

K. W. Gruenberg

A. J. Weir

Linear Geometry

2nd Edition



K. W. Gruenberg

A. J. Weir

Linear Geometry

2nd Edition



Springer-Verlag

New York Heidelberg Berlin

K. W. Gruenberg

Department of Pure Mathematics
Queen Mary College
University of London
England

A. J. Weir

School of Mathematical
and Physical Sciences
University of Sussex
England

Editorial Board

P. R. Halmos

Managing Editor
Department of Mathematics
University of California
Santa Barbara, California 93106

F. W. Gehring

Department of Mathematics
University of Michigan
Ann Arbor, Michigan 48104

C. C. Moore

Department of Mathematics
University of California at Berkeley
Berkeley, California 94720

AMS Subject Classification: 50D40

Library of Congress Cataloging in Publication Data

Gruenberg, Karl W.
Linear geometry.

(Graduate texts in mathematics ; 49)

1. Geometry, Algebraic. 2. Algebras, Linear.

I. Weir, Alan J., joint author. II. Title.

QA564.G72 1977 516'.35 76-27693

All rights reserved.

No part of this book may be translated or reproduced in any form without written permission from Springer-Verlag.

© 1967 by K. W. Gruenberg and A. J. Weir.

© 1977 by Springer-Verlag, New York Inc.

First edition published 1967 by D. Van Nostrand Company.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-90227-9 Springer-Verlag New York

ISBN 3-540-90227-9 Springer-Verlag Berlin Heidelberg

Preface

This is essentially a book on linear algebra. But the approach is somewhat unusual in that we emphasise throughout the geometric aspect of the subject. The material is suitable for a course on linear algebra for mathematics majors at North American Universities in their junior or senior year and at British Universities in their second or third year. However, in view of the structure of undergraduate courses in the United States, it is very possible that, at many institutions, the text may be found more suitable at the beginning graduate level.

The book has two aims: to provide a basic course in linear algebra up to, and including, modules over a principal ideal domain; and to explain in rigorous language the intuitively familiar concepts of euclidean, affine, and projective geometry and the relations between them. It is increasingly recognised that linear algebra should be approached from a geometric point of view. This applies not only to mathematics majors but also to mathematically-oriented natural scientists and engineers.

The material in this book has been taught for many years at Queen Mary College in the University of London and one of us has used portions of it at the University of Michigan and at Cornell University. It can be covered adequately in a full one-year course. But suitable parts can also be used for one-semester courses with either a geometric or a purely algebraic flavor. We shall give below explicit and detailed suggestions on how this can be done (in the "Guide to the Reader").

The first chapter contains in fairly concise form the definition and most elementary properties of a vector space. Chapter 2 then defines affine and projective geometries in terms of vector spaces and establishes explicitly the connexion between these two types of geometry. In Chapter 3, the idea of isomorphism is carried over from vector spaces to affine and projective geometries. In particular, we include a simple proof of the basic theorem of projective geometry, in §3.5. This chapter is also the one in which systems of linear equations make their first appearance (§3.3). They reappear in increasingly sophisticated forms in §§4.5 and 4.6.

Linear algebra proper is continued in Chapter 4 with the usual topics centred on linear mappings. In this chapter the important concept of duality in vector spaces is linked to the idea of dual geometries. In our treatment of bilinear forms in Chapter 5 we take the theory up to, and including, the classification of symmetric forms over the complex and real fields. The geometric significance of bilinear forms in terms of quadrics is

taken up in §§5.5–5.7. Chapter 6 presents the elementary facts about euclidean spaces (i.e., real vector spaces with a positive definite symmetric form) and includes the simultaneous reduction theory of a pair of symmetric forms one of which is positive definite (§6.3); as well as the structure of orthogonal transformations (§6.4). The final chapter gives the structure of modules over a polynomial ring (with coefficients in a field) and more generally over a principal ideal domain. This leads naturally to the solution of the similarity problem for complex matrices and the classification of collineations.

We presuppose very little mathematical knowledge at the outset. But the student will find that the style changes to keep pace with his growing mathematical maturity. We certainly do not expect this book to be read in mathematical isolation. In fact, we have found that the material can be taught most successfully if it is allowed to interact with a course on “abstract algebra”.

At appropriate places in the text we have inserted remarks pointing the way to further developments. But there are many more places where the teacher himself may lead off in new directions. We mention some examples. §3.6 is an obvious place at which to begin a further study of group theory (and also incidentally, to introduce exact sequences). Chapter 6 leads naturally to elementary topology and infinite-dimensional Hilbert spaces. Our notational use of \mathcal{A} and \mathcal{P} (from Chapter 2 onwards) is properly functorial and students should have their attention drawn to these examples of functors. The definition of projective geometry does not mention partially ordered sets or lattices but these concepts are there in all but name.

We have taken the opportunity of this new edition to include alternative proofs of some basic results (notably in §§5.2, 5.3) and to illustrate many of the main geometric results by means of diagrams. Of course diagrams are most helpful if drawn by the reader, but we hope that the ones given in the text will help to motivate the results and that our hints on the drawing of projective diagrams will encourage the reader to supply his own.

There are over 250 exercises. Very few of these are routine in nature. On the contrary, we have tried to make the exercises shed further light on the subject matter and to carry supplementary information. As a result, they range from the trivial to the very difficult. We have thought it worthwhile to add an appendix containing outline solutions to the more difficult exercises.

We are grateful to all our friends who helped (wittingly and unwittingly) in the writing of this book. Our thanks go also to Paul Halmos for his continuing interest in the book, an interest which has now resulted in the appearance of this new edition.

K. W. Gruenberg
A. J. Weir

April 1977

Guide to the Reader

This book can be used for linear algebra courses involving varying amounts of geometry. Apart from the obvious use of the whole book as a one year course on algebra and linear geometry, here are some other suggestions.

(A) *One semester course in basic linear algebra*

All of Chapter I.

§2.1 for the definition of coset and dimension of coset.

§3.3.

Chapter IV, but omitting §§4.2, 4.7, 4.8.

(B) *One semester course in linear geometry*

Prerequisite: (A) above or any standard introduction to linear algebra.

All of Chapter II.

§§3.1–3.4.

Then either (B₁) or (B₂) (or, of course, both if time allows):

(B₁) §§4.7, 4.8.

Chapter V up to the end of Proposition 12 (p. 118).

(B₂) §§5.1–5.4 (see Note 1, below; also Notes 2, 3, for saving time);

§5.6 but omitting Proposition 10; §5.7 to the end of Proposition 12.

§§6.1, 6.3, 6.4 to the “orientation” paragraph on p. 144.

(C) *One year course in linear algebra*

The material in (A) above.

Chapter V but omitting §§5.5–5.7.

Chapter VI but *omitting* the following: §6.1 from mid p. 127 (where distance on a coset is defined); §6.2; §6.3 from Theorem 2 onwards;

Guide to the Reader

§6.4 from mid p. 144 (where similarity classes of distances are defined).

Chapter VII, but omitting §7.6.

Notes

1. §§5.1–5.3 can be read without reference to dual spaces. In particular, the first proof of Proposition 4 (p. 93) and the first proof of Lemma 4 (p. 97) are then the ones to read.
2. The reader who is only interested in symmetric or skew-symmetric bilinear forms can ignore the distinction between \perp and \top . This will simplify parts of §5.2, and in §5.3 the notion of orthosymmetry and Proposition 6 can then be omitted.
3. In §5.3, the question of characteristic 2 arises naturally when skew-symmetric forms are discussed. But the reader who wishes to assume $2 \neq 0$ in the fields he is using can omit the latter part of §5.3.

Guide to the Reader	ix
Chapter I	
Vector Spaces	1
1.1 Sets	1
1.2 Groups, Fields and Vector Spaces	3
1.3 Subspaces	6
1.4 Dimension	8
1.5 The Ground Field	12
Chapter II	
Affine and Projective Geometry	15
2.1 Affine Geometries	15
2.2 Affine Propositions of Incidence	17
2.3 Affine Isomorphisms	20
2.4 Homogeneous Vectors	22
2.5 Projective Geometries	29
2.6 The Embedding of Affine Geometry in Projective Geometry	32
2.7 The Fundamental Incidence Theorems of Projective Geometry	38
Chapter III	
Isomorphisms	42
3.1 Affinities	42
3.2 Projectivities	44
3.3 Linear Equations	49
3.4 Affine and Projective Isomorphisms	52
3.5 Semi-linear Isomorphisms	54
3.6 Groups of Automorphisms	58
3.7 Central Collineations	62

Chapter IV	
Linear Mappings	66
4.1 Elementary Properties of Linear Mappings	66
4.2 Degenerate Affinities and Projectivities	70
4.3 Matrices	71
4.4 The Rank of a Linear Mapping	75
4.5 Linear Equations	79
4.6 Dual Spaces	80
4.7 Dualities	83
4.8 Dual Geometries	86
Chapter V	
Bilinear Forms	89
5.1 Elementary Properties of Bilinear Forms	89
5.2 Orthogonality	93
5.3 Symmetric and Alternating Bilinear Forms	97
5.4 Structure Theorems	102
5.5 Correlations	110
5.6 Projective Quadrics	111
5.7 Affine Quadrics	115
5.8 Sesquilinear Forms	120
Chapter VI	
Euclidean Geometry	125
6.1 Distances and Euclidean Geometries	125
6.2 Similarity Euclidean Geometries	130
6.3 Euclidean Quadrics	134
6.4 Euclidean Automorphisms	140
6.5 Hilbert Spaces	146
Chapter VII	
Modules	149
7.1 Rings and Modules	149
7.2 Submodules and Homomorphisms	153
7.3 Direct Decompositions	155
7.4 Equivalence of Matrices over $F[X]$	163
7.5 Similarity of Matrices over F	166
7.6 Classification of Collineations	170
Solutions	175
List of Symbols	188
Bibliography	191
Index	193

CHAPTER I

Vector Spaces

There are at least two methods of defining the basic notions of geometry. The one which appears more natural at first sight, and which is in many ways more satisfactory from the logical point of view, is the so called *synthetic* approach. This begins by postulating objects such as points, lines and planes and builds up the whole system of geometry from certain *axioms* relating these objects. In order to progress beyond a few trivial theorems, however, there must be sufficient axioms. Unfortunately, it is difficult to foresee the kind of axioms which are required in order to be able to prove what one regards as “fundamental” theorems (such as Pappus’ Theorem and Desargues’ Theorem). This method is very difficult as an introduction to the subject.

The second approach is to base the geometry on an *algebraic* foundation. We favor this approach since it allows us to “build in” enough axioms about our geometry at the outset. The axioms of the synthetic geometry now become theorems in our algebraic geometry. Moreover, the interdependence of the algebraic and geometric ideas will be seen to enrich both disciplines and to throw light on them both. (For an introduction to the synthetic approach the reader may consult [4], [9].)

1.1 Sets

We shall not define the basic notion of *set* (or collection, or aggregate) which we regard as intuitive. Further, we shall assume that the reader is familiar with the simplest properties of the set \mathbf{Z} of integers (positive, negative and zero), the set \mathbf{Q} of rational numbers, the set \mathbf{R} of real numbers, the set \mathbf{C} of complex numbers and the set \mathbf{F}_p of integers modulo a prime p .

As a shorthand for the statement “ x is an element of the set S ” we shall write $x \in S$. If S and T are two sets with the property that every element of S is an element of T , we write $S \subset T$ and say “ S is contained in T ” or that “ S is a subset of T ”; equivalently, we also write $T \supset S$ and say “ T contains S ”. Note that according to this definition $S \subset S$. We

shall say that the sets S and T are *equal*, and write $S = T$, if $S \subset T$ and $S \supset T$. If the set S consists of the elements x, y, \dots then we write $S = \{x, y, \dots\}$. Thus, for example, $x \in S$ if, and only if, $\{x\} \subset S$. Strokes through symbols usually give the negative: for example, \neq , \nsubset , \notin stand for, respectively, “is not equal to”, “is not contained in”, “is not an element of”.

If S and T are given sets then a *mapping* (or *function*) f of S into T is a rule which associates to each element s in S a unique element sf in T . In these circumstances we shall often write $f: S \rightarrow T$ or $f: s \rightarrow sf$. The element sf is called the *image* of the element s under f . (It is often also written as $f(s)$ or s' or f_s , whichever is the most convenient notation for the purpose at hand.) The set of all sf as s varies in S is the *image* of S under f , or simply the *image* of f , and is denoted by Sf . If $Sf = T$ then we say that f is a mapping of S *onto* T ; if the images under f of any two distinct elements of S are distinct elements of T , then f is a *one-one* mapping. (The above definition of mapping seems to involve the undefined notion of “rule”. A more sophisticated definition can be given in terms of the “graph” of f which is the set of all ordered pairs (s, sf) for s in S . The definition can thus be thrown back on the basic concept of set.)

The notation sf for the image is particularly suitable if mappings are to be combined; more specifically, if f is a mapping of S into T and if g is a mapping of T into U , then the *product* fg is the mapping of S into U defined by the equation $s(fg) = (sf)g$. In other words fg stands for “apply first f , then g ”. If one uses the functional notation, then $(fg)(s) = g(f(s))$.

On the other hand, there is a situation in which the *index notation* f_s for the image is better than sf . This occurs when we are interested in “listing” the elements of the image of S under f . It is then usual to refer to S as the *set of indices*, to call f_s the *s-term* of f , to write f in the alternative form $(f_s)_{s \in S}$ and to call f a *family* rather than a mapping. As s runs through the set S of indices the terms f_s run through the image of S under f . It is important to realize that some of the terms will be repeated unless the mapping f is one-one.

If an arbitrary non-empty set S is given then we can always “list” the elements of S by using the identity mapping 1_S , which sends each element of S into itself.

We mention two familiar examples of this notation:

1. If I is the set of all positive integers, then $(f_i)_{i \in I}$ is a *sequence*.
2. If I is the finite set $\{1, 2, \dots, n\}$, then $(f_i)_{i \in I}$ is an *n-tuple*.

If we take note of the natural ordering of the integers, then the sequences and n -tuples above are called *ordered sequences* and *ordered n-tuples* respectively.

DEFINITION. Suppose that $(M_i)_{i \in I}$ is a family where each M_i is itself a set. We define the *intersection* $\cap(M_i; i \in I)$ of this family to be the set of all elements which belong to every M_i ($i \in I$); also, the *union* $\cup(M_i; i \in I)$ is the set of all elements which belong to at least one of the sets M_i ($i \in I$). Observe that, for this definition to make sense, I cannot be empty.

The intersection and union of the sets M_1, \dots, M_n are usually denoted by $M_1 \cap \dots \cap M_n$ and $M_1 \cup \dots \cup M_n$, respectively.

If we are simply given a (non-empty) set S whose elements M are sets, then we index S by means of the identity mapping and use the above definition. The intersection $\cap(M: M \in S)$ is therefore the set of all elements which belong to every set M in S and the union $\cup(M: M \in S)$ is the set of all elements which belong to at least one set M in S .

EXERCISES

1. Let S, T be sets, f a mapping of S into T , g a mapping of T into S , and denote by $1_S, 1_T$, respectively, the identity mappings on S and T . Prove that (i) $fg = 1_S$ implies that f is one-one; and (ii) $gf = 1_T$ implies that f is onto T . Show that if (i) and (ii) hold, then g is uniquely determined by f . (In this case we write $g = f^{-1}$ and call g the *inverse* of f .)
2. The population on an island is greater than the number of hairs on the head of any one inhabitant. Show that if nobody is bald then at least two people have the same number of hairs on their heads.
3. If f, g, h are mappings of S into T , T into U , U into V , respectively, show that $(fg)h = f(gh)$.

1.2 Groups, Fields and Vector Spaces

We assume that the reader is to some extent familiar with the concept of a vector in three dimensional euclidean space. He will know that any two vectors can be added to give another vector and any vector can be multiplied by a real number (or scalar) to give yet another vector. The primary object of this book is to generalize these ideas and to study many of their geometrical properties. In order to axiomatize the addition of vectors we introduce the concept of a *group*, and in order to generalize the notion of scalar we define a *general field*. The reader who is meeting these abstract ideas for the first time may find it helpful at the beginning to replace the general field F in our definition of a vector space by the familiar field \mathbf{R} of real numbers and to accept the other axioms as a minimum set of sensible rules which allow the usual manipulations with vectors and scalars. The subsequent sections have more geometric and algebraic motivation and are not likely to cause the same difficulty.

DEFINITION. Let G be a set together with a rule (called *multiplication*) which associates to any two elements a, b in G a further element ab in G (called the *product* of a and b). If the following axioms are satisfied then G is called a *group*:

G.1. $(ab)c = a(bc)$ for all a, b, c in G ;

G.2. there exists a unique element 1 in G (called the *identity*) such that $a1 = 1a = a$ for all a in G ;

G.3. for each element a in G there exists a unique element a^{-1} in G (called the *inverse* of a) such that $aa^{-1} = a^{-1}a = 1$.

A subset of G which is itself a group (with respect to the same rule of multiplication as G) is called a *subgroup* of G . Note that, in particular, G is a subgroup of G and so also is $\{1\}$, called the *trivial subgroup* of G .

We shall see that the order of the elements a, b in the product ab is important (see exercises 2, 3 below). This leads to a further definition.

DEFINITION. A group G is *commutative* (or *abelian*) if

G.4. $ab = ba$ for all a, b in G .

It is only a matter of convenience to make use of the words “multiplication”, “product”, “inverse” and “identity” in the definition of a group. Sometimes other terminologies and notations are more useful. The most important alternative is to call the given rule “addition”, and to replace the product ab by the *sum* $a + b$, the identity 1 by the *zero* 0 and the inverse a^{-1} by the *negative* $-a$ (minus a). When this notation and terminology is used we shall speak of G as a *group with respect to addition*; while if that of our original definition is employed we shall say that G is a *group with respect to multiplication*.

The following are important examples of groups:

1. The integers \mathbf{Z} form a commutative group with respect to addition. The set \mathbf{Z}^* of non-zero integers, however, is not a group with respect to multiplication.

2. The sets $\mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{F}_p$ are commutative groups with respect to addition. The set of non-zero elements in each of these sets is a commutative group with respect to multiplication.

3. If S is the set of all points in three dimensional euclidean space, then the rotations about the lines through a fixed point O of S may be regarded as mappings of S into S . These rotations form a group with respect to (mapping) multiplication. (The rigorous definitions of these concepts will be given in Chapter VI.)

4. The set of all *permutations* of a set S (i.e., all one-one mappings of S onto S) is a group with respect to (mapping) multiplication.

DEFINITION. Let F be a set together with rules of addition and multiplication which associate to any two elements x, y in F a sum $x + y$

and a product xy , both in F . Then F is called a *field* if the following axioms are satisfied:

F.1. F is a commutative group with respect to addition;

F.2. the set F^* , obtained from F by omitting the zero, is a commutative group with respect to multiplication;

F.3. $x(y+z) = xy + xz$ and $(y+z)x = yx + zx$ for all x, y, z in F .

The fields that we shall mainly have in mind in this book are the fields $\mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{F}_p$ listed in example 2 above.

We are now ready to define the basic object of our study.

DEFINITION. Let F be a given field and V a set together with rules of addition and multiplication which associate to any two elements a, b in V a sum $a+b$ in V , and to any two elements x in F, a in V a product xa in V . Then V is called a *vector space over the field F* if the following axioms hold:

V.1. V is a commutative group with respect to addition;

V.2. $x(a+b) = xa + xb$,

V.3. $(x+y)a = xa + ya$,

V.4. $(xy)a = x(ya)$,

V.5. $1a = a$ where 1 is the identity element of F ,
for all x, y in F and all a, b in V .

We shall refer to the elements of V as *vectors* and the elements of F as *scalars*. The only notational distinction we shall make between vectors and scalars is to denote the zero elements of V and F by 0_V and 0_F respectively. Since $x0_V = 0_V$ for all x in F and $0_F a = 0_V$ for all a in V (see exercise 7 below) even this distinction will almost always be dropped and $0_V, 0_F$ be written simply as 0 .

The following examples show how ubiquitous vector spaces are in mathematics. The first example is particularly important for our purposes in this book.

1. Let F be a field and denote by F^n the set of all n -tuples (x_1, \dots, x_n) where $x_1, \dots, x_n \in F$. We define the following rules of addition and multiplication:

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n),$$

$$x(x_1, \dots, x_n) = (xx_1, \dots, xx_n)$$

for all $x, x_1, \dots, x_n, y_1, \dots, y_n$ in F .

With these rules F^n is a vector space over F .

2. If F is a subfield of a field E , then E can be regarded as a vector space over F in the following way: E is already a group with respect to addition and we define the product of an element a of E (a "vector")

by an element x of F (a "scalar") to be xa , their ordinary product as elements of E . It is important to note that the elements in F now have two quite distinct parts to play: on the one hand, as elements of F , they are scalars; but on the other hand, as elements of the containing field E , they are vectors.

We mention some special cases: F is always a vector space over F ; \mathbf{R} is a vector space over \mathbf{Q} ; \mathbf{C} is a vector space over \mathbf{R} and also over \mathbf{Q} .

3. The set $F[X]$ of all polynomials in the indeterminate X with coefficients in the field F is a vector space over F .

4. The set of all Cauchy sequences with elements in \mathbf{Q} is a vector space over \mathbf{Q} .

EXERCISES

1. Extend rule G.1 to show that parentheses are unnecessary in a product (or sum) of any finite number of elements of a group.
2. Show that the rotation group of example 3 is not commutative.
3. Show that the permutation groups of example 4 are not commutative if S contains more than two elements.
4. Show from the axioms that a field must contain at least two elements. Write out the addition and multiplication tables for a field with just two elements.
5. Let V be a vector space over the field F . Show that any finite *linear combination* $x_1a_1 + x_2a_2 + \cdots + x_ra_r = \sum_{i=1}^r x_i a_i$, where the x_i 's are scalars and the a_i 's are vectors, can be written unambiguously without the use of parentheses.
6. If $a, b \in V$ show that the equation $v + b = a$ has a unique solution v in V . This solution is denoted by $a - b$.
7. Show that $0_F a = 0_V$ for all a in V and $x0_V = 0_V$ for all x in F . Show further that $(-1)a = -a$ for every a in V . (For the first equation use $(0_F + 0_F)a = 0_F a$ and exercise 6.)

1.3 Subspaces

DEFINITION. A subset M of a vector space V over F is called a *subspace* of V if M is a vector space over F in its own right, but with respect to the same addition and scalar multiplication as V .

Observe that a vector space contains, by definition, a zero vector and so a subspace can never be empty. In order to check that a (non-empty) subset M is a subspace, we need only verify that if $a, b \in M$ and $x \in F$, then $a + b \in M$ and $xa \in M$. (In verifying that M is a subgroup of V with respect to addition we use the fact that $(-1)a = -a$.)

Our definition clearly ensures that V is a subspace (of itself). At the other extreme, the set $\{0_V\}$ is a subspace, called the *zero subspace*, and we usually write this simply as 0_V . It is also clear that 0_V is contained in every subspace of V .

We shall base our construction of subspaces on the following simple proposition.

PROPOSITION 1. *The intersection of any family of subspaces of V is again a subspace of V .*

PROOF. Put $M = \bigcap (M_i : i \in I)$. Since $0_V \in M_i$ for each i , M is not empty. If $a, b \in M$ and $x \in F$, then $a + b \in M_i$ and $xa \in M_i$ for each i ; thus $a + b \in M$ and $xa \in M$.

DEFINITION. If S is any set of vectors in V then we denote by $[S]$ the intersection of all the subspaces of V which contain S . (There is always at least one subspace containing S , namely V itself, and so this intersection is defined.) The subspace $[S]$ is the “least” subspace containing S , in the sense that if K is any subspace containing S , then K contains $[S]$. We say that $[S]$ is the subspace *spanned* (or *generated*) by S .

This definition of $[S]$ may be referred to as the definition “from above”. Provided that S is not empty there is an equivalent definition “from below”: We form the set M of all (finite) linear combinations $x_1 s_1 + \cdots + x_r s_r$, where $x_i \in F$ and $s_i \in S$. It is immediately seen that M is a subspace of V ; that M contains S ; and, in fact, that any subspace K of V which contains S must contain all of M . Hence $M = [S]$.

It might be expected that the union of several subspaces of V would be a subspace, but it is easily shown by means of examples that this is not the case. We are thus led to the following definition.

DEFINITION. The *sum* (or *join*) of any family of subspaces is the subspace spanned by their union. In other words, the sum of the subspaces M_i ($i \in I$) is the least subspace containing them all. The sum is denoted by $+(M_i : i \in I)$ or simply $+(M_i)$. The sum of subspaces M_1, \dots, M_n is usually written $M_1 + M_2 + \cdots + M_n$.

DEFINITION. If $M \cap N = 0$ we call $M + N$ the *direct sum* of M and N , and write it as $M \oplus N$. More generally, the sum of the subspaces M_i ($i \in I$) is *direct*, and written $\bigoplus (M_i : i \in I)$ if, for each j in I , we have $+(M_i : i \in I, i \neq j) \cap M_j = 0$.

Note that the condition above on the subspaces M_i is stronger than the mere requirement that $M_i \cap M_j = 0$ for all $i \neq j$ (see exercise 7). If $v \in M_1 \oplus \cdots \oplus M_r$, then v can be written *uniquely* in the form $v = m_1 + \cdots + m_r$, where $m_i \in M_i$ for $i = 1, \dots, r$.

EXERCISES

1. If M is a subspace of V , show that the zero vector of M is the same as the zero vector of V .
2. Show that the set of all polynomials $f(X)$ in $F[X]$ satisfying $f(x_i) = 0$ ($i = 1, \dots, r$) for given x_1, \dots, x_r in F is a subspace of $F[X]$. Show that the set of all polynomials of degree less than n (including the zero polynomial) is a subspace of $F[X]$.
3. If the mn elements a_{ij} ($i = 1, \dots, m; j = 1, \dots, n$) lie in a field F , show that the set of all solutions (x_1, \dots, x_n) in F^n of the linear equations

$$\sum_{j=1}^n a_{ij} X_j = 0 \quad (i = 1, \dots, m)$$

is a subspace of F^n .

4. Give precise meaning to the statement that $M \cap N$ is the "greatest" subspace of V contained in both M and N .
5. Give an example of two subspaces of a vector space whose union is not a subspace.
6. Prove that $v \in M + N$ if, and only if, v can be expressed in the form $m + n$ where $m \in M$, $n \in N$; and

$$v \in (M_i : i \in I) \quad \text{if, and only if,} \quad v = m_{i_1} + \dots + m_{i_r}$$

for some i_k in I and m_{i_k} in M_{i_k} ($k = 1, \dots, r$).

7. Consider the following subsets of F^3 : M_1 consists of all $(x, 0, 0)$; M_2 consists of all $(0, x, 0)$; and M_3 consists of all (x, x, y) , where $x, y \in F$. Show that M_1, M_2, M_3 are subspaces of F^3 which satisfy $M_i \cap M_j = 0$ for all $i \neq j$; that $F^3 = M_1 + M_2 + M_3$; but that F^3 is not the direct sum of M_1, M_2, M_3 .
8. Prove the last statement made before these exercises.
9. If V is a vector space over F_p , prove that every subgroup of V with respect to addition is a subspace.

1.4 Dimension

The essentially geometrical character of a vector space will emerge as we proceed. Our immediate task is to define the fundamental concept of dimension; and we shall do this by using the even more primitive notion of *linear dependence*.

DEFINITION. If S is a subset of a vector space V over a field F , then we say that the vectors of S are *linearly dependent* if the zero vector of V is a non-trivial linear combination of distinct vectors in S ; i.e., if there exist scalars x_1, \dots, x_r in F , not all 0, and distinct vectors s_1, \dots, s_r in S such that $x_1 s_1 + \dots + x_r s_r = 0$. (In these circumstances we shall