Basics of Algebra and Analysis
For Computer Science

Jean Gallier
Department of Computer and Information Science
University of Pennsylvania
Philadelphia, PA 19104, USA
e-mail: jean@cis.upenn.edu

© Jean Gallier

February 9, 2011
# Contents

1 Introduction 5

2 Linear Algebra 7
   2.1 Groups, Rings, and Fields ........................................ 7
   2.2 Vector Spaces ..................................................... 12
   2.3 Linear Independence, Subspaces .................................. 13
   2.4 Bases of a Vector Space ........................................... 17
   2.5 Linear Maps ........................................................ 22
   2.6 Quotient Spaces .................................................... 26
   2.7 Matrices ............................................................. 27
   2.8 Direct Sums .......................................................... 36
   2.9 The Dual Space $E^*$ and Linear Forms .......................... 44
   2.10 Hyperplanes and Linear Forms ................................... 51
   2.11 Transpose of a Linear Map and of a Matrix .................... 52

3 Determinants 55
   3.1 Permutations, Signature of a Permutation ....................... 55
   3.2 Alternating Multilinear Maps ..................................... 58
   3.3 Definition of a Determinant ...................................... 62
   3.4 Inverse Matrices and Determinants .............................. 68
   3.5 Systems of Linear Equations and Determinant .................. 71
   3.6 Determinant of a Linear Map ..................................... 72
   3.7 Gaussian Elimination, LU and Cholesky Factorization .......... 73
   3.8 Further Readings .................................................... 87

4 Basics of Affine Geometry 89
   4.1 Affine Spaces ....................................................... 89
   4.2 Examples of Affine Spaces ...................................... 96
   4.3 Chasles’s Identity .................................................. 98
   4.4 Affine Combinations, Barycenters ............................... 99
   4.5 Affine Subspaces .................................................. 102
   4.6 Affine Independence and Affine Frames ......................... 108
   4.7 Affine Maps ......................................................... 113
## CONTENTS

4.8 Affine Groups .......................................................... 119  
4.9 Affine Geometry: A Glimpse ........................................ 121  
4.10 Affine Hyperplanes .................................................. 125  
4.11 Problems ............................................................... 127  

5 Polynomials, PID’s and UFD’s ........................................ 141  
5.1 Multisets ................................................................. 141  
5.2 Polynomials ............................................................. 142  
5.3 Euclidean Division of Polynomials .................................. 148  
5.4 Ideals, PID’s, and Greatest Common Divisors ................... 150  
5.5 Factorization and Irreducible Factors in $K[X]$ .................. 157  
5.6 Roots of Polynomials .................................................. 161  
5.7 Unique Factorization Domains (Factorial Rings) ............... 168  
5.8 Noetherian Rings and Hilbert’s Basis Theorem .................. 182  
5.9 Eigenvectors and Eigenvalues ....................................... 186  
5.10 Polynomial Interpolation (Lagrange, Newton, Hermite) ....... 190  
5.11 Further Readings ...................................................... 196  

6 Topology ................................................................. 197  
6.1 Metric Spaces and Normed Vector Spaces ....................... 197  
6.2 Topological Spaces .................................................... 201  
6.3 Continuous Functions, Limits ....................................... 206  
6.4 Continuous Linear and Multilinear Maps ......................... 211  
6.5 Normed Affine Spaces ................................................. 216  
6.6 Further Readings ....................................................... 217  

7 Differential Calculus ................................................... 219  
7.1 Directional Derivatives, Total Derivatives ....................... 219  
7.2 Jacobian Matrices ..................................................... 226  
7.3 The Implicit and The Inverse Function Theorems ............... 232  
7.4 Tangent Spaces and Differentials .................................. 235  
7.5 Second-Order and Higher-Order Derivatives ..................... 237  
7.6 Taylor’s formula, Faà di Bruno’s formula ........................ 242  
7.7 Vector Fields, Covariant Derivatives, Lie Brackets .............. 245  
7.8 Further Readings ....................................................... 247  

8 Appendix: Zorn’s Lemma; Some Applications ..................... 249  
8.1 Statement of Zorn’s Lemma ........................................ 249  
8.2 Proof of the Existence of a Basis in a Vector Space .......... 250  
8.3 Existence of Maximal Proper Ideals ............................... 251  

Bibliography ............................................................. 252
Chapter 1

Introduction
Chapter 2
Linear Algebra

2.1 Groups, Rings, and Fields

In this chapter, the basic algebraic structures (groups, rings, fields, vector spaces) are reviewed, with a major emphasis on vector spaces. Basic notions of linear algebra such as vector spaces, subspaces, linear combinations, linear independence, bases, quotient spaces, linear maps, matrices, change of bases, direct sums, linear forms, dual spaces, hyperplanes, transpose of a linear maps, are reviewed.

The set \( \mathbb{R} \) of real numbers has two operations \( +: \mathbb{R} \times \mathbb{R} \to \mathbb{R} \) (addition) and \( \ast: \mathbb{R} \times \mathbb{R} \to \mathbb{R} \) (multiplication) satisfying properties that make \( \mathbb{R} \) into an abelian group under \( + \), and \( \mathbb{R} - \{0\} = \mathbb{R}^\ast \) into an abelian group under \( \ast \). Recall the definition of a group.

**Definition 2.1** A *group* is a set \( G \) equipped with an operation \( \cdot: G \times G \to G \) having the following properties: \( \cdot \) is associative, has an identity element \( e \in G \), and every element in \( G \) is invertible (w.r.t. \( \cdot \)). More explicitly, this means that the following equations hold for all \( a, b, c \in G \):

- \( a \cdot (b \cdot c) = (a \cdot b) \cdot c \) (associativity);
- \( a \cdot e = e \cdot a = a \) (identity);
- For every \( a \in G \), there is some \( a^{-1} \in G \) such that \( a \cdot a^{-1} = a^{-1} \cdot a = e \) (inverse).

A group \( G \) is *abelian* (or *commutative*) if

\[
a \cdot b = b \cdot a
\]

for all \( a, b \in G \).

A set \( M \) together with an operation \( \cdot: M \times M \to M \) and an element \( e \) satisfying only conditions (G1) and (G2) is called a *monoid*. For example, the set \( \mathbb{N} = \{0,1,\ldots,n\ldots\} \) of natural numbers is a (commutative) monoid. However, it is not a group. Some examples of groups are given below.
Example 2.1

1. The set $\mathbb{Z} = \{\ldots, -n, \ldots, -1, 0, 1, \ldots, n \ldots\}$ of integers is a group under addition, with identity element 0. However, $\mathbb{Z}^* = \mathbb{Z} - \{0\}$ is not a group under multiplication.

2. The set $\mathbb{Q}$ of rational numbers is a group under addition, with identity element 0. The set $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ is also a group under multiplication, with identity element 1.

3. Similarly, the sets $\mathbb{R}$ of real numbers and $\mathbb{C}$ of complex numbers are groups under addition (with identity element 0), and $\mathbb{R}^* = \mathbb{R} - \{0\}$ and $\mathbb{C}^* = \mathbb{C} - \{0\}$ are groups under multiplication (with identity element 1).

4. The sets $\mathbb{R}^n$ and $\mathbb{C}^n$ of $n$-tuples of real or complex numbers are groups under componentwise addition:

\[(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n),\]

with identity element $(0, \ldots, 0)$. All these groups are abelian.

5. Given any nonempty set $S$, the set of bijections $f: S \to S$, also called permutations of $S$, is a group under function composition (i.e., the multiplication of $f$ and $g$ is the composition $g \circ f$), with identity element the identity function $\text{id}_S$. This group is not abelian as soon as $S$ has more than two elements.

6. The set of $n \times n$ matrices with real (or complex) coefficients is a group under addition of matrices, with identity element the null matrix. It is denoted by $M_n(\mathbb{R})$ (or $M_n(\mathbb{C})$).

7. The set $\mathbb{R}[X]$ of polynomials in one variable with real coefficients is a group under addition of polynomials.

8. The set of $n \times n$ invertible matrices with real (or complex) coefficients is a group under matrix multiplication, with identity element the identity matrix $I_n$. This group is called the general linear group and is usually denoted by $\text{GL}(n, \mathbb{R})$ (or $\text{GL}(n, \mathbb{C})$).

9. The set of $n \times n$ invertible matrices with real (or complex) coefficients and determinant $+1$ is a group under matrix multiplication, with identity element the identity matrix $I_n$. This group is called the special linear group and is usually denoted by $\text{SL}(n, \mathbb{R})$ (or $\text{SL}(n, \mathbb{C})$).

10. The set of $n \times n$ invertible matrices with real coefficients such that $RR^\top = I_n$ and of determinant $+1$ is a group called the orthogonal group and is usually denoted by $\text{SO}(n)$ (where $R^\top$ is the transpose of the matrix $R$, i.e., the rows of $R^\top$ are the columns of $R$). It corresponds to the rotations in $\mathbb{R}^n$. 
11. Given an open interval \( ]a, b[ \) the set \( C(]a, b[) \) of continuous functions \( f: ]a, b[ \to \mathbb{R} \) is a group under the operation \( f + g \) defined such that
\[
(f + g)(x) = f(x) + g(x)
\]
for all \( x \in ]a, b[ \).

The groups \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{R}[X], \) and \( \mathbb{M}_n(\mathbb{R}) \) are more than an abelian groups, they are also commutative rings. Furthermore, \( \mathbb{Q}, \mathbb{R}, \) and \( \mathbb{C} \) are fields. We now introduce rings and fields.

**Definition 2.2** A ring is a set \( A \) equipped with two operations \( +: A \times A \to A \) (called addition) and \( \ast: A \times A \to A \) (called multiplication) having the following properties:

- (R1) \( A \) is an abelian group w.r.t. \(+\);
- (R2) \( \ast \) is associative and has an identity element \( 1 \in A \);
- (R3) \( \ast \) is distributive w.r.t. \(+\).

The identity element for addition is denoted 0, and the additive inverse of \( a \in A \) is denoted by \(-a\). More explicitly, the axioms of a ring are the following equations which hold for all \( a, b, c \in A \):

\[
\begin{align*}
a + (b + c) &= (a + b) + c \quad \text{(associativity of +)} \\
a + b &= b + a \quad \text{(commutativity of +)} \\
a + 0 &= 0 + a = a \quad \text{(zero)} \\
a + (-a) &= (-a) + a = 0 \quad \text{(additive inverse)} \\
a \ast (b \ast c) &= (a \ast b) \ast c \quad \text{(associativity of \ast)} \\
a \ast 1 &= 1 \ast a = a \quad \text{(identity for \ast)} \\
(a + b) \ast c &= (a \ast c) + (b \ast c) \quad \text{(distributivity)} \\
a \ast (b + c) &= (a \ast b) + (a \ast c) \quad \text{(distributivity)}
\end{align*}
\]

The ring \( A \) is **commutative** if
\[
a \ast b = b \ast a
\]
for all \( a, b \in A \).

From (2.7) and (2.8), we easily obtain
\[
\begin{align*}
a \ast 0 &= 0 \ast a = 0 \quad \text{(2.9)} \\
a \ast (-b) &= (-a) \ast b = -(a \ast b) \quad \text{(2.10)}
\end{align*}
\]

Note that (2.9) implies that if \( 1 = 0 \), then \( a = 0 \) for all \( a \in A \), and thus, \( A = \{0\} \). The ring \( A = \{0\} \) is called the **trivial ring**. A ring for which \( 1 \neq 0 \) is called **nontrivial**. The multiplication \( a \ast b \) of two elements \( a, b \in A \) is often denoted by \( ab \).
Example 2.2

1. The additive groups \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \), are commutative rings.

2. The group \( \mathbb{R}[X] \) of polynomials in one variable with real coefficients is a ring under multiplication of polynomials. It is a commutative ring.

3. The group of \( n \times n \) matrices \( \mathbb{M}_n(\mathbb{R}) \) is a ring under matrix multiplication. However, it is not a commutative ring.

4. The group \( C([a, b]) \) of continuous functions \( f: [a, b] \to \mathbb{R} \) is a ring under the operation \( f \cdot g \) defined such that
   \[
   (f \cdot g)(x) = f(x)g(x)
   \]
   for all \( x \in [a, b] \).

When \( ab = 0 \) for \( a \neq 0 \) and \( b \neq 0 \), we say that \( a \) is a zero divisor (and so is \( b \)). A ring \( A \) is an integral domain (or an entire ring) if \( 0 \neq 1 \), \( A \) is commutative, and \( ab = 0 \) implies that \( a = 0 \) or \( b = 0 \), for all \( a, b \in A \). In other words, an integral domain is a nontrivial commutative ring with no zero divisors.

Example 2.3

1. The rings \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \), are integral domains.

2. The ring \( \mathbb{R}[X] \) of polynomials in one variable with real coefficients is an integral domain.

3. For any positive integer, \( p \in \mathbb{N} \), define a relation on \( \mathbb{Z} \), denoted \( m \equiv n \) (mod \( p \)), as follows:
   \[
   m \equiv n \text{ (mod } p) \iff m - n = kp \text{ for some } k \in \mathbb{Z}
   \]
   The reader will easily check that this is an equivalence relation, and, moreover, it is compatible with respect to addition and multiplication, which means that if \( m_1 \equiv n_1 \) (mod \( p \)) and \( m_2 \equiv n_2 \) (mod \( p \)), then \( m_1 + m_2 \equiv n_1 + n_2 \) (mod \( p \)) and \( m_1m_2 \equiv n_1n_2 \) (mod \( p \)). Consequently, we can define an addition operation and a multiplication operation of the set of equivalence classes (mod \( p \)):
   \[
   [m] + [n] = [m + n]
   \]
   and
   \[
   [m] \cdot [n] = [mn].
   \]
   Again, the reader will easily check that the ring axioms are satisfied, with \( [0] \) as zero and \( [1] \) as multiplicative unit. The resulting ring is denoted by \( \mathbb{Z}/p\mathbb{Z} \).

4. Observe that if \( p \) is composite, then this ring has zero-divisors. For example, if \( p = 4 \), then we have \( 2 \cdot 2 \equiv 0 \) (mod \( 4 \)).

\(^1\)The notation \( \mathbb{Z}_p \) is sometimes used instead of \( \mathbb{Z}/p\mathbb{Z} \) but it clashes with the notation for the \( p \)-adic integers so we prefer not to use it.
However, the reader should prove that $\mathbb{Z}/p\mathbb{Z}$ is an integral domain if $p$ is prime (in fact, it is a field).

4. The ring of $n \times n$ matrices $M_n(\mathbb{R})$ is not an integral domain. It has zero divisors (see Example 2.12).

A homomorphism between rings is a mapping preserving addition, multiplications (and 0 and 1).

**Definition 2.3** Given two rings $A$ and $B$, a homomorphism between $A$ and $B$ is a function $h: A \to B$ satisfying the following conditions for all $x, y \in A$:

- $h(x + y) = h(x) + h(y)$
- $h(xy) = h(x)h(y)$
- $h(0) = 0$
- $h(1) = 1$.

Actually, because $B$ is a group under addition, $h(0) = 0$ follows from $h(x + y) = h(x) + h(y)$.

**Example 2.4**

1. If $A$ is a ring, for any integer $n \in \mathbb{Z}$, for any $a \in A$, we define $n \cdot a$ by

$$n \cdot a = a + \cdots + a$$

if $n \geq 0$ (with $0 \cdot a = 0$) and

$$n \cdot a = -(n) \cdot a$$

if $n < 0$. Then, the map $h: \mathbb{Z} \to A$ given by

$$h(n) = n \cdot 1_A$$

is a ring homomorphism (where $1_A$ is the multiplicative identity of $A$).

2. Given any real $\lambda \in \mathbb{R}$, the evaluation map $\eta_\lambda: \mathbb{R}[X] \to \mathbb{R}$ defined by

$$\eta_\lambda(f(X)) = f(\lambda)$$

for every polynomial $f(X) \in \mathbb{R}[X]$ is a ring homomorphism.

A field is a commutative ring $K$ for which $A - \{0\}$ is a group under multiplication.

**Definition 2.4** A set $K$ is a field if it is a ring and the following properties hold:
(F1) $0 \neq 1$;

(F2) $K^* = K - \{0\}$ is a group w.r.t. $*$ (i.e., every $a \neq 0$ has an inverse w.r.t. $*$);

(F3) $*$ is commutative.

If $*$ is not commutative but (F1) and (F2) hold, we say that we have a skew field (or noncommutative field).

Note that we are assuming that the operation $*$ of a field is commutative. This convention is not universally adopted, but since $*$ will be commutative for most fields we will encounter, we may as well include this condition in the definition.

Example 2.5

1. The rings $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields.

2. The set of (formal) fractions $f(X)/g(X)$ of polynomials $f(X), g(X) \in \mathbb{R}[X]$, where $g(X)$ is not the null polynomial, is a field.

3. The ring $C^*([a, b])$ of continuous functions $f:]a, b[\to \mathbb{R}$ such that $f(x) \neq 0$ for all $x \in ]a, b[$ is a field.

4. The ring $\mathbb{Z}/p\mathbb{Z}$ is a field whenever $p$ is prime.

2.2 Vector Spaces

For every $n \geq 1$, let $\mathbb{R}^n$ be the set of $n$-tuples $x = (x_1, \ldots, x_n)$. Addition can be extended to $\mathbb{R}^n$ as follows:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n).$$

We can also define an operation $\cdot: \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$ as follows:

$$\lambda \cdot (x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n).$$

The resulting algebraic structure has some interesting properties, those of a vector space.

Definition 2.5 Given a field $K$, a vector space over $K$ (or $K$-vector space) is a set $E$ (of vectors) together with two operations $+: E \times E \to E$ (called vector addition),$^2$ and $\cdot: K \times E \to E$ (called scalar multiplication) satisfying the following conditions for all $\alpha, \beta \in K$ and all $u, v \in E$;

(V0) $E$ is an abelian group w.r.t. $+$, with identity element $0$;

$^2$The symbol $+$ is overloaded, since it denotes both addition in the field $K$ and addition of vectors in $E$. However, if we write elements of $E$ as vectors, i.e., of the form $u$, it will always be clear from the type of the arguments which $+$ is intended.
(V1) $\alpha \cdot (u + v) = (\alpha \cdot u) + (\alpha \cdot v)$;

(V2) $(\alpha + \beta) \cdot u = (\alpha \cdot u) + (\beta \cdot u)$;

(V3) $(\alpha \ast \beta) \cdot u = \alpha \cdot (\beta \cdot u)$;

(V4) $1 \cdot u = u$.

Given $\alpha \in K$ and $v \in E$, the element $\alpha \cdot v$ is also denoted by $\alpha v$. The field $K$ is often called the field of scalars.

Unless specified otherwise or unless we are dealing with several different fields, in the rest of this chapter, we assume that all $K$-vector spaces are defined with respect to a fixed field $K$. Thus, we will refer to a $K$-vector space simply as a vector space. In most cases, the field $K$ will be the field $\mathbb{R}$ of reals.

From (V0), a vector space always contains the null vector 0, and thus is nonempty. From (V1), we get $\alpha \cdot 0 = 0$, and $\alpha \cdot (-v) = - (\alpha \cdot v)$. From (V2), we get $0 \cdot v = 0$, and $(-\alpha) \cdot v = -(\alpha \cdot v)$. The field $K$ itself can be viewed as a vector space over itself, addition of vectors being addition in the field, and multiplication by a scalar being multiplication in the field.

Example 2.6

1. The fields $\mathbb{R}$ and $\mathbb{C}$ are vector spaces over $\mathbb{R}$.

2. The groups $\mathbb{R}^n$ and $\mathbb{C}^n$ are vector spaces over $\mathbb{R}$, and $\mathbb{C}^n$ is a vector space over $\mathbb{C}$.

3. The ring $\mathbb{R}[X]$ of polynomials is a vector space over $\mathbb{R}$, and $\mathbb{C}[X]$ is a vector space over $\mathbb{R}$ and $\mathbb{C}$. The ring of $n \times n$ matrices $M_n(\mathbb{R})$ is a vector space over $\mathbb{R}$.

4. The ring $C^*([a, b])$ of continuous functions $f: [a, b] \to \mathbb{R}$ is a vector space over $\mathbb{R}$.

Let $E$ be a vector space. We would like to define the important notions of linear combination and linear independence. These notions can be defined for sets of vectors in $E$, but it will turn out to be more convenient to define them for families $(v_i)_{i \in I}$, where $I$ is any arbitrary index set.

## 2.3 Linear Independence, Subspaces

One of the most useful properties of vector spaces is that there possess bases. What this means is that in every vector space, $E$, there is some set of vectors, $\{e_1, \ldots, e_n\}$, such that every vector, $v \in E$, can be written as a linear combination,

$$v = \lambda_1 e_1 + \cdots + \lambda_n e_n,$$
of the $e_i$, for some scalars, $\lambda_1, \ldots, \lambda_n \in K$. Furthermore, the $n$-tuple, $(\lambda_1, \ldots, \lambda_n)$, as above is unique.

This description is fine when $E$ has a finite basis, $\{e_1, \ldots, e_n\}$, but this is not always the case! For example, the vector space of real polynomials, $\mathbb{R}[X]$, does not have a finite basis but instead it has an infinite basis, namely

$$1, X, X^2, \ldots, X^n, \ldots$$

One might wonder if it is possible for a vector space to have bases of different sizes, or even to have a finite basis as well as an infinite basis. We will see later on that this is not possible; all bases of a vector space have the same number of elements (cardinality), which is called the \textit{dimension} of the space. However, we have the following problem: If a vector space has an infinite basis, $\{e_1, e_2, \ldots\}$, how do we define linear combinations? Do we allow linear combinations

$$\lambda_1 e_1 + \lambda_2 e_2 + \cdots$$

with infinitely many nonzero coefficients?

If we allow linear combinations with infinitely many nonzero coefficients, then we have to make sense of these sums and this can only be done reasonably if we define such a sum as the limit of the sequence of vectors, $s_1, s_2, \ldots, s_n, \ldots$, with $s_1 = \lambda_1 e_1$ and

$$s_{n+1} = s_n + \lambda_{n+1} e_{n+1}.$$ 

But then, how do we define such limits? Well, we have to define some topology on our space, by means of a norm, a metric or some other mechanism. This can indeed be done and this is what Banach spaces and Hilbert spaces are all about but this seems to require a lot of machinery.

A way to avoid limits is to restrict our attention to linear combinations involving only \textit{finitely many} vectors. We may have an infinite supply of vectors but we only form linear combinations involving finitely many nonzero coefficients. Technically, this can be done by introducing \textit{families of finite support}. This gives us the ability to manipulate families of scalars indexed by some fixed infinite set and yet to be treat these families as if they were finite. With these motivations in mind, let us review the notion of an indexed family.

Given a set $A$, a family $(a_i)_{i \in I}$ of elements of $A$ is simply a function $a: I \to A$.

\textbf{Remark:} When considering a family $(a_i)_{i \in I}$, there is no reason to assume that $I$ is ordered. The crucial point is that every element of the family is uniquely indexed by an element of $I$. Thus, unless specified otherwise, we do not assume that the elements of an index set are ordered.

If $A$ is an abelian group (usually, when $A$ is a ring or a vector space) with identity $0$, we say that a family $(a_i)_{i \in I}$ has \textit{finite support} if $a_i = 0$ for all $i \in I - J$, where $J$ is a finite subset of $I$ (the support of the family).
We can deal with an arbitrary set \( X \) by viewing it as the family \((X_x)_{x \in X}\) corresponding to the identity function \( id: X \to X \). We agree that when \( I = \emptyset \), \((a_i)_{i \in I} = \emptyset \). A family \((a_i)_{i \in I}\) is finite if \( I \) is finite.

Given two disjoint sets \( I \) and \( J \), the union of two families \((u_i)_{i \in I}\) and \((v_j)_{j \in J}\), denoted as \((u_i)_{i \in I} \cup (v_j)_{j \in J}\), is the family \((w_k)_{k \in (I \cup J)}\) defined such that \( w_k = u_k \) if \( k \in I \), and \( w_k = v_k \) if \( k \in J \). Given a family \((u_i)_{i \in I}\) and any element \( v \), we denote by \((u_i)_{i \in I} \cup \{v\}\) the family \((u_i)_{i \in I} \cup \{k\}\) defined such that \( w_i = u_i \) if \( i \in I \), and \( w_k = v \), where \( k \) is any index such that \( k \notin I \). Given a family \((u_i)_{i \in I}\), a subfamily of \((u_i)_{i \in I}\) is a family \((u_j)_{j \in J}\) where \( J \) is any subset of \( I \).

In this chapter, unless specified otherwise, it is assumed that all families of scalars have finite support.

**Definition 2.6** Let \( E \) be a vector space. A vector \( v \in E \) is a linear combination of a family \((u_i)_{i \in I}\) of elements of \( E \) if there is a family \((\lambda_i)_{i \in I}\) of scalars in \( K \) such that

\[
v = \sum_{i \in I} \lambda_i u_i.
\]

When \( I = \emptyset \), we stipulate that \( v = 0 \). We say that a family \((u_i)_{i \in I}\) is linearly independent if for every family \((\lambda_i)_{i \in I}\) of scalars in \( K \),

\[
\sum_{i \in I} \lambda_i u_i = 0 \quad \text{implies that} \quad \lambda_i = 0 \text{ for all } i \in I.
\]

Equivalently, a family \((u_i)_{i \in I}\) is linearly dependent if there is some family \((\lambda_i)_{i \in I}\) of scalars in \( K \) such that

\[
\sum_{i \in I} \lambda_i u_i = 0 \quad \text{and} \quad \lambda_j \neq 0 \text{ for some } j \in I.
\]

We agree that when \( I = \emptyset \), the family \( \emptyset \) is linearly independent.

A family \((u_i)_{i \in I}\) is linearly dependent iff some \( u_j \) in the family can be expressed as a linear combination of the other vectors in the family. Indeed, there is some family \((\lambda_i)_{i \in I}\) of scalars in \( K \) such that

\[
\sum_{i \in I} \lambda_i u_i = 0 \quad \text{and} \quad \lambda_j \neq 0 \text{ for some } j \in I,
\]

which implies that

\[
u_j = \sum_{i \in (I - \{j\})} -\lambda_j^{-1}\lambda_i u_i.
\]

When \( I \) is nonempty, if the family \((u_i)_{i \in I}\) is linearly independent, note that \( u_i \neq 0 \) for all \( i \in I \), since otherwise we would have \( \sum_{i \in I} \lambda_i u_i = 0 \) with some \( \lambda_i \neq 0 \), since \( 0u_i = 0 \).
Example 2.7

1. Any two distinct scalars \( \lambda, \mu \neq 0 \) in \( K \) are linearly independent.

2. In \( \mathbb{R}^3 \), the vectors \((1, 0, 0), (0, 1, 0), \) and \((0, 0, 1)\) are linearly independent.

3. In \( \mathbb{R}^4 \), the vectors \((1, 1, 1, 1), (0, 1, 1, 1), (0, 0, 1, 1), \) and \((0, 0, 0, 1)\) are linearly independent.

4. In \( \mathbb{R}^2 \), the vectors \( u = (1, 1), v = (0, 1) \) and \( w = (2, 3) \) are linearly dependent, since
   \[ w = 2u + v. \]

Note that a family \( (u_i)_{i \in I} \) is linearly independent iff \( (u_j)_{j \in J} \) is linearly independent for every finite subset \( J \) of \( I \) (even when \( I = \emptyset \)). Indeed, when \( \sum_{i \in I} \lambda_i u_i = 0 \), the family \( (\lambda_i)_{i \in I} \) of scalars in \( K \) has finite support, and thus \( \sum_{i \in I} \lambda_i u_i = 0 \) really means that \( \sum_{j \in J} \lambda_j u_j = 0 \) for a finite subset \( J \) of \( I \). When \( I \) is finite, we often assume that it is the set \( I = \{1, 2, \ldots, n\} \).

In this case, we denote the family \( (u_i)_{i \in I} \) as \( (u_1, \ldots, u_n) \).

The notion of a subspace of a vector space is defined as follows.

Definition 2.7 Given a vector space \( E \), a subset \( F \) of \( E \) is a linear subspace (or subspace) of \( E \) if \( F \) is nonempty and \( \lambda u + \mu v \in F \) for all \( u, v \in F \), and all \( \lambda, \mu \in K \).

It is easy to see that a subspace \( F \) of \( E \) is indeed a vector space, since the restriction of \( +: E \times E \to E \) to \( F \times F \) is indeed a function \( +: F \times F \to F \), and the restriction of \( \cdot: K \times E \to E \) to \( K \times F \) is indeed a function \( \cdot: K \times F \to F \). It is also easy to see that a subspace \( F \) of \( E \) is closed under arbitrary linear combinations of vectors from \( F \), and that any intersection of subspaces is a subspace. Letting \( \lambda = \mu = 0 \), we see that every subspace contains the vector 0. The subspace \( \{0\} \) will be denoted by \( (0) \), or even \( 0 \) (with a mild abuse of notation).

Example 2.8

1. In \( \mathbb{R}^2 \), the set of vectors \( u = (x, y) \) such that
   \[ x + y - 1 = 0 \]
   is a subspace.

2. In \( \mathbb{R}^3 \), the set of vectors \( u = (x, y, z) \) such that
   \[ x + y + z - 1 = 0 \]
   is a subspace.

3. For any \( n \geq 0 \), the set of polynomials \( f(X) \in \mathbb{R}[X] \) of degree at most \( n \) is a subspace of \( \mathbb{R}[X] \).

4. The set of upper triangular \( n \times n \) matrices is a subspace of the space of \( n \times n \) matrices.
2.4 Bases of a Vector Space

Given a vector space $E$, given a family $(v_i)_{i \in I}$ of vectors $v_i \in V$ spans $V$ or generates $V$ if for every $v \in V$, there is some family $(\lambda_i)_{i \in I}$ of scalars in $K$ such that

$$v = \sum_{i \in I} \lambda_i v_i.$$  

We also say that the elements of $(v_i)_{i \in I}$ are generators of $V$ and that $V$ is spanned by $(v_i)_{i \in I}$, or generated by $(v_i)_{i \in I}$. If a subspace $V$ of $E$ is generated by a finite family $(v_i)_{i \in I}$, we say that $V$ is finitely generated. A family $(u_i)_{i \in I}$ that spans $V$ and is linearly independent is called a basis of $V$.

Example 2.9

1. In $\mathbb{R}^3$, the vectors $(1, 0, 0), (0, 1, 0), \text{and } (0, 0, 1)$ form a basis.

2. In the subspace of polynomials in $\mathbb{R}[X]$ of degree at most $n$, the polynomials $1, X, X^2, \ldots, X^n$ form a basis.

3. The polynomials \( \binom{n}{k} (1 - X)^k X^{n-k} \) for $k = 0, \ldots, n$, also form a basis of that space.

It is a standard result of linear algebra that every vector space $E$ has a basis, and that for any two bases $(u_i)_{i \in I}$ and $(v_j)_{j \in J}$, $I$ and $J$ have the same cardinality. In particular, if $E$ has a finite basis of $n$ elements, every basis of $E$ has $n$ elements, and the integer $n$ is called the dimension of the vector space $E$. We begin with a crucial lemma.

Lemma 2.1 Given a linearly independent family $(u_i)_{i \in I}$ of elements of a vector space $E$, if $v \in E$ is not a linear combination of $(u_i)_{i \in I}$, then the family $(u_i)_{i \in I} \cup_k (v)$ obtained by adding $v$ to the family $(u_i)_{i \in I}$ is linearly independent (where $k \notin I$).

Proof. Assume that $\mu v + \sum_{i \in I} \lambda_i u_i = 0$, for any family $(\lambda_i)_{i \in I}$ of scalars in $K$. If $\mu \neq 0$, then $\mu$ has an inverse (because $K$ is a field), and thus we have $v = -\sum_{i \in I} (\mu^{-1} \lambda_i) u_i$, showing that $v$ is a linear combination of $(u_i)_{i \in I}$ and contradicting the hypothesis. Thus, $\mu = 0$. But then, we have $\sum_{i \in I} \lambda_i u_i = 0$, and since the family $(u_i)_{i \in I}$ is linearly independent, we have $\lambda_i = 0$ for all $i \in I$. \qed

The next theorem holds in general, but the proof is more sophisticated for vector spaces that do not have a finite set of generators. Thus, in this chapter, we only prove the theorem for finitely generated vector spaces.
Theorem 2.2 Given any finite family \(S = (u_i)_{i \in I}\) generating a vector space \(E\) and any linearly independent subfamily \(L = (u_j)_{j \in J}\) of \(S\) (where \(J \subseteq I\)), there is a basis \(B\) of \(E\) such that \(L \subseteq B \subseteq S\).

Proof. Consider the set of linearly independent families \(B\) such that \(L \subseteq B \subseteq S\). Since this set is nonempty and finite, it has some maximal element, say \(B = (u_h)_{h \in H}\). We claim that \(B\) generates \(E\). Indeed, if \(B\) does not generate \(E\), then there is some \(u_p \in S\) that is not a linear combination of vectors in \(B\) (since \(S\) generates \(E\)), with \(p \notin H\). Then, by Lemma 2.1, the family \(B' = (u_h)_{h \in H \cup \{p\}}\) is linearly independent, and since \(L \subseteq B \subseteq B' \subseteq S\), this contradicts the maximality of \(B\). Thus, \(B\) is a basis of \(E\) such that \(L \subseteq B \subseteq S\). \(\Box\)

Remark: Theorem 2.2 also holds for vector spaces that are not finitely generated. In this case, the problem is to guarantee the existence of a maximal linearly independent family \(B\) such that \(L \subseteq B \subseteq S\). The existence of such a maximal family can be shown using Zorn’s lemma, see Appendix 8 and the references given there.

The following proposition giving useful properties characterizing a basis is an immediate consequence of Theorem 2.2.

Proposition 2.3 Given a vector space \(E\), for any family \(B = (v_i)_{i \in I}\) of vectors of \(E\), the following properties are equivalent:

1. \(B\) is a basis of \(E\).
2. \(B\) is a maximal linearly independent family of \(E\).
3. \(B\) is a minimal generating family of \(E\).

The following replacement proposition shows the relationship between finite linearly independent families and finite families of generators of a vector space.

Proposition 2.4 Given a vector space \(E\), let \((u_i)_{i \in I}\) be any finite linearly independent family in \(E\), where \(|I| = m\), and let \((v_j)_{j \in J}\) be any finite family such that every \(u_i\) is a linear combination of \((v_j)_{j \in J}\), where \(|J| = n\). Then, there exists a set \(L\) and an injection \(\rho: L \to J\) such that \(L \cap I = \emptyset\), \(|L| = n - m\), and the families \((u_i)_{i \in I} \cup (v_{\rho(l)})_{l \in L}\) and \((v_j)_{j \in J}\) generate the same subspace of \(E\). In particular, \(m \leq n\).

Proof. We proceed by induction on \(|I| = m\). When \(m = 0\), the family \((u_i)_{i \in I}\) is empty, and the proposition holds trivially with \(L = J\) (\(\rho\) is the identity). Assume \(|I| = m + 1\). Consider the linearly independent family \((u_i)_{i \in (I - \{p\})}\), where \(p\) is any member of \(I\). By the induction hypothesis, there exists a set \(L\) and an injection \(\rho: L \to J\) such that \(L \cap (I - \{p\}) = \emptyset\), \(|L| = n - m\), and the families \((u_i)_{i \in (I - \{p\})} \cup (v_{\rho(l)})_{l \in L}\) and \((v_j)_{j \in J}\) generate the same subspace of \(E\). If \(p \in L\), we can replace \(L\) by \((L - \{p\}) \cup \{p'\}\) where \(p'\) does not belong to \(I \cup L\), and replace \(\rho\) by the injection \(\rho'\) which agrees with \(\rho\) on \(L - \{p\}\) and such that \(\rho'(p') = \rho(p)\). Thus, we can always assume that \(L \cap I = \emptyset\). Since \(u_p\) is a linear combination of \((v_j)_{j \in J}\)
and the families \((u_i)_{i \in (I - \{p\})} \cup (v_{p(l)})_{l \in L}\) and \((v_j)_{j \in J}\) generate the same subspace of \(E\), \(u_p\) is a linear combination of \((u_i)_{i \in (I - \{p\})} \cup (v_{p(l)})_{l \in L}\). Let

\[
    u_p = \sum_{i \in (I - \{p\})} \lambda_i u_i + \sum_{l \in L} \lambda_l v_{p(l)}. \tag{1}
\]

If \(\lambda_l = 0\) for all \(l \in L\), we have

\[
    \sum_{i \in (I - \{p\})} \lambda_i u_i - u_p = 0,
\]

contradicting the fact that \((u_i)_{i \in I}\) is linearly independent. Thus, \(\lambda_l \neq 0\) for some \(l \in L\), say \(l = q\). Since \(\lambda_q \neq 0\), we have

\[
    v_{\rho(q)} = \sum_{i \in (I - \{p\})} (-\lambda_q^{-1} \lambda_i) u_i + \lambda_q^{-1} u_p + \sum_{l \in (L - \{q\})} (-\lambda_q^{-1} \lambda_l) v_{p(l)}. \tag{2}
\]

We claim that the families \((u_i)_{i \in (I - \{p\})} \cup (v_{p(l)})_{l \in L}\) and \((u_i)_{i \in I} \cup (v_{p(l)})_{l \in (L - \{q\})}\) generate the same subset of \(E\). Indeed, the second family is obtained from the first by replacing \(v_{\rho(q)}\) by \(u_p\), and vice-versa, and \(u_p\) is a linear combination of \((u_i)_{i \in (I - \{p\})} \cup (v_{p(l)})_{l \in L}\), by (1), and \(v_{\rho(q)}\) is a linear combination of \((u_i)_{i \in I} \cup (v_{p(l)})_{l \in (L - \{q\})}\), by (2). Thus, the families \((u_i)_{i \in I} \cup (v_{p(l)})_{l \in (L - \{q\})}\) and \((v_j)_{j \in J}\) generate the same subspace of \(E\), and the proposition holds for \(L - \{q\}\) and the restriction of the injection \(\rho: L \to J\) to \(L - \{q\}\), since \(L \cap I = \emptyset\) and \(|L| = n - m\) imply that \((L - \{q\}) \cap I = \emptyset\) and \(|L - \{q\}| = n - (m + 1)\). \(\square\)

Actually, one can prove that Proposition 2.4 implies Theorem 2.2 when the vector space is finitely generated. Putting Theorem 2.2 and Proposition 2.4 together, we obtain the following fundamental theorem.

**Theorem 2.5** Let \(E\) be a finitely generated vector space. Any family \((u_i)_{i \in I}\) generating \(E\) contains a subfamily \((v_j)_{j \in J}\) which is a basis of \(E\). Furthermore, for every two bases \((u_i)_{i \in I}\) and \((v_j)_{j \in J}\) of \(E\), we have \(|I| = |J| = n|.

**Proof.** The first part follows immediately by applying Theorem 2.2 with \(L = \emptyset\) and \(S = (u_i)_{i \in I}\). Assume that \((u_i)_{i \in I}\) and \((v_j)_{j \in J}\) are bases of \(E\). Since \((u_i)_{i \in I}\) is linearly independent and \((v_j)_{j \in J}\) spans \(E\), proposition 2.4 implies that \(|I| \leq |J|\). A symmetric argument yields \(|J| \leq |I|\). \(\square\)

**Remark:** Theorem 2.5 also holds for vector spaces that are not finitely generated. This can be shown as follows. Let \((u_i)_{i \in I}\) be a basis of \(E\), let \((v_j)_{j \in J}\) be a generating family of \(E\), and assume that \(I\) is infinite. For every \(j \in J\), let \(L_j \subseteq I\) be the finite set

\[
    L_j = \{i \in I \mid v_j = \sum_{i \in I} v_i u_i, \; v_i \neq 0\}.
\]
Let $L = \bigcup_{j \in J} L_j$. Since $(u_i)_{i \in I}$ is a basis of $E$, we must have $I = L$, since otherwise $(u_i)_{i \in L}$ would be another basis of $E$, and by Lemma 2.1, this would contradict the fact that $(u_i)_{i \in I}$ is linearly independent. Furthermore, $J$ must be infinite, since otherwise, because the $L_j$ are finite, $I$ would be finite. But then, since $I = \bigcup_{j \in J} L_j$ with $J$ infinite and the $L_j$ finite, by a standard result of set theory, $|I| \leq |J|$. If $(v_j)_{j \in J}$ is also a basis, by a symmetric argument, we obtain $|J| \leq |I|$, and thus, $|I| = |J|$ for any two bases $(u_i)_{i \in I}$ and $(v_j)_{j \in J}$ of $E$.

When $|I|$ is infinite, we say that $E$ is of infinite dimension, the dimension $|I|$ being a cardinal number which depends only on the vector space $E$. The dimension of a vector space $E$ is denoted by $\dim(E)$. Clearly, if the field $K$ itself is viewed as a vector space, then every family $(a)$ where $a \in K$ and $a \neq 0$ is a basis. Thus $\dim(K) = 1$.

Let $(u_i)_{i \in I}$ be a basis of a vector space $E$. For any vector $v \in E$, since the family $(u_i)_{i \in I}$ generates $E$, there is a family $(\lambda_i)_{i \in I}$ of scalars in $K$, such that

$$v = \sum_{i \in I} \lambda_i u_i.$$ 

A very important fact is that the family $(\lambda_i)_{i \in I}$ is unique.

**Proposition 2.6** Given a vector space $E$, let $(u_i)_{i \in I}$ be a family of vectors in $E$. Let $v \in E$, and assume that $v = \sum_{i \in I} \lambda_i u_i$. Then, the family $(\lambda_i)_{i \in I}$ of scalars such that $v = \sum_{i \in I} \lambda_i u_i$ is unique iff $(u_i)_{i \in I}$ is linearly independent.

**Proof.** First, assume that $(u_i)_{i \in I}$ is linearly independent. If $(\mu_i)_{i \in I}$ is another family of scalars in $K$ such that $v = \sum_{i \in I} \mu_i u_i$, then we have

$$\sum_{i \in I} (\lambda_i - \mu_i) u_i = 0,$$

and since $(u_i)_{i \in I}$ is linearly independent, we must have $\lambda_i - \mu_i = 0$ for all $i \in I$, that is, $\lambda_i = \mu_i$ for all $i \in I$. The converse is shown by contradiction. If $(u_i)_{i \in I}$ was linearly dependent, there would be a family $(\mu_i)_{i \in I}$ of scalars not all null such that

$$\sum_{i \in I} \mu_i u_i = 0$$

and $\mu_j \neq 0$ for some $j \in I$. But then,

$$v = \sum_{i \in I} \lambda_i u_i + 0 = \sum_{i \in I} \lambda_i u_i + \sum_{i \in I} \mu_i u_i = \sum_{i \in I} (\lambda_i + \mu_i) u_i,$$

with $\lambda_j \neq \lambda_j + \mu_j$ since $\mu_j \neq 0$, contradicting the assumption that $(\lambda_i)_{i \in I}$ is the unique family such that $v = \sum_{i \in I} \lambda_i u_i$. \[\Box\]
If \((u_i)_{i \in I}\) is a basis of a vector space \(E\), for any vector \(v \in E\), if \((v_i)_{i \in I}\) is the unique family of scalars in \(K\) such that
\[
v = \sum_{i \in I} v_i u_i,
\]
each \(v_i\) is called the component (or coordinate) of index \(i\) of \(v\) with respect to the basis \((u_i)_{i \in I}\).

Given a field \(K\) and any (nonempty) set \(I\), we can form a vector space \(K(I)\) which, in some sense, is the standard vector space of dimension \(|I|\).

**Definition 2.9** Given a field \(K\) and any (nonempty) set \(I\), let \(K(I)\) be the subset of the cartesian product \(K^I\) consisting of all families \((\lambda_i)_{i \in I}\) with finite support of scalars in \(K\).\footnote{Where \(K^I\) denotes the set of all functions from \(I\) to \(K\).}

We define addition and multiplication by a scalar as follows:
\[
(\lambda_i)_{i \in I} + (\mu_i)_{i \in I} = (\lambda_i + \mu_i)_{i \in I},
\]
and
\[
\lambda \cdot (\mu_i)_{i \in I} = (\lambda \mu_i)_{i \in I}.
\]

It is immediately verified that addition and multiplication by a scalar are well defined. Thus, \(K(I)\) is a vector space. Furthermore, because families with finite support are considered, the family \((e_i)_{i \in I}\) of vectors \(e_i\), defined such that \((e_i)_j = 0\) if \(j \neq i\) and \((e_i)_i = 1\), is clearly a basis of the vector space \(K(I)\). When \(I = \{1, \ldots, n\}\), we denote \(K(I)\) by \(K^n\). The function \(\iota: I \to K(I)\), such that \(\iota(i) = e_i\) for every \(i \in I\), is clearly an injection.

When \(I\) is a finite set, \(K(I) = K^I\), but this is false when \(I\) is infinite. In fact, \(\dim(K(I)) = |I|\), but \(\dim(K^I)\) is strictly greater when \(I\) is infinite.

Many interesting mathematical structures are vector spaces. A very important example is the set of linear maps between two vector spaces to be defined in the next section. Here is an example that will prepare us for the vector space of linear maps.

**Example 2.10** Let \(X\) be any nonempty set and let \(E\) be a vector space. The set of all functions \(f: X \to E\) can be made into a vector space as follows: Given any two functions \(f: X \to E\) and \(g: X \to E\), let \((f + g): X \to E\) be defined such that
\[
(f + g)(x) = f(x) + g(x)
\]
for all \(x \in X\), and for every \(\lambda \in K\), let \(\lambda f: X \to E\) be defined such that
\[
(\lambda f)(x) = \lambda f(x)
\]
for all \(x \in X\). The axioms of a vector space are easily verified. Now, let \(E = K\), and let \(I\) be the set of all nonempty subsets of \(X\). For every \(S \in I\), let \(f_S: X \to E\) be the function such that \(f_S(x) = 1\) iff \(x \in S\), and \(f_S(x) = 0\) iff \(x \notin S\). We leave as an exercise to show that \((f_S)_{S \in I}\) is linearly independent.
2.5 Linear Maps

A function between two vector spaces that preserves the vector space structure is called a homomorphism of vector spaces, or linear map. Linear maps formalize the concept of linearity of a function. In the rest of this section, we assume that all vector spaces are over a given field $K$ (say $\mathbb{R}$).

**Definition 2.10** Given two vector spaces $E$ and $F$, a linear map between $E$ and $F$ is a function $f: E \rightarrow F$ satisfying the following two conditions:

\[
\begin{align*}
  f(x + y) &= f(x) + f(y) & \text{for all } x, y \in E; \\
  f(\lambda x) &= \lambda f(x) & \text{for all } \lambda \in K, x \in E.
\end{align*}
\]

Setting $x = y = 0$ in the first identity, we get $f(0) = 0$. The basic property of linear maps is that they transform linear combinations into linear combinations. Given a family $(u_i)_{i \in I}$ of vectors in $E$, given any family $(\lambda_i)_{i \in I}$ of scalars in $K$, we have

\[
f(\sum_{i \in I} \lambda_i u_i) = \sum_{i \in I} \lambda_i f(u_i).
\]

The above identity is shown by induction on the size of the support of the family $(\lambda_i u_i)_{i \in I}$, using the properties of Definition 2.10.

**Example 2.11**

1. The map $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ defined such that

\[
\begin{align*}
  x' &= x - y \\
  y' &= x + y
\end{align*}
\]

is a linear map.

2. The map $D: \mathbb{R}[X] \rightarrow \mathbb{R}[X]$ defined such that

\[
D(f(X)) = f'(X),
\]

where $f'(X)$ is the derivative of the polynomial $f(X)$, is a linear map.

Given a linear map $f: E \rightarrow F$, we define its **image (or range)** $\text{Im } f = f(E)$, as the set

\[
\text{Im } f = \{ y \in F \mid f(x) = y, \text{ for some } x \in E \},
\]

and its **Kernel (or nullspace)** $\text{Ker } f = f^{-1}(0)$, as the set

\[
\text{Ker } f = \{ x \in E \mid f(x) = 0 \}.
\]
2.5. LINEAR MAPS

Proposition 2.7. Given a linear map $f: E \to F$, the set $\text{Im} f$ is a subspace of $F$ and the set $\text{Ker} f$ is a subspace of $E$. The linear map $f: E \to F$ is injective iff $\text{Ker} f = 0$ (where 0 is the trivial subspace $\{0\}$).

Proof. Given any $x, y \in \text{Im} f$, there are some $u, v \in E$ such that $x = f(u)$ and $y = f(v)$, and for all $\lambda, \mu \in K$, we have
\[
f(\lambda u + \mu v) = \lambda f(u) + \mu f(v) = \lambda x + \mu y,
\]
and thus, $\lambda x + \mu y \in \text{Im} f$, showing that $\text{Im} f$ is a subspace of $F$. Given any $x, y \in \text{Ker} f$, we have $f(x) = 0$ and $f(y) = 0$, and thus,
\[
f(\lambda x + \mu y) = \lambda f(x) + \mu f(y) = 0,
\]
that is, $\lambda x + \mu y \in \text{Ker} f$, showing that $\text{Ker} f$ is a subspace of $E$. Note that $f(x) = f(y)$ iff $f(x - y) = 0$. Thus, $f$ is injective iff $\text{Ker} f = 0$. $\square$

A fundamental property of bases in a vector space is that they allow the definition of linear maps as unique homomorphic extensions, as shown in the following proposition.

Proposition 2.8. Given any two vector spaces $E$ and $F$, given any basis $(u_i)_{i \in I}$ of $E$, given any other family of vectors $(v_i)_{i \in I}$ in $F$, there is a unique linear map $f: E \to F$ such that $f(u_i) = v_i$ for all $i \in I$. Furthermore, $f$ is injective iff $(v_i)_{i \in I}$ is linearly independent, and $f$ is surjective iff $(v_i)_{i \in I}$ generates $F$.

Proof. If such a linear map $f: E \to F$ exists, since $(u_i)_{i \in I}$ is a basis of $E$, every vector $x \in E$ can written uniquely as a linear combination
\[
x = \sum_{i \in I} x_i u_i,
\]
and by linearity, we must have
\[
f(x) = \sum_{i \in I} x_i f(u_i) = \sum_{i \in I} x_i v_i.
\]
Define the function $f: E \to F$, by letting
\[
f(x) = \sum_{i \in I} x_i v_i
\]
for every $x = \sum_{i \in I} x_i u_i$. It is easy to verify that $f$ is indeed linear, it is unique by the previous reasoning, and obviously, $f(u_i) = v_i$.

Now, assume that $f$ is injective. Let $(\lambda_i)_{i \in I}$ be any family of scalars, and assume that
\[
\sum_{i \in I} \lambda_i v_i = 0.
\]
Since \( v_i = f(u_i) \) for every \( i \in I \), we have
\[
f(\sum_{i \in I} \lambda_i u_i) = \sum_{i \in I} \lambda_i f(u_i) = \sum_{i \in I} \lambda_i v_i = 0.
\]

Since \( f \) is injective iff Ker \( f = 0 \), we have
\[
\sum_{i \in I} \lambda_i u_i = 0,
\]
and since \( (u_i)_{i \in I} \) is a basis, we have \( \lambda_i = 0 \) for all \( i \in I \), and \( (u_i)_{i \in I} \) is linearly independent. Conversely, assume that \( (v_i)_{i \in I} \) is linearly independent. If
\[
f(\sum_{i \in I} \lambda_i u_i) = 0,
\]
then
\[
\sum_{i \in I} \lambda_i v_i = \sum_{i \in I} \lambda_i f(u_i) = f(\sum_{i \in I} \lambda_i u_i) = 0,
\]
and \( \lambda_i = 0 \) for all \( i \in I \), since \( (v_i)_{i \in I} \) is linearly independent. Since \( (u_i)_{i \in I} \) is a basis of \( E \), we just showed that Ker \( f = 0 \), and \( f \) is injective. The part where \( f \) is surjective is left as a simple exercise. \( \square \)

By the second part of Proposition 2.8, an injective linear map \( f: E \to F \) sends a basis \( (u_i)_{i \in I} \) to a linearly independent family \( (f(u_i))_{i \in I} \) of \( F \), which is also a basis when \( f \) is bijective. Also, when \( E \) and \( F \) have the same finite dimension \( n \), \( (u_i)_{i \in I} \) is a basis of \( E \), and \( f: E \to F \) is injective, then \( (f(u_i))_{i \in I} \) is a basis of \( F \) (by Proposition 2.3).

We can now show that the vector space \( K^{(I)} \) of Definition 2.9 has a universal property that amounts to saying that \( K^{(I)} \) is the vector space freely generated by \( I \). Recall that \( \iota: I \to K^{(I)} \), such that \( \iota(i) = e_i \) for every \( i \in I \), is an injection from \( I \) to \( K^{(I)} \).

**Proposition 2.9** Given any set \( I \), for any vector space \( F \), and for any function \( f: I \to F \), there is a unique linear map \( \overline{f}: K^{(I)} \to F \), such that
\[
f = \overline{f} \circ \iota,
\]
as in the following diagram:

\[
\begin{array}{c}
I \xrightarrow{\iota} K^{(I)} \\
\downarrow f \quad \downarrow \overline{f} \\
F
\end{array}
\]

**Proof.** If such a linear map \( \overline{f}: K^{(I)} \to F \) exists, since \( f = \overline{f} \circ \iota \), we must have
\[
f(i) = \overline{f}(\iota(i)) = \overline{f}(e_i),
\]
for every \( i \in I \). However, the family \((e_i)_{i \in I}\) is a basis of \( K^{(I)}\), and \((f(i))_{i \in I}\) is a family of vectors in \( F \), and by Proposition 2.8, there is a unique linear map \( \mathcal{F}:K^{(I)} \to F \) such that \( \mathcal{F}(e_i) = f(i) \) for every \( i \in I \), which proves the existence and uniqueness of a linear map \( \mathcal{F} \) such that \( f = \mathcal{F} \circ \iota \). □

The following simple proposition is also useful.

**Proposition 2.10** Given any two vector spaces \( E \) and \( F \), with \( F \) nontrivial, given any family \((u_i)_{i \in I}\) of vectors in \( E \), the following properties hold:

1. The family \((u_i)_{i \in I}\) generates \( E \) iff for every family of vectors \((v_i)_{i \in I}\) in \( F \), there is at most one linear map \( f:E \to F \) such that \( f(u_i) = v_i \) for all \( i \in I \).

2. The family \((u_i)_{i \in I}\) is linearly independent iff for every family of vectors \((v_i)_{i \in I}\) in \( F \), there is some linear map \( f:E \to F \) such that \( f(u_i) = v_i \) for all \( i \in I \).

**Proof.** (1) If there is any linear map \( f:E \to F \) such that \( f(u_i) = v_i \) for all \( i \in I \), since \((u_i)_{i \in I}\) generates \( E \), every vector \( x \in E \) can be written as some linear combination

\[
x = \sum_{i \in I} x_i u_i,
\]

and by linearity, we must have

\[
f(x) = \sum_{i \in I} x_i f(u_i) = \sum_{i \in I} x_i v_i.
\]

This shows that \( f \) is unique if it exists. Conversely, assume that \((u_i)_{i \in I}\) does not generate \( E \). Since \( F \) is nontrivial, there is some some vector \( y \in F \) such that \( y \neq 0 \). Since \((u_i)_{i \in I}\) does not generate \( E \), there is some vector \( w \in E \) that is not in the subspace generated by \((u_i)_{i \in I}\). By Theorem 2.2, there is a linearly independent subfamily \((u_i)_{i \in I_0}\) of \((u_i)_{i \in I}\) generating the same subspace. Since by hypothesis, \( w \in E \) is not in the subspace generated by \((u_i)_{i \in I_0}\), by Lemma 2.1 and by Theorem 2.2 again, there is a basis \((e_j)_{j \in I_0 \cup J}\) of \( E \), such that \( e_i = u_i \), for all \( i \in I_0 \), and \( w = e_{j_0} \), for some \( j_0 \in J \). Letting \((v_i)_{i \in I}\) be the family in \( F \) such that \( v_i = 0 \) for all \( i \in I \), defining \( f:E \to F \) to be the constant linear map with value 0, we have a linear map such that \( f(u_i) = 0 \) for all \( i \in I \). By Proposition 2.8, there is a unique linear map \( g:E \to F \) such that \( g(w) = y \), and \( g(e_j) = 0 \), for all \( j \in (I_0 \cup J) - \{j_0\} \). By definition of the basis \((e_j)_{j \in I_0 \cup J}\) of \( E \), we have, \( g(u_i) = 0 \) for all \( i \in I \), and since \( f \neq g \), this contradicts the fact that there is at most one such map.

(2) If the family \((u_i)_{i \in I}\) is linearly independent, then by Theorem 2.2, \((u_i)_{i \in I}\) can be extended to a basis of \( E \), and the conclusion follows by Proposition 2.8. Conversely, assume that \((u_i)_{i \in I}\) is linearly dependent. Then, there is some family \((\lambda_i)_{i \in I}\) of scalars (not all zero) such that

\[
\sum_{i \in I} \lambda_i u_i = 0.
\]
By the assumption, for any nonzero vector, \( y \in F \), for every \( i \in I \), there is some linear map \( f_i : E \to F \), such that \( f_i(u_i) = y \), and \( f_i(u_j) = 0 \), for \( j \in I \setminus \{ i \} \). Then, we would get

\[
0 = f_i(\sum_{i \in I} \lambda_i u_i) = \sum_{i \in I} \lambda_i f_i(u_i) = \lambda_i y,
\]
and since \( y \neq 0 \), this implies \( \lambda_i = 0 \), for every \( i \in I \). Thus, \( (u_i)_{i \in I} \) is linearly independent. \( \square \)

Although in this book, we will not have many occasions to use quotient spaces, they are fundamental in algebra. The next section may be omitted until needed.

2.6 Quotient Spaces

Let \( E \) be a vector space, and let \( M \) be any subspace of \( E \). The subspace \( M \) induces a relation \( \equiv_M \) on \( E \), defined as follows: For all \( u, v \in E \),

\[
u \equiv_M v \text{ iff } u - v \in M.
\]

We have the following simple proposition.

**Proposition 2.11** Given any vector space \( E \) and any subspace \( M \) of \( E \), the relation \( \equiv_M \) is an equivalence relation with the following two congruental properties:

1. If \( u_1 \equiv_M v_1 \) and \( u_2 \equiv_M v_2 \), then \( u_1 + u_2 \equiv_M v_1 + v_2 \), and
2. if \( u \equiv_M v \), then \( \lambda u \equiv_M \lambda v \).

**Proof.** It is obvious that \( \equiv_M \) is an equivalence relation. Note that \( u_1 \equiv_M v_1 \) and \( u_2 \equiv_M v_2 \) are equivalent to \( u_1 - v_1 = w_1 \) and \( u_2 - v_2 = w_2 \), with \( w_1, w_2 \in M \), and thus,

\[
(u_1 + u_2) - (v_1 + v_2) = w_1 + w_2,
\]
and \( w_1 + w_2 \in M \), since \( M \) is a subspace of \( E \). Thus, we have \( u_1 + u_2 \equiv_M v_1 + v_2 \). If \( u - v = w \), with \( w \in M \), then

\[
\lambda u - \lambda v = \lambda w,
\]
and \( \lambda w \in M \), since \( M \) is a subspace of \( E \), and thus \( \lambda u \equiv_M \lambda v \). \( \square \)

Proposition 2.11 shows that we can define addition and multiplication by a scalar on the set \( E/M \) of equivalence classes of the equivalence relation \( \equiv_M \).

**Definition 2.11** Given any vector space \( E \) and any subspace \( M \) of \( E \), we define the following operations of addition and multiplication by a scalar on the set \( E/M \) of equivalence classes of the equivalence relation \( \equiv_M \) as follows: for any two equivalence classes \( [u], [v] \in E/M \), we have

\[
[u] + [v] = [u + v],
\]

\[
\lambda [u] = [\lambda u].
\]
By Proposition 2.11, the above operations do not depend on the specific choice of representatives in the equivalence classes \([u], [v] \in E/M\). It is also immediate to verify that \(E/M\) is a vector space. The function \(\pi: E \to E/F\), defined such that \(\pi(u) = [u]\) for every \(u \in E\), is a surjective linear map called the natural projection of \(E\) onto \(E/F\). The vector space \(E/M\) is called the quotient space of \(E\) by the subspace \(M\).

Given any linear map \(f: E \to F\), we know that \(\text{Ker } f\) is a subspace of \(E\), and it is immediately verified that \(\text{Im } f\) is isomorphic to the quotient space \(E/\text{Ker } f\).

### 2.7 Matrices

Proposition 2.8 shows that given two vector spaces \(E\) and \(F\) and a basis \((u_j)_{j \in J}\) of \(E\), every linear map \(f: E \to F\) is uniquely determined by the family \((f(u_j))_{j \in J}\) of the images under \(f\) of the vectors in the basis \((u_j)_{j \in J}\). Thus, in particular, taking \(F = K^{|J|}\), we get an isomorphism between any vector space \(E\) of dimension \(|J|\) and \(K^{|J|}\). If \(J = \{1, \ldots, n\}\), a vector space \(E\) of dimension \(n\) is isomorphic to the vector space \(K^n\). If we also have a basis \((v_i)_{i \in I}\) of \(F\), then every vector \(f(u_j)\) can be written in a unique way as

\[
f(u_j) = \sum_{i \in I} a_{ij} v_i,
\]

where \(j \in J\), for a family \((a_{ij})_{i \in I}\) of \(E\), and the index \(I\) to the basis \((v_i)_{i \in I}\) of \(F\), so that the rows of the matrix \(M(f)\) associated with \(f: E \to F\) are indexed by \(I\), and the columns of the matrix \(M(f)\) are indexed by \(J\). Obviously, this causes a mildly unpleasant reversal. If we had considered the bases \((u_i)_{i \in I}\) of \(E\) and \((v_j)_{j \in J}\) of \(F\), we would obtain a \(J \times I\)-matrix \(M(f) = (a_{ji})_{j \in J, i \in I}\). No matter what we do, there will be a reversal! We decided to stick to the bases \((u_j)_{j \in J}\) of \(E\) and \((v_i)_{i \in I}\) of \(F\), so that we get an \(I \times J\)-matrix \(M(f)\), knowing that we may occasionally suffer from this decision!

When \(I\) and \(J\) are finite, and say, when \(|I| = m\) and \(|J| = n\), the linear map \(f\) is determined by the matrix \(M(f)\) whose entries in the \(j\)-th column are the components of the vector \(f(u_j)\) over the basis \((v_1, \ldots, v_m)\), that is, the matrix

\[
M(f) = \begin{pmatrix}
    a_{11} & a_{12} & \cdots & a_{1n} \\
    a_{21} & a_{22} & \cdots & a_{2n} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{m1} & a_{m2} & \cdots & a_{mn}
\end{pmatrix}
\]

whose entry on row \(i\) and column \(j\) is \(a_{ij}\) (\(1 \leq i \leq m, 1 \leq j \leq n\)).
Given vector spaces $E$, $F$, and $G$, and linear maps $f: E \to F$ and $g: F \to G$, it is easily verified that the composition $g \circ f: E \to G$ of $f$ and $g$ is a linear map. A linear map $f: E \to F$ is an isomorphism iff there is a linear map $g: F \to E$, such that $g \circ f = \text{id}_E$, and $f \circ g = \text{id}_F$. It is immediately verified that such a map $g$ is unique. The map $g$ is called the inverse of $f$ and it is also denoted by $f^{-1}$.

One can verify that if $f: E \to F$ is a bijective linear map, then its inverse $f^{-1}: F \to E$ is also a linear map, and thus $f$ is an isomorphism. We leave as an easy exercise to show that if $E$ and $F$ are two vector spaces, $(u_i)_{i \in I}$ is a basis of $E$, and $f: E \to F$ is a linear map which is an isomorphism, then the family $(f(u_i))_{i \in I}$ is a basis of $F$.

The set of all linear maps between two vector spaces $E$ and $F$ is denoted as $L(E; F)$. The set $L(E; F)$ is a vector space under the operations defined at the end of Section 2.1, namely

$$(f + g)(x) = f(x) + g(x)$$

for all $x \in E$, and

$$(\lambda f)(x) = \lambda f(x)$$

for all $x \in E$. The point worth checking carefully is that $\lambda f$ is indeed a linear map, which uses the commutativity of $*$ in the field $K$. Indeed, we have

$$(\lambda f)(\mu x) = \lambda f(\mu x) = \lambda \mu f(x) = \mu \lambda f(x) = \mu(\lambda f)(x).$$

When $E$ and $F$ have finite dimensions, the vector space $L(E; F)$ also has finite dimension, as we shall see shortly. When $E = F$, a linear map $f: E \to E$ is also called an endomorphism. It is also important to note that composition confers to $L(E; E)$ a ring structure. Indeed, composition is an operation $\circ: L(E; E) \times L(E; E) \to L(E; E)$, which is associative and has an identity $\text{id}_E$, and the distributivity properties hold:

$$(g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f;$$

$$g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2.$$
and similarly every vector \( y \in F \) can be written in a unique way as
\[
y = y_1 v_1 + \cdots + y_m v_m.
\]
Let \( f: E \to F \) be a linear map between \( E \) and \( F \). Then, for every \( x = x_1 u_1 + \cdots + x_n u_n \) in \( E \), by linearity, we have
\[
f(x) = x_1 f(u_1) + \cdots + x_n f(u_n).
\]
Let
\[
f(u_j) = a_{1j} v_1 + \cdots + a_{mj} v_m,
\]
or more concisely,
\[
f(u_j) = \sum_{i=1}^{m} a_{ij} v_i,
\]
for every \( j, 1 \leq j \leq n \). Then, substituting the right-hand side of each \( f(u_j) \) into the expression for \( f(x) \), we get
\[
f(x) = x_1 \left( \sum_{i=1}^{m} a_{i1} v_i \right) + \cdots + x_n \left( \sum_{i=1}^{m} a_{in} v_i \right),
\]
which, by regrouping terms to obtain a linear combination of the \( v_i \), yields
\[
f(x) = \left( \sum_{j=1}^{n} a_{1j} x_j \right) v_1 + \cdots + \left( \sum_{j=1}^{n} a_{mj} x_j \right) v_m.
\]
Thus, letting \( f(x) = y = y_1 v_1 + \cdots + y_m v_m \), we have
\[
y_i = \sum_{j=1}^{m} a_{ij} x_j \tag{1}
\]
for all \( i, 1 \leq i \leq m \). Let us now consider how the composition of linear maps is expressed in terms of bases.

Let \( E, F, \) and \( G \) be three vectors spaces with respective bases \( (u_1, \ldots, u_p) \) for \( E \), \( (v_1, \ldots, v_n) \) for \( F \), and \( (w_1, \ldots, w_m) \) for \( G \). Let \( g: E \to F \) and \( f: F \to G \) be linear maps. As explained earlier, \( g: E \to F \) is determined by the images of the basis vectors \( u_j \), and \( f: F \to G \) is determined by the images of the basis vectors \( v_k \). We would like to understand how \( f \circ g: E \to G \) is determined by the images of the basis vectors \( u_j \).

**Remark:** Note that we are considering linear maps \( g: E \to F \) and \( f: F \to G \), instead of \( f: E \to F \) and \( g: F \to G \), which yields the composition \( f \circ g: E \to G \) instead of \( g \circ f: E \to G \). Our perhaps unusual choice is motivated by the fact that if \( f \) is represented by a matrix \( M(f) = (a_{ik}) \) and \( g \) is represented by a matrix \( M(g) = (b_{kj}) \), then \( f \circ g: E \to G \) is represented by the product \( AB \) of the matrices \( A \) and \( B \). If we had adopted the other choice
where \( f: E \to F \) and \( g: F \to G \), then \( g \circ f: E \to G \) would be represented by the product \( BA \). Personally, we find it easier to remember the formula for the entry in row \( i \) and column of \( j \) of the product of two matrices when this product is written by \( AB \), rather than \( BA \). Obviously, this is a matter of taste! We will have to live with our perhaps unorthodox choice.

Thus, let

\[
f(v_k) = \sum_{i=1}^{m} a_{ik} w_i,
\]

for every \( k, 1 \leq k \leq n \), and let

\[
g(u_j) = \sum_{k=1}^{n} b_{kj} v_k,
\]

for every \( j, 1 \leq j \leq p \). By previous considerations, for every

\[
x = x_1 u_1 + \cdots + x_p u_p,
\]

letting \( g(x) = y = y_1 v_1 + \cdots + y_n v_n \), we have

\[
y_k = \sum_{j=1}^{p} b_{kj} x_j
\]

(2)

for all \( k, 1 \leq k \leq n \), and for every

\[
y = y_1 v_1 + \cdots + y_n v_n,
\]

letting \( f(y) = z = z_1 w_1 + \cdots + z_m w_m \), we have

\[
z_i = \sum_{k=1}^{n} a_{ik} y_k
\]

(3)

for all \( i, 1 \leq i \leq m \). Then, if \( y = g(x) \) and \( z = f(y) \), we have \( z = f(g(x)) \), and in view of (2) and (3), we have

\[
z_i = \sum_{k=1}^{n} a_{ik} \left( \sum_{j=1}^{p} b_{kj} x_j \right)
\]

\[
= \sum_{k=1}^{n} \left( \sum_{j=1}^{p} a_{ik} b_{kj} \right) x_j
\]

\[
= \sum_{j=1}^{p} \left( \sum_{k=1}^{n} a_{ik} b_{kj} \right) x_j
\]

\[
= \sum_{j=1}^{p} \left( \sum_{k=1}^{n} a_{ik} b_{kj} \right) x_j.
\]
Thus, defining $c_{ij}$ such that
\[ c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}, \]
for $1 \leq i \leq m$, and $1 \leq j \leq p$, we have
\[ z_i = \sum_{j=1}^{p} c_{ij} x_j \quad (4) \]

Identity (4) suggests defining a multiplication operation on matrices, and we proceed to do so. We have the following definitions.

**Definition 2.12** Given a field $K$, an $m \times n$-matrix is a family $(a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}$ of scalars in $K$, represented as an array
\[
\begin{pmatrix}
\begin{array}{cccc}
  a_{11} & a_{12} & \cdots & a_{1n} \\
  a_{21} & a_{22} & \cdots & a_{2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{m1} & a_{m2} & \cdots & a_{mn}
\end{array}
\end{pmatrix}
\]

In the special case where $m = 1$, we have a *row vector*, represented as
\[
(a_{11}, \ldots, a_{1n})
\]
and in the special case where $n = 1$, we have a *column vector*, represented as
\[
\begin{pmatrix}
  a_{11} \\
  \vdots \\
  a_{m1}
\end{pmatrix}
\]

In these last two cases, we usually omit the constant index 1 (first index in case of a row, second index in case of a column). The set of all $m \times n$-matrices is denoted by $M_{m,n}(K)$ or $M_{m,n}$. An $n \times n$-matrix is called a *square matrix of dimension* $n$. The set of all square square matrices of dimension $n$ is denoted by $M_n(K)$, or $M_n$.

**Remark:** As defined, a matrix $A = (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}$ is a *family*, that is, a function from $\{1,2,\ldots,m\} \times \{1,2,\ldots,n\}$ to $K$. As such, there is no reason to assume an ordering on the indices. Thus, the matrix $A$ can be represented in many different ways as an array, by adopting different orders for the rows or the columns. However, it is customary (and usually convenient) to assume the natural ordering on the sets $\{1,2,\ldots,m\}$ and $\{1,2,\ldots,n\}$, and to represent $A$ as an array according to this ordering of the rows and columns.

We also define some operations on matrices as follows.
Definition 2.13 Given two \( m \times n \) matrices \( A = (a_{ij}) \) and \( B = (b_{ij}) \), we define their sum \( A + B \) as the matrix \( C = (c_{ij}) \) such that \( c_{ij} = a_{ij} + b_{ij} \). Given a scalar \( \lambda \in K \), we define the matrix \( \lambda A \) as the matrix \( C = (c_{ij}) \) such that \( c_{ij} = \lambda a_{ij} \). Given an \( m \times n \) matrices \( A = (a_{ik}) \) and an \( n \times p \) matrices \( B = (b_{kj}) \), we define their product \( AB \) as the \( m \times p \) matrix \( C = (c_{ij}) \) such that

\[
c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj},
\]

for \( 1 \leq i \leq m, \) and \( 1 \leq j \leq p \). Given an \( m \times n \) matrix \( A = (a_{ij}) \), its transpose \( A^\top = (a_{ji}) \), is the \( n \times m \)-matrix such that \( a_{ji}^\top = a_{ij} \), for all \( i, 1 \leq i \leq m, \) and all \( j, 1 \leq j \leq n \). The transpose of a matrix \( A \) is sometimes denoted by \( A^t \), or even by \( {}^tA \).

In the product \( AB = C \) shown below

\[
\begin{pmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{m1} & a_{m2} & \cdots & a_{mn}
\end{pmatrix}
\begin{pmatrix}
b_{11} & b_{12} & \cdots & b_{1p} \\
b_{21} & b_{22} & \cdots & b_{2p} \\
\vdots & \vdots & \ddots & \vdots \\
b_{n1} & b_{n2} & \cdots & b_{np}
\end{pmatrix}
= \begin{pmatrix}
c_{11} & c_{12} & \cdots & c_{1p} \\
c_{21} & c_{22} & \cdots & c_{2p} \\
\vdots & \vdots & \ddots & \vdots \\
c_{m1} & c_{m2} & \cdots & c_{mp}
\end{pmatrix}
\]

note that the entry of index \( i \) and \( j \) of the matrix \( AB \) is obtained by multiplying the matrices \( A \) and \( B \) can be identified with the product of the row matrix corresponding to the \( i \)-th row of \( A \) with the column matrix corresponding to the \( j \)-column of \( B \):

\[
(a_{i1}, \ldots, a_{in}) \begin{pmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{pmatrix} = (\sum_{k=1}^{n} a_{ik} b_{kj})
\]

The square matrix \( I_n \) of dimension \( n \) containing 1 on the diagonal and 0 everywhere else is called the identity matrix. It is denoted as

\[
\begin{pmatrix}
1 & 0 & \cdots & 0 \\
0 & 1 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 1
\end{pmatrix}
\]

Note that the transpose \( A^\top \) of a matrix \( A \) has the property that the \( j \)-th row of \( A^\top \) is the \( j \)-th column of \( A \). In other words, transposition exchanges the rows and the columns of a matrix. For every square matrix \( A \) of dimension \( n \), it is immediately verified that \( AI_n = I_n A = A \). If a matrix \( B \) such that \( AB = BA = I_n \) exists, then it is unique, and it is called the inverse of \( A \). The matrix \( B \) is also denoted by \( A^{-1} \).

Consider the \( m \times n \)-matrices \( E_{ij} = (e_{hk}) \), defined such that \( e_{ij} = 1 \), and \( e_{hk} = 0 \), if \( h \neq i \) or \( k \neq j \). It is clear that every matrix \( A = (a_{ij}) \in M_{m,n}(K) \) can be written in a unique way as

\[
A = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} E_{ij}.
\]
Thus, the family \((E_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}\) is a basis of the vector space \(M_{m,n}(K)\), which has dimension \(mn\).

**Remark:** Definition 2.12 and Definition 2.13 also make perfect sense when \(K\) is a (commutative) ring rather than a field. In this more general setting, the framework of vector spaces is too narrow, but we can consider structures over a commutative ring \(A\) satisfying all the axioms of Definition 2.5. Such structures are called *modules*. The theory of modules is (much) more complicated than that of vector spaces. For example, modules do not always have a basis, and other properties holding for vector spaces usually fail for modules. When a module has a basis, it is called a *free module*. For example, when \(A\) is a commutative ring, the structure \(A^n\) is a module such that the vectors \(e_i\), with \((e_i)_j = 1\) and \((e_i)_j = 0\) for \(j \neq i\), form a basis of \(A^n\). Many properties of vector spaces still hold for \(A^n\). Thus, \(A^n\) is a free module. As another example, when \(A\) is a commutative ring, \(M_{m,n}(A)\) is a free module with basis \((E_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}\). Polynomials over a commutative ring also form a free module of infinite dimension.

Square matrices provide a natural example of a noncommutative ring with zero divisors.

**Example 2.12** For example, letting \(A, B\) be the \(2 \times 2\)-matrices

\[
A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},
\]

then

\[
AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},
\]

and

\[
BA = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.
\]

We now formalize the representation of linear maps by matrices.

**Definition 2.14** Let \(E\) and \(F\) be two vector spaces, and let \((u_1, \ldots, u_n)\) be a basis for \(E\), and \((v_1, \ldots, v_m)\) be a basis for \(F\). Each vector \(x \in E\) expressed in the basis \((u_1, \ldots, u_n)\) as \(x = x_1u_1 + \cdots + x_nu_n\) is represented by the column matrix

\[
M(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}
\]

and similarly for each vector \(y \in F\) expressed in the basis \((v_1, \ldots, v_m)\).

Every linear map \(f: E \to F\) is represented by the matrix \(M(f) = (a_{ij})\), where \(a_{ij}\) is the \(i\)-th component of the vector \(f(u_j)\) over the basis \((v_1, \ldots, v_m)\), i.e., where

\[
f(u_j) = \sum_{i=1}^{m} a_{ij}v_i,
\]
for every \( j, 1 \leq j \leq n \). Explicitly, we have

\[
M(f) = \begin{pmatrix}
a_{11} & a_{12} & \ldots & a_{1n} \\
a_{21} & a_{22} & \ldots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{m1} & a_{m2} & \ldots & a_{mn}
\end{pmatrix}
\]

The matrix \( M(f) \) associated with the linear map \( f: E \to F \) is called the matrix of \( f \) with respect to the bases \((u_1, \ldots, u_n)\) and \((v_1, \ldots, v_m)\). When \( E = F \) and the basis \((v_1, \ldots, v_m)\) is identical to the basis \((u_1, \ldots, u_n)\) of \( E \), the matrix \( M(f) \) associated with \( f: E \to E \) (as above) is called the matrix of \( f \) with respect to the base \((u_1, \ldots, u_n)\).

**Remark:** As in the remark after Definition 2.12, there is no reason to assume that the vectors in the bases \((u_1, \ldots, u_n)\) and \((v_1, \ldots, v_m)\) are ordered in any particular way. However, it is often convenient to assume the natural ordering. When this is so, authors sometimes refer to the matrix \( M(f) \) as the matrix of \( f \) with respect to the ordered bases \((u_1, \ldots, u_n)\) and \((v_1, \ldots, v_m)\).

Then, given a linear map \( f: E \to F \) represented by the matrix \( M(f) = (a_{ij}) \) w.r.t. the bases \((u_1, \ldots, u_n)\) and \((v_1, \ldots, v_m)\), by equations (1) and the definition of matrix multiplication, the equation \( y = f(x) \) correspond to the matrix equation \( M(y) = M(f)M(x) \), that is,

\[
\begin{pmatrix}
y_1 \\
\vdots \\
y_m
\end{pmatrix} = \begin{pmatrix}
a_{11} & \ldots & a_{1n} \\
\vdots & \ddots & \vdots \\
a_{m1} & \ldots & a_{mn}
\end{pmatrix} \begin{pmatrix}
x_1 \\
\vdots \\
x_n
\end{pmatrix}
\]

The function that associates to a linear map \( f: E \to F \) the matrix \( M(f) \) w.r.t. the bases \((u_1, \ldots, u_n)\) and \((v_1, \ldots, v_m)\) has the property that matrix multiplication corresponds to composition of linear maps. The following proposition states the main properties of the mapping \( f \mapsto M(f) \) between \( \text{L}(E; F) \) and \( \text{M}_{m,n} \). In short, it is an isomorphism of vector spaces.

**Proposition 2.12** Given three vector spaces \( E, F, G \), with respective bases \((u_1, \ldots, u_p)\), \((v_1, \ldots, v_n)\), and \((w_1, \ldots, w_m)\), the mapping \( M: \text{L}(E; F) \to \text{M}_{n,p} \) that associates the matrix \( M(g) \) to a linear map \( g: E \to F \) satisfies the following properties for all \( x \in E \), all \( g, h: E \to F \), and all \( f: F \to G \):

\[
M(g(x)) = M(g)M(x)
\]

\[
M(g + h) = M(g) + M(h)
\]

\[
M(\lambda g) = \lambda M(g)
\]

\[
M(f \circ g) = M(f)M(g).
\]

Thus, \( M: \text{L}(E; F) \to \text{M}_{n,p} \) is an isomorphism of vector spaces, and when \( p = n \) and the basis \((v_1, \ldots, v_n)\) is identical to the basis \((u_1, \ldots, u_p)\), \( M: \text{L}(E; E) \to \text{M}_n \) is an isomorphism of rings.
2.7. MATRICES

Proposition 2.13

Let $E$ be a vector space, and let $(u_1, \ldots, u_n)$ be a basis of $E$. For every family $(v_1, \ldots, v_n)$, let $P = (a_{ij})$ be the matrix defined such that $v_j = \sum_{i=1}^{n} a_{ij}u_i$. The matrix $P$ is invertible iff $(v_1, \ldots, v_n)$ is a basis of $E$.

Proof. Note that we have $P = M(f)$, the matrix associated with the unique linear map $f: E \to E$ such that $f(u_i) = v_i$. By Proposition 2.8, $f$ is bijective iff $(v_1, \ldots, v_n)$ is a basis of $E$. Furthermore, it is obvious that the identity matrix $I_n$ is the matrix associated with the identity id: $E \to E$ w.r.t. any basis. If $f$ is an isomorphism, then $f \circ f^{-1} = f^{-1} \circ f = \text{id}$, and by Proposition 2.12, we get $M(f)M(f^{-1}) = M(f^{-1})M(f) = I_n$, showing that $P$ is invertible and that $M(f^{-1}) = P^{-1}$. □

Proposition 2.13 suggests the following definition.

Definition 2.15

Given a vector space $E$ of dimension $n$, for any two bases $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$ of $E$, let $P = (a_{ij})$ be the invertible matrix defined such that

$$v_j = \sum_{i=1}^{n} a_{ij}u_i,$$

which is also the matrix of the identity id: $E \to E$ with respect to the bases $(v_1, \ldots, v_n)$ and $(u_1, \ldots, u_n)$, in that order (indeed, we express each id$v_j = v_j$ over the basis $(u_1, \ldots, u_n)$).

The matrix $P$ is called the change of basis matrix from $(u_1, \ldots, u_n)$ to $(v_1, \ldots, v_n)$. Clearly, the change of basis matrix from $(v_1, \ldots, v_n)$ to $(u_1, \ldots, u_n)$ is $P^{-1}$. Since $P = (a_{ij})$ is the matrix of the identity id: $E \to E$ with respect to the bases $(v_1, \ldots, v_n)$ and
(\(u_1, \ldots, u_n\)), given any vector \(x \in E\), if \(x = x_1u_1 + \cdots + x_nu_n\) over the basis \((u_1, \ldots, u_n)\) and \(x = x'_1v_1 + \cdots + x'_nv_n\) over the basis \((v_1, \ldots, v_n)\), from Proposition 2.12, we have

\[
\begin{pmatrix}
x_1 \\
\vdots \\
x_n
\end{pmatrix} = \begin{pmatrix}
a_{11} & \cdots & a_{1n} \\
\vdots & \ddots & \vdots \\
a_{n1} & \cdots & a_{nn}
\end{pmatrix} \begin{pmatrix}
x'_1 \\
\vdots \\
x'_n
\end{pmatrix}
\]

showing that the old coordinates \((x_i)\) of \(x\) (over \((u_1, \ldots, u_n)\)) are expressed in terms of the new coordinates \((x'_i)\) of \(x\) (over \((v_1, \ldots, v_n)\)). Since the matrix \(P\) expresses the new basis \((v_1, \ldots, v_n)\) in terms of the old basis \((u_1, \ldots, u_n)\), we observe that the coordinates \((x_i)\) of a vector \(x\) vary in the opposite direction of the change of basis. For this reason, vectors are sometimes said to be contravariant. However, this expression does not make sense! Indeed, a vector in an intrinsic quantity that does not depend on a specific basis. What makes sense is that the coordinates of a vector vary in a contravariant fashion.

The effect of a change of bases on the representation of a linear map is described in the following proposition.

**Proposition 2.14** Let \(E\) and \(F\) be vector spaces, let \((u_1, \ldots, u_n)\) and \((u'_1, \ldots, u'_n)\) be two bases of \(E\), and let \((v_1, \ldots, v_m)\) and \((v'_1, \ldots, v'_m)\) be two bases of \(F\). Let \(P\) be the change of basis matrix from \((u_1, \ldots, u_n)\) to \((u'_1, \ldots, u'_n)\), and let \(Q\) be the change of basis matrix from \((v_1, \ldots, v_m)\) to \((v'_1, \ldots, v'_m)\). For any linear map \(f: E \to F\), let \(M(f)\) be the matrix associated to \(f\) w.r.t. the bases \((u_1, \ldots, u_n)\) and \((v_1, \ldots, v_m)\), and let \(M'(f)\) be the matrix associated to \(f\) w.r.t. the bases \((u'_1, \ldots, u'_n)\) and \((v'_1, \ldots, v'_m)\). We have

\[
M'(f) = Q^{-1}M(f)P.
\]

**Proof.** Since \(f: E \to F\) can be written as \(f = \text{id}_F \circ f \circ \text{id}_E\), since \(P\) is the matrix of \(\text{id}_E\) w.r.t. the bases \((u_1, \ldots, u_n)\) and \((u_1, \ldots, u_n)\), and \(Q^{-1}\) is the matrix of \(\text{id}_F\) w.r.t. the bases \((v_1, \ldots, v_m)\) and \((v'_1, \ldots, v'_m)\), by Proposition 2.12, we have \(M'(f) = Q^{-1}M(f)P\).

As a corollary, we get the following result.

**Corollary 2.15** Let \(E\) be a vector space, and let \((u_1, \ldots, u_n)\) and \((u'_1, \ldots, u'_n)\) be two bases of \(E\). Let \(P\) be the change of basis matrix from \((u_1, \ldots, u_n)\) to \((u'_1, \ldots, u'_n)\). For any linear map \(f: E \to E\), let \(M(f)\) be the matrix associated to \(f\) w.r.t. the basis \((u_1, \ldots, u_n)\), and let \(M'(f)\) be the matrix associated to \(f\) w.r.t. the basis \((u'_1, \ldots, u'_n)\). We have

\[
M'(f) = P^{-1}M(f)P.
\]

### 2.8 Direct Sums

Before considering linear forms and hyperplanes, we define the notion of direct sum and prove some simple propositions. There is a subtle point, which is that if we attempt to define the...
2.8. **DIRECT SUMS**

direct sum $E \oplus F$ of two vector spaces using the cartesian product $E \times F$, we don’t quite get the right notion because elements of $E \times F$ are ordered pairs, but we want $E \oplus F = F \oplus E$. Thus, we want to think of the elements of $E \oplus F$ as unordered pairs of elements. It is possible to do so by considering the direct sum of a family $(E_i)_{i \in \{1,2\}}$, and more generally of a family $(E_i)_{i \in I}$. For simplicity, we begin by considering the case where $I = \{1,2\}$.

**Definition 2.16** Given a family $(E_i)_{i \in \{1,2\}}$ of two vector spaces, we define the *(external)* direct sum $E_1 \oplus E_2$ of the family $(E_i)_{i \in \{1,2\}}$ as the set

$$E_1 \oplus E_2 = \{\langle 1, u \rangle, \langle 2, v \rangle \mid u \in E_1, \, v \in E_2\},$$

with addition

$$\{\langle 1, u_1 \rangle, \langle 2, v_1 \rangle \} + \{\langle 1, u_2 \rangle, \langle 2, v_2 \rangle \} = \{\langle 1, u_1 + u_2 \rangle, \langle 2, v_1 + v_2 \rangle \},$$

and scalar multiplication

$$\lambda \{\langle 1, u \rangle, \langle 2, v \rangle \} = \{\langle 1, \lambda u \rangle, \langle 2, \lambda v \rangle \}.$$  

We define the *injections* $in_1 : E_1 \to E_1 \oplus E_2$ and $in_2 : E_2 \to E_1 \oplus E_2$ as the linear maps defined such that,

$$in_1(u) = \{\langle 1, u \rangle, \langle 2, 0 \rangle \},$$

and

$$in_2(v) = \{\langle 1, 0 \rangle, \langle 2, v \rangle \}.$$  

Note that

$$E_2 \oplus E_1 = \{\{\langle 2, v \rangle, \langle 1, u \rangle \mid v \in E_2, \, u \in E_1\} = E_1 \oplus E_2.$$  

Thus, every member $\{\langle 1, u \rangle, \langle 2, v \rangle \}$ of $E_1 \oplus E_2$ can be viewed as an *unordered pair* consisting of the two vectors $u$ and $v$, tagged with the index 1 and 2, respectively.

**Remark:** In fact, $E_1 \oplus E_2$ is just the product $\prod_{i \in \{1,2\}} E_i$ of the family $(E_i)_{i \in \{1,2\}}$.

This is not to be confused with the cartesian product $E_1 \times E_2$. The vector space $E_1 \times E_2$ is the set of all ordered pairs $\langle u, v \rangle$, where $u \in E_1$, and $v \in E_2$, with addition and multiplication by a scalar defined such that

$$\langle u_1, v_1 \rangle + \langle u_2, v_2 \rangle = \langle u_1 + u_2, v_1 + v_2 \rangle,$$

$$\lambda \langle u, v \rangle = \langle \lambda u, \lambda v \rangle.$$  

There is a bijection between $\prod_{i \in \{1,2\}} E_i$ and $E_1 \times E_2$, but as we just saw, elements of $\prod_{i \in \{1,2\}} E_i$ are certain sets.
Of course, we can define $E_1 \times \cdots \times E_n$ for any number of vector spaces, and when $E_1 = \ldots = E_n$, we denote this product by $E^n$.

The following property holds.

**Proposition 2.16** Given any two vector spaces, $E_1$ and $E_2$, the set $E_1 \oplus E_2$ is a vector space. For every pair of linear maps, $f: E_1 \to G$ and $g: E_2 \to G$, there is a unique linear map, $f + g: E_1 \oplus E_2 \to G$, such that $(f + g) \circ in_1 = f$ and $(f + g) \circ in_2 = g$, as in the following diagram:

![Diagram](image)

**Proof.** Define

$$(f + g)(\{(1, u), (2, v)\}) = f(u) + g(v),$$

for every $u \in E_1$ and $v \in E_2$. It is immediately verified that $f + g$ is the unique linear map with the required properties. $\square$

We already noted that $E_1 \oplus E_2$ is in bijection with $E_1 \times E_2$. If we define the *projections* $\pi_1: E_1 \oplus E_2 \to E_1$ and $\pi_2: E_1 \oplus E_2 \to E_2$, such that

$$\pi_1(\{(1, u), (2, v)\}) = u,$$

and

$$\pi_2(\{(1, u), (2, v)\}) = v,$$

we have the following proposition.

**Proposition 2.17** Given any two vector spaces, $E_1$ and $E_2$, for every pair of linear maps, $f: D \to E_1$ and $g: D \to E_2$, there is a unique linear map, $f \times g: D \to E_1 \oplus E_2$, such that $\pi_1 \circ (f \times g) = f$ and $\pi_2 \circ (f \times g) = g$, as in the following diagram:

![Diagram](image)
2.8. DIRECT SUMS

Proof. Define

$$(f \times g)(w) = \{(1, f(w)), (2, g(w))\},$$

for every $w \in D$. It is immediately verified that $f \times g$ is the unique linear map with the required properties. □

Remark: It is a peculiarity of linear algebra that direct sums and products of finite families are isomorphic. However, this is no longer true for products and sums of infinite families.

When $U, V$ are subspaces of a vector space $E$, letting $i_1: U \to E$ and $i_2: V \to E$ be the inclusion maps, if $U \oplus V$ is isomorphic to $E$ under the map $i_1 + i_2$ given by Proposition 2.16, we say that $E$ is a direct (internal) sum of $U$ and $V$, and we write $E = U \oplus V$ (with a slight abuse of notation, since $E$ and $U \oplus V$ are only isomorphic). It is also convenient to define the sum $U + V$ of $U$ and $V$.

Definition 2.17 Given a vector space $E$, let $U, V$ be any subspaces of $E$. We define the sum $U + V$ of $U$ and $V$ as the set

$$U + V = \{w \in E \mid w = u + v, \text{ for some } u \in U \text{ and some } v \in V\}.$$  

We say that $E$ is the (internal) direct sum of $U$ and $V$, denoted by $E = U \oplus V$, if for every $x \in E$, there exist unique vectors $u \in U$ and $v \in V$, such that $x = u + v$.

It is immediately verified that $U + V$ is the least subspace of $E$ containing $U$ and $V$. Note that by definition, $U + V = V + U$, and $U \oplus V = V \oplus U$. The following two simple propositions holds.

Proposition 2.18 Let $E$ be a vector space. The following properties are equivalent:

1. $E = U \oplus V$.
2. $E = U + V$ and $U \cap V = 0$.

Proof. First, assume that $E$ is the direct sum of $U$ and $V$. If $x \in U \cap V$ and $x \neq 0$, since $x$ can be written both as $x + 0$ and $0 + x$, we have a contradiction. Thus $U \cap V = 0$. Conversely, assume that $x = u + v$ and $x = u' + v'$, where $u, u' \in U$ and $v, v' \in V$. Then,

$$v' - v = u - u',$$

where $v' - v \in V$ and $u - u' \in U$. Since $U \cap V = 0$, we must have $u' = u$ and $v' = v$, and thus $E = U \oplus V$. □

Proposition 2.19 Let $E$ be a vector space, and assume that $E = U \oplus V$. Then,

$$\dim(E) = \dim(U) + \dim(V).$$

Again, with a slight abuse of notation!
Proof. Let \((u_i)_{i \in I}\) be a basis of \(U\) and let \((v_j)_{j \in J}\) be a basis of \(V\), where \(I\) and \(J\) are disjoint. Clearly, \((u_i)_{i \in I} \cup (v_j)_{j \in J}\) is a basis of \(E\). \(\square\)

We now give the definition of a direct sum for any arbitrary nonempty index set \(I\). First, let us recall the notion of the product of a family \((E_i)_{i \in I}\). Given a family of sets \((E_i)_{i \in I}\), its product \(\prod_{i \in I} E_i\), is the set of all functions \(f: I \to \bigcup_{i \in I} E_i\), such that, \(f(i) \in E_i\), for every \(i \in I\). It is one of the many versions of the axiom of choice, that, if \(E_i \neq \emptyset\) for every \(i \in I\), then \(\prod_{i \in I} E_i \neq \emptyset\). A member \(f \in \prod_{i \in I} E_i\), is often denoted as \((f_i)_{i \in I}\).

The following proposition is an obvious generalization of Proposition 2.16.

**Proposition 2.20** Let \(I\) be any nonempty set, let \((E_i)_{i \in I}\) be a family of vector spaces, and let \(G\) be any vector space. The direct sum \(\bigoplus_{i \in I} E_i\) of the family \((E_i)_{i \in I}\) is defined as follows:

\[
\bigoplus_{i \in I} E_i = \{ (f_i)_{i \in I} \mid \text{finite support}, \lambda(f_i)_{i \in I}, \lambda(f_i)_{i \in I} \}
\]

We also have injection maps \(i_n: E_i \to \bigoplus_{i \in I} E_i\), defined such that, \(i_n(x) = (f_i)_{i \in I}\), where \(f_i = x\), and \(f_j = 0\), for all \(j \in (I - \{i\})\).

The following proposition is an obvious generalization of Proposition 2.16.

**Proposition 2.21** Let \(E\) and \(F\) be vector spaces, and let \(f: E \to F\) be a linear map. If \(f: E \to F\) is injective, then, there is a surjective linear map \(r: F \to E\) called a retraction, such that \(r \circ f = \text{id}_E\). If \(f: E \to F\) is surjective, then, there is an injective linear map \(s: F \to E\) called a section, such that \(f \circ s = \text{id}_F\).
2.8. DIRECT SUMS

Proof. Let \((u_i)_{i \in I}\) be a basis of \(E\). Since \(f: E \to F\) is an injective linear map, by Proposition 2.8, \((f(u_i))_{i \in I}\) is linearly independent in \(F\). By Theorem 2.2, there is a basis \((v_j)_{j \in J}\) of \(F\), where \(I \subseteq J\), and where \(v_i = f(u_i)\), for all \(i \in I\). By Proposition 2.8, a linear map \(r: F \to E\) can be defined such that \(r(v_i) = u_i\) for all \(i \in I\), and \(r(v_j) = w\) for all \(j \in (J - I)\), where \(w\) is any given vector in \(E\), say \(w = 0\). Since \(r(f(u_i)) = u_i\) for all \(i \in I\), by Proposition 2.8, we have \(r \circ f = \text{id}_E\).

Now, assume that \(f: E \to F\) is surjective. Let \((v_j)_{j \in J}\) be a basis of \(F\). Since \(f: E \to F\) is surjective, for every \(v_j \in F\), there is some \(u_j \in E\) such that \(f(u_j) = v_j\). Since \((v_j)_{j \in J}\) is a basis of \(F\), by Proposition 2.8, there is a unique linear map \(s: F \to E\) such that \(s(v_j) = u_j\). Also, since \(f(s(v_j)) = v_j\), by Proposition 2.8 (again), we must have \(f \circ s = \text{id}_F\).

The converse of Proposition 2.21 is obvious. We now have the following fundamental Proposition.

Proposition 2.22 Let \(E, F\) and \(G\), be three vector spaces, \(f: E \to F\) an injective linear map, \(g: F \to G\) a surjective linear map, and assume that \(\text{Im } f = \text{Ker } g\). Then, the following properties hold. (a) For any section \(s: G \to F\) of \(g\), \(\text{Ker } g \oplus \text{Im } s\) is isomorphic to \(F\), and the linear map \(f + s: E \oplus G \to F\) is an isomorphism.\(^5\)

(b) For any retraction \(r: F \to E\) of \(f\), \(\text{Im } f \oplus \text{Ker } r\) is isomorphic to \(F\).\(^6\)

Proof. (a) Since \(s: G \to F\) is a section of \(g\), we have \(g \circ s = \text{id}_G\), and for every \(u \in F\),

\[g(u - s(g(u))) = g(u) - g(s(g(u))) = g(u) - g(u) = 0.\]

Thus, \(u - s(g(u)) \in \text{Ker } g\), and we have \(F = \text{Ker } g + \text{Im } s\). On the other hand, if \(u \in \text{Ker } g \cap \text{Im } s\), then \(u = s(v)\) for some \(v \in G\) because \(u \in \text{Im } s\), \(g(u) = 0\) because \(u \in \text{Ker } g\), and so,

\[g(u) = g(s(v)) = v = 0,\]

because \(g \circ s = \text{id}_G\), which shows that \(u = s(v) = 0\). Thus, \(F = \text{Ker } g \oplus \text{Im } s\), and since by assumption, \(\text{Im } f = \text{Ker } g\), we have \(F = \text{Im } f \oplus \text{Im } s\). But then, since \(f\) and \(s\) are injective, \(f + s: E \oplus G \to F\) is an isomorphism. The proof of (b) is very similar. \(\square\)

Given a sequence of linear maps \(E \xrightarrow{f} F \xrightarrow{g} G\), when \(\text{Im } f = \text{Ker } g\), we say that the sequence \(E \xrightarrow{f} F \xrightarrow{g} G\) is exact at \(F\). If in addition to being exact at \(F\), \(f\) is injective and \(g\) is surjective, we say that we have a short exact sequence, and this is denoted as

\[0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0.\]

The property of a short exact sequence given by Proposition 2.22 is often described by saying that \(0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0\) is a (short) split exact sequence.

As a corollary of Proposition 2.22, we have the following result.

---

\(^5\)The existence of a section \(s: G \to F\) of \(g\) follows from Proposition 2.21.

\(^6\)The existence of a retraction \(r: F \to E\) of \(f\) follows from Proposition 2.21.
Corollary 2.23 Let $E$ and $F$ be vector spaces, and let $f: E \rightarrow F$ be a linear map. Then, $E$ is isomorphic to $\text{Ker } f \oplus \text{Im } f$, and thus,

$$\dim(E) = \dim(\text{Ker } f) + \dim(\text{Im } f).$$

Proof. Consider

$$\text{Ker } f \rightarrow i \rightarrow E \rightarrow f' \rightarrow \text{Im } f,$$

where $\text{Ker } f \rightarrow i \rightarrow E$ is the inclusion map, and $E \xrightarrow{f'} \text{Im } f$ is the surjection associated with $E \xrightarrow{f} F$. Then, we apply Proposition 2.22 to any section $\text{Im } f \rightarrow s \rightarrow E$ of $f'$ to get an isomorphism between $E$ and $\text{Ker } f \oplus \text{Im } f$, and Proposition 2.19, to get $\dim(E) = \dim(\text{Ker } f) + \dim(\text{Im } f)$. □

The following Proposition will also be useful.

Proposition 2.24 Let $E$ be a vector space. If $E = U \oplus V$ and $E = U \oplus W$, then there is an isomorphism $f: V \rightarrow W$ between $V$ and $W$.

Proof. Let $R$ be the relation between $V$ and $W$, defined such that

$$\langle v, w \rangle \in R \text{ iff } w - v \in U.$$

We claim that $R$ is a functional relation that defines a linear isomorphism $f: V \rightarrow W$ between $V$ and $W$, where $f(v) = w$ iff $\langle v, w \rangle \in R$ ($R$ is the graph of $f$). If $w - v \in U$ and $w' - v \in U$, then $w' - w \in U$, and since $U \oplus W$ is a direct sum, $U \cap W = 0$, and thus $w' - w = 0$, that is $w' = w$. Thus, $R$ is functional. Similarly, if $w - v \in U$ and $w - v' \in U$, then $v' - v \in U$, and since $U \oplus V$ is a direct sum, $U \cap V = 0$, and $v' = v$. Thus, $f$ is injective. Since $E = U \oplus V$, for every $w \in W$, there exists a unique pair $\langle u, v \rangle \in U \times V$, such that $w = u + v$. Then, $w - v \in U$, and $f$ is surjective. We also need to verify that $f$ is linear. If

$$w - v = u$$

and

$$w' - v' = u',$$

where $u, u' \in U$, then, we have

$$(w + w') - (v + v') = (u + u'),$$

where $u + u' \in U$. Similarly, if

$$w - v = u$$

where $u \in U$, then we have

$$\lambda w - \lambda v = \lambda u,$$

where $\lambda u \in U$. Thus, $f$ is linear. □
2.8. DIRECT SUMS

Given a vector space $E$ and any subspace $U$ of $E$, Proposition 2.24 shows that the dimension of any subspace $V$ such that $E = U \oplus V$ depends only on $U$. We call $\dim(V)$ the codimension of $U$, and we denote it by $\text{codim}(U)$. A subspace $U$ of codimension 1 is called a hyperplane.

The notion of rank of a linear map or of a matrix is an important one, both theoretically and practically, since it is the key to the solvability of linear equations.

**Definition 2.19** Given two vector spaces $E$ and $F$ and a linear map $f : E \to F$, the rank $\text{rk}(f)$ of $f$ is the dimension $\dim(\text{Im}(f))$ of the image subspace $\text{Im}(f)$ of $F$.

We have the following simple proposition.

**Proposition 2.25** Given a linear map $f : E \to F$, the following properties hold:

1. $\text{rk}(f) = \text{codim}(\text{Ker}(f))$.
2. $\text{rk}(f) + \dim(\text{Ker}(f)) = \dim(E)$.
3. $\text{rk}(f) \leq \min(\dim(E), \dim(F))$.

**Proof.** Since by Proposition 2.23, $\dim(E) = \dim(\text{Ker}(f)) + \dim(\text{Im}(f))$, and by definition, $\text{rk}(f) = \dim(\text{Im}(f))$, we have $\text{rk}(f) = \text{codim}(\text{Ker}(f))$. Since $\text{rk}(f) = \dim(\text{Im}(f))$, (ii) follows from $\dim(E) = \dim(\text{Ker}(f)) + \dim(\text{Im}(f))$. As for (iii), since $\text{Im}(f)$ is a subspace of $F$, we have $\text{rk}(f) \leq \dim(F)$, and since $\text{rk}(f) + \dim(\text{Ker}(f)) = \dim(E)$, we have $\text{rk}(f) \leq \dim(E)$. □

The rank of a matrix is defined as follows.

**Definition 2.20** Given a $m \times n$-matrix $A = (a_{ij})$ over the field $K$, the rank $\text{rk}(A)$ of the matrix $A$ is the maximum number of linearly independent columns of $A$ (viewed as vectors in $K^m$).

In view of Proposition 2.3, the rank of a matrix $A$ is the dimension of the subspace of $K^m$ generated by the columns of $A$. Let $E$ and $F$ be two vector spaces, and let $(u_1, \ldots, u_n)$ be a basis of $E$, and $(v_1, \ldots, v_m)$ a basis of $F$. Let $f : E \to F$ be a linear map, and let $M(f)$ be its matrix w.r.t. the bases $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_m)$. Since the rank $\text{rk}(f)$ of $f$ is the dimension of $\text{Im}(f)$, which is generated by $(f(u_1), \ldots, f(u_n))$, the rank of $f$ is the maximum number of linearly independent vectors in $(f(u_1), \ldots, f(u_n))$, which is equal to the number of linearly independent columns of $M(f)$, since $F$ and $K^m$ are isomorphic. Thus, we have $\text{rk}(f) = \text{rk}(M(f))$, for every matrix representing $f$.

We will see later, using duality, that the rank of a matrix $A$ is also equal to the maximal number of linearly independent rows of $A$.

If $U$ is a hyperplane, then $E = U \oplus V$ for some subspace $V$ of dimension 1. However, a subspace $V$ of dimension 1 is generated by any nonzero vector $v \in V$, and thus we denote
V by $Kv$, and we write $E = U \oplus Kv$. Clearly, $v \notin U$. Conversely, let $x \in E$ be a vector such that $x \notin U$ (and thus, $x \neq 0$). We claim that $E = U \oplus Kx$. Indeed, since $U$ is a hyperplane, we have $E = U \oplus Kv$ for some $v \notin U$ (with $v \neq 0$). Then, $x \in E$ can be written in a unique way as $x = u + \lambda v$, where $u \in U$, and since $x \notin U$, we must have $\lambda \neq 0$, and thus, $v = -\lambda^{-1} u + \lambda^{-1} x$. Since $E = U \oplus Kv$, this shows that $E = U + Kx$. Since $x \notin U$, we have $U \cap Kx = 0$, and thus $E = U \oplus Kx$. This argument shows that a hyperplane is a maximal proper subspace $H$ of $E$.

In the next section, we shall see that hyperplanes are precisely the Kernels of nonnull linear maps $f: E \to K$, called linear forms.

### 2.9 The Dual Space $E^*$ and Linear Forms

We already observed that the field $K$ itself is a vector space (over itself). The vector space $L(E; K)$ of linear maps $f: E \to K$, the linear forms, plays a particular role. We take a quick look at the connection between $E$ and $L(E; K)$, its dual space.

**Definition 2.21** Given a vector space $E$, the vector space $L(E; K)$ of linear maps $f: E \to K$ is called the dual space (or dual) of $E$. The space $L(E; K)$ is also denoted by $E^*$, and the linear maps in $E^*$ are called the linear forms, or covectors. The dual space $E^{**}$ of the space $E^*$ is called the bidual of $E$.

As a matter of notation, linear forms $f: E \to K$ will also be denoted by starred symbol, such as $u^*$, $x^*$, etc.

Given a linear form $u^* \in E^*$ and a vector $v \in E$, the result $u^*(v)$ of applying $u^*$ to $v$ is also denoted by $\langle u^*, v \rangle$. This defines a binary operation $\langle -,- \rangle: E^* \times E \to K$ satisfying the following properties:

\[
\begin{align*}
\langle u_1^* + u_2^*, v \rangle & = \langle u_1^*, v \rangle + \langle u_2^*, v \rangle \\
\langle u^*, v_1 + v_2 \rangle & = \langle u^*, v_1 \rangle + \langle u^*, v_2 \rangle \\
\langle \lambda u^*, v \rangle & = \lambda \langle u^*, v \rangle \\
\langle u^*, \lambda v \rangle & = \lambda \langle u^*, v \rangle.
\end{align*}
\]

The above identities mean that $\langle -,- \rangle$ is a bilinear map. In view of the above identities, given any fixed vector $v \in E$, the map $\tilde{v}: E^* \to K$ defined such that

\[
\tilde{v}(u^*) = \langle u^*, v \rangle
\]

for every $u^* \in E^*$ is a linear map from $E^*$ to $K$, that is, $\tilde{v}$ is a linear form in $E^{**}$. Again from the above identities, the map $c_E: E \to E^{**}$, defined such that

\[
c_E(v) = \tilde{v}
\]

for every $v \in E$, is a linear map. We shall see that it is injective, and that it is an isomorphism when $E$ has finite dimension.
2.9. THE DUAL SPACE $E^*$ AND LINEAR FORMS

Definition 2.22 Given a vector space $E$ and its dual $E^*$, we say that a vector $v \in E$ and a linear form $u^* \in E^*$ are orthogonal if $\langle u^*, v \rangle = 0$. Given a subspace $V$ of $E$ and a subspace $U$ of $E^*$, we say that $V$ and $U$ are orthogonal if $\langle u^*, v \rangle = 0$ for every $u^* \in U$ and every $v \in V$. Given a subset $V$ of $E$ (resp. a subset $U$ of $E^*$), the orthogonal $V^0$ of $V$ is the subspace $V$ defined such that

$$V^0 = \{ u^* \in E^* \mid \langle u^*, v \rangle = 0, \text{ for every } v \in V \}$$

(resp. the orthogonal $U^0$ of $U$ is the subspace $U^0$ of $E$ defined such that

$$U^0 = \{ v \in E \mid \langle u^*, v \rangle = 0, \text{ for every } u^* \in U \}$$

Observe that $E^0 = 0$, and $\{0\}^0 = E^*$.

It is also easy to see that if $M \subseteq N \subseteq E$, then $N^0 \subseteq M^0 \subseteq E^*$. From this, it follows that $V \subseteq V^{00}$ for every subspace $V$ of $E$, and that $U \subseteq U^{00}$ for every subspace $U$ of $E^*$. However, even though $V = V^{00}$ is always true, when $E$ is of infinite dimension, it is not always true that $U = U^{00}$.

Given a vector space $E$ and any basis $(u_i)_{i \in I}$ for $E$, we can associate to each $u_i$ a linear form $u_i^* \in E^*$, and the $u_i^*$ have some remarkable properties.

Definition 2.23 Given a vector space $E$ and any basis $(u_i)_{i \in I}$ for $E$, by Proposition 2.8, for every $i \in I$, there is a unique linear form $u_i^*$ such that

$$u_i^*(u_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j, \end{cases}$$

for every $j \in I$. The linear form $u_i^*$ is called the coordinate form of index $i$ w.r.t. the basis $(u_i)_{i \in I}$.

Given an index set $I$, authors often define the so called “Kronecker symbol” $\delta_{ij}$, such that

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j, \end{cases}$$

for all $i, j \in I$. Then, $u_i^*(u_j) = \delta_{ij}$.

Given a vector space $E$ and a subspace $U$ of $E$, by Theorem 2.2, every basis $(u_i)_{i \in I}$ of $U$ can be extended to a basis $(u_j)_{j \in I \cup J}$ of $E$, where $I \cap J = \emptyset$. We have the following important theorem.

Theorem 2.26 Let $E$ be a vector space. The following properties hold:

(a) For every basis $(u_i)_{i \in I}$ of $E$, the family $(u_i^*)_{i \in I}$ of coordinate forms is linearly independent.
(b) For every subspace $V$ of $E$, we have $V^{00} = V$.

(c) For every subspace $V$ of finite codimension $m$ of $E$, for every subspace $W$ of $E$ such that $E = V \oplus W$ (where $W$ is of finite dimension $m$), for every basis $(u_i)_{i \in I}$ of $E$ such that $(u_1, \ldots, u_m)$ is a basis of $W$, the family $(u_i^*, \ldots, u_m^*)$ is a basis of the orthogonal $V^0$ of $V$ in $E^*$. Furthermore, we have $V^{00} = V$, and

$$\dim(V) + \dim(V^0) = \dim(E).$$

(d) For every subspace $U$ of finite dimension $m$ of $E^*$, the orthogonal $U^0$ of $U$ in $E$ is of finite codimension $m$, $U^{00} = U$, and

$$\dim(U) + \dim(U^0) = \dim(E).$$

Proof. (a) Assume that

$$\sum_{i \in I} \lambda_i u_i^* = 0,$$

for a family $(\lambda_i)_{i \in I}$ (of scalars in $K$). Since $(\lambda_i)_{i \in I}$ has finite support, there is a finite subset $J$ of $I$ such that $\lambda_i = 0$ for all $i \in I - J$, and we have

$$\sum_{j \in J} \lambda_j u_j^* = 0.$$

Applying the linear form $\sum_{j \in J} \lambda_j u_j^*$ to each $u_j$ ($j \in J$), by Definition 2.23, since $u_i^*(u_j) = 1$ if $i = j$ and 0 otherwise, we get $\lambda_j = 0$ for all $j \in J$, that is $\lambda_i = 0$ for all $i \in I$ (by definition of $J$ as the support). Thus, $(u_i^*)_{i \in I}$ is linearly independent.

(b) Let $(u_i)_{i \in I \cup J}$ be a basis of $E$ such that $(u_i)_{i \in I}$ is a basis of $V$ (where $I \cap J = \emptyset$). Clearly, we have $V \subseteq V^{00}$. If $V \neq V^{00}$, then $u_{j_0} \in V^{00}$ for some $j_0 \in J$ (and thus, $j_0 \notin I$). Since $u_{j_0} \in V^{00}$, $u_{j_0}$ is orthogonal to every linear form in $V^0$. In particular, let $g^*$ be the linear form defined such that

$$g^*(u_i) = \begin{cases} 1 & \text{if } i = j_0 \\ 0 & \text{if } i \neq j_0, \end{cases}$$

where $i \in I \cup J$. Then, it is clear that $g^*(u_i) = 0$ for all $i \in I$, and thus that $g^* \in V^0$. However, $g^*(u_{j_0}) = 1$, contradicting the fact that $u_{j_0}$ is orthogonal to every linear form in $V^0$. Thus, $V = V^{00}$.

(c) Let $J = I - \{1, \ldots, m\}$. Every linear form $f^* \in V^0$ is orthogonal to every $u_j$, for $j \in J$, and thus, $f^*(u_j) = 0$, for all $j \in J$. For such a linear form $f^* \in V^0$, let

$$g^* = f^*(u_1)u_1^* + \cdots + f^*(u_m)u_m^*.$$

We have $g^*(u_i) = f^*(u_i)$, for every $i$, $1 \leq i \leq m$. Furthermore, by definition, $g^*$ vanishes on all $u_j$, where $j \in J$. Thus, $f^*$ and $g^*$ agree on the basis $(u_i)_{i \in I}$ of $E$, and so, $g^* = f^*$. 


This shows that \((u_1^*, \ldots, u_m^*)\) generates \(V^0\), and since it is also a linearly independent family, \((u_1^*, \ldots, u_m^*)\) is a basis of \(V^0\). It is then obvious that \(\dim(V) + \dim(V^0) = \dim(E)\), and by part (b), we have \(V^{00} = V\).

(d) Let \((u_1^*, \ldots, u_m^*)\) be a basis of \(U\). Note that the map \(h: E \rightarrow K^m\) defined such that
\[
h(v) = (u_1^*(v), \ldots, u_m^*(v))
\]
for every \(v \in E\), is a linear map, and that its kernel \(\text{Ker} h\) is precisely \(U^0\). Then, by Proposition 2.23,
\[
\dim(E) = \dim(\text{Ker} h) + \dim(\text{Im} h) \leq \dim(U^0) + m,
\]
since \(\dim(\text{Im} h) \leq m\). Thus, \(U^0\) is a subspace of \(E\) of finite codimension at most \(m\), and by (c), we have \(\dim(U^0) + \dim(U^{00}) = \dim(E)\). However, it is clear that \(U \subseteq U^{00}\), which implies \(\dim(U) \leq \dim(U^{00})\), and so \(\dim(U^0) + \dim(U) \leq \dim(E)\). Thus, \(U^0\) is of finite codimension at least \(m\), which implies \(\text{codim}(U^0) = m\). But then, \(\text{codim}(U^0) = m = \dim(U)\), and since \(\dim(U^0) + \dim(U^{00}) = \dim(E)\), we have \(\dim(U^{00}) = m\), and we must have \(U = U^{00}\).

Part (a) of Theorem 2.26 shows that
\[
\dim(E) \leq \dim(E^*).
\]
When \(E\) is of finite dimension \(n\) and \((u_1, \ldots, u_n)\) is a basis of \(E\), by part (c), the family \((u_1^*, \ldots, u_n^*)\) is a basis of the dual space \(E^*\), called the dual basis of \((u_1, \ldots, u_n)\). By part (c) and (d) of theorem 2.26, the maps \(V \mapsto V^0\) and \(U \mapsto U^0\), where \(V\) is a subspace of finite codimension of \(E\) and \(U\) is a subspace of finite dimension of \(E^*\), are inverse bijections. These maps set up a duality between subspaces of finite codimension of \(E\), and subspaces of finite dimension of \(E^*\).

One should be careful that this bijection does not extend to subspaces of \(E^*\) of infinite dimension.

When \(E\) is of infinite dimension, for every basis \((u_i)_{i \in I}\) of \(E\), the family \((u_i^*)_{i \in I}\) of coordinate forms is never a basis of \(E^*\). It is linearly independent, but it is “too small” to generate \(E^*\). For example, if \(E = \mathbb{R}^{(\mathbb{N})}\), where \(\mathbb{N} = \{0, 1, 2, \ldots\}\), the map \(f: E \rightarrow \mathbb{R}\) that sums the nonzero coordinates of a vector in \(E\) is a linear form, but it is easy to see that it cannot be expressed as a linear combination of coordinate forms. As a consequence, when \(E\) is of infinite dimension, \(E\) and \(E^*\) are not isomorphic.

When \(E\) is of finite dimension \(n\) and \((u_1, \ldots, u_n)\) is a basis of \(E\), we noted that the family \((u_1^*, \ldots, u_n^*)\) is a basis of the dual space \(E^*\) (called the dual basis of \((u_1, \ldots, u_n)\)). Let us see how the coordinates of a linear form \(\varphi^*\) vary under a change of basis.

Let \((u_1, \ldots, u_n)\) and \((v_1, \ldots, v_n)\) be two bases of \(E\), and let \(P = (a_{ij})\) be the change of basis matrix from \((u_1, \ldots, u_n)\) to \((v_1, \ldots, v_n)\), so that
\[
v_j = \sum_{i=1}^{n} a_{ij} u_i,
\]
and let $P^{-1} = (b_{ij})$ be the inverse of $P$, so that

$$u_i = \sum_{j=1}^{n} b_{ij} v_j.$$ 

Since $u^*_i(u_j) = \delta_{ij}$ and $v^*_i(v_j) = \delta_{ij}$, we get

$$v^*_j(u_i) = v^*_j(\sum_{k=1}^{n} b_{ki} v_k) = b_{ji},$$

and thus

$$v^*_j = \sum_{i=1}^{n} b_{ji} u^*_i,$$

and similarly

$$u^*_i = \sum_{j=1}^{n} a_{ij} v^*_j.$$ 

Since

$$\varphi^* = \sum_{i=1}^{n} \varphi_i u^*_i = \sum_{i=1}^{n} \varphi'_i v^*_i,$$

we get

$$\varphi'_j = \sum_{i=1}^{n} a_{ij} \varphi_i.$$ 

Comparing with the change of basis

$$v_j = \sum_{i=1}^{n} a_{ij} u_i,$$

we note that this time, the coordinates $(\varphi_i)$ of the linear form $\varphi^*$ change in the same direction as the change of basis. For this reason, we say that the coordinates of linear forms are covariant. By abuse of language, it is often said that linear forms are covariant, which explains why the term covector is also used for a linear form.

**Remark:** In many texts using tensors, vectors are often indexed with lower indices. If so, it is more convenient to write the coordinates of a vector $x$ over the basis $(u_1, \ldots, u_n)$ as $(x^i)$, using an upper index, so that

$$x = \sum_{i=1}^{n} x^i u_i,$$

and in a change of basis, we have

$$v_j = \sum_{i=1}^{n} a^j_i u_i.$$
2.9. THE DUAL SPACE $E^*$ AND LINEAR FORMS

and

$$x^i = \sum_{j=1}^{n} a_{ij} x^j.$$ 

Dually, linear forms are indexed with upper indices. Then, it is more convenient to write the coordinates of a covector $\varphi^*$ over the dual basis $(u^*1, \ldots, u^*n)$ as $(\varphi_i)$, using a lower index, so that

$$\varphi^* = \sum_{i=1}^{n} \varphi_i u^*i$$

and in a change of basis, we have

$$u^*i = \sum_{j=1}^{n} a_{ji} v^*j$$

and

$$\varphi'_j = \sum_{i=1}^{n} a_{ji} \varphi_i.$$ 

With these conventions, the index of summation appears once in upper position and once in lower position, and the summation sign can be safely omitted, a trick due to Einstein. For example, we can write

$$\varphi'_j = a_{ji} \varphi_i$$

as an abbreviation for

$$\varphi'_j = \sum_{i=1}^{n} a_{ji} \varphi_i.$$ 

We will now pin down the relationship between a vector space $E$ and its bidual $E^{**}$.

**Proposition 2.27** Let $E$ be a vector space. The following properties hold:

(a) The linear map $c_E : E \to E^{**}$ defined such that

$$c_E(v) = \tilde{v},$$

that is, $c_E(v)(u^*) = \langle u^*, v \rangle$ for every $u^* \in E^*$, is injective.

(b) When $E$ is of finite dimension $n$, the linear map $c_E : E \to E^{**}$ is an isomorphism (called the canonical isomorphism).

**Proof.** (a) Let $(u_i)_{i \in I}$ be a basis of $E$, and let $v = \sum_{i \in I} v_i u_i$. If $c_E(v) = 0$, then in particular, $c_E(v)(u^*_i) = 0$ for all $u^*_i$, and since

$$c_E(v)(u^*_i) = \langle u^*_i, v \rangle = v_i,$$

we have $v_i = 0$ for all $i \in I$, that is, $v = 0$, showing that $c_E : E \to E^{**}$ is injective.
If $E$ is of finite dimension $n$, by Theorem 2.26, for every basis $(u_1, \ldots, u_n)$, the family $(u_1^*, \ldots, u_n^*)$ is a basis of the dual space $E^*$, and thus the family $(u_1^{**}, \ldots, u_n^{**})$ is a basis of the bidual $E^{**}$. This shows that $\dim(E) = \dim(E^{**}) = n$, and since by part (a), we know that $c_E: E \to E^{**}$ is injective, in fact, $c_E: E \to E^{**}$ is bijective (because an injective map carries a linearly independent family to a linearly independent family, and in a vector space of dimension $n$, a linearly independent family of $n$ vectors is a basis, see Proposition 2.3).

When a vector space $E$ has infinite dimension, $E$ and its bidual $E^{**}$ are never isomorphic.

When $E$ is of finite dimension and $(u_1, \ldots, u_n)$ is a basis of $E$, in view of the canonical isomorphism $c_E: E \to E^{**}$, the basis $(u_1^*, \ldots, u_n^*)$ of the bidual is identified with $(u_1, \ldots, u_n)$.

Proposition 2.27 can be reformulated very fruitfully in terms of pairings.

**Definition 2.24** Given two vector spaces $E$ and $F$ over $K$, a pairing between $E$ and $F$ is a bilinear map $\langle -, - \rangle: E \times F \to K$. Such a pairing is non-singular if for every $u \in E$, if $\langle u, v \rangle = 0$ for all $v \in F$, then $u = 0$, and for every $v \in F$, if $\langle u, v \rangle = 0$ for all $u \in E$, then $v = 0$.

For example, the map $\langle -, - \rangle: E^* \times E \to K$ defined earlier is a non-singular pairing (use the proof of (a) in lemma 2.27).

Given a pairing $\langle -, - \rangle: E \times F \to K$, we can define two maps $\varphi: E \to F^*$ and $\psi: F \to E^*$ as follows: For every $u \in E$, we define the linear form $\varphi(u)$ in $F^*$ such that

$$\varphi(u)(v) = \langle u, v \rangle$$

for every $v \in F$, and we define the linear form $\psi(u)$ in $E^*$ such that

$$\psi(v)(u) = \langle u, v \rangle$$

for every $u \in E$. We have the following useful proposition.

**Proposition 2.28** Given two vector spaces $E$ and $F$ over $K$, for every non-singular pairing $\langle -, - \rangle: E \times F \to K$ between $E$ and $F$, the maps $\varphi: E \to F^*$ and $\psi: F \to E^*$ are linear and injective. Furthermore, if $E$ and $F$ have finite dimension, then this dimension is the same and $\varphi: E \to F^*$ and $\psi: F \to E^*$ are bijections.

*Proof.* The maps $\varphi: E \to F^*$ and $\psi: F \to E^*$ are linear because a pairing is bilinear. If $\varphi(u) = 0$ (the null form), then

$$\varphi(u)(v) = \langle u, v \rangle = 0$$

for every $v \in F$, and since $\langle -, - \rangle$ is non-singular, $u = 0$. Thus, $\varphi: E \to F^*$ is injective. Similarly, $\psi: F \to E^*$ is injective. When $F$ has finite dimension $n$, we have seen that $F$ and $F^*$ have the same dimension. Since $\varphi: E \to F^*$ is injective, we have $m = \dim(E) \leq$
2.10. Hyperplanes and Linear Forms

Actually, Proposition 2.29 below follows from parts (c) and (d) of Theorem 2.26, but we feel that it is also interesting to give a more direct proof.

**Proposition 2.29** Let $E$ be a vector space. The following properties hold:

(a) Given any nonnull linear form $f^* \in E^*$, its kernel $H = \ker f^*$ is a hyperplane.

(b) For any hyperplane $H$ in $E$, there is a (nonnull) linear form $f^* \in E^*$ such that $H = \ker f^*$.

(c) Given any hyperplane $H$ in $E$ and any (nonnull) linear form $f^* \in E^*$ such that $H = \ker f^*$, for every linear form $g^* \in E^*$, $H = \ker g^*$ iff $g^* = \lambda f^*$ for some $\lambda \neq 0$ in $K$.

**Proof.** (a) If $f^* \in E^*$ is nonnull, there is some vector $v_0 \in E$ such that $f^*(v_0) \neq 0$. Let $H = \ker f^*$. For every $v \in E$, we have

$$f^*(v - \frac{f^*(v)}{f^*(v_0)} v_0) = f^*(v) - \frac{f^*(v)}{f^*(v_0)} f^*(v_0) = f^*(v) - f^*(v) = 0.$$ 

Thus, 

$$v - \frac{f^*(v)}{f^*(v_0)} v_0 = h \in H,$$
and 

$$v = h + \frac{f^*(v)}{f^*(v_0)} v_0,$$

that is, $E = H + K v_0$. Also, since $f^*(v_0) \neq 0$, we have $v_0 \notin H$, that is, $H \cap K v_0 = 0$. Thus, $E = H \oplus K v_0$, and $H$ is a hyperplane.

(b) If $H$ is a hyperplane, $E = H \oplus K v_0$ for some $v_0 \notin H$. Then, every $v \in E$ can be written in a unique way as $v = h + \lambda v_0$. Thus, there is a well-defined function $f^*: E \to K$, such that $f^*(v) = \lambda$, for every $v = h + \lambda v_0$. We leave as a simple exercise the verification that $f^*$ is a linear form. Since $f^*(v_0) = 1$, the linear form $f^*$ is nonnull. Also, by definition, it is clear that $\lambda = 0$ iff $v \in H$, that is, $\ker f^* = H$.

(c) Let $H$ be a hyperplane in $E$, and let $f^* \in E^*$ be any (nonnull) linear form such that $H = \ker f^*$. Clearly, if $g^* = \lambda f^*$ for some $\lambda \neq 0$, then $H = \ker g^*$. Conversely, assume that...
$H = \text{Ker } g^*$ for some nonnull linear form $g^*$. From (a), we have $E = H \oplus Kv_0$, for some $v_0$ such that $f^*(v_0) \neq 0$ and $g^*(v_0) \neq 0$. Then, observe that

$$g^* - \frac{g^*(v_0)}{f^*(v_0)}f^*$$

is a linear form that vanishes on $H$, since both $f^*$ and $g^*$ vanish on $H$, but also vanishes on $Kv_0$. Thus, $g^* = \lambda f^*$, with

$$\lambda = \frac{g^*(v_0)}{f^*(v_0)}.$$

If $E$ is a vector space of finite dimension $n$ and $(u_1, \ldots, u_n)$ is a basis of $E$, for any linear form $f^* \in E^*$, for every $x = x_1u_1 + \cdots + x_nu_n \in E$, we have

$$f^*(x) = \lambda_1x_1 + \cdots + \lambda_nx_n,$$

where $\lambda_i = f^*(u_i) \in K$, for every $i$, $1 \leq i \leq n$. Thus, with respect to the basis $(u_1, \ldots, u_n)$, $f^*(x)$ is a linear combination of the coordinates of $x$, as expected.

We leave as an exercise the fact that every subspace $V \neq E$ of a vector space $E$, is the intersection of all hyperplanes that contain $V$. We now consider the notion of transpose of a linear map and of a matrix.

### 2.11 Transpose of a Linear Map and of a Matrix

Given a linear map $f: E \to F$, it is possible to define a map $f^\top: F^* \to E^*$ which has some interesting properties.

**Definition 2.25** Given a linear map $f: E \to F$, the **transpose** $f^\top: F^* \to E^*$ of $f$ is the linear map defined such that

$$f^\top(v^*) = v^* \circ f,$$

for every $v^* \in F^*$. Equivalently, the linear map $f^\top: F^* \to E^*$ is defined such that

$$\langle v^*, f(u) \rangle = \langle f^\top(v^*), u \rangle,$$

for all $u \in E$ and all $v^* \in F^*$.

It is easy to verify that the following properties hold:

$$(f^\top)^\top = f,$$

$$(f + g)^\top = f^\top + g^\top,$$

$$(g \circ f)^\top = f^\top \circ g^\top,$$

$id_E^\top = id_{E^*}.$

Note the reversal of composition on the right-hand side of $(g \circ f)^\top = f^\top \circ g^\top$. 
2.11. **TRANSPOSE OF A LINEAR MAP AND OF A MATRIX**

The following proposition shows the relationship between orthogonality and transposition.

**Proposition 2.30** Given a linear map \( f : E \to F \), for any subspace \( U \) of \( E \), we have

\[
\begin{align*}
  f(U)^0 &= (f^\top)^{-1}(U^0). 
\end{align*}
\]

As a consequence, \( \ker f^\top = (\text{Im } f)^0 \) and \( \ker f = (\text{Im } f^\top)^0 \).

**Proof.** We have

\[
\langle v^*, f(u) \rangle = \langle f^\top(v^*), u \rangle,
\]

for all \( u \in E \) and all \( v^* \in F^* \), and thus, we have \( \langle v^*, f(u) \rangle = 0 \) for every \( u \in U \), i.e., \( v^* \in f(U)^0 \), iff \( \langle f^\top(v^*), u \rangle = 0 \) for every \( u \in U \), i.e., \( v^* \in (f^\top)^{-1}(U^0) \), proving that

\[
\begin{align*}
  f(U)^0 &= (f^\top)^{-1}(U^0). 
\end{align*}
\]

Since we already observed that \( E^0 = 0 \), letting \( U = E \) in the above identity, we obtain that

\[
\ker f^\top = (\text{Im } f)^0.
\]

The identity \( \ker f = (\text{Im } f^\top)^0 \) holds because \( (f^\top)^\top = f \). \(\square\)

The following theorem shows the relationship between the rank of \( f \) and the rank of \( f^\top \).

**Theorem 2.31** Given a linear map \( f : E \to F \), the following properties hold.

(a) The dual \( (\text{Im } f)^* \) of \( \text{Im } f \) is isomorphic to \( \text{Im } f^\top = f^\top(\text{I}^*) \).

(b) \( \text{rk}(f) \leq \text{rk}(f^\top) \). If \( \text{rk}(f) \) is finite, we have \( \text{rk}(f) = \text{rk}(f^\top) \).

**Proof.** (a) Consider the linear maps

\[
E \xrightarrow{p} \text{Im } f \xrightarrow{j} F,
\]

where \( E \xrightarrow{p} \text{Im } f \) is the surjective map induced by \( E \xrightarrow{j} F \), and \( \text{Im } f \xrightarrow{j} F \) is the injective inclusion map of \( \text{Im } f \) into \( F \). By definition, \( f = j \circ p \). To simplify the notation, let \( I = \text{Im } f \). Since \( E \xrightarrow{p} I \) is surjective, let \( I \xrightarrow{s} E \) be a section of \( p \), and since \( I \xrightarrow{j} F \) is injective, let \( F \xrightarrow{r} I \) be a retraction of \( j \). Then, we have \( p \circ s = \text{id}_I \) and \( r \circ j = \text{id}_I \), and since \( (p \circ s)^\top = s^\top \circ p^\top \), \( (r \circ j)^\top = j^\top \circ r^\top \), and \( \text{id}^\top = \text{id}_I \), we have

\[
\begin{align*}
  s^\top \circ p^\top &= \text{id}_I^*, \\
  j^\top \circ r^\top &= \text{id}_I^*.
\end{align*}
\]

and

\[
\text{id}_I^*.
\]
Thus, $F^* \overset{j^\top}{\to} I^*$ is surjective, and $I^* \overset{p^\top}{\to} E^*$ is injective. Since $f = j \circ p$, we also have

$$f^\top = (j \circ p)^\top = p^\top \circ j^\top,$$

and since $F^* \overset{j^\top}{\to} I^*$ is surjective, and $I^* \overset{p^\top}{\to} E^*$ is injective, we have an isomorphism between $(\text{Im } f)^*$ and $f^\top(F^*)$.

(b) We already noted that part (a) of Theorem 2.26 shows that $\dim(E) \leq \dim(E^*)$, for every vector space $E$. Thus, $\dim(\text{Im } f) \leq \dim((\text{Im } f)^*)$, which, by (a), shows that $\text{rk}(f) \leq \text{rk}(f^\top)$. When $\dim(\text{Im } f)$ is finite, we already observed that as a corollary of Theorem 2.26, $\dim(\text{Im } f) = \dim((\text{Im } f)^*)$, and thus, we have $\text{rk}(f) = \text{rk}(f^\top)$. \hfill $\square$

The following proposition shows the relationship between the matrix representing a linear map $f: E \to F$ and the matrix representing its transpose $f^\top: F^* \to E^*$.

**Proposition 2.32** Let $E$ and $F$ be two vector spaces, and let $(u_1, \ldots, u_n)$ be a basis for $E$, and $(v_1, \ldots, v_m)$ be a basis for $F$. Given any linear map $f: E \to F$, if $M(f)$ is the $m \times n$-matrix representing $f$ w.r.t. the bases $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_m)$, the $n \times m$-matrix $M(f^\top)$ representing $f^\top: F^* \to E^*$ w.r.t. the dual bases $(v_1^*, \ldots, v_m^*)$ and $(u_1^*, \ldots, u_n^*)$ is the transpose $M(f)^\top$ of $M(f)$.

**Proof.** Recall that the entry $a_{ij}$ in row $i$ and column $j$ of $M(f)$ is the $i$-th coordinate of $f(u_j)$ over the basis $(v_1, \ldots, v_m)$. By definition of $v_i^*$, we have $\langle v_i^*, f(u_j) \rangle = a_{ij}$. The entry $a_{ji}^\top$ in row $j$ and column $i$ of $M(f^\top)$ is the $j$-th coordinate of $f^\top(v_i^*)$ over the basis $(u_1^*, \ldots, u_n^*)$, which is just $f^\top(v_i^*)(u_j) = \langle f^\top(v_i^*), u_j \rangle$. Since

$$\langle v_i^*, f(u_j) \rangle = \langle f^\top(v_i^*), u_j \rangle,$$

we have $a_{ij} = a_{ji}^\top$, proving that $M(f^\top) = M(f)^\top$. \hfill $\square$

We now can give a very short proof of the fact that the rank of a matrix is equal to the rank of its transpose.

**Proposition 2.33** Given a $m \times n$ matrix $A$ over a field $K$, we have $\text{rk}(A) = \text{rk}(A^\top)$.

**Proof.** The matrix $A$ corresponds to a linear map $f: K^n \to K^m$, and by Theorem 2.31, $\text{rk}(f) = \text{rk}(f^\top)$. By Proposition 2.32, the linear map $f^\top$ corresponds to $A^\top$. Since $\text{rk}(A) = \text{rk}(f)$, and $\text{rk}(A^\top) = \text{rk}(f^\top)$, we conclude that $\text{rk}(A) = \text{rk}(A^\top)$. \hfill $\square$

Thus, given an $m \times n$-matrix $A$, the maximum number of linearly independent columns is equal to the maximum number of linearly independent rows. There are other ways of proving this fact that do not involve the dual space, but instead some elementary transformations on rows and columns.
Chapter 3

Determinants

3.1 Permutations, Signature of a Permutation

This chapter contains a review of determinants and their use in linear algebra. We begin with permutations and the signature of a permutation. Next, we define multilinear maps and alternating multilinear maps. Determinants are introduced as alternating multilinear maps taking the value 1 on the unit matrix (following Emil Artin). It is then shown how to compute a determinant using the Laplace expansion formula, and the connection with the usual definition is made. It is shown how determinants can be used to invert matrices and to solve (at least in theory!) systems of linear equations (the Cramer formulae). Finally, the determinant of a linear map is defined.

Determinants can be defined in several ways. For example, determinants can be defined in a fancy way in terms of the exterior algebra (or alternating algebra) of a vector space. We will follow a more algorithmic approach due to Emil Artin. No matter which approach is followed, we need a few preliminaries about permutations on a finite set. We need to show that every permutation on \( n \) elements is a product of transpositions, and that the parity of the number of transpositions involved is an invariant of the permutation.

Let \( I_n = \{1, 2, \ldots, n\} \), where \( n \in \mathbb{N} \), and \( n > 0 \).

**Definition 3.1** A permutation on \( n \) elements is a bijection \( \pi: I_n \to I_n \). When \( n = 1 \), the only function from \( \{1\} \) to \( \{1\} \) is the constant map \( 1 \mapsto 1 \). Thus, we will assume that \( n \geq 2 \).

A transposition is a permutation \( \tau: I_n \to I_n \) such that, for some \( i < j \) (with \( 1 \leq i < j \leq n \)), \( \tau(i) = j, \tau(j) = i \), and \( \tau(k) = k \), for all \( k \in I_n - \{i, j\} \). In other words, a transposition exchanges two distinct elements \( i, j \in I_n \). A cyclic permutation of order \( k \) (or \( k \)-cycle) is a permutation \( \sigma: I_n \to I_n \) such that, for some \( i_1, i_2, \ldots, i_k \), with \( 1 \leq i_1 < i_2 < \ldots < i_k \leq n \), and \( k \geq 2 \),

\[
\sigma(i_1) = i_2, \ldots, \sigma(i_{k-1}) = i_k, \quad \sigma(i_k) = i_1,
\]

and \( \sigma(j) = j \), for \( j \in I_n - \{i_1, \ldots, i_k\} \). The set \( \{i_1, \ldots, i_k\} \) is called the domain of the cyclic permutation, and the cyclic permutation is sometimes denoted by \((i_1, i_2, \ldots, i_k)\).
If \( \tau \) is a transposition, clearly, \( \tau \circ \tau = \text{id} \). Also, a cyclic permutation of order 2 is a transposition, and for a cyclic permutation \( \sigma \) of order \( k \), we have \( \sigma^k = \text{id} \). The following proposition shows the importance of cyclic permutations and transpositions. We will also use the terminology product of permutations (or transpositions), as a synonym for composition of permutations.

**Proposition 3.1** For every \( n \geq 2 \), for every permutation \( \pi : I_n \to I_n \), there is a partition of \( I_n \) into \( r \) subsets, with \( 1 \leq r \leq n \), where each set \( J \) in this partition is either a singleton \( \{i\} \), or it is of the form

\[
J = \{i, \pi(i), \pi^2(i), \ldots, \pi^{r_i-1}(i)\},
\]

where \( r_i \) is the smallest integer, such that, \( \pi^{r_i}(i) = i \) and \( 2 \leq r_i \leq n \). If \( \pi \) is not the identity, then it can be written in a unique way as a composition \( \pi = \sigma_1 \circ \cdots \circ \sigma_s \) of cyclic permutations (where \( 1 \leq s \leq r \)). Every permutation \( \pi : I_n \to I_n \) can be written as a nonempty composition of transpositions.

**Proof.** Consider the relation \( R_\pi \) defined on \( I_n \) as follows: \( iR_\pi j \) iff there is some \( k \geq 1 \) such that \( j = \pi^k(i) \). We claim that \( R_\pi \) is an equivalence relation. Transitivity is obvious. We claim that for every \( i \in I_n \), there is some least \( r \) (\( 1 \leq r \leq n \)) such that \( \pi^r(i) = i \). Indeed, consider the following sequence of \( n + 1 \) elements:

\[
\langle i, \pi(i), \pi^2(i), \ldots, \pi^n(i) \rangle.
\]

Since \( I_n \) only has \( n \) distinct elements, there are some \( h, k \) with \( 0 \leq h < k \leq n \) such that

\[
\pi^h(i) = \pi^k(i),
\]

and since \( \pi \) is a bijection, this implies \( \pi^{k-h}(i) = i \), where \( 0 \leq k - h \leq n \). Thus, \( R_\pi \) is reflexive. It is symmetric, since if \( j = \pi^k(i) \), letting \( r \) be the least \( r \geq 1 \) such that \( \pi^r(i) = i \), then

\[
i = \pi^{kr}(i) = \pi^{k(r-1)}(\pi^k(i)) = \pi^{k(r-1)}(j).
\]

Now, for every \( i \in I_n \), the equivalence class of \( i \) is a subset of \( I_n \), either the singleton \( \{i\} \) or a set of the form

\[
J = \{i, \pi(i), \pi^2(i), \ldots, \pi^{r_i-1}(i)\},
\]

where \( r_i \) is the smallest integer such that \( \pi^{r_i}(i) = i \) and \( 2 \leq r_i \leq n \), and in the second case, the restriction of \( \pi \) to \( J \) induces a cyclic permutation \( \sigma_i \), and \( \pi = \sigma_1 \circ \cdots \circ \sigma_s \), where \( s \) is the number of equivalence classes having at least two elements.

For the second part of the proposition, we proceed by induction on \( n \). If \( n = 2 \), there are exactly two permutations on \( \{1, 2\} \), the transposition \( \tau \) exchanging 1 and 2, and the identity. However, \( \text{id}_2 = \tau^2 \). Now, let \( n \geq 3 \). If \( \pi(n) = n \), since by the induction hypothesis, the restriction of \( \pi \) to \( \{1, \ldots, n-1\} \) can be written as a product of transpositions, \( \pi \) itself can be written as a product of transpositions. If \( \pi(n) = k \neq n \), letting \( \tau \) be the transposition such
3.1. PERMUTATIONS, SIGNATURE OF A PERMUTATION

that \( \tau(n) = k \) and \( \tau(k) = n \), it is clear that \( \tau \circ \pi \) leaves \( n \) invariant, and by the induction hypothesis, we have \( \tau \circ \pi = \tau_m \circ \cdots \circ \tau_1 \) for some transpositions, and thus

\[
\pi = \tau \circ \tau_m \circ \cdots \circ \tau_1,
\]
a product of transpositions (since \( \tau \circ \tau = \text{id}_n \)). □

**Remark:** When \( \pi = \text{id}_n \) is the identity permutation, we can agree that the composition of 0 transpositions is the identity. The second part of Proposition 3.1 shows that the transpositions generate the set of all permutations.

In writing a permutation \( \pi \) as a composition \( \pi = \sigma_1 \circ \cdots \circ \sigma_s \) of cyclic permutations, it is clear that the order of the \( \sigma_i \) does not matter, since their domains are disjoint. Given a permutation written as a product of transpositions, we now show that the parity of the number of transpositions is an invariant.

**Definition 3.2** For every \( n \geq 2 \), since every permutation \( \pi: I_n \to I_n \) defines a partition of \( r \) subsets over which \( \pi \) acts either as the identity or as a cyclic permutation, let \( \epsilon(\pi) \), called the *signature* of \( \pi \), be defined by \( \epsilon(\pi) = (-1)^{n-r} \), where \( r \) is the number of sets in the partition.

If \( \tau \) is a transposition exchanging \( i \) and \( j \), it is clear that the partition associated with \( \tau \) consists of \( n-1 \) equivalence classes, the set \( \{i, j\} \), and the \( n-2 \) singleton sets \( \{k\} \), for \( k \in I_n - \{i, j\} \), and thus, \( \epsilon(\tau) = (-1)^{n-(n-1)} = (-1)^1 = -1 \).

**Proposition 3.2** For every \( n \geq 2 \), for every permutation \( \pi: I_n \to I_n \), for every transposition \( \tau \), we have

\[
\epsilon(\tau \circ \pi) = -\epsilon(\pi).
\]

Consequently, for every product of transpositions such that \( \pi = \tau_m \circ \cdots \circ \tau_1 \), we have

\[
\epsilon(\pi) = (-1)^m,
\]
which shows that the parity of the number of transpositions is an invariant.

**Proof.** Assume that \( \tau(i) = j \) and \( \tau(j) = i \), where \( i < j \). There are two cases, depending whether \( i \) and \( j \) are in the same equivalence class \( J_i \) of \( R_\pi \), or if they are in distinct equivalence classes. If \( i \) and \( j \) are in the same class \( J_i \), then if

\[
J_i = \{i_1, \ldots, i_p, \ldots i_q, \ldots i_k\},
\]
where \( i_p = i \) and \( i_q = j \), since

\[
\tau(\pi(\pi^{-1}(i_p))) = \tau(i_p) = \tau(i) = j = i_q
\]
and

\[
\tau(\pi(i_{q-1})) = \tau(i_q) = \tau(j) = i = i_p.
\]
it is clear that $J_l$ splits into two subsets, one of which is $\{i_p, \ldots, i_{q-1}\}$, and thus, the number of classes associated with $\tau \circ \pi$ is $r + 1$, and $\epsilon(\tau \circ \pi) = (-1)^{n-r-1} = -(-1)^{n-r} = -\epsilon(\pi)$. If $i$ and $j$ are in distinct equivalence classes $J_l$ and $J_m$, say

$$\{i_1, \ldots, i_p \ldots i_b\}$$

and

$$\{j_1, \ldots, j_q \ldots j_k\},$$

where $i_p = i$ and $j_q = j$, since

$$\tau(\pi(\pi^{-1}(i_p))) = \tau(i_p) = \tau(i) = j = j_q$$

and

$$\tau(\pi(\pi^{-1}(j_q))) = \tau(j_q) = \tau(j) = i = i_p,$$

we see that the classes $J_l$ and $J_m$ merge into a single class, and thus, the number of classes associated with $\tau \circ \pi$ is $r - 1$, and $\epsilon(\tau \circ \pi) = (-1)^{n-r+1} = -(-1)^{n-r} = -\epsilon(\pi)$.

Now, let $\pi = \tau_m \circ \ldots \circ \tau_1$ be any product of transpositions. By the first part of the proposition, we have

$$\epsilon(\pi) = (-1)^{m-1} \epsilon(\tau_1) = (-1)^{m-1}(-1) = (-1)^m,$$

since $\epsilon(\tau_1) = -1$ for a transposition. □

**Remark:** When $\pi = \text{id}_n$ is the identity permutation, since we agreed that the composition of 0 transpositions is the identity, it it still correct that $(-1)^0 = \epsilon(\text{id}) = +1$. From the proposition, it is immediate that $\epsilon(\pi' \circ \pi) = \epsilon(\pi') \epsilon(\pi)$. In particular, since $\pi^{-1} \circ \pi = \text{id}_n$, we get $\epsilon(\pi^{-1}) = \epsilon(\pi)$.

We can now proceed with the definition of determinants.

### 3.2 Alternating Multilinear Maps

First, we define multilinear maps, symmetric multilinear maps, and alternate multilinear maps.

**Remark:** Most of the definitions and results presented in this section also hold when $K$ is a commutative ring, and when we consider modules over $K$ (free modules, when bases are needed).

Let $E_1, \ldots, E_n$, and $F$, be vector spaces over a field $K$, where $n \geq 1$. 
3.2. ALTERNATING Multilinear Maps

Definition 3.3 A function \( f: E_1 \times \ldots \times E_n \to F \) is a multilinear map (or an \( n \)-linear map) if it is linear in each argument, holding the others fixed. More explicitly, for every \( i, 1 \leq i \leq n \), for all \( x_1 \in E_1, \ldots, x_{i-1} \in E_{i-1}, x_{i+1} \in E_{i+1}, \ldots, x_n \in E_n \), for all \( x, y \in E_i \), for all \( \lambda \in K \),

\[
f(x_1, \ldots, x_{i-1}, x + y, x_{i+1}, \ldots, x_n) = f(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_n) + f(x_1, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_n),
\]

\[
f(x_1, \ldots, x_{i-1}, \lambda x, x_{i+1}, \ldots, x_n) = \lambda f(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_n).
\]

When \( F = K \), we call \( f \) an \( n \)-linear form (or multilinear form). If \( n \geq 2 \) and \( E_1 = E_2 = \ldots = E_n \), an \( n \)-linear map \( f: E \times \ldots \times E \to F \) is called symmetric, if \( f(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)}) \), for every permutation \( \pi \) on \( \{1, \ldots, n\} \). An \( n \)-linear map \( f: E \times \ldots \times E \to F \) is called alternating, if \( f(x_1, \ldots, x_n) = 0 \) whenever \( x_i = x_{i+1} \), for some \( i, 1 \leq i \leq n - 1 \) (in other words, when two adjacent arguments are equal). It does not harm to agree that when \( n = 1 \), a linear map is considered to be both symmetric and alternating, and we will do so.

When \( n = 2 \), a 2-linear map \( f: E_1 \times E_2 \to F \) is called a bilinear map. We have already seen several examples of bilinear maps. Multiplication \( \cdot: K \times K \to K \) is a bilinear map, treating \( K \) as a vector space over itself. More generally, multiplication \( \cdot: A \times A \to A \) in a ring \( A \) is a bilinear map, viewing \( A \) as a module over itself.

The operation \( \langle -, - \rangle: E^* \times E \to K \) applying a linear form to a vector is a bilinear map.

Symmetric bilinear maps (and multilinear maps) play an important role in geometry (inner products, quadratic forms), and in differential calculus (partial derivatives).

A bilinear map is symmetric if \( f(u, v) = f(v, u) \), for all \( u, v \in E \).

Alternating multilinear maps satisfy the following simple but crucial properties.

Proposition 3.3 Let \( f: E \times \ldots \times E \to F \) be an \( n \)-linear alternating map, with \( n \geq 2 \). The following properties hold:

1. \( f(\ldots, x_i, x_{i+1}, \ldots) = -f(\ldots, x_{i+1}, x_i, \ldots) \)

2. \( f(\ldots, x_i, \ldots, x_j, \ldots) = 0 \),

where \( x_i = x_j \), and \( 1 \leq i < j \leq n \).

3. \( f(\ldots, x_i, \ldots, x_j, \ldots) = -f(\ldots, x_j, \ldots, x_i, \ldots) \),

where \( 1 \leq i < j \leq n \).
(4) \[ f(\ldots, x_i, \ldots) = f(\ldots, x_i + \lambda x_j, \ldots), \]
for any \( \lambda \in K \), and where \( i \neq j \).

Proof. (1) By multilinearity applied twice, we have
\[
f(\ldots, x_i + x_{i+1}, x_i + x_{i+1}, \ldots) = f(\ldots, x_i, x_i, \ldots) + f(\ldots, x_{i+1}, x_{i+1}, \ldots) + f(\ldots, x_{i+1}, x_i, \ldots) + f(\ldots, x_i, x_{i+1}, \ldots),
\]
and since \( f \) is alternating, this yields
\[ 0 = f(\ldots, x_i, x_{i+1}, \ldots) + f(\ldots, x_{i+1}, x_i, \ldots), \]
that is, \( f(\ldots, x_i, x_{i+1}, \ldots) = -f(\ldots, x_{i+1}, x_i, \ldots) \).

(2) If \( x_i = x_j \) and \( i \) and \( j \) are not adjacent, we can interchange \( x_i \) and \( x_{i+1} \), and then \( x_i \) and \( x_{i+2} \), etc, until \( x_i \) and \( x_j \) become adjacent. By (1),
\[ f(\ldots, x_i, \ldots, x_j, \ldots) = \epsilon f(\ldots, x_i, x_j, \ldots), \]
where \( \epsilon = +1 \) or \(-1 \), but \( f(\ldots, x_i, x_j, \ldots) = 0 \), since \( x_i = x_j \), and (2) holds.

(3) follows from (2) as in (1). (4) is an immediate consequence of (2). \( \square \)

Proposition 3.3 will now be used to show a fundamental property of alternating linear maps. First, we need to extend the matrix notation a little bit. Let \( E \) be a vector space over \( K \). Given an \( n \times n \) matrix \( A = (a_{ij}) \) over \( K \), we can define a map \( L(A): E^n \to E^n \) as follows:
\[
L(A)_1(u_1) = a_{11}u_1 + \cdots + a_{1n}u_n,
\]
\[
L(A)_2(u_2) = a_{21}u_1 + \cdots + a_{2n}u_n,
\]
\[
\vdots
\]
\[
L(A)_n(u_n) = a_{n1}u_1 + \cdots + a_{nn}u_n,
\]
for all \( u_1, \ldots, u_n \in E \). It is immediately verified that \( L(A) \) is linear. Then, given two \( n \times n \) matrices \( A = (a_{ij}) \) and \( B = (b_{ij}) \), by repeating the calculations establishing the product of matrices (just before Definition 2.12), we can show that
\[ L(AB) = L(A) \circ L(B). \]

It is then convenient to use the matrix notation to describe the effect of the linear map \( L(A) \), as
\[
\begin{pmatrix}
L(A)_1(u_1) \\
L(A)_2(u_2) \\
\vdots \\
L(A)_n(u_n)
\end{pmatrix} =
\begin{pmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n1} & a_{n2} & \cdots & a_{nn}
\end{pmatrix}
\begin{pmatrix}
u_1 \\
u_2 \\
\vdots \\
u_n
\end{pmatrix}.
\]
Lemma 3.4 Let $f: E \times \ldots \times E \to F$ be an $n$-linear alternating map. Let $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$ be two families of $n$ vectors, such that,

\[
v_1 = a_{11}u_1 + \cdots + a_{1n}u_n, \quad \ldots \quad v_n = a_{1n}u_1 + \cdots + a_{nn}u_n.
\]

Equivalently, letting

\[
A = \begin{pmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n1} & a_{n2} & \cdots & a_{nn}
\end{pmatrix}
\]

assume that we have

\[
\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = A^\top \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}.
\]

Then,

\[
f(v_1, \ldots, v_n) = \left( \sum_{\pi} \epsilon(\pi)a_{\pi(1)}a_{\pi(2)}\cdots a_{\pi(n)} \right) f(u_1, \ldots, u_n),
\]

where the sum ranges over all permutations $\pi$ on $\{1, \ldots, n\}$.

Proof. Expanding $f(v_1, \ldots, v_n)$ by multilinearity, we get a sum of terms of the form

\[
a_{\pi(1)}a_{\pi(2)}\cdots a_{\pi(n)}f(u_{\pi(1)}, \ldots, u_{\pi(n)}),
\]

for all possible functions $\pi: \{1, \ldots, n\} \to \{1, \ldots, n\}$. However, because $f$ is alternating, only the terms for which $\pi$ is a permutation are nonzero. By Proposition 3.1, every permutation $\pi$ is a product of transpositions, and by Proposition 3.2, the parity $\epsilon(\pi)$ of the number of transpositions only depends on $\pi$. Then, applying Proposition 3.3 (3) to each transposition in $\pi$, we get

\[
a_{\pi(1)}a_{\pi(2)}\cdots a_{\pi(n)}f(u_{\pi(1)}, \ldots, u_{\pi(n)}) = \epsilon(\pi)a_{\pi(1)}a_{\pi(2)}\cdots a_{\pi(n)}f(u_1, \ldots, u_n).
\]

Thus, we get the expression of the lemma. $\square$

The quantity

\[
\det(A) = \sum_{\pi} \epsilon(\pi)a_{\pi(1)}a_{\pi(2)}\cdots a_{\pi(n)}
\]

is in fact the value of the determinant of $A$ (which, as we shall see shortly, is also equal to the determinant of $A^\top$). However, working directly with the above definition is quite awkward, and we will proceed via a slightly indirect route.
3.3 Definition of a Determinant

Recall that the set of all square $n \times n$-matrices with coefficients in a field $K$ is denoted by $M_n(K)$.

**Definition 3.4** A determinant is defined as any map

$$D: M_n(K) \to K,$$

which, when viewed as a map on $(K^n)^n$, i.e., a map of the $n$ columns of a matrix, is $n$-linear alternating and such that $D(I_n) = 1$ for the identity matrix $I_n$. Equivalently, we can consider a vector space $E$ of dimension $n$, some fixed basis $(e_1, \ldots, e_n)$, and define

$$D: E^n \to K$$

as an $n$-linear alternating map such that $D(e_1, \ldots, e_n) = 1$.

First, we will show that such maps $D$ exist, using an inductive definition that also gives a recursive method for computing determinants. Actually, we will define a family $(\mathcal{D}_n)_{n \geq 1}$ of (finite) sets of maps $D: M_n(K) \to K$. Second, we will show that determinants are in fact uniquely defined, that is, we will show that each $\mathcal{D}_n$ consists of a single map. This will show the equivalence of the direct definition $\det(A)$ of Lemma 3.4 with the inductive definition $D(A)$. Finally, we will prove some basic properties of determinants, using the uniqueness theorem. Given a matrix $A \in M_n(K)$, we denote its $n$ columns by $A^1, \ldots, A^n$.

**Definition 3.5** For every $n \geq 1$, we define a finite set $\mathcal{D}_n$ of maps $D: M_n(K) \to K$ inductively as follows:

When $n = 1$, $\mathcal{D}_1$ consists of the single map $D$ such that, $D(A) = a$, where $A = (a)$, with $a \in K$.

Assume that $\mathcal{D}_{n-1}$ has been defined, where $n \geq 2$. We define the set $\mathcal{D}_n$ as follows. For every matrix $A \in M_n(K)$, let $A_{i,j}$ be the $(n-1) \times (n-1)$-matrix obtained from $A = (a_{i,j})$ by deleting row $i$ and column $j$. Then, $\mathcal{D}_n$ consists of all the maps $D$ such that, for some $i$, $1 \leq i \leq n$,

$$D(A) = (-1)^{i+1}a_{i1}D(A_{i1}) + \cdots + (-1)^{i+n}a_{in}D(A_{in}),$$

where for every $j$, $1 \leq j \leq n$, $D(A_{ij})$ is the result of applying any $D$ in $\mathcal{D}_{n-1}$ to $A_{ij}$.

We confess that the use of the same letter $D$ for the member of $\mathcal{D}_n$ being defined, and for members of $\mathcal{D}_{n-1}$, may be slightly confusing. We considered using subscripts to distinguish, but this seems to complicate things unnecessarily. One should not worry too much anyway, since it will turn out that each $\mathcal{D}_n$ contains just one map.
3.3. DEFINITION OF A DETERMINANT

Each $(-1)^{i+j}D(A_{ij})$ is called the cofactor of $a_{ij}$, and the inductive expression for $D(A)$ is called a Laplace expansion of $D$ according to the $i$-th row. Given a matrix $A \in M_n(K)$, each $D(A)$ is called a determinant of $A$.

We will prove shortly that $D(A)$ is uniquely defined (at the moment, it is not clear that $D_n$ consists of a single map). Assuming this fact, given a $n \times n$-matrix $A = (a_{ij})$,

$$A = \begin{pmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n1} & a_{n2} & \cdots & a_{nn}
\end{pmatrix}$$

its determinant is denoted by $D(A)$ or $\det(A)$, or more explicitly by

$$\det(A) = \begin{vmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n1} & a_{n2} & \cdots & a_{nn}
\end{vmatrix}$$

First, let us first consider some examples.

**Example 3.1**

1. When $n = 2$, if

$$A = \begin{pmatrix}
a & b \\
c & d
\end{pmatrix}$$

expanding according to any row, we have

$$D(A) = ad - bc.$$

2. When $n = 3$, if

$$A = \begin{pmatrix}
a_{11} & a_{12} & a_{13} \\
a_{21} & a_{22} & a_{23} \\
a_{31} & a_{32} & a_{33}
\end{pmatrix}$$

expanding according to the first row, we have

$$D(A) = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

that is,

$$D(A) = a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31}),$$

which gives the explicit formula

$$D(A) = a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{11}a_{32}a_{23} - a_{21}a_{12}a_{33} - a_{31}a_{22}a_{13}.$$
We now show that each $D \in \mathcal{D}_n$ is a determinant (map).

**Lemma 3.5** For every $n \geq 1$, for every $D \in \mathcal{D}_n$ as defined in Definition 3.5, $D$ is an alternate linear map such that $D(I_n) = 1$.

**Proof.** By induction on $n$, it is obvious that $D(I_n) = 1$. Let us now prove that $D$ is multilinear. Let us show that $D$ is linear in each column. Consider any column $k$. Since

$$D(A) = (-1)^{i+1}a_{i1}D(A_{i1}) + \cdots + (-1)^{i+j}a_{ij}D(A_{ij}) + \cdots + (-1)^{i+n}a_{in}D(A_{in}),$$

if $j \neq k$, then by induction, $D(A_{ij})$ is linear in column $k$, and $a_{ij}$ does not belong to column $k$, so $(-1)^{i+j}a_{ij}D(A_{ij})$ is linear in column $k$. If $j = k$, then $D(A_{ij})$ does not depend on column $k = j$, since $A_{ij}$ is obtained from $A$ by deleting row $i$ and column $j = k$, and $a_{ij}$ belongs to column $j = k$. Thus, $(-1)^{i+j}a_{ij}D(A_{ij})$ is linear in column $k$. Consequently, in all cases, $(-1)^{i+j}a_{ij}D(A_{ij})$ is linear in column $k$, and thus, $D(A)$ is linear in column $k$.

Let us now prove that $D$ is alternating. Assume that two adjacent rows of $A$ are equal, say $A^k = A^{k+1}$. First, let $j \neq k$ and $j \neq k + 1$. Then, the matrix $A_{ij}$ has two identical adjacent columns, and by the induction hypothesis, $D(A_{ij}) = 0$. The remaining terms of $D(A)$ are

$$(-1)^{i+k}a_{ik}D(A_{ik}) + (-1)^{i+k+1}a_{ik+1}D(A_{ik+1}).$$

However, the two matrices $A_{ik}$ and $A_{ik+1}$ are equal, since we are assuming that columns $k$ and $k + 1$ of $A$ are identical, and since $A_{ik}$ is obtained from $A$ by deleting row $i$ and column $k$, and $A_{ik+1}$ is obtained from $A$ by deleting row $i$ and column $k + 1$. Similarly, $a_{ik} = a_{ik+1}$, since columns $k$ and $k + 1$ of $A$ are equal. But then,

$$(-1)^{i+k}a_{ik}D(A_{ik}) + (-1)^{i+k+1}a_{ik+1}D(A_{ik+1}) = (-1)^{i+k}a_{ik}D(A_{ik}) - (-1)^{i+k}a_{ik}D(A_{ik}) = 0.$$ 

This shows that $D$ is alternating, and completes the proof. $\square$

Lemma 3.5 shows the existence of determinants. We now prove their uniqueness.

**Theorem 3.6** For every $n \geq 1$, for every $D \in \mathcal{D}_n$, for every matrix $A \in M_n(K)$, we have

$$D(A) = \sum_{\pi} \epsilon(\pi)a_{\pi(1)}a_{\pi(2)} \cdots a_{\pi(n)}n,$$

where the sum ranges over all permutations $\pi$ on $\{1, \ldots, n\}$. As a consequence, $\mathcal{D}_n$ consists of a single map for every $n \geq 1$, and this map is given by the above explicit formula.

**Proof.** Consider the standard basis $(e_1, \ldots, e_n)$ of $K^n$, where $(e_i)_j = 1$ and $(e_i)_j = 0$, for $j \neq i$. Then, each column $A^j$ of $A$ corresponds to a vector $v_j$ whose coordinates over the basis $(e_1, \ldots, e_n)$ are the components of $A^j$, that is, we can write

$$v_1 = a_{11}e_1 + \cdots + a_{n1}e_n,$$

$$\cdots$$

$$v_n = a_{1n}e_1 + \cdots + a_{nn}e_n.$$
3.3. DEFINITION OF A DETERMINANT

Since by Lemma 3.5, each $D$ is a multilinear alternating map, by applying Lemma 3.4, we get

$$D(A) = D(v_1, \ldots, v_n) = \left( \sum_\pi \epsilon(\pi) a_{\pi(1)} \cdots a_{\pi(n)} \right) D(e_1, \ldots, e_n),$$

where the sum ranges over all permutations $\pi$ on $\{1, \ldots, n\}$. But $D(e_1, \ldots, e_n) = D(I_n)$, and by Lemma 3.5, we have $D(I_n) = 1$. Thus,

$$D(A) = \sum_\pi \epsilon(\pi) a_{\pi(1)} \cdots a_{\pi(n)},$$

where the sum ranges over all permutations $\pi$ on $\{1, \ldots, n\}$. $\square$

We can now prove some properties of determinants.

**Corollary 3.7** For every matrix $A \in M_n(K)$, we have $D(A) = D(A^\top)$.

**Proof.** By Theorem 3.6, we have

$$D(A) = \sum_\pi \epsilon(\pi) a_{\pi(1)} \cdots a_{\pi(n)},$$

where the sum ranges over all permutations $\pi$ on $\{1, \ldots, n\}$. Since a permutation is invertible, every product

$$a_{\pi(1)} \cdots a_{\pi(n)}$$

can be rewritten as

$$a_1 {\pi}^{-1}(1) \cdots a_n {\pi}^{-1}(n),$$

and since $\epsilon({\pi}^{-1}) = \epsilon(\pi)$ and the sum is taken over all permutations on $\{1, \ldots, n\}$, we have

$$\sum_\pi \epsilon(\pi) a_{\pi(1)} \cdots a_{\pi(n)} = \sum_\sigma \epsilon(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)},$$

where $\pi$ and $\sigma$ range over all permutations. But it is immediately verified that

$$D(A^\top) = \sum_\sigma \epsilon(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$  

$\square$

A useful consequence of Corollary 3.7 is that the determinant of a matrix is also a multilinear alternating map of its rows. This fact, combined with the fact that the determinant of a matrix is a multilinear alternating map of its columns is often useful for finding short-cuts in computing determinants. We illustrate this point on the following example which shows up in polynomial interpolation.
Example 3.2 Consider the so-called Vandermonde determinant

\[
V(x_1, \ldots, x_n) = \begin{vmatrix}
1 & 1 & \ldots & 1 \\
x_1 & x_2 & \ldots & x_n \\
x_1^2 & x_2^2 & \ldots & x_n^2 \\
\vdots & \vdots & \ddots & \vdots \\
x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1}
\end{vmatrix}.
\]

We claim that

\[
V(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_j - x_i),
\]

with \(V(x_1, \ldots, x_n) = 1\), when \(n = 1\). We prove it by induction on \(n \geq 1\). The case \(n = 1\) is obvious. Assume \(n \geq 2\). We proceed as follows: multiply row \(n - 1\) by \(x_1\) and subtract it from row \(n\) (the last row), then multiply row \(n - 2\) by \(x_1\) and subtract it from row \(n - 1\), etc, multiply row \(i - 1\) by \(x_1\) and subtract it from row \(i\), until we reach row 1. We obtain the following determinant:

\[
V(x_1, \ldots, x_n) = \begin{vmatrix}
1 & 1 & \ldots & 1 \\
0 & x_2 - x_1 & \ldots & x_n - x_1 \\
0 & x_2(x_2 - x_1) & \ldots & x_n(x_n - x_1) \\
\vdots & \vdots & \ddots & \vdots \\
0 & x_2^{n-2}(x_2 - x_1) & \ldots & x_n^{n-2}(x_n - x_1)
\end{vmatrix}.
\]

Now, expanding this determinant according to the first column and using multilinearity, we can factor \((x_i - x_1)\) from the column of index \(i - 1\) of the matrix obtained by deleting the first row and the first column, and thus

\[
V(x_1, \ldots, x_n) = (x_2 - x_1)(x_3 - x_1) \cdots (x_n - x_1)V(x_2, \ldots, x_n),
\]

which establishes the induction step.

Lemma 3.4 can be reformulated nicely as follows.

**Proposition 3.8** Let \(f: E \times \ldots \times E \to F\) be an \(n\)-linear alternating map. Let \((u_1, \ldots, u_n)\) and \((v_1, \ldots, v_n)\) be two families of \(n\) vectors, such that

\[
v_1 = a_{11}u_1 + \cdots + a_{1n}u_n,
\]

\[
\ldots
\]

\[
v_n = a_{n1}u_1 + \cdots + a_{nn}u_n.
\]

Equivalently, letting

\[
A = \begin{pmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n1} & a_{n2} & \cdots & a_{nn}
\end{pmatrix}
\]

and

\[
A = \begin{pmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{n1} & a_{n2} & \cdots & a_{nn}
\end{pmatrix}
\]

we have

\[
v_1 = Au_1,
\]

\[
\ldots
\]

\[
v_n = Au_n.
\]
3.3. DEFINITION OF A DETERMINANT

assume that we have
\[
\begin{pmatrix}
v_1 \\
v_2 \\
\vdots \\
v_n
\end{pmatrix} = A
\begin{pmatrix}
u_1 \\
u_2 \\
\vdots \\
u_n
\end{pmatrix}.
\]

Then,
\[
f(v_1,\ldots,v_n) = D(A)f(u_1,\ldots,u_n).
\]

Proof. The only difference with Lemma 3.4 is that here, we are using \(A^\top\) instead of \(A\). Thus, by Lemma 3.4 and Corollary 3.7, we get the desired result. \(\square\)

As a consequence, we get the very useful property that the determinant of a product of matrices is the product of the determinants of these matrices.

**Proposition 3.9** For any two \(n \times n\)-matrices \(A\) and \(B\), we have \(D(AB) = D(A)D(B)\).

Proof. We use Proposition 3.8 as follows: let \((e_1,\ldots,e_n)\) be the standard basis of \(K^n\), and let
\[
\begin{pmatrix}
w_1 \\
w_2 \\
\vdots \\
w_n
\end{pmatrix} = AB
\begin{pmatrix}
e_1 \\
e_2 \\
\vdots \\
e_n
\end{pmatrix}.
\]

Then, we get
\[
D(w_1,\ldots,w_n) = D(AB)D(e_1,\ldots,e_n) = D(AB),
\]
since \(D(e_1,\ldots,e_n) = 1\). Now, letting
\[
\begin{pmatrix}
v_1 \\
v_2 \\
\vdots \\
v_n
\end{pmatrix} = B
\begin{pmatrix}
e_1 \\
e_2 \\
\vdots \\
e_n
\end{pmatrix},
\]
we get
\[
D(v_1,\ldots,v_n) = D(B),
\]
and since
\[
\begin{pmatrix}
w_1 \\
w_2 \\
\vdots \\
w_n
\end{pmatrix} = A
\begin{pmatrix}
v_1 \\
v_2 \\
\vdots \\
v_n
\end{pmatrix},
\]
we get
\[
D(w_1,\ldots,w_n) = D(A)D(v_1,\ldots,v_n) = D(A)D(B).
\]
It should be noted that all the results of this section, up to now, also hold when $K$ is a commutative ring, and not necessarily a field. We can now characterize when an $n \times n$-matrix $A$ is invertible in terms of its determinant $D(A)$.

### 3.4 Inverse Matrices and Determinants

In the next two sections, $K$ is a commutative ring and when needed, a field.

**Definition 3.6** Let $K$ be a commutative ring. Given a matrix $A \in M_n(K)$, let $\tilde{A} = (b_{ij})$ be the matrix defined such that

$$b_{ij} = (-1)^{i+j}D(A_{ji}),$$

the cofactor of $a_{ji}$. The matrix $A_{ji}$ is called a minor of the matrix $A$.

Note the reversal of the indices in

$$b_{ij} = (-1)^{i+j}D(A_{ji}).$$

Thus, $\tilde{A}$ is the transpose of the matrix of cofactors of elements of $A$.

We have the following proposition.

**Proposition 3.10** Let $K$ be a commutative ring. For every matrix $A \in M_n(K)$, we have

$$A\tilde{A} = \tilde{A}A = \det(A)I_n.$$

As a consequence, $A$ is invertible iff $\det(A)$ is invertible, and if so, $A^{-1} = (\det(A))^{-1}\tilde{A}$.

**Proof.** If $\tilde{A} = (b_{ij})$ and $A\tilde{A} = (c_{ij})$, we know that the entry $c_{ij}$ in row $i$ and column $j$ of $A\tilde{A}$ is

$$c_{ij} = a_{i1}b_{1j} + \cdots + a_{ik}b_{kj} + \cdots + a_{in}b_{nj},$$

which is equal to

$$a_{i1}(-1)^{j+1}D(A_{j1}) + \cdots + a_{in}(-1)^{j+n}D(A_{jn}).$$

If $j = i$, then we recognize the expression of the expansion of $\det(A)$ according to the $i$-th row:

$$c_{ii} = \det(A) = a_{i1}(-1)^{i+1}D(A_{i1}) + \cdots + a_{in}(-1)^{i+n}D(A_{in}).$$

If $j \neq i$, we can form the matrix $A'$ by replacing the $j$-th row of $A$ by the $i$-th row of $A$. Now, the matrix $A_{jk}$ obtained by deleting row $j$ and column $k$ from $A$ is equal to the matrix
3.4. INVERSE MATRICES AND DETERMINANTS

$A'_{jk}$ obtained by deleting row $j$ and column $k$ from $A'$, since $A$ and $A'$ only differ by the $j$-th row. Thus,

$$D(A_{jk}) = D(A'_{jk}),$$

and we have

$$c_{ij} = a_{i1}(-1)^{j+1}D(A'_{j1}) + \cdots + a_{in}(-1)^{j+n}D(A'_{jn}).$$

However, this is the expansion of $D(A')$ according to the $j$-th row, since the $j$-th row of $A'$ is equal to the $i$-th row of $A$, and since $A'$ has two identical rows $i$ and $j$, because $D$ is an alternating map of the rows (see an earlier remark), we have $D(A') = 0$. Thus, we have shown that $c_{ii} = \det(A)$, and $c_{ij} = 0$, when $j \neq i$, and so

$$A\tilde{A} = \det(A)I_n.$$ 

It is also obvious from the definition of $\tilde{A}$, that

$$\tilde{A}^\top = \tilde{A}^\top.$$ 

Then, applying the first part of the argument to $A^\top$, we have

$$A^\top \tilde{A}^\top = \det(A^\top)I_n,$$

and since, $\det(A^\top) = \det(A)$, $\tilde{A}^\top = A^\top$, and $(\tilde{A}A)^\top = A^\top \tilde{A}^\top$, we get

$$\det(A)I_n = A^\top \tilde{A}^\top = A^\top \tilde{A}^\top = (\tilde{A}A)^\top,$$

that is,

$$(\tilde{A}A)^\top = \det(A)I_n,$$

which yields

$$\tilde{A}A = \det(A)I_n,$$

since $I_n^\top = I_n$. This proves that

$$A\tilde{A} = \tilde{A}A = \det(A)I_n.$$ 

As a consequence, if $\det(A)$ is invertible, we have $A^{-1} = (\det(A))^{-1}\tilde{A}$. Conversely, if $A$ is invertible, from $AA^{-1} = I_n$, by Proposition 3.9, we have $\det(A)\det(A^{-1}) = 1$, and $\det(A)$ is invertible. \(\square\)

When $K$ is a field, an element $a \in K$ is invertible iff $a \neq 0$. In this case, the second part of the proposition can be stated as $A$ is invertible iff $\det(A) \neq 0$. Note in passing that this method of computing the inverse of a matrix is usually not practical.

We now consider some applications of determinants to linear independence and to solving systems of linear equations. Although these results hold for matrices over an integral domain,
their proofs require more sophisticated methods (it is necessary to use the fraction field of the integral domain, $K$). Therefore, we assume again that $K$ is a field.

Let $A$ be an $n \times n$-matrix, $X$ a column vectors of variables, and $B$ another column vector, and let $A^1, \ldots, A^n$ denote the columns of $A$. Observe that the system of equation $AX = B$,

\[
\begin{pmatrix}
  a_{11} & a_{12} & \ldots & a_{1n} \\
  a_{21} & a_{22} & \ldots & a_{2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{n1} & a_{n2} & \ldots & a_{nn}
\end{pmatrix}
\begin{pmatrix}
  x_1 \\
  x_2 \\
  \vdots \\
  x_n
\end{pmatrix}
= 
\begin{pmatrix}
  b_1 \\
  b_2 \\
  \vdots \\
  b_n
\end{pmatrix}
\]

is equivalent to

\[x_1 A^1 + \cdots + x_j A^j + \cdots + x_n A^n = B,
\]

since the equation corresponding to the $i$-th row is in both cases

\[a_{i1} x_1 + \cdots + a_{ij} x_j + \cdots + a_{in} x_n = b_i.
\]

First, we characterize linear independence of the column vectors of a matrix $A$ in terms of its determinant.

**Proposition 3.11** Given an $n \times n$-matrix $A$ over a field $K$, the columns $A^1, \ldots, A^n$ of $A$ are linearly dependent iff $D(A) = D(A^1, \ldots, A^n) = 0$. Equivalently, $A$ has rank $n$ iff $D(A) \neq 0$.

**Proof.** First, assume that the columns $A^1, \ldots, A^n$ of $A$ are linearly dependent. Then, there are $x_1, \ldots, x_n \in K$, such that

\[x_1 A^1 + \cdots + x_j A^j + \cdots + x_n A^n = 0,
\]

where $x_j \neq 0$ for some $j$. If we compute

\[D(A^1, \ldots, x_1 A^1 + \cdots + x_j A^j + \cdots + x_n A^n, \ldots, A^n) = D(A^1, \ldots, 0, \ldots, A^n) = 0,
\]

where 0 occurs in the $j$-th position, by multilinearity, all terms containing two identical columns $A^k$ for $k \neq j$ vanish, and we get

\[x_j D(A^1, \ldots, A^n) = 0
\]

for every $j$, $1 \leq j \leq n$. Since $x_j \neq 0$ for some $j$, and $K$ is a field, we must have $D(A^1, \ldots, A^n) = 0$.

Conversely, we show that if the columns $A^1, \ldots, A^n$ of $A$ are linearly independent, then $D(A^1, \ldots, A^n) \neq 0$. If the columns $A^1, \ldots, A^n$ of $A$ are linearly independent, then they
3.5 Systems of Linear Equations and Determinant

We now characterize when a system of linear equations of the form $AX = B$ has a unique solution.

**Proposition 3.12** Given an $n \times n$-matrix $A$ over a field $K$, the following properties hold:

1. For every column vector $B$, there is a unique column vector $X$ such that $AX = B$ iff the only solution to $AX = 0$ is the trivial vector $X = 0$, iff $D(A) \neq 0$.

2. If $D(A) \neq 0$, the unique solution of $AX = B$ is given by the expressions

$$X_j = \frac{D(A^1, \ldots, A^{j-1}, B, A^{j+1}, \ldots, A^n)}{D(A^1, \ldots, A^{j-1}, A^j, A^{j+1}, \ldots, A^n)},$$

known as Cramer’s rules.

3. The system of linear equations $AX = 0$ has a nonzero solution iff $D(A) = 0$.

**Proof.** Assume that $AX = B$ has a single solution $X_0$, and assume that $AY = 0$ with $Y \neq 0$. Then,

$$A(X_0 + Y) = AX_0 + AY = AX_0 + 0 = B,$$

and $X_0 + Y \neq X_0$ is another solution of $AX = B$, contradicting the hypothesis that $AX = B$ has a single solution $X_0$. Thus, $AX = 0$ only has the trivial solution. Now, assume that $AX = 0$ only has the trivial solution. This means that the columns $A^1, \ldots, A^n$ of $A$ are linearly independent, and by Proposition 3.11, we have $D(A) \neq 0$. Finally, if $D(A) \neq 0$, by Proposition 3.10, this means that $A$ is invertible, and then, for every $B$, $AX = B$ is equivalent to $X = A^{-1}B$, which shows that $AX = B$ has a single solution.
(2) Assume that $AX = B$. If we compute
\[ D(A^1, \ldots, x_1A^1 + \cdots + x_jA^j + \cdots + x_nA^n, \ldots, A^n) = D(A^1, \ldots, B, \ldots, A^n), \]
where $B$ occurs in the $j$-th position, by multilinearity, all terms containing two identical columns $A^k$ for $k \neq j$ vanish, and we get
\[ x_j D(A^1, \ldots, A^n) = D(A^1, \ldots, A^{j-1}, B, A^{j+1}, \ldots, A^n), \]
for every $j$, $1 \leq j \leq n$. Since we assumed that $D(A) = D(A^1, \ldots, A^n) \neq 0$, we get the desired expression.

(3) Note that $AX = 0$ has a nonzero solution iff $A^1, \ldots, A^n$ are linearly dependent (as observed in the proof of Proposition 3.11), which, by Proposition 3.11, is equivalent to $D(A) = D(A^1, \ldots, A^n) = 0$. \qed

As pleasing as Cramer’s rules are, it is usually impractical to solve systems of linear equations using the above expressions.

### 3.6 Determinant of a Linear Map

We close this chapter with the notion of determinant of a linear map $f: E \to E$.

Given a vector space $E$ of finite dimension $n$, given a basis $(u_1, \ldots, u_n)$ of $E$, for every linear map $f: E \to E$, if $M(f)$ is the matrix of $f$ w.r.t. the basis $(u_1, \ldots, u_n)$, we can define $\det(f) = \det(M(f))$. If $(v_1, \ldots, v_n)$ is any other basis of $E$, and if $P$ is the change of basis matrix, by Corollary 2.15, the matrix of $f$ with respect to the basis $(v_1, \ldots, v_n)$ is $P^{-1}M(f)P$. Now, by proposition 3.9, we have
\[ \det(P^{-1}M(f)P) = \det(P^{-1}) \det(M(f)) \det(P) = \det(P^{-1}) \det(P) \det(M(f)) \det(M(f)) = \det(M(f)). \]
Thus, $\det(f)$ is indeed independent of the basis of $E$.

**Definition 3.7** Given a vector space $E$ of finite dimension, for any linear map $f: E \to E$, we define the *determinant* $\det(f)$ of $f$ as the determinant $\det(M(f))$ of the matrix of $f$ in any basis (since, from the discussion just before this definition, this determinant does not depend on the basis).

Then, we have the following proposition.

**Proposition 3.13** Given any vector space $E$ of finite dimension $n$, a linear map $f: E \to E$ is invertible iff $\det(f) \neq 0$.

**Proof.** The linear map $f: E \to E$ is invertible iff its matrix $M(f)$ in any basis is invertible (by Proposition 2.12), iff $\det(M(f)) \neq 0$, by Proposition 3.10.

Given a vector space of finite dimension $n$, it is easily seen that the set of bijective linear maps $f: E \to E$ such that $\det(f) = 1$ is a group under composition. This group is a subgroup of the general linear group $\text{GL}(E)$. It is called the *special linear group* (of $E$), and it is denoted by $\text{SL}(E)$, or when $E = K^n$, by $\text{SL}(n, K)$, or even by $\text{SL}(n)$. 


3.7  Gaussian Elimination, LU-Factorization, and Cholesky Factorization

Let $A$ be an $n \times n$ matrix, let $b \in \mathbb{R}^n$ be an $n$-dimensional vector and assume that $A$ is invertible. Our goal is to solve the system $Ax = b$. Since $A$ is assumed to be invertible, we know that this system has a unique solution, $x = A^{-1}b$. Experience shows that two counter-intuitive facts are revealed:

(1) One should avoid computing the inverse, $A^{-1}$, of $A$ explicitly. This is because this would amount to solving the $n$ linear systems, $Au(j) = e_j$, for $j = 1, \ldots, n$, where $e_j = (0, \ldots, 1, \ldots, 0)$ is the $j$th canonical basis vector of $\mathbb{R}^n$ (with a 1 is the $j$th slot). By doing so, we would replace the resolution of a single system by the resolution of $n$ systems, and we would still have to multiply $A^{-1}$ by $b$.

(2) One does not solve (large) linear systems by computing determinants (using Cramer’s formulae). This is because this method requires a number of additions (resp. multiplications) proportional to $(n + 1)!$ (resp. $(n + 2)!$).

The key idea on which most direct methods (as opposed to iterative methods, that look for an approximation of the solution) are based is that if $A$ is an upper-triangular matrix, which means that $a_{ij} = 0$ for $1 \leq j < i \leq n$ (resp. lower-triangular, which means that $a_{ij} = 0$ for $1 \leq i < j \leq n$), then computing the solution, $x$, is trivial. Indeed, say $A$ is an upper-triangular matrix

$$
A = \begin{pmatrix}
a_{11} & a_{12} & \cdots & a_{1,n-2} & a_{1,n-1} & a_{1n} \\
0 & a_{22} & \cdots & a_{2,n-2} & a_{2,n-1} & a_{2n} \\
0 & 0 & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & \cdots & 0 & a_{n-1,n-1} & a_{n-1n} \\
0 & 0 & \cdots & 0 & 0 & a_{nn}
\end{pmatrix}.
$$

Then, $\det(A) = a_{11}a_{22}\cdots a_{nn} \neq 0$, and we can solve the system $Ax = b$ from bottom-up by back-substitution, i.e., first we compute $x_n$ from the last equation, next plug this value of $x_n$ into the next to the last equation and compute $x_{n-1}$ from it, etc. This yields

$$
x_n = a_{nn}^{-1}b_n \\
x_{n-1} = a_{n-1,n-1}^{-1}(b_{n-1} - a_{n-1,n}x_n) \\
\vdots \\
x_1 = a_{11}^{-1}(b_1 - a_{12}x_2 - \cdots - a_{1,n}x_n).
$$

If $A$ was lower-triangular, we would solve the system from top-down by forward-substitution.
Thus, what we need is a method for transforming a matrix to an equivalent one in upper-triangular form. This can be done by elimination. Let us illustrate this method on the following example:

\[
\begin{align*}
2x + y + z &= 5 \\
4x - 6y &= -2 \\
-2x + 7y + 2z &= 9.
\end{align*}
\]

We can eliminate the variable \( x \) from the second and the third equation as follows: Subtract twice the first equation from the second and add the first equation to the third. We get the new system

\[
\begin{align*}
2x + y + z &= 5 \\
-8y - 2z &= -12 \\
8y + 3z &= 14.
\end{align*}
\]

This time, we can eliminate the variable \( y \) from the third equation by adding the second equation to the third:

\[
\begin{align*}
2x + y + z &= 5 \\
-8y - 2z &= -12 \\
z &= 2.
\end{align*}
\]

This last system is upper-triangular. Using back-substitution, we find the solution: \( z = 2 \), \( y = 1 \), \( x = 1 \).

Observe that we have performed only row operations. The general method is to iteratively eliminate variables using simple row operations (namely, adding or subtracting a multiple of a row to another row of the matrix) while simultaneously applying these operations to the vector \( b \), to obtain a system, \( MAx = Mb \), where \( MA \) is upper-triangular. Such a method is called Gaussian elimination. However, one extra twist is needed for the method to work in all cases: It may be necessary to permute rows, as illustrated by the following example:

\[
\begin{align*}
x + y + z &= 1 \\
x + y + 3z &= 1 \\
2x + 5y + 8z &= 1.
\end{align*}
\]

In order to eliminate \( x \) from the second and third row, we subtract the first row from the second and we subtract twice the first row from the third:

\[
\begin{align*}
x + y + z &= 1 \\
2z &= 0 \\
3y + 6z &= -1.
\end{align*}
\]

Now, the trouble is that \( y \) does not occur in the second row; so, we can’t eliminate \( y \) from the third row by adding or subtracting a multiple of the second row to it. The remedy is simple: Permute the second and the third row! We get the system:

\[
\begin{align*}
x + y + z &= 1 \\
3y + 6z &= -1 \\
2z &= 0,
\end{align*}
\]
which is already in triangular form. Another example where some permutations are needed is:

\[
\begin{align*}
  z &= 1 \\
  -2x + 7y + 2z &= 1 \\
  4x - 6y &= -1.
\end{align*}
\]

First, we permute the first and the second row, obtaining

\[
\begin{align*}
  z &= 1 \\
  -2x + 7y + 2z &= 1 \\
  4x - 6y &= -1,
\end{align*}
\]

and then, we add twice the first row to the third, obtaining:

\[
\begin{align*}
  z &= 1 \\
  8y + 4z &= 1.
\end{align*}
\]

Again, we permute the second and the third row, getting

\[
\begin{align*}
  z &= 1 \\
  8y + 4z &= 1
\end{align*}
\]

an upper-triangular system. Of course, in this example, \( z \) is already solved and we could have eliminated it first, but for the general method, we need to proceed in a systematic fashion.

We now describe the method of Gaussian Elimination applied to a linear system, \( Ax = b \), where \( A \) is assumed to be invertible. We use the variable \( k \) to keep track of the stages of elimination. Initially, \( k = 1 \).

1. The first step is to pick some nonzero entry, \( a_{11} \), in the first column of \( A \). Such an entry must exist, since \( A \) is invertible (otherwise, we would have \( \det(A) = 0 \)). The actual choice of such an element has some impact on the numerical stability of the method, but this will be examined later. For the time being, we assume that some arbitrary choice is made. This chosen element is called the pivot of the elimination step and is denoted \( \pi_1 \) (so, in this first step, \( \pi_1 = a_{11} \)).

2. Next, we permute the row \((i)\) corresponding to the pivot with the first row. Such a step is called pivoting. So, after this permutation, the first element of the first row is nonzero.

3. We now eliminate the variable \( x_2 \) from all rows except the first by adding suitable multiples of the first row to these rows. More precisely we add \( -a_{i1}/\pi_1 \) times the first row to the \( i \)th row, for \( i = 2, \ldots, n \). At the end of this step, all entries in the first column are zero except the first.
(4) Increment $k$ by 1. If $k = n$, stop. Otherwise, $k < n$, and then iteratively repeat steps (1), (2), (3) on the $(n - k + 1) \times (n - k + 1)$ subsystem obtained by deleting the first $k - 1$ rows and $k - 1$ columns from the current system.

If we let $A_1 = A$ and $A_k = (a^k_{ij})$ be the matrix obtained after $k - 1$ elimination steps $(2 \leq k \leq n)$, then the $k$th elimination step is as follows: The matrix, $A_k$, is of the form

$$A_k = \begin{pmatrix}
a^k_{11} & a^k_{12} & \cdots & \cdots & \cdots & a^k_{1n} \\
a^k_{21} & a^k_{22} & \cdots & \cdots & \cdots & a^k_{2n} \\
 \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\
 a^k_{kk} & \cdots & \cdots & a^k_{kn} \\
 \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\
a^k_{nk} & \cdots & \cdots & a^k_{nn} \\
\end{pmatrix}.$$ 

Now, we will prove later that $\det(A_k) = \pm \det(A)$. Since $A$ is invertible, some entry $a^k_{ik}$ with $k \leq i \leq n$ is nonzero; so, one of these entries can be chosen as pivot, and we permute the $k$th row with the $i$th row, obtaining the matrix $\alpha^k = (\alpha^k_{ij})$. The new pivot is $\pi_k = \alpha^k_{kk}$, and we zero the entries $i = k + 1, \ldots, n$ in column $k$ by adding $-\alpha^k_{ik}/\pi_k$ times row $k$ to row $i$. At the end of this step, we have $A_{k+1}$. Observe that the first $k - 1$ rows of $A_k$ are identical to the first $k - 1$ rows of $A_{k+1}$.

It is easy to figure out what kind of matrices perform the elementary row operations used during Gaussian elimination. The permutation of the $k$th row with the $i$th row is achieved by multiplying $A$ on the left by the transposition matrix, $P(i, k)$, with

$$P(i, k)_{jl} = \begin{cases} 
1 & \text{if } j = l, \text{ where } j \neq i \text{ and } l \neq k \\
0 & \text{if } j = l = i \text{ or } j = l = k \\
1 & \text{if } j = i \text{ and } l = k \text{ or } j = k \text{ and } l = i,
\end{cases}$$

i.e.,

$$P(i, k) = \begin{pmatrix}
1 & & & & 1 \\
1 & & & 1 & \\
0 & \ddots & \ddots & \ddots & \ddots \\
1 & \ddots & \ddots & \ddots & \ddots \\
1 & 0 & \cdots & \cdots & 1
\end{pmatrix}.$$ 

Observe that $\det(P(i, k)) = -1$. Therefore, during the permutation step (2), if row $k$ and row $i$ need to be permuted, the matrix $A$ is multiplied on the left by the matrix $P_k$ such that $P_k = P(i, k)$, else we set $P_k = I$. 


Adding $\beta$ times row $j$ to row $i$ is achieved by multiplying $A$ on the left by the elementary matrix, $E_{i,j;\beta} = I + \beta e_{i,j}$, where

$$(e_{i,j})_{kl} = \begin{cases} 1 & \text{if } k = i \text{ and } l = j \\ 0 & \text{if } k \neq i \text{ or } l \neq j, \end{cases}$$

i.e.,

$$E_{i,j;\beta} = \begin{pmatrix} 1 & 1 & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & \ddots & & \\ & & & & 1 & \\ \beta & & & & & 1 \end{pmatrix}.$$ 

Observe that the inverse of $E_{i,j;\beta} = I + \beta e_{i,j}$ is $E_{i,j;-\beta} = I - \beta e_{i,j}$ and that $\det(E_{i,j;\beta}) = 1$. Therefore, during step 3 (the elimination step), the matrix $A$ is multiplied on the left by a product, $E_k$, of matrices of the form $E_{i,k;\beta_{i,k}}$. Consequently, we see that

$$A_{k+1} = E_k P_k A_k.$$ 

The fact that $\det(P(i,k)) = -1$ and that $\det(E_{i,j;\beta}) = 1$ implies immediately the fact claimed above: We always have $\det(A_k) = \pm \det(A)$. Furthermore, since

$$A_{k+1} = E_k P_k A_k$$

and since Gaussian elimination stops for $k = n$, the matrix

$$A_n = E_{n-1}P_{n-1} \cdots E_2 P_2 E_1 P_1 A$$

is upper-triangular. Also note that if we let $M = E_{n-1}P_{n-1} \cdots E_2 P_2 E_1 P_1$, then $\det(M) = \pm 1$, and

$$\det(A) = \pm \det(A_n).$$

We can summarize all this in the following theorem:

**Theorem 3.14 (Gaussian Elimination)** Let $A$ be an $n \times n$ matrix (invertible or not). Then there is some invertible matrix, $M$, so that $U = MA$ is upper-triangular. The pivots are all nonzero iff $A$ is invertible.
Proposition 3.15 Let $A$ be an invertible $n \times n$-matrix. Then, $A$, has an $LU$-factorization, $A = LU$, iff every matrix $A[1..k, 1..k]$ is invertible for $k = 1, \ldots, n$.

Proof. First, assume that $A = LU$ is an $LU$-factorization of $A$. We can write

$$A = \begin{pmatrix} A[1..k, 1..k] & A_2 \\ A_3 & A_4 \end{pmatrix} = \begin{pmatrix} L_1 & 0 \\ P & L_4 \end{pmatrix} \begin{pmatrix} U_1 & Q \\ 0 & U_4 \end{pmatrix} = \begin{pmatrix} L_1U_1 & L_1Q \\ PU_1 & PQ + L_4U_4 \end{pmatrix},$$

Remark: Obviously, the matrix $M$ can be computed as

$$M = E_{n-1}P_{n-1} \cdots E_2P_2E_1P_1,$$

but this expression is of no use. Indeed, what we need is $M^{-1}$; when no permutations are needed, it turns out that $M^{-1}$ can be obtained immediately from the matrices $E_k$’s, in fact, from their inverses, and no multiplications are necessary.

Remark: Instead of looking for an invertible matrix, $M$, so that $MA$ is upper-triangular, we can look for an invertible matrix, $M$, so that $MA$ is a diagonal matrix. Only a simple change to Gaussian elimination is needed. At every stage, $k$, after the pivot has been found and pivoting been performed, we can look for an invertible matrix, $E_k$, that diagonalizes the $k$th row to the rows below row $k$ in order to zero the entries in column $k$ for $i = k+1, \ldots, n$, also add suitable multiples of the $k$th row to the rows above row $k$ in order to zero the entries in column $k$ for $i = 1, \ldots, k-1$. Such steps are also achieved by multiplying on the left by elementary matrices $E_{i,k; \beta, k}$, except that $i < k$, so that these matrices are not lower-diagonal matrices. Nevertheless, at the end of the process, we find that $A_n = MA$, is a diagonal matrix. This method is called the Gauss-Jordan factorization. Because it is more expansive than Gaussian elimination, this method is not used much in practice. However, Gauss-Jordan factorization can be used to compute the inverse of a matrix, $A$. Indeed, we find the $j$th column of $A^{-1}$ by solving the system $Ax^{(j)} = e_j$ (where $e_j$ is the $j$th canonical basis vector of $\mathbb{R}^n$). By applying Gauss-Jordan, we are led to a system of the form $D_jx^{(j)} = M_je_j$, where $D_j$ is a diagonal matrix, and we can immediately compute $x^{(j)}$.

It remains to discuss the choice of the pivot, and also conditions that guarantee that no permutations are needed during the Gaussian elimination process.

We begin by stating a necessary and sufficient condition for an invertible matrix to have an $LU$-factorization (i.e., Gaussian elimination does not require pivoting). We say that an invertible matrix, $A$, has an $LU$-factorization if it can be written as $A = LU$, where $U$ is upper-triangular invertible and $L$ is lower-triangular, with $L_{i,i} = 1$ for $i = 1, \ldots, n$. A lower-triangular matrix with diagonal entries equal to 1 is called a unit lower-triangular matrix. Given an $n \times n$ matrix, $A = (a_{ij})$, for any $k$, with $1 \leq k \leq n$, let $A[1..k, 1..k]$ denote the submatrix of $A$ whose entries are $a_{ij}$, where $1 \leq i, j \leq k$.

Proof. We already proved the theorem when $A$ is invertible, as well as the last assertion. Now, $A$ is singular iff some pivot is zero, say at stage $k$ of the elimination. If so, we must have $a_{i,k} = 0$, for $i = k, \ldots, n$; but in this case, $A_{k+1} = A_k$ and we may pick $P_k = E_k = I$. \(\square\)
3.7. GAUSSIAN ELIMINATION, LU AND CHOLESKY FACTORIZATION

where $L_1, L_4$ are unit lower-triangular and $U_1, U_4$ are upper-triangular. Thus,

$$A[1..k, 1..k] = L_1U_1,$$

and since $U$ is invertible, $U_1$ is also invertible (the determinant of $U$ is the product of the diagonal entries in $U$, which is the product of the diagonal entries in $U_1$ and $U_4$). As $L_1$ is invertible (since its diagonal entries are equal to 1), we see that $A[1..k, 1..k]$ is invertible for $k = 1, \ldots, n$.

Conversely, assume that $A[1..k, 1..k]$ is invertible, for $k = 1, \ldots, n$. We just need to show that Gaussian elimination does not need pivoting. We prove by induction on $k$ that the $k$th step does not need pivoting. This holds for $k = 1$, since $A[1..1, 1..1] = (a_{11})$, so, $a_{11} \neq 0$. Assume that no pivoting was necessary for the first $k$ steps ($1 \leq k \leq n - 1$). In this case, we have

$$E_{k-1} \cdots E_2E_1A = A_k,$$

where $L = E_{k-1} \cdots E_2E_1$ is a unit lower-triangular matrix and $A_k[1..k, 1..k]$ is upper-triangular, so that $LA = A_k$ can be written as

$$
\begin{pmatrix}
L_1 & 0 \\
P & L_4
\end{pmatrix}
\begin{pmatrix}
A[1..k, 1..k] & A_2 \\
A_3 & A_4
\end{pmatrix}
= 
\begin{pmatrix}
U_1 & B_2 \\
0 & B_4
\end{pmatrix},
$$

where $L_1$ is unit lower-triangular and $U_1$ is upper-triangular. But then,

$$L_1A[1..k, 1..k]) = U_1,$$

where $L_1$ is invertible and $U_1$ is also invertible since its diagonal elements are the first $k$ pivots, by hypothesis. Therefore, $A[1..k, 1..k]$ is also invertible. □

**Corollary 3.16 (LU-Factorization)** Let $A$ be an invertible $n \times n$-matrix. If every matrix $A[1..k, 1..k]$ is invertible for $k = 1, \ldots, n$, then Gaussian elimination requires no pivoting and yields an LU-factorization, $A = LU$.

**Proof.** We proved in Proposition 3.15 that in this case Gaussian elimination requires no pivoting. Then, since every elementary matrix $E_{i,k;\beta}$ is lower-triangular (since we always arrange that the pivot, $\pi_k$, occurs above the rows that it operates on), since $E_{i,k;\beta}^{-1} = E_{i,k;\beta}^{-1}$ and the $E_k$'s are products of $E_{i,k;\beta}$'s, from

$$E_{n-1} \cdots E_2E_1A = U,$$

where $U$ is an upper-triangular matrix, we get

$$A = LU,$$

where $L = E_1^{-1}E_2^{-1} \cdots E_{n-1}^{-1}$ is a lower-triangular matrix. Furthermore, as the diagonal entries of each $E_{i,k;\beta}$ are 1, the diagonal entries of each $E_k$ are also 1. □
The reader should verify that the example below is indeed an \( LU \)-factorization.

\[
\begin{pmatrix}
  2 & 1 & 1 & 0 \\
  4 & 3 & 3 & 1 \\
  8 & 7 & 9 & 5 \\
  6 & 7 & 9 & 8 \\
\end{pmatrix} = \begin{pmatrix}
  1 & 0 & 0 & 0 \\
  2 & 1 & 0 & 0 \\
  4 & 3 & 1 & 0 \\
  3 & 4 & 1 & 1 \\
\end{pmatrix} \begin{pmatrix}
  2 & 1 & 1 & 0 \\
  0 & 1 & 1 & 1 \\
  0 & 0 & 2 & 2 \\
  0 & 0 & 0 & 2 \\
\end{pmatrix}.
\]

One of the main reasons why the existence of an \( LU \)-factorization for a matrix, \( A \), is interesting is that if we need to solve several linear systems, \( Ax = b \), corresponding to the same matrix, \( A \), we can do this cheaply by solving the two triangular systems

\[
Lw = b, \quad \text{and} \quad Ux = w.
\]

As we will see a bit later, symmetric positive definite matrices satisfy the condition of Proposition 3.15. Therefore, linear systems involving symmetric positive definite matrices can be solved by Gaussian elimination without pivoting. Actually, it is possible to do better: This is the Cholesky factorization.

The following easy proposition shows that, in principle, \( A \) can be premultiplied by some permutation matrix, \( P \), so that \( PA \) can be converted to upper-triangular form without using any pivoting.

**Proposition 3.17** Let \( A \) be an invertible \( n \times n \)-matrix. Then, there is some permutation matrix, \( P \), so that \( PA[1..k, 1..k] \) is invertible for \( k = 1, \ldots, n \).

**Proof.** The case \( n = 1 \) is trivial, and so is the case \( n = 2 \) (we swap the rows if necessary). If \( n \geq 3 \), we proceed by induction. Since \( A \) is invertible, its columns are linearly independent; so, in particular, its first \( n - 1 \) columns are also linearly independent. Delete the last column of \( A \). Since the remaining \( n - 1 \) columns are linearly independent, there are also \( n - 1 \) linearly independent rows in the corresponding \( n \times (n - 1) \) matrix. Thus, there is a permutation of these \( n \) rows so that the \( (n - 1) \times (n - 1) \) matrix consisting of the first \( n - 1 \) rows is invertible. But, then, there is a corresponding permutation matrix, \( P_1 \), so that the first \( n - 1 \) rows and columns of \( P_1A \) form an invertible matrix, \( A' \). Applying the induction hypothesis to the \( (n - 1) \times (n - 1) \) matrix, \( A' \), we see that there some permutation matrix, \( P_2 \), so that \( P_2P_1A[1..k, 1..k] \) is invertible, for \( k = 1, \ldots, n - 1 \). Since \( A \) is invertible in the first place and \( P_1 \) and \( P_2 \) are invertible, \( P_1P_2A \) is also invertible, and we are done. \( \square \)

**Remark:** One can also prove Proposition 3.17 using a clever reordering of the Gaussian elimination steps. Indeed, we know that if \( A \) is invertible, then there are permutation matrices, \( P_i \), and products of elementary matrices, \( E_i \), so that

\[
A_n = E_{n-1}P_{n-1} \cdots E_2P_2E_1P_1A,
\]

where \( U = A_n \) is upper-triangular. For example, when \( n = 4 \), we have \( E_3P_3E_2P_2E_1P_1A = U \). We can define new matrices \( E'_1, E'_2, E'_3 \) which are still products of elementary matrices and we have

\[
E'_3E'_2E'_1P_3P_2P_1A = U.
\]
Indeed, if we let $E_3' = E_3$, $E_2' = P_3E_2P_3^{-1}$, and $E_1' = P_3P_2E_1P_2^{-1}P_3^{-1}$, we easily verify that each $E_k'$ is a product of elementary matrices and that

$$E_3'E_2'E_1P_3P_2P_1 = E_3(P_3E_2P_3^{-1})(P_3P_2E_1P_2^{-1}P_3^{-1})P_3P_2P_1 = E_3P_3E_2P_2E_1P_1.$$ 

In general, we let

$$E_k' = P_{n-1} \cdots P_{k+1}E_kP_{k+1}^{-1} \cdots P_{n-1}^{-1},$$

and we have

$$E_{n-1}' \cdots E_1'P_{n-1} \cdots P_1A = U.$$ 

**Theorem 3.18** For every invertible $n \times n$-matrix, $A$, there is some permutation matrix, $P$, some upper-triangular matrix, $U$, and some unit lower-triangular matrix, $L$, so that $PA = LU$ (recall, $L_{ii} = 1$ for $i = 1, \ldots, n$). Furthermore, if $P = I$, then $L$ and $U$ are unique and they are produced as a result of Gaussian elimination without pivoting. Furthermore, if $P = I$, then $L$ is simply obtained from the $E_k^{-1}$'s.

**Proof.** The only part that has not been proved is the uniqueness part and how $L$ arises from the $E_k^{-1}$'s. Assume that $A$ is invertible and that $A = L_1U_1 = L_2U_2$, with $L_1, L_2$ unit lower-triangular and $U_1, U_2$ upper-triangular. Then, we have

$$L_2^{-1}L_1 = U_2U_1^{-1}.$$ 

However, it is obvious that $L_2^{-1}$ is lower-triangular and that $U_1^{-1}$ is upper-triangular, and so, $L_2^{-1}L_1$ is lower-triangular and $U_2U_1^{-1}$ is upper-triangular. Since the diagonal entries of $L_1$ and $L_2$ are 1, the above equality is only possible if $U_2U_1^{-1} = I$, that is, $U_1 = U_2$, and so, $L_1 = L_2$. Finally, since $L = E_n^{-1}E_{n-1}^{-1} \cdots E_1^{-1}$ and each $E_k^{-1}$ is a product of elementary matrices of the form $E_{i,k-\beta_{i,k}}$ with $k \leq i \leq n$, we see that $L$ is simply the lower-triangular matrix whose $k$th column is the $k$th column of $E_k^{-1}$, with $1 \leq k \leq n-1$ (with $L_{ii} = 1$ for $i = 1, \ldots, n$). □

**Remark:** It can be shown that Gaussian elimination + back-substitution requires $n^3/3 + O(n^2)$ additions, $n^3/3 + O(n^2)$ multiplications and $n^2/2 + O(n)$ divisions.

Let us now briefly comment on the choice of a pivot. Although theoretically, any pivot can be chosen, the possibility of roundoff errors implies that it is not a good idea to pick very small pivots. The following example illustrates this point. Consider the linear system

$$10^{-4}x + y = 1$$

$$x + y = 2.$$ 

Since $10^{-4}$ is nonzero, it can be taken as pivot, and we get

$$10^{-4}x + y = 1$$

$$(1 - 10^4)y = 2 - 10^4.$$
Thus, the exact solution is

$$x = \frac{1}{1 - 10^{-4}}, \quad y = \frac{1 - 2 \times 10^{-4}}{1 - 10^{-4}}.$$  

However, if roundoff takes place on the fourth digit, then $1 - 10^4 = -9999$ and $2 - 10^4 = -9998$ will be rounded off both to $-9990$, and then, the solution is $x = 0$ and $y = 1$, very far from the exact solution where $x \approx 1$ and $y \approx 1$. The problem is that we picked a very small pivot. If instead we permute the equations, the pivot is 1, and after elimination, we get the system

$$\begin{align*}
x + y &= 2 \\
(1 - 10^{-4})y &= 1 - 2 \times 10^{-4}.
\end{align*}$$

This time, $1 - 10^{-4} = -0.9999$ and $1 - 2 \times 10^{-4} = -0.9998$ are rounded off to 0.999 and the solution is $x = 1, y = 1$, much closer to the exact solution.

To remedy this problem, one may use the strategy of partial pivoting. This consists of choosing during step $k \ (1 \leq k \leq n - 1)$ one of the entries $a^k_{ik}$ such that

$$|a^k_{ik}| = \max_{k \leq p \leq n} |a^k_{pk}|.$$  

By maximizing the value of the pivot, we avoid dividing by undesirably small pivots.

**Remark:** A matrix, $A$, is called strictly column diagonally dominant iff

$$|a_{jj}| > \sum_{i=1, i \neq j}^{n} |a_{ij}|, \quad \text{for } j = 1, \ldots, n$$

(resp. strictly row diagonally dominant iff

$$|a_{ii}| > \sum_{j=1, j \neq i}^{n} |a_{ij}|, \quad \text{for } i = 1, \ldots, n.$$)

It has been known for a long time (before 1900, say by Hadamard) that if a matrix, $A$, is strictly column diagonally dominant (resp. strictly row diagonally dominant), then it is invertible. (This is a good exercise, try it!) It can also be shown that if $A$ is strictly column diagonally dominant, then Gaussian elimination with partial pivoting does not actually require pivoting.

Another strategy, called complete pivoting, consists in choosing some entry $a^k_{ij}$, where $k \leq i, j \leq n$, such that

$$|a^k_{ij}| = \max_{k \leq p, q \leq n} |a^k_{pq}|.$$  

However, in this method, if the chosen pivot is not in column $k$, it is also necessary to permute columns. This is achieved by multiplying on the right by a permutation matrix.
However, complete pivoting tends to be too expansive in practice, and partial pivoting is the method of choice.

A special case where the LU-factorization is particularly efficient is the case of tridiagonal matrices, which we now consider.

Consider the tridiagonal matrix

\[
A = \begin{pmatrix}
    b_1 & c_1 & & & \\
    a_2 & b_2 & c_2 & & \\
    & a_3 & b_3 & c_3 & \\
    & & \ddots & \ddots & \ddots \\
    & & & a_{n-2} & b_{n-2} & c_{n-2} \\
    & & & & a_{n-1} & b_{n-1} & c_{n-1} \\
    & & & & & a_n & b_n \\
\end{pmatrix}.
\]

Define the sequence

\[
\delta_0 = 1, \quad \delta_1 = b_1, \quad \delta_k = b_k\delta_{k-1} - a_kc_{k-1}\delta_{k-2}, \quad 2 \leq k \leq n.
\]

**Proposition 3.19** If \(A\) is the tridiagonal matrix above, then \(\delta_k = \det(A[1..k,1..k])\), for \(k = 1, \ldots, n\).

**Proof.** By expanding \(\det(A[1..k,1..k])\) with respect to its last row, the proposition follows by induction on \(k\). \(\square\)

**Theorem 3.20** If \(A\) is the tridiagonal matrix above and \(\delta_k \neq 0\) for \(k = 1, \ldots, n\), then \(A\) has the following LU-factorization:

[Diagonal matrix equation]

**Proof.** Since \(\delta_k = \det(A[1..k,1..k]) \neq 0\) for \(k = 1, \ldots, n\), by Theorem 3.18 (and Proposition 3.15), we know that \(A\) has a unique LU-factorization. Therefore, it suffices to check that
the proposed factorization works. We easily check that

\[
\begin{align*}
(LU)_{k,k+1} &= c_k, \quad 1 \leq k \leq n - 1 \\
(LU)_{k,k-1} &= a_k, \quad 2 \leq k \leq n \\
(LU)_{k,l} &= 0, \quad |k-l| \geq 2 \\
(LU)_{11} &= \frac{\delta_1}{\delta_0} = b_1 \\
(LU)_{k,k} &= \frac{a_k \delta_{k-2} + \delta_k}{\delta_{k-1}} = b_k, \quad 2 \leq k \leq n,
\end{align*}
\]

since \(\delta_k = b_k \delta_{k-1} - a_k c_{k-1} \delta_{k-2}\).

It follows that there is a simple method to solve a linear system, \(Ax = d\), where \(A\) is tridiagonal (and \(\delta_k \neq 0\) for \(k = 1, \ldots, n\)). For this, it is convenient to “squeeze” the diagonal matrix, \(\Delta\), defined such that \(\Delta_{k,k} = \delta_k / \delta_{k-1}\), into the factorization so that \(A = (L\Delta)(\Delta^{-1}U)\), and if we let

\[
\begin{align*}
z_1 &= \frac{c_1}{b_1}, \\
z_k &= c_k \frac{\delta_{k-2}}{\delta_k}, \quad 2 \leq k \leq n,
\end{align*}
\]

then \(A = (L\Delta)(\Delta^{-1}U)\) is written as

\[
A = \begin{pmatrix}
c_1 \\
z_1 \\
a_2 & c_2 \\
z_2 \\
a_3 & c_3 \\
z_3 \\
\vdots & \ddots & \ddots \\
a_{n-1} & c_{n-1} \\
z_{n-1} \\
a_n & c_n \\
z_n
\end{pmatrix}
\begin{pmatrix}
1 & z_1 \\
& 1 & z_2 \\
& & \ddots & \ddots \\
& & & 1 & z_{n-2} \\
& & & & 1 & z_{n-1} \\
& & & & & 1
\end{pmatrix}.
\]

As a consequence, the system \(Ax = d\) can be solved by constructing three sequences: First, the sequence

\[
\begin{align*}
z_1 &= \frac{c_1}{b_1}, \\
z_k &= \frac{c_k}{b_k - a_k z_{k-1}}, \quad k = 2, \ldots, n,
\end{align*}
\]

corresponding to the recurrence \(\delta_k = b_k \delta_{k-1} - a_k c_{k-1} \delta_{k-2}\) and obtained by dividing both sides of this equation by \(\delta_{k-1}\), next

\[
\begin{align*}
w_1 &= \frac{d_1}{b_1}, \\
w_k &= \frac{d_k - a_k w_{k-1}}{b_k - a_k z_{k-1}}, \quad k = 2, \ldots, n,
\end{align*}
\]
corresponding to solving the system \( L \Delta w = d \), and finally

\[
x_n = w_n, \quad x_k = w_k - z_k x_{k+1}, \quad k = n - 1, n - 2, \ldots, 1,
\]
corresponding to solving the system \( \Delta^{-1} U x = w \).

**Remark:** It can be verified that this requires \( 3(n - 1) \) additions, \( 3(n - 1) \) multiplications, and \( 2n \) divisions, a total of \( 8n - 6 \) operations, which is much less than the \( O(2n^3/3) \) required by Gaussian elimination in general.

We now consider the special case of symmetric positive definite matrices. Recall that an \( n \times n \) symmetric matrix, \( A \), is positive definite iff

\[
x^\top A x > 0 \quad \text{for all } x \in \mathbb{R} \text{ with } x \neq 0.
\]

Equivalently, \( A \) is symmetric positive definite iff all its eigenvalues are strictly positive. The following facts about a symmetric positive definite matrix, \( A \), are easily established (some left as exercise):

1. The matrix \( A \) is invertible. (Indeed, if \( A x = 0 \), then \( x^\top A x = 0 \), which implies \( x = 0 \).)
2. We have \( a_{ii} > 0 \) for \( i = 1, \ldots, n \). (Just observe that for \( x = e_i \), the \( i \)th canonical basis vector of \( \mathbb{R}^n \), we have \( e_i^\top A e_i = a_{ii} > 0 \).)
3. For every \( n \times n \) invertible matrix, \( Z \), the matrix \( Z^\top A Z \) is symmetric positive definite iff \( A \) is symmetric positive definite.

Next, we prove that a symmetric positive definite matrix has a special \( LU \)-factorization of the form \( A = BB^\top \), where \( B \) is a lower-triangular matrix whose diagonal elements are strictly positive. This is the Cholesky factorization.

First, we note that a symmetric positive definite matrix satisfies the condition of Proposition 3.15.

**Proposition 3.21** If \( A \) is a symmetric positive definite matrix, then \( A[1..k, 1..k] \) is invertible for \( k = 1, \ldots, n \).

**Proof.** If \( w \in \mathbb{R}^k \), with \( 1 \leq k \leq n \), we let \( x \in \mathbb{R}^n \) be the vector with \( x_i = w_i \) for \( i = 1, \ldots, k \) and \( x_i = 0 \) for \( i = k + 1, \ldots, n \). Now, since \( A \) is symmetric positive definite, we have \( x^\top A x > 0 \) for all \( x \in \mathbb{R}^n \) with \( x \neq 0 \). This holds in particular for all vectors \( x \) obtained from nonzero vectors \( w \in \mathbb{R}^k \) as defined earlier, which proves that each \( A[1..k, 1..k] \) is symmetric positive definite. Thus, \( A[1..k, 1..k] \) is also invertible. \( \square \)

Let \( A \) be a symmetric positive definite matrix and write

\[
A = \begin{pmatrix} a_{11} & W^\top \\ W & B \end{pmatrix}.
\]
Since $A$ is symmetric positive definite, $a_{11} > 0$, and we can compute $\alpha = \sqrt{a_{11}}$. The trick is that we can factor $A$ uniquely as

$$A = \begin{pmatrix} a_{11} & W^T \\ W & B \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ W/\alpha & I \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & B - WW^T/a_{11} \end{pmatrix} \begin{pmatrix} \alpha & W^T/\alpha \\ 0 & I \end{pmatrix},$$

i.e., as $A = B_1 A_1 B_1^T$, where $B_1$ is lower-triangular with positive diagonal entries. Thus, $B_1$ is invertible, and by fact (3) above, $A_1$ is also symmetric positive definite.

**Theorem 3.22 (Cholesky Factorization)** Let $A$ be a symmetric positive definite matrix. Then, there is some lower-triangular matrix, $B$, so that $A = BB^T$. Furthermore, $B$ can be chosen so that its diagonal elements are strictly positive, in which case, $B$ is unique.

**Proof.** We proceed by induction on $k$. For $k = 1$, we must have $a_{11} > 0$, and if we let $\alpha = \sqrt{a_{11}}$ and $B = (\alpha)$, the theorem holds trivially. If $k \geq 2$, as we explained above, again we must have $a_{11} > 0$, and we can write

$$A = \begin{pmatrix} a_{11} & W^T \\ W & B \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ W/\alpha & I \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & B - WW^T/a_{11} \end{pmatrix} \begin{pmatrix} \alpha & W^T/\alpha \\ 0 & I \end{pmatrix} = B_1 A_1 B_1^T,$$

where $\alpha = \sqrt{a_{11}}$, the matrix $B_1$ is invertible and

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & B - WW^T/a_{11} \end{pmatrix}$$

is symmetric positive definite. However, this implies that $B - WW^T/a_{11}$ is also symmetric positive definite (consider $x^T A_1 x$ for every $x \in \mathbb{R}^n$ with $x \neq 0$ and $x_1 = 0$). Thus, we can apply the induction hypothesis to $B - WW^T/a_{11}$, and we find a unique lower-triangular matrix, $L$, with positive diagonal entries, so that

$$B - WW^T/a_{11} = LL^T.$$

But then, we get

$$A = \begin{pmatrix} \alpha & 0 \\ W/\alpha & I \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & B - WW^T/a_{11} \end{pmatrix} \begin{pmatrix} \alpha & W^T/\alpha \\ 0 & I \end{pmatrix}$$

$$= \begin{pmatrix} \alpha & 0 \\ W/\alpha & I \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & LL^T \end{pmatrix} \begin{pmatrix} \alpha & W^T/\alpha \\ 0 & I \end{pmatrix}$$

$$= \begin{pmatrix} \alpha & 0 \\ W/\alpha & I \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & L \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & L^T \end{pmatrix} \begin{pmatrix} \alpha & W^T/\alpha \\ 0 & I \end{pmatrix}$$

$$= \begin{pmatrix} \alpha & 0 \\ W/\alpha & L \end{pmatrix} \begin{pmatrix} \alpha & W^T/\alpha \\ 0 & L^T \end{pmatrix}.$$

Therefore, if we let

$$B = \begin{pmatrix} \alpha & 0 \\ W/\alpha & L \end{pmatrix},$$
we have a unique lower-triangular matrix with positive diagonal entries and $A = BB^T$. \qed

**Remark:** If $A = BB^T$, where $B$ is any invertible matrix, then $A$ is symmetric positive definite. Obviously, $BB^T$ is symmetric, and since $B$ is invertible and

$$x^T Ax = x^T BB^T x = (B^T x)^T B^T x,$$

it is clear that $x^T Ax > 0$ if $x \neq 0$.

The proof of Theorem 3.22 immediately yields an algorithm to compute $B$ from $A$. For $j = 1, \ldots, n$,

$$b_{jj} = \left( a_{jj} - \sum_{k=1}^{j-1} b_{jk}^2 \right)^{1/2},$$

and for $i = j + 1, \ldots, n$,

$$b_{ij} = \left( a_{ij} - \sum_{k=1}^{j-1} b_{ik} b_{jk} \right) / b_{jj}.$$  

The Cholesky factorization can be used to solve linear systems, $Ax = b$, where $A$ is symmetric positive definite: Solve the two systems $Bw = b$ and $B^T x = w$.

**Remark:** It can be shown that this methods requires $n^3/6 + O(n^2)$ additions, $n^3/6 + O(n^2)$ multiplications, $n^2/2 + O(n)$ divisions, and $O(n)$ square root extractions. Thus, the Cholesky method requires half of the number of operations required by Gaussian elimination (since Gaussian elimination requires $n^3/3 + O(n^2)$ additions, $n^3/3 + O(n^2)$ multiplications, and $n^2/2 + O(n)$ divisions). It also requires half of the space (only $B$ is needed, as opposed to both $L$ and $U$). Furthermore, it can be shown that Cholesky’s method is numerically stable.

For more on the stability analysis and efficient implementation methods of Gaussian elimination, $LU$-factoring and Cholesky factoring, see Demmel [14], Trefethen and Bau [54], Ciarlet [12], Golub and Van Loan [23], Strang [50, 51], and Kincaid and Cheney [28].

### 3.8 Futher Readings

Thorough expositions of the material covered in Chapter 2 and 3 can be found in Strang [51, 50], Lang [31], Artin [1], Mac Lane and Birkhoff [34], Bourbaki [7, 8], Van Der Waerden [55], Bertin [6], and Horn and Johnson [27]. These notions of linear algebra are nicely put to use in classical geometry, see Berger [3, 4], Tisseron [53] and Dieudonné [15].

Another rather complete reference is the text by Walter Noll [40]. But beware, the notation and terminology is a bit strange!