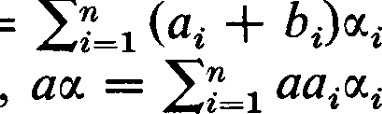
PROOF. Let A = {0%, , be a basis of V, and let B = {F be a linearly independent set (m n). The set {#1, . . . m' OCI' • spans V. If this set is linearly dependent (and it surely is if m > 0) then some element is a linear combination of the preceding elements (Theorem 2.2). This element cannot be one of the Pi's for then B would be linearly dependent. But then this can be removed to obtain a smaller set spanning V (Theorem 2.5). We continue in this way, discarding elements as long as we have a linearly dependent spanning set. At no stage do we discard one of the Pi's. Since our spanning set is finite this process must terminate with a basis containing B as a subset. D

Theorem 3.6 is one of the most frequently used theorems in the book. It is often used in the following way. A non-zero vector with a certain desired property is selected. Since the vector is non-zero, the set consisting of that vector alone is a linearly independent set. An application of Theorem 3.6 shows that there is a basis containing that vector. This is usually the first step of a proof by induction in which a basis is obtained for which all the vectors in the basis have the desired property. 

LetA = WI, , G} be an arbitrary basis of V, a vector space of dimension n over the field F. Let oc be any vector in V. Since A is a spanning set oc can be represented as a linear combination of the form cc a u . Since A is linearly independent this representation is unique, that is, the coeffcients at are uniquely determined by (for the given basis A). On the other hand, for each n-tuple (al, . . . , an) there is a vector in V of the form a.oc.. Thus there is a one-to-one correspondence between the vectors in V and the n-tuples (al, . . .

If = a m the scalar ai is called the i-th coordinate of u, and apti is called the i-th component of 0'. Generally, coordinates and components depend on the choice of the entire basis and cannot be determined from individual vectors in the basis. Because of the rather simple correspondence between coordinates and components there is a tendency to confuse them and to use both terms for both concepts. Since the intended meaning is usually clear from context, this is seldom a source of diffculty.

a corresponds to the n-tuple (a , an) and F = 21\_1 bioti corresponds to the n-tuple (b , bn), then + = corresponds to the n-tuple (al + b a + bn). Also corresponds to the n-tuple (aal, aan). Thus the definitions of vector addition and scalar multiplication among n-tuples defined in Example (9) correspond exactly to the corresponding operations in V among the vectors which they represent. When two sets of objects can be put into a one-to-one correspondence which preserves all significant relations among their elements, we say the two sets are isomorphic; that is, they have the same form. Using this terminology, we can say that every vector space of dimension n over a given field F is isomorphic to the n-dimensional coordinate space Fn . Two sets which are isomorphic differ in details which are not related to their internal structure. They are essentially the same. Furthermore, since two sets isomorphic to a third are isomorphic to each other we see that all n-dimensional vector spaces over the same field of scalars are isomorphic.



(a

i

+

The set of n-tuples together with the rules for addition and scalar multiplication forms a vector spaceinitsown right. However, when a basis is chosen in an abstract vector space V the correspondence described above establishes an isomorphism between V and Fn . In this context we consider Fn to be a representation of V. Because of the existence of this isomorphism a study of vector spaces could be confined to a study of coordinate spaces. However, the exact nature of the correspondence between V and Fn depends upon the choice of a basis in V. If another basis were chosen in V a correspondence between the e V and the n-tuples would exist as before, but the correspondence would be quite different. We choose to regard the vector space V and the vectors in V as the basic concepts and their representation by n-tuples as a tool for computation and convenience. There are two important benefits from this viewpoint. Since we are free to choose the basis we can try to choose a coordinatization for which the computations are particularly simple or for which some fact that we wish to demonstrate is particularly evident. In fact, the choice of a basis and the consequences of a change in basis is the central theme of matrix theory. In addition, this distinction between a vector and its representation removes the confusion that always occurs when we define a vector as an n-tuple and then use another n-tuple to represent it.

Only the most elementary types of calculations can be carried out in the abstract. Elaborate or complicated calculations usually require the introduction of a representing coordinate space. In particular, this will be required extensively in the exercises in this text. But the introduction of coordinates can result in confusions that are diffcult to clarify without extensive verbal description or awkward notation. Since we wish to avoid cumbersome notation and keep descriptive material at a minimum in the exercises, it is helpful to spend some time clarifying conventional notations and circumlocutions that will appear in the exercises.

The introduction of a coordinate representation for V involves the selection of a basis WI, . , n} for V. With this choice is represented by (l, 0, , O), is represented by (0, l, 0, , 0), etc. While it may be necessary to find a basis with certain desired properties the basis that is introduced at first is arbitrary and serves only to express whatever problem we face in a form suitable for computation. Accordingly, it is customary to suppress specific reference to the basis given initially. In this context it is customary to speak of "the vector (al, a2, . . . , an)" rather than "the vector ot whose representation with respect to the given basis {al, . . . , In} is (a a , an)." Such short-cuts may be disgracefully inexact, but they are so common that we must learn how to interpret them.

For example, let V be a two-dimensional vector space over R. Let A — WI, u2} be the selected basis. If — + and ß2 = --11 + then B = {#1, is also a basis of V. With the convention discussed above we would identify with (1, 0), with (0, l), with (l, l), and with ( l, 1). Thus, we would refer to the basis B = {(1, l), (—1, l)}. Since oti — 1 — 2 2, has the representation (b, —l) with respect to the basis B. If we are not careful we can end up by saying that "(l, 0) is represented by



EXERCISES

To show that a given set is a basis by direct appeal to the definition means that we must show the set is linearly independent and that it spans V. In any given situation, however, the task is very much simpler. Since V is n-dimensional a proposed basis must have n elements. Whether this is the case can be told at a glance. In view of Theorems 3.3 and 3.4 if a set has n elements, to show that it is a basis it sumces to show either that it spans V or that it is linearly independent.

1. In R3 show that {(1, 1, O), (l , 0, 1), ((), 1, 1)} is a basis by showing that it is linearly independent.
2. Show that {(1, 1, O), (1, O, 1), (O, 1, 1)} is a basis by showing that 1, O),

(1, O, 1), (O, l, 1)) contains (1, O, O), (0, 1, O) and (0, O, l). Why does this sumce?

1. In R4 let A = 1, O, 0), (0, O, 1, 1), (1, O, 1, 0), (0, 1, O, be a basis

(is it?) and let B = {(1 2 , , —1)} be a linearly independent set (is it ?). Extend B to a basis of R4. (There are many ways to extend B to a basis. It is intended here that the student carry out the steps of the proof of Theorem 3.6 for this particular case.)

1. Find a basis of R4 containing the vector (1, 2, 3, 4). (This is another even simpler application of the proof of Theorem 3.6. This, however, is one of the most important applications of this theorem, to find a basis containing a particular vector.)
2. Show that a maximal linearly independent set is a basis.
3. Show that a minimal spanning set is a basis.

4 1 Subspaces

Definition. A subspace W of a vector space V is a non-empty subset of V which is itself a vector space with respect to the operations of addition and scalar multiplication defined in V. In particular, the subspace must be a vector space over the same field F.

The first problem that must be settled is the problem of determining the conditions under which a subset W is in fact a subspace. It should be clear that axioms A2, AS, B2, B3, B4, and B5 need not be checked as they are valid in any subset of V. The most innocuous conditions seem to be Al and Bl but it is precisely these conditions that must be checked. If Bl holds for a non-empty subset W, there is an oc e W so that Oot = 0 e W. Also, for each = —u e W. Thus A 3 and A4 follow from Bl in any nonempty subset of a vector space and it is sumcient to check that W is nonempty and closed under addition and scalar multiplication.

The two closure conditions can be combined into one statement: if u, e W and a, b e F, then au + bß e W. This may seem to be a small change, but it is a very convenient form of the conditions. It is also equivalent

to the statement that all linear combinations of elements in W are also in W; that is, < W) = W. It follows directly from this statement that for any subset A, (A) is a subspace. Thus, instead of speaking of the subset spanned by A, we speak of the subspace spanned by A.

Every vector space V has V and the zero space {0} as subspaces. As a rule we are interested in subspaces other than these and {o distinguish them we call the subspaces other than V and {0} proper subspaces. In addition, if W is a subspace we designate subspaces of W other than W and {0} as proper subspaces of W.

In Examples (l) and (2) we can take a fixed finite set {c x of elements of F and define W to be the set of all polynomials such that P (Xl) = p(X2) — = p(xm) = O. To show that W is a subspace it is sumcient to show that the sum of two polynomials which vanish at the also vanishes at the Xi, and the product of a scalar and a polynomial vanishing at the also vanishes at the Xi. What is the situation in Pn if m > n? Similar subspaces can be defined in examples (3), (4), (5), (6), and

The space Pm is a subspace of P, and also a subspace of Pn for m n. In Rn , for each m, O m < n, the set of all = (a a . . . , an) such that al = a2 =  = 0 is a subspace of Rn . This subspace is proper if 0 < m < n.

Notice that the set of all n-tuples of rational numbers is a subset of Rn and it is a vector space over the rational numbers, but it is not a subspace of Rn since it is not a vector space over the real numbers. Why?

Theorem 4.1. The intersection of any collection of subspaces is a subspace. PROOF. Let Wg •.g GM be an indexed collection of subspaces of V. n GMWg is not empty since it contains O. Let u, e ngeMWg and a, b e F. Then u, e wg for each e M. Since wg is a subspace au + bß e wu for each e M, and hence am + bß e . Thus mg GMWg is a subspace. 

Let A be any subset of V, not necessarily a subspace. There exist subspaces W c V which contain A; in fact, V is one of them. The intersection W of all such subspaces is a subspace containing A. It is the smallest subspace containing A.

Theorem 4.2. For any A c A c WVW = that is, the smallest subspace containing A is exactly the subspace spanned by A.

PROOF. Since n A c w wg is a subspace containing A, it contains all linear combinations of elements of A. Thus (A) c n W . On the other hand (A) is a subspace containing A, that is, (A) is one of the wg and hence n W c Thus n W =

WI + W2 is defined to be the set of all vectors of the form + where G WI and e W2.

Theorem 4.3. If WI and W2 are subspaces of V, then WI + W2 isa subspace

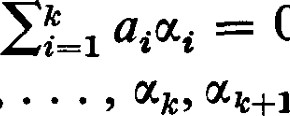
PROOF. If = OCI + e WI + W2, = PI + WI + W2, and a, b e F, then acc + bß = + + b(ßl + 2 ) = (aul + bßl) + (au2 + bß2) e WI + W2. Thus WI + W2 is a subspace. 

Theorem 4.4. WI + W2 is the smallest subspace containing both WI and W2,• that is, WI + W2 = (WI u WD. If Al spans WI and A2 spans W2, then Al U A2 spans WI + W2.

PROOF. Since 0 e WI, W2 C WI + W2. Similarly, WI C WI + W2. Since WI + W2 is a subspace containing WI U W2, (WI U W2) c WI + W2. For any e WI + W2, oc can be written in the form oc = + where and W2. Then c U WO and U WD. Since < WI U WD is a subspace, — + U WO. Thus WI + WI u WD.

The second part of the theorem now follows directly. WI = (Al) c (Al u AD and W2 = <A2) c (Al u AD so that WI u W2 c (Al u AD c < WI U WD, and hence (WI U W2) = (Al U A2). 

Theorem 4.5. A subspace W of an n-dimensional vector space V is a finite dimensional vector space of dimension m n.

PROOF. If W = {O}, then W is 0-dimensional. Otherwise, there is a nonzero vector e W. If (WI) = W, Wis I-dimensional. Otherwise, there is an  in W. We continue in this fashion as long as possible. Suppose we have obtained the linearly independent set {a , otk} and that it does not span W. Then there exists an e W, (0%, . . . , Wk). In a linear relation of the form = 0 we could not have 0 for then  e (0%, . . . , Wk). But then the relation reduces to the form Since {0%, . . . , uk} is linearly independent, all ai = O. Thus is linearly independent. In general, any linearly independent set in W that does not span W can be expanded into a larger linearly independent set in W. This process cannot go on indefinitely for in that event we would obtain more than n linearly independent vectors in V. Thus there exists an m such that oc ) = W. It is clear that m n. 



.



Theorem 4.6. Given any subspace W of dimension m in an n-dimensional vector space V, there exists a basis {0'1, } of V such that oc } is a basis of W.

PROOF. By the previous theorem we see that W has a basis VI, . . . , um} This set is also linearly independent when considered in V, and hence by Theorem 3.6 it can be extended to a basis of V. 

Theorem 4.7. If two subspaces U and W of a vector space V have the same finite dimension and U c W, then U = W.

PROOF. By the previous theorem there exists a basis of U which can be extended to a basis of W. But since dim U = dim W, the basis of W can have no more elements than does the basis of U. This means a basis of U is also a basis of W; that is, U = W. 

Theorem 4.8. If WI and W2 are any two subspaces of a finite dimensional vector space V, then dim (WI + W2) = dim WI + dim W2 — dim (WI n WD.

PROOF. Let {0%, } be a basis of WI n W2. This basis can be extended to a basis {011, . . . , ßs} of WI and also to a basis  71, , yt} of W2. It is clear that {0%, . . . , 1,

, yt} spans WI + W2; we wish to show that this set is linearly independent.

Suppose + bißj + = 0 is a linear relation. Then --2k Ck)'k. The left side is in WI and the right side is in W2, and hence both are in WI n W2. Each side is then expressible as a linear combination of the {occ.}. Since any representation of an element as a linear combination of the {0%, . . . , G, 1, . . . , ßs} is unique, this means that

|

— 0 for all j. By a symmetric argument we see that all c = O. Finally, this means that i apt,. = O from which it follows that all ai = o. This shows that the spanning set {al, . . .  , yt} is linearly independent and a basis of WI + W2. Thus dim (WI + W2) = r + s + t \_ (r +•s) + (r + t) — r = dim WI + dim W2 — dim (WI n WD. 

As an example, consider in R3 the subspaces WI = 0, 2), (l, 2, 2)) and W2 = 1, 0), (0, l, 1)). Both subspaces are of dimension 2. Since WI c WI + W2 c R3 we see that 2 dim (WI + WD 3. Because of Theorem 4.8 this implies that 1 dim (WI n W2) < 2. In more familiar terms, WI and W2 are planes in a 3-dimensional space. Since both planes contain the origin, they do intersect. Their intersection is either a line or, in case they coincide, a plane. The first problem is to find a basis for WI n W2. Any e WI n W2 must be expressible in the forms = a(l, O, 2) +

= c(l, 1, O) + d(0, l, l). This leads to the three equations:

2b = c + d



These equations have the solutions b , = —2a, d = —4a. Thus  = a(l, O, 2) — 3a(l, 2, 2) = , —6, —4). As a check we also have  = —2a(l, 1, 0) — 4a(0, 1, 1) = , —6, —4). We have determined that {(1, 3, 2)} is a basis of WI n W2. Also {(1, 3, 2), (l, 0, 2)} is a basis of WI and {(1, 3, 2), (l, l, 0)} is a basis of W2.

We are all familiar with the theorem from solid geometry to the effect that two non-parallel planes intersect in a line, and the example above is an illustration of that theorem. In spaces of dimension higher than 3, however, it is possible for two subspaces of dimension 2 to have but one point in common. For example, in R4 the subspaces WI = 0, O, O), (0, l, 0, 0)) and W2 = O, l, O), (0, 0, O, 1)) are each 2-dimensional and WI n

Those cases in which dim (WI n WD = 0 deserve special mention. If WI n W2 = {O} we say that the sum WI + W2 is direct: WI + W2 is a direct sum of WI and W2. To indicate that a sum is direct we use the notation, WI O W2. For e WI O W2 there exist e WI and e W2 such that  = + u2. This much is true for any sum of two subspaces. If the sum is direct, however, and are uniquely determined by a. For if oc = + = oc'l + 0('2, then — Since the left side is in WI and the right side is in W2, both are in WI n W2. But this means — 1 = 0 and oc,2 — = 0; that is, the decomposition of into a sum of an element in WI plus an element in W2 is unique. If V is the direct sum of WI and W2, we say that WI and W2 are complementary and that W2 is a complementary subspace of WI, or a complement of WI.



1

2

The notion of a direct sum can be extended to a sum of any finite number of subspaces. The sum WI + • • • + Wk is said to be direct if for each i, Wi n (i. # . W,) = {0}. If the sum of several subspaces is direct, we use the notation WI O W2 0 • • • O Wk. In this case, too, e WI 0 • • • C Wk can be expressed uniquely in the form • Ott. , O'i e Wi.

Theorem 4.9. If W is a subspace of V there exists a subspace W' such that



PROOF. Let {al, . um} be a basis of W. Extend this linearly independent set to a basis {0%, . . . } of V. Let W' be the subspace spanned by {um+1, , an}. Clearly, W n W' = {0} and the sum V = W + W' is direct. 

Thus every subspace of a finite dimensional vector space has a complementary subspace. The complement is not unique, however. If for W there exists a subspace W' such that V = WO W', we say that W is a direct summand of V.

Theorem 4.10. For a sum of several subspaces of a finite dimensional vector space to be direct it is necessary and suffcient that dim (WI + • • + Wk) = dim WI + • • • + dim Wk.

PROOF. This is an immediate consequence of Theorem 4.8 and the principle of mathematical induction. D

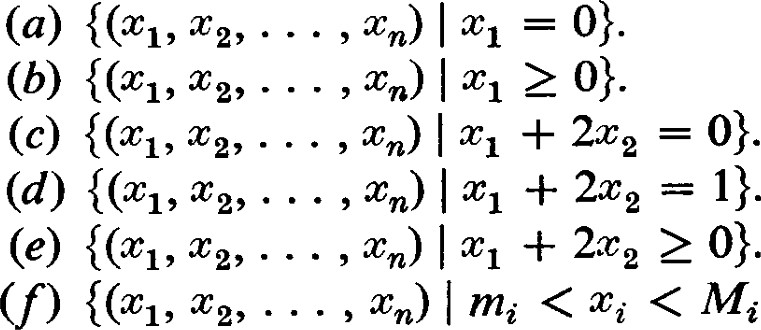
EXERCISES

1. Let P be the space of all polynomials with real coemcients. Determine which of the following subsets of P are subspaces. (a) {p@) Ip(l) = O}.
   1. {p@) I constant term ofp@) = 0}.
   2. {p(x) I degree of p(x)
   3. {p(x) I degree ofp@) 3}.

(Strictly speaking, the zero polynomial does not have a degree associated with it. It is sometimes convenient to agree that the zero polynomial has degree less than any integer, positive or negative. With this convention the zero polynomial is included in the set described above, and it is not necessary to add a separate comment to include it.)

* 1. {Ax) I degree ofp@) is even} u {O}.

1. Determine which of the following subsets of Rn are subspaces.

< Mi: i = 1, 2, are constants}.



n where the mi and Mi

| 25

1. What is the essential difference between the condition used to define the subset in (c) of Exercise 2 and the condition used in (d)? Is the lack of a non-zero constant term important in (c) ?
2. What is the essential difference between the condition used to define the subset in (c) of Exercise 2 and the condition used in (e)? What, in general, are the differences between the conditions in (a), (c), and (g) and those in (b), (e), and (f)?
3. Show that {(1, 1, O, O), (1, O, 1, 1)} and {(2, , —1, —1)} span the same subspace of R4.
4. Let W be the subspace of R5 spanned by {(1, 1, 1, 1, 1), (1, O, 1, O, 1),



Find a basis for W and the dimension of W.

1. Show that {(1, -1, 2, —3), (1, 1, 2, 0), (3, —1, 6, and O, 1, 0), (O, 2, 0, 3)} do not span the same subspace.
2. Let W = 2, 3, 6), (4, 3, 6), (5, 1, 6, 12)) and  —1, 1, 1), (2, —1, 4, 5)) be subspaces of R4. Find bases for WI W2and WI + W2. Extend the basis of WI W2 to a basis of WI, and extend the basis of WI W2 to a basis of W2. From these bases obtain a basis of WI + W2.
3. Let P be the space of all polynomials with real coemcients, and let WI — {p@) I p(l) = O} and W2 = {p@) Ip(2) = O}. Determine WI W2 and WI + W2. (These spaces are infinite dimensional and the student is not expected to find bases for these subspaces. What is expected is a simple criterion or description of these subspaces.)
4. We have already seen (Section 1, Exercise 11) that the real numbers form a vector space over the rationals. Show that {1, 8/5} and {1 — A/5, 1 + A/i} span the same subspace.
5. Show that if WI and W2 are subspaces, then WI u W2 is not a subspace unless one is a subspace of the other.
6. Show that the set of all vectors (Xl, x2, 4, 4) e R4 satisfying the equations



2 — — .34 = o

is a subspace of R4. Find a basis for this subspace. (Hint: Solve the equations for and in terms of and x4. Then specify various values for and to obtain as many linearly independent vectors as are needed.)

1. Let S, T, and T\* be three subspaces of V (of finite dimension) for which (a) S T = S n T\* , (b) S + T = S + , (c) T c T\*. Show that T = T\*.
2. Show by example that it is possible to have S O T = S O T\* without having
3. If V = WI O W2 and W is any subspace of V such that WI c W, show that W = (W n WI) C (W n WD. Show by an example that the condition WI c W (or W2 c W) is necessary.