ADVANCED LINEAR ALGEBRA

WOLFGANG GLOBKE
SCHOOL OF MATHEMATICAL SCIENCES
THE UNIVERSITY OF ADELAIDE

Version of November 3, 2013.

Preface

This text grew out of a set of lecture notes for a second course on *Linear Algebra for Computer Scientists* given by me in the summer term 2012 at the Karlsruhe Institute of Technology in Karlsruhe, Germany. It has been adapted to fit the Australian curriculum by adding an introductory section on algebraic structures such as groups, rings and fields. As these topics are not part of the compulsory first year courses, I decided to give the text the new title *Advanced Linear Algebra*, which also indicates that some knowledge of abstract vector spaces and linear maps is assumed.

The aim of this text is to teach teach those advanced topics of linear algebra which are of the greatest importance to computer scientists and engineers. The first of these is the theory of matrix canonical forms, which is precluded by a solid introduction to divisibility in Euclidean rings. Even though it is possible to introduce canonical forms without this strong algebraic underpinning, I believe the additional work invested in understanding it will greatly benefit the reader, for this approach provides a deeper insight into the structure of endomorphisms and the beautiful interplay of algebra and geometry involved. Moreover, this sets the foundation to understanding the basic principles of coding theory and cryptography. The second part of the text then studies the geometry of Euclidean vector spaces. We explore how the notion of an inner product is derived from the metric properties of Euclidean geometry in the plane, and introduce isometry groups of Euclidean spaces. Eventually, this leads to an introduction to self-adjoint endomorphisms.

The appendix contains some additional information which is not part of the lecture itself, but can facilitate the understanding in some parts.

For helpful comments on the original German text I am grateful to my colleagues Sandra Lenz and Diego De Filippi at the Karlsruhe Institute of Technology, as well as the students Felix Benz-Baldas and Michael Tobias.

For the English translation I owe gratitude to...

Contents

Prerequisites and Notations

For this text, some prior knowledge of fundamental Linear Algebra is required. In this section, we will provide an overview over the facts which are assumed to be known throughout the text, and we will also introduce some notation that will be used throughout.

Vector Spaces

A **vector space** V over a field[1)] $\mathbb{K}$, is a set V with two operations

$$+ : V \times V \to V \quad \text{and} \quad \cdot : \mathbb{K} \times V \to V$$

with the following properties:

(a) $v_1 + (v_2 + v_3) = (v_1 + v_2) + v_3$ for all $v_1, v_2, v_3 \in V$.

(b) $v_1 + v_2 = v_2 + v_1$ for all $v_1, v_2 \in V$.

(c) There exists an element $0 \in V$ such that $v + 0 = v$ for all $v \in V$.

(d) For every $v \in V$ there exists an element $-v$ satisfying $v + (-v) = 0$.

(e) $\lambda \cdot (v_1 + v_2) = \lambda \cdot v_1 + \lambda \cdot v_2$ for all $\lambda \in \mathbb{K}$ and all $v_1, v_2 \in V$.

(f) $(\lambda_1 + \lambda_2) \cdot v = \lambda_1 \cdot v + \lambda_2 \cdot v$ for all $\lambda_1, \lambda_2 \in \mathbb{K}$ and all $v \in V$.

(g) If 1 denotes the identity element in $\mathbb{K}$, then $1 \cdot v = v$ for all $v \in V$.

In the terminology of chapter **??**, properties (a) to (d) state that $(V, +)$ is an *abelian group*. The properties (e) and (f) are the *laws of distributivity*.

The basic example of a vector space is $\mathbb{K}^n$, the space of the column vectors

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad x_1, \ldots, x_n \in \mathbb{K},$$

with n entries from $\mathbb{K}$. The operation $+$ is the usual componentwise addition, and the multiplication by a scalar $\lambda \in \mathbb{K}$ is by multiplying all components by λ.

[1)] For the definition of a *field*, see **??**. The reader yet unfamiliar with fields may assume $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$.

A **vector subspace** of a vector space V is a subset $U \subseteq V$ which satisfies the above properties (a) to (g) for the operations $+$ and $\cdot$ inherited from V. In particular, U is closed under addition and mutliplication with scalars. Equivalently, a vector subspace is a subset $U \subseteq V$ which is not empty and such that $x, y \in U$ implies $x - y \in U$. If U, W are vector subspaces of V, then so are $U \cap W$ and $U + W = \{u + w \mid u \in U, w \in W\}$. If $U \cap W = \{0\}$, then the sum $U + W$ is called a **direct sum** of vector spaces, written $U \oplus W$. In this case, every element $x \in U \oplus W$ is *uniquely* represented as a sum $x = u + w$ with $u \in U$, $w \in W$.

Given vectors $v_1, \ldots, v_k \in V$, one obtains new vectors as **linear combinations** of these vectors,

$$v = \lambda_1 v_1 + \ldots + \lambda_k v_k$$

with $\lambda_1, \ldots, \lambda_k \in \mathbb{K}$. For a given set of vectors $S \subset V$, the set of all possible linear combinations is called the **span** (or **linear hull**) of S, which we write as

$$\operatorname{span}(S) = \{\lambda_1 v_1 + \ldots + \lambda_k v_k \mid k \in \mathbb{N}, \lambda_i \in \mathbb{K}, v_i \in S\}.$$

It is a vector subspace of V.

The vectors $v_1, \ldots, v_k$ are **linearly independent** if the identity

$$\lambda_1 v_1 + \ldots + \lambda_k v_k = 0$$

implies $0 = \lambda_1 = \ldots = \lambda_k$. Geometrically, this means that none of the v_j can be written as a linear combination of of the remaining ones. The vectors are called **linearly dependent** if they are not linearly independent.

A **basis** B of V is a maximal set of linearly independent vectors in V, or equivalently, a generating set of V (meaning $\operatorname{span}(B) = V$) of minimal cardinality. The cardinality of B is called the **dimension** of V, written $\dim V$. The dimension of a vectors space V is an invariant of V, meaning that all bases of V have the same cardinality.

We will be mostly concerned with vector spaces of finite dimension, concisely indicated by $\dim V < \infty$. For example, $\mathbb{K}^n$ is of dimension n, and its **canonical basis** consists of the vectors

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

In finite dimensions, for vector subspaces $U, W \subset V$, the important **dimension formula** holds:

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W).$$

If the sum is direct, this means

$$\dim(U \oplus W) = \dim U + \dim W.$$

Given a basis $B = \{b_1, \ldots, b_n\}$ of a finite dimensional vector space V, we can write each element $v \in V$ as a linear combination

$$v = \lambda_1 b_1 + \ldots + \lambda_n b_n,$$

where the scalars $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ are uniquely determined by v (for the given basis B). This gives rise to a **coordinate representation** $\varrho_B(v)$ of elements $v \in V$ by column vectors in $\mathbb{K}^n$:

$$\varrho_B(\lambda_1 b_1 + \ldots + \lambda_n b_n) = \lambda_1 e_1 + \ldots + \lambda_n e_n = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}.$$

In particular, the basis vectors $b_1, \ldots, b_n$ in V are represented by the canonical basis vectors $e_1, \ldots, e_n$ in $\mathbb{K}^n$. In the terminology introduced below, the map ϱ_B is a *vector space isomorphism* from V to $\mathbb{K}^n$.

It is important to understand how to transform basis representations for different bases into one another. So let $B = \{b_1, \ldots, b_n\}$, $C = \{c_1, \ldots, c_n\}$ be bases of V. Every element of B can be expressed as a linear combination of the elements of the basis C:

$$\begin{aligned} b_1 &= \mu_{11} \cdot c_1 + \ldots + \mu_{n1} \cdot c_n, \\ &\vdots \\ b_n &= \mu_{1n} \cdot c_1 + \ldots + \mu_{nn} \cdot c_n \end{aligned}$$

for suitable scalars $\mu_{ij} \in \mathbb{K}$. If we replace the c_i by their respective column vector representations $\varrho_C(c_i) = e_i$, we now find

$$\varrho_C(b_i) = \mu_{1i} \cdot \varrho_C(c_1) + \ldots + \mu_{ni} \cdot \varrho_C(c_n) = \begin{pmatrix} \mu_{1i} \\ \vdots \\ \mu_{ni} \end{pmatrix}$$

for $i = 1, \ldots, n$. Let $M_C^B = (\mu_{ij}) \in \mathbb{K}^{n \times n}$, the matrix whose colums are the $\varrho_C(b_i)$. So multiplying M_C^B with the ith canonical basis vector $e_i = \varrho_B(b_i)$ yields $\varrho_C(b_i)$. By linearity of matrix multiplication, this means

$$\varrho_C(v) = M_C^B \cdot \varrho_B(v)$$

is the **change of basis** from B to C for $v \in V$. The reverse change of basis from C to B is given by multiplication with the matrix

$$M_B^C = (M_C^B)^{-1}.$$

Linear Maps and Matrices

Let V and W be $\mathbb{K}$-vector spaces. A **$\mathbb{K}$-linear map** (or **homomorphism of $\mathbb{K}$-vector spaces**) $\Phi : V \to W$ is a map with the following properties:

(a) $\Phi(v_1 + v_2) = \Phi(v_1) + \Phi(v_2)$ for all $v_1, v_2 \in V$.

(b) $\Phi(\lambda \cdot v) = \lambda \cdot \Phi(v)$ for all $\lambda \in \mathbb{K}$ and $v \in V$.

The property (a) means Φ is a *homorphisms of groups* from $(V, +)$ to $(W, +)$. Linearity of a map encodes the notion compatibility with the algebraic structures of V and W.

The set of all $\mathbb{K}$-linear maps $V \to W$ is denoted by $\mathrm{Hom}_{\mathbb{K}}(V, W)$. It is a $\mathbb{K}$-vector space when addition and scalar multiplication are defined pointwise,

$$(\Phi_1 + \Phi_2)(x) = \Phi_1(x) + \Phi_2(x), \quad (\lambda \cdot \Phi)(x) = \lambda \cdot \Phi(x).$$

If Φ has an inverse linear map $\Phi^{-1} : W \to V$, then Φ is called an **isomorphism** of vector spaces. If $V = W$, a linear map $\Phi : V \to V$ is called an **endomorphism** of V, and an endomorphism which is also an isomorphism is called an **automorphism** of V. The vector space of endomorphisms of V is denoted by $\mathrm{End}(V)$. It is also closed under composition of endomorphisms, so it is even a $\mathbb{K}$-algebra. The set of all automorphisms of V is denoted $\mathbf{Aut}(V)$ or $\mathbf{GL}(V)$.[2)] With composition of maps as a product, it forms a group.

The **image** $\mathrm{im}\,\Phi$ of Φ is a vector subspace of W, and the **rank** of Φ is

$$\mathrm{rk}\,\Phi = \dim \mathrm{im}\,\Phi.$$

The **kernel** of Φ is the vector subspace of V

$$\ker \Phi = \{v \in V \mid \Phi(v) = 0\}.$$

The linear map Φ is injective if and only if its kernel is trivial, $\ker \Phi = \{0\}$.

Assume V is of finite dimension. For a linear map $\Phi : V \to W$ the following **dimension formula** holds:

$$\dim V = \mathrm{rk}\,\Phi + \dim \ker \Phi.$$

A linear map is completely defined by its images on a basis of V. As noted above, if V and W are of finite dimensions $\dim V = n$, $\dim W = m$, we can choose bases B of V and C of W, respectively, and identify V with $\mathbb{K}^n$ and W with $\mathbb{K}^m$

[2)] The notation $\mathbf{GL}(V)$ indicates $\mathbf{GL}(V) \cong \mathbf{GL}_n(\mathbb{K})$ for an n-dimensional $\mathbb{K}$-vector space V.

via coordinate representations $\varrho_B : V \to \mathbb{K}^n$ and $\varrho_C : W \to \mathbb{K}^m$. To find a compatible coordinate expression of the linear map Φ, we express the images of $b_1, \ldots, b_n \in B$ as linear combinations of elements of C,

$$\begin{aligned} \Phi(b_1) &= \alpha_{11} \cdot c_1 + \ldots + \alpha_{m1} \cdot c_m, \\ &\vdots \\ \Phi(b_n) &= \alpha_{1n} \cdot c_1 + \ldots + \alpha_{mn} \cdot c_m, \end{aligned}$$

for sutiable scalars $\alpha_{ij} \in \mathbb{K}$. Mapping these expression isomorphically to $\mathbb{K}^m$ via ϱ_C, we find

$$\varrho_C(\Phi(b_i)) = \alpha_{1i} \cdot e_1 + \ldots + \alpha_{mi} \cdot e_m = \begin{pmatrix} \alpha_{1i} \\ \vdots \\ \alpha_{mi} \end{pmatrix},$$

the ith column of the $m \times n$-matrix

$$A = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{pmatrix}.$$

The ith column is also obtained as

$$A \cdot e_i = A \cdot \varrho_B(b_i),$$

so that in the coordinates defined by C in W and B in V, Φ is represented by the matrix multiplication

$$x \mapsto A \cdot x, \quad x \in \mathbb{K}^n.$$

That is to say, the following diagram commutes:

$$\begin{array}{ccc} V & \xrightarrow{\Phi} & W \\ {\scriptstyle \varrho_B}\downarrow & & \downarrow{\scriptstyle \varrho_C} \\ \mathbb{K}^n & \xrightarrow[x \mapsto Ax]{} & \mathbb{K}^m \end{array}$$

We use the notation

$$\varrho_C^B(\Phi) = A$$

to indicate that A is the matrix representing Φ with respect to the bases B and C. The identity map $\mathrm{id}_V : V \to V$ is represented by the identity matrix I_n.

If B' and C' are other bases in V and W, respectively, then the representation matrix $\varrho_{C'}^{B'}(\Phi)$ is obtained by composition with the respective changes of basis,

$$\varrho_{C'}^{B'}(\Phi) = M_{C'}^{C} \cdot \varrho_{C}^{B}(\Phi) \cdot M_{B}^{B'}.$$

The composition of two linear maps $\Psi \circ \Phi$ corresponds to the product of the representation matrices,

$$\varrho_{D}^{B}(\Psi \circ \Phi) = \varrho_{D}^{C}(\Psi) \cdot \varrho_{C}^{B}(\Phi),$$

where B, C, D are suitable bases in the corresponding vector spaces.

Conversely, every matrix $A \in \mathbb{K}^{m \times n}$ defines a linear map $\Phi_A : \mathbb{K}^m \to \mathbb{K}^n$ via

$$\Phi_A(x) = A \cdot x.$$

Therefore, $\mathrm{Hom}_{\mathbb{K}}(V, W)$ is isomorphic to the vector space $\mathbb{K}^{m \times n}$ of $m \times n$-matrices, both as a vector space and as a ring.

Due to the correspondence of matrices and linear maps, we define the terms **rank** $\mathrm{rk}\, A$, **kernel** $\ker A$ and **image** $\mathrm{im}\, A$ by the corresponding notions for the linear map Φ_A.

Systems of Linear Equations

A **linear equation** in the unknowns $x_1, \ldots, x_n$ is a an equation in which only first powers of the x_i appear,

$$a_1 \cdot x_1 + \ldots + a_n \cdot x_n = b$$

with scalar coefficients $a_i \in \mathbb{K}$ and the right hand side $b \in \mathbb{K}$.

Accordingly, a **system of linear equations** is a collection of m linear equations in the same unknowns $x_1, \ldots, x_n$ which are to be solved simultaneously,

$$\begin{aligned} a_{11} \cdot x_1 + \ldots + a_{1n} \cdot x_n &= b_1, \\ &\vdots \\ a_{m1} \cdot x_1 + \ldots + a_{mn} \cdot x_n &= b_m. \end{aligned}$$

The system is **homogeneous** if $0 = b_1 = \ldots = b_n$, and **inhomogeneous** otherwise.

By collecting the coefficients $a_{ij} \in \mathbb{K}$ in a matrix $A = (a_{ij}) \in \mathbb{K}^{m \times n}$ and the b_i in a vector $b = (b_i) \in \mathbb{K}^m$, the system of linear equations is conveniently expressed as a matrix-vector equation

$$A \cdot x = b.$$

This system can be conveniently solved by the well-known **Gauß Algorithm**, which by means of elementary row operations transforms the extended matrix (A, b) to a form $(\tilde{A}, \tilde{b})$ from which the solutions can be easily inferred. Each elementary row operation can be realised by a multiplication on the left with a certain invertible $m \times m$-matrix, so that

$$S \cdot (A, b) = (\tilde{A}, \tilde{b})$$

holds for some $S \in \mathbf{GL}_m(\mathbb{K})$.

In general, a solution to $A \cdot x = b$ exists if and only

$$\operatorname{rk}(A, b) = \operatorname{rk} A.$$

This means b is a linear combination of the columns of A. The set of solutions is described by the following:

(i) For a homogeneous system $A \cdot x = 0$, the set of solutions is the kernel of A. In particular, the vector $x = 0$ is always a solution in this case.

(ii) If one particular solution x_0 of $A \cdot x = b$ is known, then the set of all solutions is given by
$$x_0 + \ker A.$$

(iii) If $m = n$ and $A \in \mathbf{GL}_n(\mathbb{K})$, there is precisely one solution given by
$$x = A^{-1} \cdot b.$$

Duality

Associated to each vector space V is its dual vector space $V^\star$, the space of linear map from V to $\mathbb{K}$. The elements of $V^\star$ are called **linear forms** or **linear functionals**.

For finite dimensional vector spaces it holds that $\dim V = \dim V^\star$, and for each basis $B = \{b_1, \ldots, b_n\}$ of V there exists a **dual basis** $B^\star = \{b_1^\star, \ldots, b_n^\star\}$ of $V^\star$ defined by the property

$$b_i^\star(b_k) = \delta_{ik} = \begin{cases} 1 & \text{if } i = k, \\ 0 & \text{if } i \neq k. \end{cases}$$

In particular, for $V = \mathbb{K}^n$, the linear functionals are represented by $1 \times n$-matrices, or row vectors. The dual basis of the canoncial basis $e_1, \ldots, e_n$ of V is then represented (with respect to the canoncial basis) by the tranposes of these vectors,

$e_1^\top, \dots, e_n^\top$. The operation of every $\xi \in (\mathbb{K}^n)^\star$ can be written as the product of a row and a column vector,

$$\xi(x) = \begin{pmatrix} \xi_1 & \cdots & \xi_n \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Given two vector spaces V, W, for every linear map $\Phi : V \to W$, there exists a **dual map** $\Phi^\star : W^\star \to V^\star$ defined by

$$\Phi^\star : W^\star \to V^\star, \quad \zeta \mapsto \zeta \circ \Phi.$$

If V and W are finite-dimensional with respective bases B and C, then $\Phi^\star$ has a matrix representation with respect to the dual bases $C^\star$ and $B^\star$ given by

$$\varrho_{B^\star}^{C^\star}(\Phi^\star) = \varrho_C^B(\Phi)^\top.$$

The **bi-dual space** $V^{\star\star}$ of V is the dual space of $V^\star$. If V is finite-dimensional, then there exists a canonical isomorphism

$$V \to V^{\star\star}, \quad x \mapsto x^{\star\star},$$

where for every $x \in V$ the linear form $x^{\star\star}$ on $V^\star$ is defined as

$$x^{\star\star} : V^\star \to \mathbb{K}, \quad \xi \mapsto \xi(x).$$

However, for vector spaces of infinite dimension, V, $V^\star$ and $V^{\star\star}$ are not isomorphic in general.

Determinants

The **determinant** $\det(A)$ of an $n \times n$-matrix $A = (a_{ij}) \in \mathbb{K}^{n\times n}$ (with columns $a_1, \dots, a_n$) is a map $\det : \mathbb{K}^{n\times n} \to \mathbb{K}$ defined by the properties

(a) $\det$ is **multilinear**, that is,

$$\det(a_1, \dots, a_i + b_i, \dots, a_n) = \det(a_1, \dots, a_i, \dots, a_n) + \det(a_1, \dots, b_i, \dots, a_n)$$
$$\det(a_1, \dots, \lambda \cdot a_i, \dots, a_n) = \lambda \cdot \det(a_1, \dots, a_i, \dots, a_n)$$

for all $\lambda \in \mathbb{K}$ and $a_1, \dots, a_n, b_i \in \mathbb{K}^n$.

(b) $\det$ is **alternating**,

$$\det(a_1, \dots, a_i, \dots, a_k, \dots, a_n) = -\det(a_1, \dots, a_k, \dots, a_i, \dots, a_n).$$

(c) det is normalised such that

$$\det(I_n) = 1.$$

From these properties, it can be inferred that the function det is unique and given by the **Leibniz formula**:

$$\det(A) = \sum_{\sigma \in \mathsf{S}_n} \operatorname{sgn}(\sigma) \cdot a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

For practical purposes, the recursive **Laplace expansion** by the ith row (or jth column) is helpful:

$$\det(A) = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det(A_{ik}) \left(= \sum_{k=1}^{n} (-1)^{k+j} a_{kj} \det(A_{kj}) \right),$$

where $A_{ik} \in \mathbb{K}^{(n-1)\times(n-1)}$ denotes the matrix obtained from A by deleting the ith row and kth column. It is easily seen from this that

$$\det(A) = \det(A^\top).$$

Because det is alternating, the determinant of a matrix does not change when a column a_i of A is replaced by a linear combination of a_i and the other columns. In particular, $\det(A) = 0$ if the columns of A are linearly dependent. The analogue statements hold for the rows of A.

A matrix $A \in \mathbb{K}^{n\times n}$ is invertible if and only if $\det(A) \neq 0$, so the general linear group can be characterised by

$$\mathbf{GL}_n(\mathbb{K}) = \{A \in \mathbb{K}^{n\times n} \mid \det(A) \neq 0\}.$$

This implies that a system of n linear equations in n unknowns, given by

$$A \cdot x = b \quad \text{with } b \neq 0,$$

has a solution if and only if $\det(A) \neq 0$. In this case, the solution $x = (x_i) \in \mathbb{K}^n$ of this system can be given in closed form by **Cramer's rule**:

$$x_i = \frac{\det(A_{[i]})}{\det(A)},$$

where $A_{[i]}$ is the matrix obtained from A by replacing the ith column of A by b. Note though that the computational complexity of Cramer's rule is in $\mathsf{O}(n!)$ compared to the Gauß Algorithm's $\mathsf{O}(n^3)$.

From Cramer's rule one can also deduce a closed form for the inverse of a matrix $A \in \mathbf{GL}_n(\mathbb{K})$, given by

$$A^{-1} = \frac{1}{\det(A)} \cdot A^{\#}$$

where the matrix $A^{\#} = (a_{ij}^{\#})$ is obtained from A by setting

$$a_{ij}^{\#} = (-1)^{i+j} \det(A_{ij}).$$

The determinant satisfies

$$\det(AB) = \det(A) \cdot \det(B),$$

in particular, the determinant of a matrix $B \in \mathbb{K}^{n \times n}$ does not change under conjugation by a matrix $A \in \mathbf{GL}_n(\mathbb{K})$,

$$\det(ABA^{-1}) = \det(B).$$

A geometric interpretation of the determinant in $\mathbb{R}^n$ is given as follows: If the sides of a parallelepiped P in $\mathbb{R}^n$ are spanned by vectors $a_1, \ldots, a_n \in \mathbb{R}^n$, then its volume is given by

$$\mathrm{vol}(P) = |\det(A)|,$$

where A is the matrix with columns $a_1, \ldots, a_n$. In this sense, matrices with determinant ± 1 describe volume-preserving linear transformations of $\mathbb{R}^n$.

Eigenvalues and Eigenvectors

Given an endomorphism $\Phi : V \to V$ of some $\mathbb{K}$-vector space V, an **eigenvector** x with **eigenvalue** $\lambda \in \mathbb{K}$ of Φ is a vector $x \in V \setminus \{0\}$ satisfying

$$\Phi(x) = \lambda \cdot x.$$

The set of all eigenvalues of an endomorphism Φ is called its **spectrum** $\mathrm{Spec}\, \Phi$.

The **eigenspace** of Φ for the eigenvalue λ is the span of all eigenvectors for λ,

$$E_\lambda(\Phi) = \mathrm{span}\{x \in V \mid \Phi(x) = \lambda x\}.$$

Note that in particular

$$E_0(\Phi) = \ker \Phi.$$

Eigenvectors, eigenvalues and eigenspaces for a matrix $A \in \mathbb{K}^{n \times n}$ are defined via the corresponding linear map $\Phi_A(x) = A \cdot x$.

If x is an eigenvector for the eigenvalue λ of a matrix A, then $A \cdot x = \lambda \cdot x$ is equivalent to

$$(\lambda \cdot I_n - A) \cdot x = 0.$$

In other words, the matrix $A - \lambda \cdot I_n$ has non-trivial kernel and therefore is not invertible. But then

$$\det(\lambda \cdot I_n - A) = 0$$

holds. So replacing λ by a variable X yields a polynomial in X of degree n,

$$f_A = \det(X \cdot I_n - A),$$

and the zeros of this polynomial f_A are precisely the eigenvalues of A. We call f_A the **characteristic polynomial** of A (as determinants are invariant under conjugation, and all representation matrices of an endomorphism Φ are conjugate by some base change, we can define the characteristic polynomial of Φ by that of any of its representation matrices $\varrho_B^B(\Phi)$). By the famous **Cayley-Hamilton Theorem**, the characteristic polynomial annihilates A,

$$f_A(A) = 0.$$

The characteristic polynomial provides us with a tool to determine the eigenvalues of A (at least in principle), and once the eigenvalues are known, the eigenspaces can be computed as

$$E_\lambda(A) = \ker(\lambda \cdot I_n - A)$$

using the Gauß Algorithm.

An endomorphism Φ or a matrix A can have at most n distinct eigenvalues in $\mathbb{K}$ (as the degree of f_A in n). Eigenspaces $E_\lambda(\Phi), E_\mu(\Phi)$ for two different eigenvalues $\lambda, \mu \in \operatorname{Spec} \Phi$ have trivial intersection, $E_\lambda(\Phi) \cap E_\mu(\Phi) = \{0\}$. An endomorphism Φ is called **diagonalisable** if

$$V = E_{\lambda_1}(\Phi) \oplus \ldots \oplus E_{\lambda_k}(\Phi),$$

that is, V completely decomposes into a direct sum of eigenspaces, and there exists a basis B of V consisting of eigenvectors of Φ. With respect to this basis, Φ is represented by a **diagonal matrix**

$$\varrho_B^B(\Phi) = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_k \end{pmatrix} \in \mathbb{K}^{n \times n},$$

where the eigenvalues λ_i can appear on the diagonal with multiplicities given by $\dim E_{\lambda_i}(\Phi)$. A matrix A is diagonalisable if the endomorphism Φ_A is, and in this case A is conjugate to a diagonal matrix.

Part I
Polynomials and Endomorphisms

We choose to go to the moon in this decade and do the other things,
not because they are easy, but because they are hard.
– JOHN F. KENNEDY

Our aim in this part of the text is to derive a complete classification of the conjugacy classes of complex matrices. This means that every matrix $A \in \mathbb{C}^{n\times n}$ is conjugate to a unique matrix $\tilde{A}$ which is of a particularly simple form and depends only on the conjugacy class of A. This is the *Jordan canonical form* of A. It is a generalisation of the well-known diagonal form of diagonalisable matrices.

The Jordan canonical form is intimately connected with the characteristic polynomial f_A of A. For this reason, we will first study the structure of the polynomial rings $\mathbb{K}[X]$ more closely in chapter 1. In doing so, we will emphasise the analogies to the rings $\mathbb{Z}$ of integer numbers and the modular rings $\mathbb{Z}/n\mathbb{Z}$. As an added benefit, these investigations enable us to already understand a few simple cryptographic methods.

1 Divisibility in Rings

Unless stated otherwise, R is assumed to be a ring with unit 1 throughout this chapter.

1.1 Units, Ideals and Divisibility

One of the simplest rings known to us is the ring $\mathbb{Z}$ of integer numbers. The only elements of $\mathbb{Z}$ with an inverse with respect to multiplication are -1 and $+1$, and every element $n \in \mathbb{Z}$ can be written as a product

$$n = p_1^{\nu_1} \cdots p_k^{\nu_k}$$

of distinct prime numbers $p_1, \ldots, p_k$. This representation is unique up to the order and multiplication of some p_i with a factor -1; for example,

$$60 = 2^2 \cdot 3 \cdot 5 = (-5) \cdot 2^2 \cdot (-3).$$

The multiples of a number a form a set $a\mathbb{Z}$, and if n is a multiple of a as well as of b, then

$$n \in a\mathbb{Z} \cap b\mathbb{Z}.$$

In particular, the above decomposition of n into primes means:

$$n \in p_1^{\nu_1}\mathbb{Z} \cap \ldots \cap p_k^{\nu_k}\mathbb{Z}.$$

If $|a| > |b|$ holds for two non-invertible elements $a, b \in \mathbb{Z}\backslash\{\pm 1\}$, we can apply division with remainder to obtain

$$a = q \cdot b + r,$$

where the remainder r satisfies $|r| < |b|$. Expressed in the language of congruences, this means

$$a \equiv r \bmod b \qquad (\text{or } \overline{a} = \overline{r} \in \mathbb{Z}/b\mathbb{Z})$$

and a is divisible by b if and only if $r = 0$ holds. By repeated application of division with remainder (this time to b and r), we can determine the greatest common divisor of a and b (Algorithm 1.29).

So we can compute comfortably in the ring $\mathbb{Z}$. In this chapter we will study rings R with similar benign properties. To this end, we will generalise the above-mentioned properties of $\mathbb{Z}$ to abstract rings, and study the class of rings with these generalised properties (which we will come to know as *Euclidean rings*). Of particular interest to us is the ring $\mathbb{K}[X]$ of polynomials over a field $\mathbb{K}$.

At first, we study the multiplicatively invertible elements of R.

Definition 1.1 Let R be a ring with unit. An element $x \in R$ is called a **unit** if there exists an element $x' \in R$ such that

$$x \cdot x' = 1 = x' \cdot x.$$

We write x^{-1} for x'. The set of all units of R is called the **group of units** and is denoted by $R^\times$.

The name is justified by the following lemma:

Lemma 1.2 *The group of units $R^\times$ with the ring multiplication of R is a group with neutral element 1.*

PROOF: The multiplication in R is associative, as R is a ring. We have $1 \in R^\times$, as $1 \cdot 1 = 1$. By definition of $R^\times$ there exists an inverse $x^{-1} \in R^\times$ for every $x \in R^\times$. By associativity, for $x, y \in R^\times$ it holds that

$$(xy)(y^{-1}x^{-1}) = 1 = (y^{-1}x^{-1})(xy),$$

so $(xy)^{-1} = y^{-1}x^{-1}$. Therefore, $R^\times$ is closed under multiplication. ◇

Example 1.3 (Groups of units)

(a) For $R = \mathbb{Z}$,
$$\mathbb{Z}^\times = \{-1, 1\}.$$

(b) Let $R = \mathbb{Z}/6\mathbb{Z}$. For a class $\overline{n} = n + 6\mathbb{Z}$ to be a unit in $\mathbb{Z}/6\mathbb{Z}$, there needs to exist a $m \in \mathbb{Z}$ satisfying
$$\overline{n} \cdot \overline{m} = \overline{1},$$
which is equivalent to
$$n \cdot m = q \cdot 6 + 1$$
for a suitable $q \in \mathbb{Z}$. Among the numbers from 1 to 6, this is satisfied by 1 and 5:
$$1 \cdot 1 = 0 \cdot 6 + 1,$$
$$5 \cdot 5 = 4 \cdot 6 + 1.$$
The other numbers $n = 2, 3, 4, 6$ each have a common prime factor p (either 2 or 3) with 6. Thus $n \cdot m = q \cdot 6 + 1$ is equivalent to
$$\underbrace{n \cdot m - q \cdot 6}_{\in p\mathbb{Z}} = 1 \notin p\mathbb{Z},$$
a contradiction. Therefore,
$$(\mathbb{Z}/6\mathbb{Z})^\times = \{\overline{1}, \overline{5}\}.$$

(c) In a field $\mathbb{K}$ all elements $x \in \mathbb{K}\backslash\{0\}$ are invertible by definition. Thus
$$\mathbb{K}^\times = \mathbb{K}\backslash\{0\}.$$

(d) In the polynomial ring $\mathbb{K}[X]$ over a field $\mathbb{K}$, the invertible elements are precisely the constant polynomials $\neq 0$, that is,
$$\mathbb{K}[X]^\times = \mathbb{K}^\times.$$

(e) In the ring $\mathbb{K}^{n\times n}$ of $n \times n$-matrices over a field $\mathbb{K}$ the group of units is (by definition) the general linear group
$$(\mathbb{K}^{n\times n})^\times = \mathbf{GL}_n(\mathbb{K}) = \{A \in \mathbb{K}^{n\times n} \mid \det(A) \neq 0\}.$$
More generally, for $n \times n$-matrices with coefficients in a commutative ring R with unit, the group of units is given by
$$\mathbf{GL}_n(R) = \{A \in R^{n\times n} \mid \det(A) \in R^\times\}.$$
This can be seen from the closed expression for the inverse of a matrix, which is defined if and only if division by the determinant is possible. ♡

We will now determine which properties a ring R should have in order to have divisibility properties similar to $\mathbb{Z}$. Firstly, we require that R be *commutative*, for otherwise the equality

$$a \cdot b = c \quad \text{(for some suitable } b\text{)}$$

would not automatically imply

$$b' \cdot a = c \quad \text{(for some suitable } b'\text{)}.$$

Therefore, we would have to make an inconvenient distinction between "left-divisors" and "right-divisors". Moreover, for all $a \in \mathbb{Z}$, the cancellation law

$$\text{“}a \neq 0 \text{ and } a \cdot b = a \cdot c \text{ imply } b = c\text{”},$$

holds, and we want to keep this law in the more general case R. We thus require the ring R to be *free of zero divisors*, as this implies the cancellation law.

Definition 1.4 An **integral domain** (or **integral ring**) is a commutative ring with unit which does not contain zero divisors.

Example 1.5 The rings $\mathbb{Z}$ and $\mathbb{K}[X]$ are integral. If n is not a prime number, the rings $\mathbb{Z}/n\mathbb{Z}$ contain zero divisors and are therefore not integral. But as they are quotients of the integral domain $\mathbb{Z}$, several properties of $\mathbb{Z}/n\mathbb{Z}$ can be deduced from the divisibility properties in $\mathbb{Z}$ (as it was done in Examples 1.3 (b)). ♡

Definition 1.6 Let R be an integral domain.

(a) Let $x, y \in R$. We say x **divides** y (written $x \mid y$), if there exists a $q \in R$ such that $q \cdot x = y$.

(b) Let $x_1, \ldots, x_k \in R$. An element $g \in R$ is called **greates common divisor** of $x_1, \ldots, x_k$ (written $g = \gcd(x_1, \ldots, x_k)$), if the following holds:

- g is a divisor of each $x_1, \ldots, x_k$,
- if $d \in R$ is another divisor of each $x_1, \ldots, x_k$, then d is also a divisor of g.

(c) If $\gcd(x_1, \ldots, x_k) = 1$ holds, then $x_1, \ldots, x_k$ are called **coprime**.

Remark 1.7 Note that the gcd is only determined up to multiplication with a unit in R, so the notation $\gcd(x, y) = g$ means that for every $u \in R^\times$ the element $u \cdot g$ is also a gcd of x and y.

Convention: For $R = \mathbb{Z}$, $\gcd(a, b)$ will always mean the *positive* greatest common divisor of a and b; for $R = \mathbb{K}[X]$, $\gcd(a, b)$ will always denote the *normalised* polynomial which is a greatest common divisor of a and b. Thereby, the notation becomes unambiguous.

Remark 1.8 For all $x \in R$ it holds that $1 \mid x$ and $x \mid 0$. On the other hand, for $x \neq 0$ it always holds that $0 \nmid x$ ("division by 0 is not allowed").

Exercise 1.9 The divisibility relation $\mid$ is a *quasiorder* on R, that is, it is reflexive and transitive.

Exercise 1.10 From $x \mid y$ and $x \mid z$ it follows that $x \mid y + z$.

Remark 1.11 It holds that

$$\gcd(x_1, x_2, x_3) = \gcd(\gcd(x_1, x_2), x_3),$$

as every divisor d of $\gcd(x_1, x_2)$ and x_3 satisfies $d \mid x_1$, $d \mid x_2$ in particular, and consequently $d \mid \gcd(x_1, x_2, x_3)$ by the definition of greatest common divisors.

Lemma 1.12 (Cancellation Law) *Let R be an integral domain and $a, x, y \in R$, $a \neq 0$. If $a \cdot x = a \cdot y$, then already $x = y$.*

PROOF: The condition $a \cdot x = a \cdot y$ is equivalent to $a \cdot (x - y) = 0$. As $a \neq 0$ and R has no zero divisors, it follows that $x - y = 0$. So $x = y$. ◇

Definition 1.13 Let R be a commutative Ring with unit. A subset $\mathfrak{I} \subset R$ is called an **ideal** in R if the following holds:

(i) $\mathfrak{I}$ is an additive subgroup of R, that is, $0 \in \mathfrak{I}$ and $x, y \in \mathfrak{I}$ implies $-x \in \mathfrak{I}$ and $x + y \in \mathfrak{I}$.

(ii) For all $r \in R$ and $x \in \mathfrak{I}$ it holds that $r \cdot x \in \mathfrak{I}$.

Note that ideals are *not* subrings of R, as we do not require $1 \in \mathfrak{I}$ (in fact, R itself is the only ideal containing 1).

Definition 1.14 For $x \in R$ we call

$$\langle x \rangle = \{r \cdot x \mid r \in R\}$$

the **principle ideal** generated by x in R. More generally,

$$\langle x_1, \ldots, x_n \rangle = \{r_1 \cdot x_1 + \ldots + r_n \cdot x_n \mid r_1, \ldots, r_n \in R\}$$

denotes the ideal generated by the elements $x_1, \ldots, x_n \in R$.

Example 1.15 (Ideals)

(a) In every ring R, R itself and $\{0\}$ are ideals, the *trivial ideals*.

(b) In the ring $\mathbb{Z}$ of integer numbers, for every $n \in \mathbb{Z}$ the set $n\mathbb{Z}$ is an ideal, as for $a, b \in \mathbb{Z}$

$$an + bn = (a + b)n \in n\mathbb{Z}$$

and

$$a(bn) = (ab)n \in n\mathbb{Z}$$

hold. The ideal $n\mathbb{Z}$ is the principle ideal generated by n.

(c) Let $R = \mathbb{K}[X]$. For $\alpha \in \mathbb{K}$,

$$\langle X - \alpha \rangle = \{h \cdot (X - \alpha) \mid h \in \mathbb{K}[X]\}$$

is the ideal of all polynomials with a zero at α.

(d) More generally, every polynomial $f \in \mathbb{K}[X]$ generates an ideal $\langle f \rangle$ in $\mathbb{K}[X]$ containing the multiples of f. If $\deg(f) = 0$, that is, $f \in \mathbb{K}\backslash\{0\}$, then $\langle f \rangle = \mathbb{K}[X]$. Otherwise, $\langle f \rangle$ is a proper ideal in $\mathbb{K}[X]$.

The vector subspace generated by f in $\mathbb{K}[X]$ is a proper subset of the ideal$\langle f \rangle$:

$$\operatorname{span}(f) = \{\lambda \cdot f \mid \lambda \in \mathbb{K}\} \subsetneq \{h \cdot f \mid h \in \mathbb{K}[X]\} = \langle f \rangle.$$

(e) Let $\Phi : V \to V$ be an endomorphism of a finite-dimensional $\mathbb{K}$-vector space V. Then

$$\mathfrak{I}_\Phi = \{f \in \mathbb{K}[X] \mid f(\Phi) = 0\}$$

is an ideal in the polynomial ring $\mathbb{K}[X]$. More precisely, it is the kernel of the evaluation map

$$\mathbb{K}[X] \to \operatorname{End}(V), \quad f \mapsto f(\Phi).$$

By the Cayley-Hamilton Theorem, the characteristic polynomial f_Φ of Φ is an element of $\mathfrak{I}_\Phi$. It follows from Theorem 1.35 that $\mathfrak{I}_\Phi$ is a principle ideal. The normalised generator of $\mathfrak{I}_\Phi$ is called the **minimal polynomial** of Φ. ♡

Lemma 1.16 *Let $\Phi : R_1 \to R_2$ be a homomorphism of rings. Then* $\ker \Phi = \{x \in R_1 \mid \Phi(x) = 0\}$ *is an ideal in R_1.*

PROOF: Let $r \in R_1$ and $x, y \in \ker \Phi$. As Φ is a homomorphism,

$$\Phi(x + y) = \Phi(x) + \Phi(y) = 0 + 0 = 0,$$
$$\Phi(r \cdot x) = \Phi(r) \cdot \Phi(x) = \Phi(r) \cdot 0 = 0.$$

So $x + y, r \cdot x \in \ker \Phi$, that is, $\ker \Phi$ is an ideal. ◇

Exercise 1.17 If $\mathfrak{I}_1$ and $\mathfrak{I}_2$ are ideals in R, so are $\mathfrak{I}_1 + \mathfrak{I}_2$, $\mathfrak{I}_1 \cdot \mathfrak{I}_2$ and $\mathfrak{I}_1 \cap \mathfrak{I}_2$.

Exercise 1.18 An ideal $\mathfrak{I}$ contains a unit $u \in R^\times$ if and only if $\mathfrak{I} = R$.

Exercise 1.19 If $\mathbb{K}$ is a field, the only ideals in $\mathbb{K}$ are the trivial ideals.

Divisibility in integral domains can be characterised by means of ideals:

Theorem 1.20 *Let R be an integral domain and $x, y \in R$.*

(a) *$x \mid y$ if and only if $\langle y \rangle \subset \langle x \rangle$.*

(b) *$\langle x \rangle = \langle y \rangle$ if and only if $x = u \cdot y$ for a unit $u \in R^\times$.*

(c) *If $\langle x, y \rangle = \langle g \rangle$, then $g = \gcd(x, y)$.*

(d) *If $\langle x, y \rangle = R$, then x, y are coprime.*

PROOF:

(a) We have $y = r \cdot x$ for some $r \in R$ if and only if y is an element of $\langle x \rangle$.

(b) If $x = u \cdot y$ holds, then so does $y = u^{-1} \cdot x$. With part (a) it now follows that $\langle x \rangle \subset \langle y \rangle$ and $\langle y \rangle \subset \langle x \rangle$, that is $\langle x \rangle = \langle y \rangle$.

Conversely, if $r \cdot x = y$ and $s \cdot y = x$, then $srx = x$. Cancelling x yields $sr = 1$, and thus $r, s \in R^\times$. So the unit $u = s$ satisfies $x = u \cdot y$.

(c) As $x, y \in \langle g \rangle$, g divides x and y. By assumption there exist $a, b \in R$ such that $g = ax + by$. For every common divisor d of x and y this implies $d \mid g$. Therefore $g = \gcd(x, y)$.

(d) Follows from (c) and Exercise 1.18. ◇

The corresponding statements hold for any number of elements $x_1, \ldots, x_k \in R$.

By a *prime number* one often means a $p \in \mathbb{N}$ which is "only divisible by itself and 1". When studying the ring $\mathbb{Z} \supset \mathbb{N}$, we have to admit -1 as a divisor as well. More generally, in a principle domain R we want to allow all units as divisors of

prime elements, where the condition to be "prime" shall mean that p is coprime to all elements in $R\backslash R^\times$. We will give an even more general definition here, which we will find later to precisely reflect this property in the cases of interest to us. For practical reasons, units are excluded from the definition to begin with.

Definition 1.21 Let R be an integral domain and $p \in R\backslash R^\times$, $p \neq 0$.

(a) p is called **irreducible** if in every decomposition $p = x \cdot y$ one of the elements x or y is a unit.

(b) p is called **prime** if $p \mid x \cdot y$ for some $x, y \in R$ implies $p \mid x$ or $p \mid y$.

Lemma 1.22 *If $p \in R$ is prime, then p is irreducible.*

PROOF: Let $p = x \cdot y$, in particular, p divides $x \cdot y$. As p is prime, there exists $a \in R$, such that (without loss of generality) $p \cdot a = x$ holds. Then

$$p = x \cdot y = p \cdot a \cdot y$$

and by the cancellation law

$$1 = a \cdot y.$$

Hence $y \in R^\times$. This means p is irreducible. ◇

Example 1.23 (Prime elements)

(a) The prime elements in $\mathbb{Z}$ are precisely the elements $\pm p$, where p runs through the set $\{2, 3, 5, 7, 11, \ldots\}$ of prime numbers.

(b) In $\mathbb{C}[X]$ the prime elements are precisely those polynomials

$$p = a_1 X + a_0,$$

with $a_1 \in \mathbb{C}^\times$, $a_0 \in \mathbb{C}$. This is a consequence of the Fundamental Theorem of Algebra and will be taken up again in Section 1.3.[3)]

(c) In $\mathbb{R}[X]$ the irreducible polynomials are of the form

$$p = a_1 X + a_0 \quad \text{oder} \quad q = b_2 X^2 + b_1 X + b_0,$$

where $a_1, b_2 \in \mathbb{R}^\times$, $a_0, b_1, b_0 \in \mathbb{R}$, such that the polynomial q has no real zero (otherwise q could be factored into a product of two polynomials of degree 1 by polynomial division). For example, the polynomial $X^2 + 1$ is irreducible in $\mathbb{R}[X]$, as its only zeros i and $-$i are elements of $\mathbb{C}\backslash\mathbb{R}$.

[3)] When referring to polynomials, it is customary to use the term *irreducible* instead of *prime*. In this case, the two notions are equivalent by Theorem 1.35.

(d) In polynomial rings $\mathbb{K}[X]$ over fields $\mathbb{K}$ other than $\mathbb{R}$ or $\mathbb{C}$ it is in general not easy to characterise the irreducible polynomials. The polynomials $a_1X + a_0$ of degree 1 are always irreducible, but in general there are many more. There exists a few criteria to test for irreducibility, see for example Chapter 2.8 in Bosch [1]. Also, in general there is no bound to the degree of irreducible polynomials. For example, for every prime number $p \in \mathbb{N}$ the polynomial $X^{p-1} + X^{p-2} + \ldots + X + 1$ is irreducible in $\mathbb{Q}[X]$, and the polynomial $X^p - X - 1$ is irreducible in $\mathbb{F}_p[X]$. ♡

In the language of ideals, primality can be expressed as follows:

Definition 1.24 An ideal $\mathfrak{P}$ in a ring R is called a **prime ideal** if for all $x, y \in R$ it holds that $x \cdot y \in \mathfrak{P}$ implies $x \in \mathfrak{P}$ or $y \in \mathfrak{P}$.

Lemma 1.25 *Let R be an integral domain and $p \in R$ prime. Then the principle ideal $\langle p \rangle$ is a prime ideal.*

PROOF: $x \cdot y \in \langle p \rangle$ means $p \mid x \cdot y$ by definition. So $p \mid x$ or $p \mid y$, and this again means $x \in \langle p \rangle$ or $y \in \langle p \rangle$. ◇

To further generalise the properties of the integer numbers $\mathbb{Z}$ (such as the unique prime factorisation or the ability to compute a gcd), we have to further restrict the class of rings we study. In particular, we want to be able to perform a division with remainder. These rings are the subject of the following section.

1.2 Euclidean Rings

Definition 1.26 An integral ring R is called a **Euclidean ring** if there exists a function $\delta : R \to \mathbb{N}_0$ with the following property: For all $a, b \in R$ there exists a representation

$$a = q \cdot b + r \tag{1.1}$$

with $q, r \in R$, where $r = 0$ or $\delta(r) < \delta(b)$.

In other words: In Euclidean rings division with remainder is possible. If the division leaves a remainder, then this remainder r is "smaller" (with respect to δ) than the divisor b.

Example 1.27 (Euclidean rings)

(a) The ring $\mathbb{Z}$ is a Euclidean ring with $\delta(n) = |n|$. For the division of integers we us the notation $q = a \div b$, with q, a, b as in (1.1).

(b) The polynomial ring $\mathbb{K}[X]$ is a Euclidean ring with $\delta(f) = \deg(f)$ with $f \neq 0$ and $\delta(0) = 0$. This is seen by means of the *polynomial division*: Let $f, g \in \mathbb{K}[X]\backslash\{0\}$ and

$$f = a_m X^m + \ldots + a_1 X + a_0, \quad g = b_n X^n + \ldots + b_1 X + b_0.$$

with $a_m, b_n \neq 0$, where we assume $m \geq n$ (so that $\deg(f) \geq \deg(g)$). Then set

$$q_0 = \frac{a_m}{b_n} X^{m-n}$$

and obtain (after multiplying and collecting terms)

$$f_1 = f - q_0 \cdot g = \underbrace{\left(a_m - \frac{a_m}{b_n} b_n\right)}_{=0} X^m + \left(a_{m-1} - \frac{a_m}{b_n} b_{n-1}\right) X^{m-1} + \ldots$$

If $f_1 = 0$, then $r = f_1$ and $q = q_0$ satisfy the condition (1.1). Otherwise $f_1 \neq 0$ and $\deg(f_1) \leq m - 1 < \deg(f)$. By induction on $m = \deg(f)$ we may assume, that there exists a decomposition $f_1 = q_1 \cdot g + r$ such that $\deg(r) < \deg(g)$ holds. Now

$$f = (q_1 + q_0) \cdot g + r$$

is the desired decomposition (1.1) for f with $\deg(r) < \deg(g)$ and $q = q_1 + q_0$. ♡

Example 1.28 Let $f = 2X^4 + X^2 - 3X + 2, g = -X^2 + X - 1 \in \mathbb{R}[X]$. Following Example 1.27 (b), we determine the elements $q, r \in \mathbb{R}[X]$ by means of polynomial division, such that $f = q \cdot g + r$ holds:

- Set $q_0 = -2X^2$. Then $f_1 = f - q_0 \cdot g = 2X^3 - X^2 - 3X + 2$.
- Set $q_1 = -2X$. Then $f_2 = f_1 - q_1 \cdot g = X^2 - 5X + 2$.
- Set $q_2 = -1$. Then $f_3 = f_2 - q_2 \cdot g = -4X + 1$. Now $\deg(f_3) < \deg(g)$ and for $q = q_0 + q_1 + q_2 = -2X^2 - 2X - 1$:

$$\begin{aligned} -4X + 1 = f_3 &= f_2 - q_2 \cdot g \\ &= (f_1 - q_1 \cdot g) - q_2 \cdot g = f_1 - (q_1 + q_2) \cdot g \\ &= (f - q_0 \cdot g) - (q_1 + q_2) \cdot g \\ &= f - (q_0 + q_1 + q_2) \cdot g \\ &= f - q \cdot g. \end{aligned}$$

The remainder of the division is therefore $r = f_3 = -4X + 1$. ♡

Algorithm 1.29 (Euclidean Algorithm) Let R be a Euclidean ring and $a_0, a_1 \in R$. Divide with remainder,

$$a_{i-1} = q_i \cdot a_i + a_{i+1} \qquad (\text{with } \delta(a_i) > \delta(a_{i+1})) \text{ for } i = 1, \ldots, n, \tag{1.2}$$

until the remainder $a_{n+1} = 0$ is obtained after finitely many steps. Then

$$a_n = \gcd(a_0, a_1).$$

PROOF: The sequence $\delta(a_i)$ is strictly decreasing and ≥ 0, so the algorithm terminates after a finite number of steps.

The loop invariant of the algorithm is $\gcd(a_{i-1}, a_i) = \gcd(a_i, a_{i+1})$ for $i = 1, \ldots, n$: If $g = \gcd(a_i, a_{i+1})$, then $d \mid g$ for every common divisor $d \in R$ of a_i and a_{i+1}. By definition of a_{i+1} in (1.2), d is a common divisor of a_i and a_{i+1} if and only if d is a common divisor of a_i and a_{i-1}. Hence $d \mid g$ for every common divisor d of a_i and a_{i-1}, that is, $g = \gcd(a_{i-1}, a_i)$.

In the last iteration of the algorithm, the condition

$$\gcd(a_0, a_1) = \gcd(a_1, a_2) = \ldots = \gcd(a_n, a_{n+1}) = \gcd(a_n, 0) = a_n$$

holds. ◇

Euclid's algorithm can be extended to give a constructive proof of Bézout's Lemma:

Corollary 1.30 (Bézout's Lemma) *Let R be a Euclidean ring and $a, b \in R$. There exist $s, t \in R$ such that*

$$\gcd(a, b) = sa + tb. \tag{1.3}$$

The proof is immediate from the extended version of Euclid's algorithm:

Algorithm 1.31 (Extended Euclidean Algorithm) Let R be a Euclidean ring and $a_0, a_1 \in R$. Divide with remainder,

$$a_{i-1} = q_i \cdot a_i + a_{i+1} \qquad (\text{with } \delta(a_i) > \delta(a_{i+1})) \text{ for } i = 1, \ldots, n, \tag{1.4}$$

set $A_0 = I_2$ and

$$Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}, \quad A_i = Q_i \cdot A_{i-1} \qquad \text{for } i = 1, \ldots, n, \tag{1.5}$$

until the remainder $a_{n+1} = 0$ is obtained after finitely many steps. Then

$$a_n = \gcd(a_0, a_1) = sa_0 + ta_1,$$

where $A_n = \left(\begin{smallmatrix} s & t \\ s' & t' \end{smallmatrix}\right)$.

PROOF: Algorithm 1.29 computes a sequence of remainders

$$a_{i+1} = a_{i-1} - q_i \cdot a_i, \qquad i = 1, \ldots, n$$

where $a_n = \gcd(a_0, a_1)$ and $a_{n+1} = 0$. We can express this by means of the matrices Q_i:

$$\begin{pmatrix} a_i \\ a_{i+1} \end{pmatrix} = Q_i \cdot \begin{pmatrix} a_{i-1} \\ a_i \end{pmatrix} \qquad \text{for } Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}.$$

In the extended version of Euclid's algorithm, in each step compute the matrix $A_i = Q_i \cdot A_{i-1}$, where $A_0 = I_2$. Once the algorithm terminates after n steps,

$$\begin{pmatrix} \gcd(a_0, a_1) \\ 0 \end{pmatrix} = \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix} = Q_n \cdots Q_1 \cdot \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = A_n \cdot \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

holds. So the elements s, t are now the entries in the first row of $A_n = \left(\begin{smallmatrix} s & t \\ s' & t' \end{smallmatrix}\right)$. $\diamond$

Remark 1.32 Even though the Euclidean Algorithm for $R = \mathbb{Z}$ is one of the oldest and simplest algorithm of all, its analysis is by no means easy. The complexity of this algorithm is determined by how often the division with remainder (1.2) is performed. Assume $0 \leq a_1 \leq a_0$. For the sequence of remainders in (1.2) it holds that

$$a_1 > a_2 > \ldots > a_n > 0.$$

The quotients $q_i = a_{i-1} \div a_i$ of the division with remainder thus satisfy

$$q_i \geq 1 \text{ for } 1 \leq i \leq n-1, \quad q_n \geq 2. \qquad (*)$$

For $1 \leq i \leq n-1$ this yields

$$\begin{aligned} a_{i-1} &= a_i q_i + a_{i+1} \\ &> a_{i+1} q_i + a_{i+1} \\ &= a_{i+1}(q_i + 1) \end{aligned}$$

and therefore

$$\prod_{i=1}^{n-1} a_{i-1} > \prod_{i=1}^{n-1} a_{i+1}(q_i + 1).$$

The factors $a_2, a_3, \ldots, a_{n-2}$ appear on both sides and can be cancelled:

$$\begin{aligned} a_0 a_1 &> a_{n-1} a_n \prod_{i=1}^{n-1} (q_i + 1) \\ &= a_n^2 q_n \prod_{i=1}^{n-1} (q_i + 1). \end{aligned}$$

By $(*)$ and $a_0 \geq a_1$ we can further estimate this as

$$\begin{aligned} a_0^2 &\geq a_0 a_1 \\ &> a_n^2 \cdot 2 \cdot 2^{n-1} \\ &= 2^n \gcd(a_0, a_1)^2 \\ &\geq 2^n. \end{aligned}$$

It follows that

$$2 \log(a_0) > n.$$

Hence the number of loop iterations is in $\mathsf{O}(\log(m))$ for $m = \max\{|a_0|, |a_1|\}$. The worst case occurs for $\gcd(f_{n+1}, f_n)$, where f_n is the nth *Fibonacci number* (defined by $f_{n+1} = f_n + f_{n-1}$ with $f_1 = 1$, $f_0 = 0$). In this case, the algorithm performs precisely $n - 1$ loop iterations for $n > 1$. For an in-depth analysis see Knuth [8], Section 4.5.3. For a polynomial ring, the complexity of the Euclidean algorithm is in $\mathsf{O}(m^2)$, where $m = \max\{\deg(a_0), \deg(a_1)\}$, see Lipson [10], Section VII.2.2.

Remark 1.33 By Remark 1.11, the (Extended) Euclidean Algorithm can be used to compute the gcd of any number of elements $a_1, \ldots, a_k \in R$ and find elements $s_1, \ldots, s_k \in R$ satisfying

$$\gcd(a_1, \ldots, a_k) = s_1 a_1 + \ldots + s_k a_k. \tag{1.6}$$

Example 1.34 We demonstrate the Extended Euclidean Algorithm 1.31 by two examples:

(a) Let $a = 21, b = 8 \in \mathbb{Z}$.

- $a_0 = 21, a_1 = 8$ gives $q_1 = 2, a_2 = 5$ and the matrix $Q_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -2 \end{smallmatrix}\right)$.
- $a_1 = 8, a_2 = 5$ gives $q_2 = 1, a_3 = 3$ and the matrix $Q_2 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right)$.
- $a_2 = 5, a_3 = 3$ gives $q_3 = 1, a_4 = 2$ and the matrix $Q_3 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right)$.
- $a_3 = 3, a_4 = 2$ gives $q_4 = 1, a_5 = 1$ and the matrix $Q_4 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right)$.
- $a_4 = 2, a_5 = 1$ gives $q_5 = 2, a_6 = 0$ and the matrix $Q_5 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -2 \end{smallmatrix}\right)$. The algorithm terminates in this step, as $a_6 = 0$.

Hence

$$\gcd(21, 8) = a_5 = 1$$

and

$$A_5 = Q_5 Q_4 Q_3 Q_2 Q_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -2 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & -2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -3 & 8 \\ 8 & -21 \end{smallmatrix}\right).$$

The entries in the first row of A_5 satisfy

$$1 = (-3) \cdot 21 + 8 \cdot 8.$$

(b) In $\mathbb{R}[X]$, let

$$a = X^{13} + X^{12} - 2X^9, b = -X^6 - X^5 + X^4 + X^3 + 2X^2 - 2$$

(the polynomial divisons performed in each of the following steps are not written out explicitely):

- $a_0 = X^{13} + X^{12} - 2X^9, a_1 = -X^6 - X^5 + X^4 + X^3 + 2X^2 - 2$ gives $q_1 = -X^7 - X^5 - X^3 - X, a_2 = X^5 + X^4 - 2X$ and the matrix $Q_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & X^7+X^5+X^3+X \end{smallmatrix}\right)$.
- $a_1 = -X^6 - X^5 + X^4 + X^3 + 2X^2 - 2, a_2 = X^5 + X^4 - 2X$ gives $q_2 = -X, a_3 = X^4 + X^3 - 2$ and the matrix $Q_2 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & X \end{smallmatrix}\right)$.
- $a_2 = X^5 + X^4 - 2X, a_3 = X^4 + X^3 - 2$ gives $q_3 = X$, $a_4 = 0$ and the matrix $Q_3 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -X \end{smallmatrix}\right)$. The algorithm terminates in this step, as $a_4 = 0$.

Hence

$$\begin{aligned} &\gcd(X^{13} + X^{12} - 2X^9,\ -X^6 - X^5 + X^4 + X^3 + 2X^2 - 2) \\ &= a_3 = X^4 + X^3 - 2 \end{aligned}$$

and

$$A_3 = Q_3 Q_2 Q_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -X \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 1 \\ 1 & X \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 1 \\ 1 & X^7+X^5+X^3+X \end{smallmatrix}\right) = \left(\begin{smallmatrix} X & X^8+X^6+X^4+X^2+1 \\ 1-X^2 & -X^9 \end{smallmatrix}\right).$$

The elements in the first row of A_3 satisfy

$$\begin{aligned} &X^4 + X^3 - 2 \\ &= X \cdot (X^{13} + X^{12} - 2X^9) \\ &\quad + (X^8 + X^6 + X^4 + X^2 + 1) \cdot (-X^6 - X^5 + X^4 + X^3 + 2X^2 - 2). \heartsuit \end{aligned}$$

Theorem 1.35 *Let R be a Euclidean ring.*

(a) *Every ideal $\mathfrak{I}$ in R is a principle ideal (that is, there exists $x \in R$ such that $\mathfrak{I} = \langle x \rangle$).*

(b) *An element $p \in R$ is irreducible if and only if p is prime.*

PROOF:

(a) Choose $x \in \mathfrak{I}$, $x \neq 0$, so that $\delta(x)$ is minimal among all elements in $\mathfrak{I}$ (this is possible, as δ only assumes values in $\mathbb{N}_0$). As R is Euclidean, for every $y \in \mathfrak{I}$ there exist elements $q, r \in R$ such that $y = qx + r$, where $\delta(r) < \delta(x)$ or $r = 0$. But now $r = y - qx \in \mathfrak{I}$, so that $r = 0$ by the minimality of x. Hence $y \in \langle x \rangle$, and as y is arbitrary, $\mathfrak{I} = \langle x \rangle$ follows.

(b) A prime element is irreducible by Lemma 1.22.

Now let p be irreducible and let $p \mid xy$ for certain $x, y \in R$. Assume $p \nmid y$. We need to show $p \mid x$. Let $g = \gcd(p, y)$. As p is irreducible and $g \mid p$, we have $p = hg$ with $g \in R^\times$ or $h \in R^\times$. If $h \in R^\times$, then $h^{-1}p$ would be a divisor of y and thus p a divisor of y, contradicting the assumption. So $g \in R^\times$. By means of the Extended Euclidean Algorithm we can determine elements $s, t \in R$ satisfying

$$g = sp + ty.$$

As g is a unit, we can multiply this expression by xg^{-1} and obtain

$$x = xg^{-1}sp + xg^{-1}ty = xg^{-1}sp + g^{-1}txy.$$

By assumption, p divides both summands on the right-hand side, and hence $p \mid x$. So we have shown that $p \mid xy$ implies that p divides at least one of the elements x or y. Therefore, p is prime. ◇

Theorem 1.36 (Unique Prime Factorisation) *Let R be a Euclidean ring. Every element $x \in R \backslash R^\times$, $x \neq 0$, has a factorisation*

$$x = p_1 \cdots p_k, \tag{1.7}$$

where the $p_1, \ldots, p_k$ are prime in R. This factorisation is unique up to the order and multiplication of the p_i by units in $R^\times$.

PROOF: First, we prove the *existence*:

Let $x \in R \backslash R^\times$, $x \neq 0$. By Theorem 1.35, the prime elements in R coincide with the irreducible elements. If x is irreducible itself, then $x = p_1$. Otherwise, x is a product $x = x_1 y_1$ with $x_1, y_1 \notin R^\times$. If x_1, y_1 are not both irreducible, then factorise them further until all factors are irreducible and obtain the prime factorisation in this way. This procedure terminates after a finite number of steps: For a sequence of elements $x_i \in R \backslash R^\times$ with the property $x_i \mid x_{i-1}$ for $i = 1 \ldots, n$ and $x_0 = x$, it holds by Theorem 1.20 that

$$\langle x_0 \rangle \subset \langle x_1 \rangle \subset \langle x_2 \rangle \subset \ldots$$

Then $\mathfrak{I} = \bigcup_{i=0}^{\infty} \langle x_i \rangle$ is an ideal in R and by Theorem 1.35 it is even a principle ideal. So there exists $z \in R$ with

$$\langle z \rangle = \mathfrak{I} = \bigcup_{i=0}^{\infty} \langle x_i \rangle.$$

But then $z \in \langle x_m \rangle$ holds for some $m \geq 0$, and this means $\langle z \rangle = \langle x_i \rangle$ for all $i \geq m$. So by Theorem 1.20 (b) the x_i (for $i \geq m$) differ from x_m only by a factor in $R^\times$. This leads to a contradiction if we assume the above procedure can be repeated indefinitely.

Next, we show the *uniqueness*:

Let $x = q_1 \cdots q_j$ be another prime factorisation of the form (1.7), where we assume $k \geq j$ without loss of generality. We prove the assertion by induction over k: If $k = 1$, then x itself is prime, so $j = 1$ and $p_1 = q_1 = x$. If $k > 1$, the prime factor p_k divides one of the q_i; say q_j. As q_j is prime itself (hence irreducible), q_j and p_k differ only by a factor $u \in R^\times$. By the cancellation rule (Lemma 1.12),

$$p_1 \cdots (u^{-1} p_{k-1}) = q_1 \cdots q_{j-1}.$$

Now the left-hand side consists of $k-1$ prime factors, so that the induction hypothesis applies to it. Then $k - 1 = j - 1$ and $p_i = u_i q_{\sigma(i)}$ for $u_i \in R^\times$ and a suitable permutation $\sigma \in \mathrm{S}_{k-1}$. Together with $p_k = u q_k$, the uniqueness of the factorisation follows. ◇

As an application of the Unique Factorisation Theorem we prove one of the oldest and most famous theorems in mathematics:

Theorem 1.37 (Euclid) *There exist infinitely many prime numbers in* $\mathbb{N}$ *(in* $\mathbb{Z}$*).*

EUCLID'S PROOF: Assume there are only finitely many prime numbers $p_1, \ldots, p_n$ in $\mathbb{N}$. Set

$$k = 1 + p_1 \cdots p_n.$$

For $i = 1, \ldots, n$ it holds that $k \equiv 1 \bmod p_i$, so k is not divisble by any of the p_i. But k also is not one of the units ± 1 in $\mathbb{Z}$. Therefore, the prime factorisation of k must contain additional prime numbers other than the $p_1, \ldots, p_n$, which contradicts our assumption. ◇

Exercise 1.38 In a similar manner one can prove that the polynomial ring $\mathbb{K}[X]$ contains infinitely many irreducible polynomials (this is obvious if $\mathbb{K}$ is not a finite field, as all polynomials $X + a$ with $a \in \mathbb{K}$ are irreducible).

We give a different proof of Theorem 1.37 due to Euler which uses ideas from analysis.

EULER'S PROOF: Assume there exist only finitely many prime numbers $p_1 < p_2 < \ldots < p_n$. By the formula for the geometric series,

$$\frac{1}{1-p_i^{-1}} = \sum_{k=0}^{\infty} p_i^{-k} \in \mathbb{R},$$

holds for $1 \leq i \leq n$, and the series converges because $0 < |p_i^{-1}| < 1$. As a consequence, the following expression is a well-defined product of real numbers:

$$\begin{aligned}\frac{1}{1-p_1^{-1}} \cdots \frac{1}{1-p_n^{-1}} &= \Big(\sum_{k_1=0}^{\infty} p_1^{-k}\Big) \cdots \Big(\sum_{k_n=0}^{\infty} p_n^{-k}\Big) \\ &= \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} (p_1^{-k_1} \cdots p_n^{-k_n}) = \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \frac{1}{p_1^{k_1} \cdots p_n^{k_n}} \\ &= \sum_{m=1}^{\infty} \frac{1}{m}.\end{aligned}$$

The last equality holds because by Theorem 1.36 the expressions $p_1^{k_1} \cdots p_n^{k_n}$ run through all natural Zahlen $m \in \mathbb{N}$. But the series $\sum_{m=1}^{\infty} \frac{1}{m}$ diverges, so it does not represent a real number. This contradiction implies the existence of infinitely many prime numbers. ◇

1.3 Zeros of Polynomials

In the Euclidean ring $R = \mathbb{K}[X]$ we find some important relations between divisibility properties and zeros of polynomials.

Theorem 1.39 *Let $f \in \mathbb{K}[X]$ and $\alpha, \beta \in \mathbb{K}$. Then the following holds:*

(a) *Let $g \in \mathbb{K}[X]$, $g \neq 0$, such that $g(\alpha) = 0$. If $r = f - qg$ is the remainder after polynomial division, then*

$$r(\alpha) = f(\alpha).$$

(b) *$X - \alpha$ divides f if and only if $f(\alpha) = 0$.*

(c) *$X - \alpha, X - \beta$ are coprime if and only if $\alpha \neq \beta$.*

(d) *If* $n = \deg(f)$, *then* f *has at most* n *zeros in* $\mathbb{K}$.

PROOF:

(a) $f(\alpha) = f(\alpha) - 0 = f(\alpha) - q(\alpha)g(\alpha) = r(\alpha)$.

(b) For $g = X - \alpha$ in part (a), the remainder r is the constant $r = f(\alpha)$. Moreover, $X - \alpha$ divides f if and only if the remainder is $r = 0$.

(c) The remainder after polynomial division of $X - \alpha$ by $X - \beta$ is $\beta - \alpha$.

(d) According to part (b), every zero λ of f gives rise to an irreducible divisor $X - \lambda$ of f. The zeros are uniquely determined because the prime factorisation is unique. If f had $m > n$ zeros, then the product of m linear factors would be of degree $m > \deg(f)$, a contradiction. ◇

Recall the Fundamental Theorem of Algebra, whose proof is beyond the scope of linear algebra. It can be found in Bosch [1], Section 6.3.

Theorem 1.40 (Fundamental Theorem of Algebra) *Every polynomial in* $\mathbb{C}[X]$ *of degree* ≥ 1 *has a zero in* $\mathbb{C}$.

Corollary 1.41 *Every polynomial* $f \in \mathbb{C}[X]$ *of degree* $n \geq 1$ *factors into* n *linear factors,*

$$f = \alpha \cdot (X - \lambda_1) \cdots (X - \lambda_n),$$

with $\alpha \in \mathbb{C}^\times$, *where* $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ *are not necessarily distinct.*

PROOF: According to the Fundamental Theorem of Algebra, f has a zero λ_1 and hence by Theorem 1.39 (b) a divisor $X - \lambda_1$. So there exists a polynomial h of degree $n - 1$ with $f = (X - \lambda_1) \cdot h$. Now one concludes by induction on n that h decomposes into $n - 1$ linear factors, which proves the claim. ◇

1.4 Quotient Rings

One can think of $\mathbb{Z}/n\mathbb{Z}$ arising from $\mathbb{Z}$ by introducing the new arithmetic law "$n = 0$" in $\mathbb{Z}$. Surely, with this new law, all multiples kn are identical to 0, and elements $a, b \in \mathbb{Z}$ which only differ by a multiple of n (that is, $a = b + kn$ for a suitable k), are no longer distinguishable with the new law. We express this by the notation

$$a \equiv b \bmod n.$$

Such elements are collected in the residue class $\overline{a} = a + n\mathbb{Z}$. Then $\mathbb{Z}/n\mathbb{Z}$ is the set of all these residue classes, and $\mathbb{Z}/n\mathbb{Z}$ is a ring with the operations $+$ and $\cdot$ induced by $\mathbb{Z}$.

We want to extend this notion of "introducing new arithmetic laws" to arbitrary rings. To this end, we reflect how the above example of $\mathbb{Z}/n\mathbb{Z}$ can be expressed by the concepts introduced in the previous sections: We observe that $n\mathbb{Z} = \langle n \rangle$ is the ideal generated by n, and the canonical projection $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto \overline{a}$ is a homomorphism of rings with $\ker \pi = n\mathbb{Z}$. The condition $a \equiv b \bmod n$ is equivalent to $a - b \in n\mathbb{Z}$.

This can be generalised to an arbitrary ring R, by choosing an ideal $\mathfrak{I} \subset R$ and consider those elements $a, b \in R$ as equivalent, which statisfy $a - b \in \mathfrak{I}$. Here, the idea is that $\mathfrak{I}$ contains precisely those elements which are set to 0 when introducing new arithmetic laws. Therefore, the generators of $\mathfrak{I}$ are often called *relations* and $\mathfrak{I}$ the *ideal of relations*.

Theorem 1.42 *Let R be a commutative ring and $\mathfrak{I}$ an ideal in R. Then the set*

$$R/\mathfrak{I} = \{\overline{x} = x + \mathfrak{I} \mid x \in R\} \tag{1.8}$$

is also a commutative ring, if $+$ and $\cdot$ are defined via representatives $x, y \in R$:

$$\begin{aligned} \overline{x} + \overline{y} &= \overline{x + y}, \\ \overline{x} \cdot \overline{y} &= \overline{x \cdot y}. \end{aligned}$$

The canonical projection $\pi : R \to R/\mathfrak{I}$, $x \mapsto \overline{x}$ is a surjective homomorphism of rings with kernel $\ker \pi = \mathfrak{I}$.

PROOF: The ring properties of $R/\mathfrak{I}$ are readily inherited from R. What remains to prove is that the definitions of $+$ and $\cdot$ are independent of the choice of representatives x, y ("well-defined"): Let $x - x', y - y' \in \mathfrak{I}$. Then

$$\overline{x}+\overline{y} = \overline{x + y} = \overline{(x - x') + (y - y') + x' + y'} = \underbrace{\overline{x - x'} + \overline{y - y'}}_{\in \mathfrak{I}} + \overline{x'} + \overline{y'} = \overline{x'} + \overline{y'}.$$

So the addition is well-defined. To show that the multiplication is well-defined, the fact $\mathfrak{I}$ is an ideal is crucial:

$$\begin{aligned} \overline{x} \cdot \overline{y} &= \overline{x \cdot y} = \overline{((x - x') + x') \cdot ((y - y') + y')} \\ &= \overline{\underbrace{(x - x') \cdot (y - y')}_{\in \mathfrak{I}} + \underbrace{(x - x') \cdot y'}_{\in \mathfrak{I}} + \underbrace{x' \cdot (y - y')}_{\in \mathfrak{I}} + x' \cdot y'} \\ &= \underbrace{\overline{(x - x') \cdot (y - y') + (x - x') \cdot y' + x' \cdot (y - y')}}_{\in \mathfrak{I}} + \overline{x' \cdot y'} \\ &= \overline{x' \cdot y'} = \overline{x'} \cdot \overline{y'}. \end{aligned}$$

The map π is a surjective homomorphism by construction and it kernel is $\ker \pi = \{x \in R \mid \pi(x) = \overline{0}\} = \{x \in R \mid x + \mathfrak{F} = \mathfrak{F}\} = \mathfrak{F}$. $\diamond$

Definition 1.43 The ring $R/\mathfrak{F}$ is called the **quotient ring** of R over $\mathfrak{F}$.

We also call this ring "R modulo $\mathfrak{F}$" and write

$$x \equiv y \bmod \mathfrak{F}$$

for equivalent $x, y \in R$. If $\mathfrak{F}$ is a principle ideal with generator f, then we write (in analogy to $\mathbb{Z}/n\mathbb{Z}$)

$$x \equiv y \bmod f$$

or even shorter

$$x \equiv_f y.$$

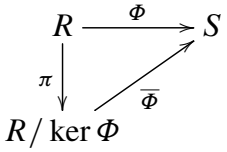
Exercise 1.44 If $\mathfrak{P}$ is a prime ideal in R, then $R/\mathfrak{P}$ contains no zero divisors.

Exercise 1.45 If R is a Euclidean ring and $\mathfrak{P}$ is a prime ideal, then $R/\mathfrak{P}$ is a field.

Theorem 1.46 (Homomorphism Theorem for Rings) *Let R, S be commutative rings and $\Phi : R \to S$ a homomorphism of rings. Then there exists a unique homomorphism of rings $\overline{\Phi} : R/\ker\Phi \to S$ such that $\overline{\Phi}$ is injective and*

$$\overline{\Phi} \circ \pi = \Phi, \tag{1.9}$$

that is, the following diagram commutes:



PROOF: Define $\overline{\Phi}$ by

$$\overline{\Phi}(\overline{x}) = \Phi(x)$$

for $x \in R$. This is equation (1.9).

- $\overline{\Phi}$ is well-defined, for if $x - x' \in \ker\Phi$, then

$$\overline{\Phi}(\overline{x}) = \Phi(x) = \Phi(x - x' + x') = \underbrace{\Phi(x - x')}_{=0} + \Phi(x') = \Phi(x') = \overline{\Phi}(\overline{x'}).$$

- $\overline{\Phi}$ is a homomorphism of rings: For $x, y \in R$,

  $$\overline{\Phi}(\overline{x} + \overline{y}) = \overline{\Phi}(\overline{x + y}) = \Phi(x + y) = \Phi(x) + \Phi(y) = \overline{\Phi}(\overline{x}) + \overline{\Phi}(\overline{y})$$

  and similarly

  $$\overline{\Phi}(\overline{x} \cdot \overline{y}) = \overline{\Phi}(\overline{x}) \cdot \overline{\Phi}(\overline{y}).$$

- $\overline{\Phi}$ is injective: Let $\overline{x} \in \ker \overline{\Phi}$, that is,

  $$0 = \overline{\Phi}(\overline{x}) = \Phi(x).$$

  Then $x \in \ker \Phi$, so $\overline{x} = \ker \Phi = \overline{0}$. Hence $\ker \overline{\Phi} = \{\overline{0}\}$. ◇

Corollary 1.47 (Isomorphism Theorem for Rings) *If Φ in Theorem 1.46 is surjective, then $\overline{\Phi}$ is an isomorphism. In particular,*

$$R/\ker \Phi \cong S. \tag{1.10}$$

PROOF: $\overline{\Phi}$ is injective, and as $\operatorname{im} \overline{\Phi} = \operatorname{im} \Phi = S$ holds, $\overline{\Phi}$ is bijective. ◇

The Euclidean Algorithm provides us with the means to test for invertibility of elements in quotient rings.

Lemma 1.48 *Let R be a Euclidean ring and $a, x \in R$. The element $\overline{x} \in R/\langle a \rangle$ is invertible if and only if* $\gcd(a, x) = 1$.

PROOF: If $\gcd(a, x) = 1$, then by means of the Extended Euclidean Algorithm we can determine elements $s, t \in R$ satisfying

$$1 = sx + ta.$$

In other words,

$$s \cdot x \equiv 1 \bmod a, \tag{$*$}$$

that is, $\overline{s} = \overline{x}^{-1}$ in $R/\langle a \rangle$.

Conversely, if $\overline{x}$ is invertible in $R/\langle a \rangle$ with inverse $\overline{s}$, it follows from $(*)$ that every gcd of a and x is a divisor of 1, meaning it is an element of $R^\times$. In particular, 1 is then a gcd of a and x. ◇

The quotient map allows us to do some interesting constructions, as the following examples demonstrate.

Example 1.49 (Evaluation map) Let $R = \mathbb{R}[X]$ and $\mathfrak{I} = \langle X - \lambda \rangle$. To determine the image of $f = a_n X^n + \ldots + a_1 X + a_0$ under the canonical projection, we divide with remainder,

$$f = (X - \lambda) \cdot h + r,$$

where $\deg(r) < \deg(X - \lambda) = 1$, so that $r \in \mathbb{R}$. It holds that

$$f(\lambda) = (\lambda - \lambda) \cdot h + r = r.$$

As $(X - \lambda) \cdot h \in \mathfrak{I}$,

$$\overline{f} = \overline{r} = \overline{f(\lambda)}.$$

The image of π consists precisely of the residue classes of the constant polynomials. If we identify each $\overline{f}$ with the constant representative $f(\lambda)$, then we can identify the canonical projection with the evaluation map $f \mapsto f(\lambda)$. The Isomorphism Theorem then gives us

$$\mathbb{R}[X]/\mathfrak{I} \cong \mathbb{R}. \quad \heartsuit$$

Example 1.50 (Complex Numbers) Let $R = \mathbb{R}[X]$ and $\mathfrak{I} = \langle X^2 + 1 \rangle$. Every polynomial $f \in \mathbb{R}[X]$ is of the form

$$f = (X^2 + 1) \cdot h + (a_1 X + a_0),$$

so that

$$f \equiv a_1 X + a_0 \bmod X^2 + 1.$$

In particular, it holds for the polynomial X that

$$\overline{X} \cdot \overline{X} = \overline{X^2} = \overline{X^2} - (\overline{X^2 + 1}) = \overline{X^2 - X^2 - 1} = -\overline{1},$$

that is, $\overline{X} = \sqrt{-1}$ in $\mathbb{R}[X]/\mathfrak{I}$. This motivates defining the map

$$\mathbb{R}[X] \to \mathbb{C}, \quad f \mapsto a_0 + \mathrm{i}a_1.$$

It is a surjective homomorphism of rings, and according to the Isomorphism Theorem,

$$\mathbb{R}[X]/\langle X^2 + 1 \rangle \cong \mathbb{C}. \quad \heartsuit$$

At the end of this section we want to study a construction for finite fields. A finite field $\mathbb{F}$ is necessarily of characteristic p (prime). We already know the finite fields $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Lemma 1.51 *If $\mathbb{F}$ is any finite field of characteristic p, then the field $\mathbb{F}_p$ is a subfield of $\mathbb{F}$.*

PROOF: The map $\Phi : \mathbb{Z} \to \mathbb{F}$, $n \mapsto \operatorname{sgn}(n) \cdot \sum_{i=1}^{|n|} 1$ is a homomorphism of rings with $\ker \Phi = p\mathbb{Z}$. By the Homomorphism Theorem there exists an injective homomorphism of fields $\overline{\Phi} : \mathbb{Z}/p\mathbb{Z} \to \mathbb{F}$, that is, $\mathbb{F}_p \cong \operatorname{im} \overline{\Phi} \subset \mathbb{F}$. $\diamond$

Corollary 1.52 *If $\mathbb{F}$ is a finite field of characteristic p, then $\mathbb{F}$ is a vector space over the field $\mathbb{F}_p$. In particular, $|\mathbb{F}| = p^k$, where $k = \dim_{\mathbb{F}_p} \mathbb{F}$.*

PROOF: By Lemma 1.51, $\mathbb{F}_p$ is a subfield of $\mathbb{F}$. So the elements of $\mathbb{F}$ can be multiplied by scalars from $\mathbb{F}_p$, making $\mathbb{F}$ into a $\mathbb{F}_p$-vector space. As $\mathbb{F}$ is finite, $\mathbb{F}$ must be of some finite dimension k over $\mathbb{F}_p$. Then there are p^k possibilities to form linear combinations out of any given basis of $\mathbb{F}$, which means that $\mathbb{F}$ has precisely p^k elements. ◇

Aus Aufgabe 1.38 folgt, dass es in $\mathbb{F}_p[X]$ irreduzible Polynome vom Grad $k > n$ für alle $n \in \mathbb{N}$ geben muss. Das ermöglicht uns die folgende Konstruktion:

Example 1.53 (Finite fields) Let $R = \mathbb{F}_p[X]$ and $f \in \mathbb{F}_p[X]$ be an irreducible polynomial of degree k. Write

$$\mathbb{F}_{p^k} = \mathbb{F}_p[X]/\langle f \rangle.$$

As f is irreducible, every element in $\mathbb{F}_{p^k}$ has an inverse (Lemma 1.48), so that $\mathbb{F}_{p^k}$ is indeed a field. Write $x = \overline{X}$. The elements $1, x, x^2, \ldots, x^{k-1}$ generate $\mathbb{F}_{p^k}$. They are linearly independent, for if

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} = 0$$

for $a_0, \ldots, a_{k-1} \in \mathbb{F}_p$, this implies that the polynomial $h = a_0 + a_1 X + \ldots + a_{k-1} X^{k-1}$ is an element of the ideal $\langle f \rangle$ and as such a multiple of f. As $\deg(f) = k > k - 1$, it follows that h must be the zero polynomial. So the set $\{1, x, x^2, \ldots, x^{k-1}\}$ is a basis of $\mathbb{F}_{p^k}$ as an $\mathbb{F}_p$-vector space.

Remark 1.54 One can show that *every* field with p^k elements is isomorphic to one of the $\mathbb{F}_{p^k}$ constructed in Example 1.53. This is the *Fundamental Theorem of Galois Theory for finite fields*, see Bosch [1], Section 3.8, Theorem 2.

1.5 The Chinese Remainder Theorem

The process of solving a complicated problem can be simplified if the problem can be *parallelised*. This means that the problem can be divided into several partial problems which are easier to solve, and a solution of the original problem can be constructed out of the solution of the partial problems.

The following example serves to illustrate this idea:

Example 1.55 (Integer determinants) We want to compute the determinant of a matrix $A \in \mathbb{Z}^{d \times d}$. We assume that the absolute value of the coefficients of A is

known to be bounded by a constant c. The Leibniz formula for determinants then provides us with the following estimate[4)]

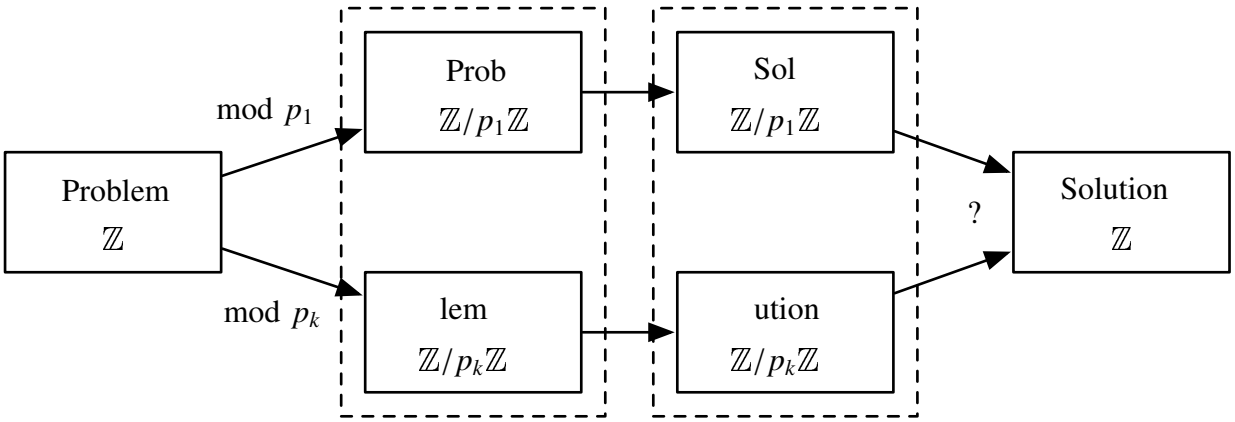
$$|\det(A)| \leq d!c^d.$$

By virtue of this upper bound we may assume that our computations take place not in $\mathbb{Z}$ but in the ring $\mathbb{Z}/m\mathbb{Z}$ for some odd integer $m \geq 2d!c^d$. Here, the factor 2 is necessary because the numbers $\overline{\frac{m-1}{2}+1}, \ldots, \overline{m-1}$ in $\mathbb{Z}/m\mathbb{Z}$ are meant to represent the numbers $-\frac{m-1}{2}, \ldots, -1$ in $\mathbb{Z}$. For large m, the computation of the determinant on a computer is extremely time- and memory-intensive. However, if one could instead project the problem to $\mathbb{Z}/p\mathbb{Z}$ for small p, the computations are sped up significantly. For this idea to work, two things have to be taken into consideration:

(i) The projection $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ must map the computations in $\mathbb{Z}/m\mathbb{Z}$ to computations in $\mathbb{Z}/p\mathbb{Z}$, that is, it has to be a homomorphism of rings. Therefore, p must be a divisor of m.

(ii) In order to prevent a loss of information, one has to compute in several $\mathbb{Z}/p_1\mathbb{Z}, \ldots, \mathbb{Z}/p_k\mathbb{Z}$, such that in total one can encode m numbers (the elements of $\mathbb{Z}/m\mathbb{Z}$). Together with (i) this means $p_1 \cdots p_k = m$ must hold.

The problem is thus translated from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k\mathbb{Z}$, where it is solved "componentwise".



The computation of the determinants via the $\mathbb{Z}/p_i\mathbb{Z}$ can be executed in parallel. The question is, if and how these partial solutions can be used to reconstruct the original determinant $\det(A)$ in $\mathbb{Z}/m\mathbb{Z}$. We will see that this is the case if

[4)] Better estimates are known.

$p_1, \ldots, p_k$ are chosen to be mutually coprime (for example, a prime factorisation of m). ♡

Before we prove this general results, we want to understand the reconstruction of an element in $\mathbb{Z}/m\mathbb{Z}$ from elements in $\mathbb{Z}/p_i\mathbb{Z}$ by means of a simple numerical example.

Example 1.56 (Simultaneous congruences) Given the elements $3 \bmod 8 \in \mathbb{Z}/8\mathbb{Z}$ and $7 \bmod 21 \in \mathbb{Z}/21\mathbb{Z}$, find $x \in \mathbb{Z}$ satisfying

$$\begin{aligned} x &\equiv 3 \bmod 8, \\ x &\equiv 7 \bmod 21. \end{aligned}$$

So this problem is about solving a system of *simultaneous congruences*. We make the following ansatz for x:

$$x = 3 + b \cdot 8.$$

Then the first congruence is satisfied in any case. Now it remains to determine b such that the second congruence is satisfied as well:

$$\begin{aligned} & 3 + b \cdot 8 \equiv 7 \bmod 21 \\ \Leftrightarrow\ & b \cdot 8 \equiv 4 \bmod 21. \end{aligned}$$

As 8 and 21 are coprime, we can compute the inverse of 8 modulo 21 by means of the Extended Euclidean Algorithm, as was already done in Example 1.34 (a): $1 = (-3) \cdot 21 + 8 \cdot 8$, so 8 itself is the inverse of 8 modulo 21. Multiplying both sides of the above congruence by 8, we obtain

$$b \equiv 4 \cdot 8 \equiv 11 \bmod 21.$$

Hence

$$x = 3 + 11 \cdot 8 = 91$$

satisfies both congruences. The set of all possible solutions is

$$x + (8 \cdot 21)\mathbb{Z} = 91 + 168\mathbb{Z}.$$

In the situation of Example 1.55, we are interested in the smallest solution between 0 and 168, which is meant to represent an element in $\mathbb{Z}/168\mathbb{Z}$. This smallest solution is already $x = 91$. ♡

We now consider this situation for arbitrary Euclidean rings. Firstly, note that for rings $R_1, \ldots, R_k$ the product $R_1 \times \cdots \times R_k$ is again a ring, if we define the ring operations componentwise:

$$\begin{aligned} (x_1, \ldots, x_k) + (y_1, \ldots, y_k) &= (x_1 + y_1, \ldots, x_k + y_k), \\ (x_1, \ldots, x_k) \cdot (y_1, \ldots, y_k) &= (x_1 \cdot y_1, \ldots, x_k \cdot y_k). \end{aligned}$$

Theorem 1.57 (Chinese Remainder Theorem) *Let R be a Euclidean ring and $p_1, \ldots, p_k \in R$ mutually coprime. For $q = p_1 \cdots p_k$, the map*

$$\Psi : R/\langle q\rangle \to R/\langle p_1\rangle \times \cdots \times R/\langle p_k\rangle, \quad a \bmod q \mapsto (a \bmod p_1, \ldots, a \bmod p_k) \tag{1.11}$$

is then an isomorphism of rings.

PROOF: The map is well-defined in every component: For $a \equiv a' \bmod q$ there exists $h \in R$, such that

$$a - a' = hq = h(p_1 \cdots p_k) = (hp_2 \cdots p_k)p_1,$$

so $a \equiv a' \bmod p_1$ and similarly for $p_2, \ldots, p_k$. Clearly, Ψ is then a homomorphism of rings.

Ψ is injective: If $a \bmod q \in \ker \Psi$, then $a \equiv 0 \bmod p_i$ for $i = 1, \ldots, k$. So a is a multiple of each p_i. As the p_i are coprime by assumption, a is also a multiple of their product $p_1 \cdots p_k = q$. Hence $\ker \Psi = \{0 \bmod q\}$ is trivial and Ψ injective.

The surjectivity of Ψ follows if we can compute a preimage in $R/\langle q\rangle$ for every element $(a_1 \bmod p_1, \ldots, a_k \bmod p_k)$ of $R/\langle p_1\rangle \times \cdots \times R/\langle p_k\rangle$. This is equivalent to solving the following system of simultaneous congruences:

$$\begin{aligned} x &\equiv a_1 \bmod p_1, \\ &\vdots \\ x &\equiv a_k \bmod p_k. \end{aligned}$$

Then $x \bmod q$ is the preimage we are looking for. Given the assumptions of the theorem, this system of congruences can be solved explicitely via Algorithm 1.58 (or Algorithm 1.59) below. ◇

Algorithm 1.58 (Newton Interpolation) Let R be a Euclidean ring, and let the following system of congruences to be solved for $x \in R$ be given:

$$\begin{aligned} x &\equiv a_1 \bmod p_1, \\ &\vdots \\ x &\equiv a_k \bmod p_k, \end{aligned}$$

where the $p_1, \ldots, p_k$ are mutually coprime. Make the ansatz

$$x = x_1 + x_2 p_1 + x_3 p_1 p_2 + \ldots + x_k p_1 \cdots p_{k-1} \tag{1.12}$$

and determine the unknown x_i iteratively:

- In the first step,
$$x \equiv x_1 \stackrel{!}{\equiv} a_1 \bmod p_1$$
holds, and we may choose $x_1 = a_1$.

- Assume, $x_1, \ldots, x_{i-1}$ have already been determined. Then
$$x \equiv x_1 + x_2 p_1 + x_3 p_1 p_2 + \ldots + x_i p_1 \cdots p_{i-1} \stackrel{!}{\equiv} a_i \bmod p_i$$
holds. So
$$x_i p_1 \cdots p_{i-1} \equiv a_i - x_1 - x_2 p_1 - x_3 p_1 p_2 - \ldots - x_{i-1} p_1 \cdots p_{i-2} \bmod p_i.$$
All elements on the right-hand side are already known at this stage in the algorithm. We can therefore solve for x_i if the $p_1 \cdots p_{i-1}$ are invertible modulo p_i. As the $p_1, \ldots, p_k$ are mutually coprime, this is possible by Lemma 1.48, and the inverse can be computed with the Extended Euclidean Algorithm. Let s_i denote the inverse of $p_1 \cdots p_{i-1}$ modulo p_i. Set
$$x_i = (a_i - x_1 - x_2 p_1 - x_3 p_1 p_2 - \ldots - x_{i-1} p_1 \cdots p_{i-2}) \cdot s_i.$$
After k of these steps, the algorithm terminates and returns a solution x.

Algorithm 1.59 (Lagrange Interpolation) Let R be a Euclidean ring, and let the following system of congruences to be solved for $x \in R$ be given:
$$\begin{aligned} x &\equiv a_1 \bmod p_1, \\ &\vdots \\ x &\equiv a_k \bmod p_k, \end{aligned}$$
where the $p_1, \ldots, p_k$ are mutually coprime. Make the ansatz
$$x = a_1 q_1 + a_2 q_2 + \ldots + a_k q_k, \tag{1.13}$$
where
$$q_i = u_i \cdot p_1 \cdots p_{i-1} \cdot p_{i+1} \cdots p_k$$
with unknown $u_i \in R$. Then
$$x \equiv a_i q_i \stackrel{!}{\equiv} a_i \bmod p_i.$$
Consequently, u_i has to be chosen such that
$$q_i = u_i \cdot p_1 \cdots p_{i-1} \cdot p_{i+1} \cdots p_k \equiv 1 \bmod p_i$$
holds. As p_i and $p_1 \cdots p_{i-1} \cdot p_{i+1} \cdots p_k$ are coprime by assumption, such a u_i can be computed by the Extended Euclidean Algorithm (Lemma 1.48). After computing $u_1, \ldots, u_k$ and $q_1, \ldots, q_k$, the expression (1.13) yields a solution x.

Remark 1.60 Once one has found a solution x of the congruences, the set of all solutions is

$$x + \langle p_1 \cdots p_k \rangle.$$

This follows from the injectivity of Ψ in the Chinese Remainder Theorem 1.57.

Remark 1.61 An advantage of Newton Interpolation over Lagrange Interpolation is that when an additional congruence $x \equiv a_{k+1} \bmod p_{k+1}$ is added, one can simply continue the computation with the result for the first k congruences by performing an additional iteration of the algorithm (whereas in the Lagrange Interpolation, all of the q_i need to be computed again). On the other hand, the advantage of Lagrange Interpolation over Newton Interpolation is that the q_i do not depend on the a_i. So for fixed $p_1, \ldots, p_k$, they have to be computed only once in order to solve systems of congruences with arbitrary and possibly varying a_i.

In numerical analysis the terms *Newton Interpolation* and *Lagrange Interpolation* denote methods to solve the interpolation problem for polynomials: *Find the polynomial f of lowest degree assuming prescribed values*

$$f(\alpha_i) = \beta_i \qquad i = 1, \ldots, k,$$

at given points $\alpha_1, \ldots, \alpha_k$. This is a system of linear equations in the coefficients of f, and by the usual methods of linear algebra one shows that this system always has a solution for pairwise distinct α_i.

The relation to the Chinese Remainder Theorem becomes evident once we recall Example 1.49: The condition

$$f(\alpha_i) = \beta_i$$

is equivalent to

$$f \equiv \beta_i \bmod X - \alpha_i.$$

The interpolation problem can thus be expressed by simultaneous congruences in the polynomial ring:

$$\begin{aligned} f &\equiv \beta_1 \bmod X - \alpha_1, \\ &\vdots \\ f &\equiv \beta_k \bmod X - \alpha_k, \end{aligned}$$

where the $X - \alpha_i$ are mutually coprime if the α_i are mutually distinct (Theorem 1.39 (c)). By applying Algorithm 1.58 or 1.59 in this special case, one obtains the classical algorithms from numerical analysis.

Example 1.62 (Polynomial Interpolation) Given the points $-1, 0, 1$ and the values

$$f(-1) = 2, \quad f(0) = -1, \quad f(1) = 1,$$

find a polynomial $f \in \mathbb{R}[X]$ of degree 2, assuming these values at the given points. The ansatz of Newton Interpolation is

$$f = f_1 + f_2(X+1) + f_3(X+1)X.$$

Determine the f_i:

- We have $f \equiv f_1 \equiv 2 \bmod X+1$. Set $f_1 = 2$.
- We have $f \equiv 2 + f_2(X+1) \equiv -1 \bmod X$. As $X+1 \equiv 1 \bmod X$, we do not need to compute an inverse in this step. Set $f_2 = -1-2 = -3$.
- We have $f \equiv 2-3(X+1)+f_3(X+1)X \equiv 1 \bmod X-1$, where $X+1 \equiv 2 \bmod X-1$ and $X \equiv 1 \bmod X-1$, that is, $2-3\cdot 2+f_3\cdot 2\cdot 1 \equiv 1 \bmod X-1$. Set $f_3 = \frac{1}{2}(1-2+6) = \frac{5}{2}$.

Then

$$f = 2-3(X+1)+\frac{5}{2}(X+1)X = \frac{5}{2}X^2 - \frac{1}{2}X - 1.$$

We show how to obtain the same result by Lagrange Interpolation. The ansatz is

$$f = 2\cdot u_1 \cdot X(X-1) + (-1)\cdot u_2 \cdot (X+1)(X-1) + 1\cdot u_3 \cdot (X+1)X.$$

To determine u_1, u_2, u_3, note that

$$\begin{aligned} X(X-1) &\equiv 2 \bmod X+1, \\ (X+1)(X-1) &\equiv -1 \bmod X, \\ (X+1)X &\equiv 2 \bmod X-1, \end{aligned}$$

so set $u_1 = \frac{1}{2}, u_2 = -1, u_3 = \frac{1}{2}$. Then

$$\begin{aligned} f &= 2\cdot\frac{1}{2}\cdot X(X-1) + (-1)\cdot(-1)\cdot(X+1)(X-1) + 1\cdot\frac{1}{2}\cdot(X+1)X \\ &= \frac{5}{2}X^2 - \frac{1}{2}X - 1. \quad \heartsuit \end{aligned}$$

Finally, we return to a concrete instance of to the introductory Example 1.55:

Example 1.63 (Integer determinants) Let

$$A = \begin{pmatrix} -17 & 23 \\ -5 & 22 \end{pmatrix} \in \mathbb{Z}^{2\times 2}$$

with $|\det(A)| \leq 2! \cdot 23^2 = 1058$. For the first three prime numbers $p_1 = 11$, $p_2 = 13$, $p_3 = 17$ it holds that

$$11 \cdot 13 \cdot 17 = 2431 > 2 \cdot 1058 + 1 = 2117.$$

(i) Consider $\det(A)$ as an element of $\mathbb{Z}/2431\mathbb{Z}$, where the numbers 1215,...,2430 represent the negative solutions in $\mathbb{Z}$.

(ii) We parallelise the computations by distributing it on $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/13\mathbb{Z}$ and $\mathbb{Z}/17\mathbb{Z}$. Compute the determinants of the modular images of the matrix A:

$$A_{11} = \begin{pmatrix} \overline{5} & \overline{1} \\ \overline{6} & \overline{0} \end{pmatrix} \in (\mathbb{Z}/11\mathbb{Z})^{2\times 2} \quad \text{with} \quad \det(A_{11}) = \overline{5},$$
$$A_{13} = \begin{pmatrix} \overline{9} & \overline{10} \\ \overline{8} & \overline{9} \end{pmatrix} \in (\mathbb{Z}/13\mathbb{Z})^{2\times 2} \quad \text{with} \quad \det(A_{13}) = \overline{1},$$
$$A_{17} = \begin{pmatrix} \overline{0} & \overline{6} \\ \overline{12} & \overline{5} \end{pmatrix} \in (\mathbb{Z}/17\mathbb{Z})^{2\times 2} \quad \text{with} \quad \det(A_{17}) = \overline{13}.$$

(iii) Now we reconstruct $\det(A) \bmod 2431$ from the congruences

$$\begin{aligned} \det(A) &\equiv 5 \bmod 11, \\ \det(A) &\equiv 1 \bmod 13, \\ \det(A) &\equiv 13 \bmod 17. \end{aligned}$$

The ansatz for Newton Interpolation is

$$\det(A) = a_1 + a_2 \cdot 11 + a_3 \cdot 11 \cdot 13.$$

- Set $a_1 = 5$.
- We have $5 + a_2 \cdot 11 \equiv 1 \bmod 13$. With the Extended Euclidean Algorithm we find $1 = 6 \cdot 11 - 5 \cdot 13$, so 6 is the inverse of 11 modulo 13. Now we can solve for a_2: $a_2 \equiv (1-5) \cdot 6 \equiv 2 \bmod 13$. Set $a_2 = 2$.
- We have $5+2\cdot 11+a_3\cdot 11\cdot 13 \equiv 13 \bmod 17$. The inverse of $11\cdot 13 = 143$ modulo 17 is 5. So $a_3 \equiv (13-5-22)\cdot 5 \equiv 15 \bmod 17$. Set $a_3 = 15$.

Then $\det(A) = 5 + 2 \cdot 11 + 15 \cdot 11 \cdot 13 = 2172 \bmod 2431$.

(iv) As $2172 > 1214$, we have to interprete this result as a negative number in $\mathbb{Z}$. Then

$$\det(A) = 2172 - 2431 = -259. \quad \heartsuit$$

Further applications of the Chinese Remainder Theorem to number theoretic and computer algebraic problems can be found in Lipson [10].

For the sake of completeness we state a more general form of the Chinese Remainder Theorem for arbitrary rings. However, this generalise form does not provide us with an algorithm to compute the inverse of the isomorphism.

Theorem 1.64 (Chinese Remainder Theorem for Arbitrary Rings) *Let R be a ring and $\mathfrak{I}_1, \ldots, \mathfrak{I}_k$ mutually coprime ideals in R. Moreover, let $\mathfrak{H} = \bigcap_{j=1}^{k} \mathfrak{I}_j$ (this is also an ideal in R). Then the map*

$$\Psi : R/\mathfrak{H} \to R/\mathfrak{I}_1 \times \cdots \times R/\mathfrak{I}_k, \quad x \bmod \mathfrak{H} \mapsto (x \bmod \mathfrak{I}_1, \ldots, x \bmod \mathfrak{I}_k) \tag{1.14}$$

is an isomorphism of rings.

For a proof, see Bosch [1], Theorem 12 in Section 2.3.

2 The Jordan Canonical Form

2.1 Invariant Subspaces

Throughout this section let V be a $\mathbb{K}$-vector space.

Definition 2.1 Let $\Phi : V \to V$ be an endomorphism. A vector subspace U of V is called **Φ-invariant**, if

$$\Phi(U) \subset U.$$

If U is Φ-invariant, then the restriction $\Phi|_U$ is an endomorphisms of U.

Definition 2.2 Let U be a Φ-invariant subspace of V. A subspace W of V satisfying $V = U \oplus W$ is called a **vector space complement** for U. If W is also Φ-invariant, then we call W an **invariant complement** for U.

Example 2.3 (Invariant subspaces)

(a) The subspaces $\{0\}$ and V are invariant for every endomorphism.

(b) Every eigenspace (in particular the kernel) of Φ is invariant. If E_λ is the eigenspace for the eigenvalue λ, then every eigenvector $x \in E_\lambda$ spans an invariant subspace $\operatorname{span}\{x\}$ of E_λ.

Every 1-dimensional invariant subspace is an eigenspace.

(c) Let e_1, e_2, e_3 denote the canonical basis of $\mathbb{R}^3$, and let Φ_α the rotation by the angle α in the e_2, e_3-plane. Then the subspace $[e_2, e_3]$ is invariant under Φ_α, as the rotation takes place within this plane. The axis of rotation is the e_1-axis, that is, $\Phi_\alpha(e_1) = e_1$. So this axis is an eigenspace, and as such an invariant complement for the plane of rotation. We can thus write $\mathbb{R}^3$ as the direct sum of two invariant subspaces:

$$\mathbb{R}^3 = \operatorname{span}\{e_1\} \oplus \operatorname{span}\{e_2, e_3\}.$$

This invariance is manifest in the block form of the matrix representing Φ_α:

$$\left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{array}\right).$$

(d) The map

$$\Phi(x) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot x$$

has the invariant subspace $\operatorname{span}\{e_1\}$.

In this example, there does not exist an invariant complement for $\operatorname{span}\{e_1\}$, for there was, it would be of dimension $\dim \mathbb{R}^2 - \dim \operatorname{span}\{e_1\} = 1$ and hence an eigenspace. As Φ has the sole eigenvalue 1, Φ would then be diagonalisable with eigenvalue 1, that is, $\Phi = \mathrm{id}_{\mathbb{R}^2}$, which is obviously not the case. ♡

These examples hint at a more general principle (in finite dimension n): Let U be a Φ-invariant subspace and $B_U = \{b_1, \ldots, b_k\}$ a basis of U. Complete B_U to a basis $B = \{b_1, \ldots, b_k, c_{k+1}, \ldots, c_n\}$ of V. Invariance means that the images $\Phi(b_i)$ take the following form with respect to the basis B:

$$\Phi(b_i) = \lambda_1 \cdot b_1 + \ldots + \lambda_k \cdot b_k + 0 \cdot c_{k+1} + \ldots + 0 \cdot c_n.$$

It follows that the matrix $\varrho_B^B(\Phi)$ representing Φ with respect to the basis B has the following block form:

$$\varrho_B^B(\Phi) = \begin{pmatrix} \varrho_{B_U}^{B_U}(\Phi|_U) & M \\ 0 & N \end{pmatrix}$$

for suitable matrices $N \in \mathbb{K}^{(n-k)\times(n-k)}$, $M \in \mathbb{K}^{n\times(n-k)}$. This representation can be made even more precise: If

$$\Phi(c_{k+i}) = \mu_{1i} \cdot b_1 + \ldots + \mu_{ki} \cdot b_k + \nu_{1i} \cdot c_{k+1} + \ldots + \nu_{n-k,i} \cdot c_n, \qquad (*)$$

then the μ_{ij} are precisely the coefficients of the matrix M and the ν_{ij} are the coefficients of the matrix N. As U is Φ-invariant, Φ induces and endomorphism[5)]

$$\overline{\Phi} : V/U \to V/U, \quad x + U \mapsto \Phi(x) + U.$$

A basis C of V/U is given by the classes of the basis vectors $c_{k+1}, \ldots, c_n$:

$$\overline{c}_1 = c_{k+1} + U, \ \ldots, \ \overline{c}_{n-k} = c_n + U.$$

As the elements $b_1, \ldots, b_k$ are contained in U, they project to 0 in V/U. Hence the representation of $\overline{\Phi}$ in the basis C is derived from $(*)$ as

$$\begin{aligned} \overline{\Phi}(\overline{c}_i) &= \underbrace{\mu_{1i} \cdot \overline{b}_1}_{=0} + \ldots + \underbrace{\mu_{ki} \cdot \overline{b}_k}_{=0} + \nu_{1i} \cdot \overline{c}_1 + \ldots + \nu_{n-k,i} \cdot \overline{c}_{n-k} \\ &= \nu_{1i} \cdot \overline{c}_1 + \ldots + \nu_{n-k,i} \cdot \overline{c}_{n-k}, \end{aligned}$$

[5)] The invariance of U crucial for $\overline{\Phi}$ to be well-defined.

that is, the matrix representing $\overline{\Phi}$ with respect to C is

$$\varrho_C^C(\overline{\Phi}) = N.$$

In total, we therefore have

$$\varrho_B^B(\Phi) = \begin{pmatrix} \varrho_{B_U}^{B_U}(\Phi|_U) & M \\ 0 & \varrho_C^C(\overline{\Phi}) \end{pmatrix}. \tag{2.1}$$

From this matrix form we immediately obtain the following lemma:

Lemma 2.4 *For U, Φ, $\overline{\Phi}$ as above, the following holds:*

(a) $\det(\Phi) = \det(\Phi|_U) \cdot \det(\overline{\Phi})$.

(b) *The characteristic polynomials satisfy*

$$f_\Phi = f_{\Phi|_U} \cdot f_{\overline{\Phi}}.$$

In particular, $f_{\Phi|_U}$ is a divisor of f_Φ.

(c) $\operatorname{Spec} \Phi = \operatorname{Spec} \Phi|_U \cup \operatorname{Spec} \overline{\Phi}$.

If U has an invariant complement W, then the basis B_U can be complete to a basis B of V by a basis B_W of W. In this case, the matrix representation (2.1) of Φ with respect to B is of the form

$$\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix},$$

where A_1 is a matrix representation of $\Phi|_U$ and A_2 is a matrix representation of $\Phi|_W$. This motivates the following notation:

Definition 2.5 Let U, W be vector subspaces of V, such that $U \oplus W = V$ holds. For endomorphisms $\Phi_U : U \to U$ and $\Phi_W : W \to W$, define their **direct sum**

$$\Phi_U \oplus \Phi_W : V \to V$$

via

$$\begin{aligned} (\Phi_U \oplus \Phi_W)(u) &= \Phi_U(u) \quad \text{for } u \in U, \\ (\Phi_U \oplus \Phi_W)(w) &= \Phi_W(w) \quad \text{for } w \in W. \end{aligned}$$

Accordingly, we define the direct sum of matrices $A \in \mathbb{K}^{n\times n}$ and $B \in \mathbb{K}^{m\times m}$ as

$$A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \in \mathbb{K}^{(n+m)\times(n+m)}.$$

Define the direct sum $\Phi_1 \oplus \ldots \oplus \Phi_k$ (or $A_1 \oplus \ldots \oplus A_k$) of k endomorphisms (or matrices) accordingly.

With this notation, we can express the results obtained previously:

Lemma 2.6 *Let U be a Φ-invariant subspace of V with invariant complement W, then*

$$\Phi = \Phi|_U \oplus \Phi|_W.$$

If B_U is a basis of U and B_W a basis of W, then Φ is represented with respect to the basis $B = B_U \cup B_W$ of V by the matrix

$$\varrho_B^B(\Phi) = \varrho_{B_U}^{B_U}(\Phi|_U) \oplus \varrho_{B_W}^{B_W}(\Phi|_W).$$

Theorem 2.7 *Let $\Phi, \Psi \in \mathrm{End}(V)$ and assume $\Phi \circ \Psi = \Psi \circ \Phi$. Then:*

(a) *Every eigenspace $E_\lambda(\Phi)$ of Φ is Ψ-invariant.*

(b) $\ker \Phi$ *is Ψ-invariant.*

(c) $\mathrm{im}\, \Phi$ *is Ψ-invariant.*

PROOF:

(a) Let $x \in E_\lambda(\Phi)$, $x \neq 0$. By assumption,

$$\lambda \cdot \Psi(x) = \Psi(\lambda \cdot x) = \Psi(\Phi(x)) = \Phi(\Psi(x)).$$

So $\Psi(x)$ is either 0 or an eigenvector of Φ, that is, $\Psi(E_\lambda(\Phi)) \subset E_\lambda(\Phi)$.

(b) $\ker \Phi = E_0$.

(c) $\Psi(\mathrm{im}\, \Phi) = \mathrm{im}(\Psi \circ \Phi) = \mathrm{im}(\Phi \circ \Psi) = \Phi(\mathrm{im}\, \Psi) \subset \mathrm{im}\, \Phi$. ◇

The analogous statements hold for pairs of commuting matrices.

Exercise 2.8 (Schur's Lemma) Let V be a $\mathbb{C}$-vector space, $\dim V < \infty$, and $\Phi \in \mathrm{End}(V)$, such that $\Phi \circ \Psi = \Psi \circ \Phi$ for all $\Psi \in \mathrm{End}(V)$ holds. Then there exists $\lambda \in \mathbb{C}$, such that

$$\Phi = \lambda \cdot \mathrm{id}_V.$$

2.2 Nilpotent Endomorphisms

Definition 2.9 An endomorphism $\Phi : V \to V$ is called k-step **nilpotent**, if

$$\Phi^k = 0 \quad \text{for some } k \in \mathbb{N},$$

and $\Phi^m \neq 0$ for $m < k$. Accordingly, a matrix $A \in \mathbb{K}^{n\times n}$ is called nilpotent, if $A^k = 0$ for some $k \in \mathbb{N}$, and $A^m \neq 0$ for $m < k$. We also call k the **degree of nilpotency** of Φ (or A, respectively).

Example 2.10 (Nilpotent matrices) The matrix

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

is 2-step nilpotent. More generally, every upper triangular $n \times n$-matrix of the form

$$A = \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}$$

is n-step nilpotent: One checks that

$$A^2 = \begin{pmatrix} 0 & 0 & 1 & & 0 \\ & \ddots & \ddots & \ddots & \\ & & \ddots & \ddots & 1 \\ & & & \ddots & 0 \\ 0 & & & & 0 \end{pmatrix}, \; A^3 = \begin{pmatrix} 0 & 0 & 0 & 1 & & 0 \\ & \ddots & \ddots & \ddots & \ddots & \\ & & \ddots & \ddots & \ddots & 1 \\ & & & \ddots & \ddots & 0 \\ & & & & \ddots & 0 \\ 0 & & & & & 0 \end{pmatrix}, \ldots,$$

$$A^{n-1} = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ & \ddots & & 0 \\ & & \ddots & \vdots \\ 0 & & & 0 \end{pmatrix}, \; A^n = 0. \qquad \heartsuit$$

Remark 2.11 The nilpotency of the matrices in Example 2.10 is reflected in their characteristic polynomial: It is $f_A = X^n$, and by the Cayley-Hamilton Theorem $f_A(A) = A^n = 0$.

Theorem 2.12 *Let V be an n-dimensional vector space. $\Phi \in \mathrm{End}(V)$ is nilpotent if and only if its characteristic polynomial is $f_\Phi = X^n$.*

PROOF: The proof is by induction on n: For $n = 1$, the theorem is obviously true. Now let $n > 1$. As 0 is a zero of f_Φ, there exists an eigenvector x of Φ for the eigenvalue 0. If we complete $\{x\}$ to a basis of V, then Φ is represented by a nilpotent matrix respect to this basis,

$$A = \begin{pmatrix} 0 & * & \cdots & * \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix} \in \mathbb{K}^{n\times n}$$

with $B \in \mathbb{K}^{(n-1)\times(n-1)}$. From this we see:

$$f_\Phi = X \cdot f_B.$$

As $A^k = 0$ holds for some $k > 0$, $B^k = 0$ holds as well. Multiplication by B therefore defines a nilpotent endomorphism of $\mathbb{K}^{n-1}$. By the induction hypothesis, $f_B = X^{n-1}$ holds. It follows that $f_\Phi = X \cdot X^{n-1} = X^n$. ◇

Corollary 2.13 *If Φ is k-step nilpotent, then $k \leq n$.*

PROOF: The characteristic polynomial of Φ is X^n. By the Cayley-Hamilton Theorem, $\Phi^n = 0$ holds. Hence $k \leq n$. ◇

Example 2.14 The two 4×4-matrices

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

are nilpotent. Here, A is 4-step nilpotent and B is 2-step nilpotent. Both matrices have the characteristic polynomial $f_A = f_B = X^4$. For A there is no polynomial $0 \neq p = p_0 + p_1X + p_2X^2 + p_3X^3$ of smaller degree satisfying $p(A) = 0$, because

$$p(A) = \begin{pmatrix} p_0 & p_1 & p_2 & p_3 \\ 0 & p_0 & p_1 & p_2 \\ 0 & 0 & p_0 & p_1 \\ 0 & 0 & 0 & p_0 \end{pmatrix} \neq 0.$$

For B on the other hand, we have $B^2 = 0$. The polynomial $h = X^2$ is the polynomial of minimal positive degree satisfying $h(B) = 0$, as for $0 \neq p = p_0 + p_1X$,

$$p(B) = \begin{pmatrix} p_0 & p_1 & 0 & 0 \\ 0 & p_0 & 0 & 0 \\ 0 & 0 & p_0 & p_1 \\ 0 & 0 & 0 & p_0 \end{pmatrix} \neq 0. \qquad \heartsuit$$

By means of the characteristic polynomial one can determine whether a matrix is nilpotent or not. But as Example 2.14 shows, it gives no clues on the degree of nilpotency. This motivates the following definition:

Definition 2.15 Let V be a vector space of finite dimension n. Moreover, let $\Phi \in \mathrm{End}(V)$. We call $h_\Phi \in \mathbb{K}[X]$ the **minimal polynomial** of Φ, if h_Φ satisfies:

(i) $h_\Phi(\Phi) = 0$.

(ii) h_Φ is normalised.

(iii) h_Φ is the polynomial of minimal degree with properties (i) and (ii).

The minimal polynomial h_A of a matrix $A \in \mathbb{K}^{n\times n}$ is defined accordingly.

Example 2.16 In Example 2.14, the matrices A and B have the respective minimal polynomials $h_A = X^4 = f_A$ and $h_B = X^2$. ♡

Remark 2.17 Recall that in $\mathbb{K}[X]$ every ideal is a principle ideal (Theorem 1.35). Then the normalised generator h of the ideal

$$\mathfrak{I}_\Phi = \{f \in \mathbb{K}[X] \mid f(\Phi) = 0\} = \langle h \rangle \tag{2.2}$$

is just the minimal polynomial of Φ. In particular, this shows that for every Φ there exists a unique minimal polynomial.

Lemma 2.18 *Let h_Φ be the minimal polynomial $\Phi \in \mathrm{End}(V)$. Then:*

(a) *For every matrix representation $A = \varrho_B^B(\Phi)$ of Φ, we have $h_A = h_\Phi$.*

(b) *h_Φ is a divisor of the characteristic polynomial f_Φ.*

PROOF:

(a) $\varrho_B^B : \mathrm{End}(V) \to \mathbb{K}^{n\times n}$ is an isomorphism of vector spaces and of rings. Hence $h_\Phi(A) = h_\Phi(\varrho_B^B(\Phi)) = \varrho_B^B(h_\Phi(\Phi)) = 0$. Moreover, h_Φ is normalised and there exists no polynomial p with $0 < \deg(p) < \deg(h_\Phi)$ satisfying $p(A) = 0$, for such a polynomial would also satisfy $p(\Phi) = (\varrho_B^B)^{-1}(p(A)) = 0$, contradicting the fact that h_Φ is the minimal polynomial of Φ. Hence $h_A = h_\Phi$.

(b) $f_\Phi \in \mathfrak{I}_\Phi = \langle h_\Phi \rangle$. ♢

Theorem 2.19 *Let V be an n-dimensional vector space. $\Phi \in \mathrm{End}(V)$ is k-step nilpotent if and only if its minimal polynomial is $h_\Phi = X^k$.*

PROOF: $\Phi^k = 0$ means $X^k \in \mathfrak{I}_\Phi$, so X^k is a multiple of h_Φ and all prime factors of h_Φ must be prime factors of X^k. As X is the only prime factor of X^k, it follows that $h_\Phi = X^m$ for some $m > 0$. As $\Phi^m \neq 0$ for $m < k$ and $\deg(h_\Phi)$ is minimal in $\mathfrak{I}_\Phi$, it follows that $h_\Phi = X^k$.

Conversely, if $h_\Phi = X^k$, then $\Phi^k = 0$ and $\Phi^m \neq 0$ for $m < k$ by definition of the minimal polynomial. ◇

2.3 The Programme

Deriving the Jordan canonical form is a somewhat arduous endeavour and certainly easier to keep track of if we know what we are looking for beforehand. Therefore, we shall sketch the steps necessary to derive the Jordan canonical form in this section.

We will see that every endomorphism Φ of an n-dimensional $\mathbb{C}$-vector space V can be represented by its **Jordan canonical form**

$$J(\Phi) = \begin{pmatrix} \boxed{\begin{matrix} \lambda_1 & 1 & & & \\ & \lambda_1 & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda_1 & 1 \\ & & & & \lambda_1 \end{matrix}} & & & \\ & \boxed{\begin{matrix} \lambda_2 & 1 & & & \\ & \lambda_2 & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda_2 & 1 \\ & & & & \lambda_2 \end{matrix}} & & \\ & & \ddots & \\ & & & \boxed{\begin{matrix} \lambda_k & 1 & & & \\ & \lambda_k & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda_k & 1 \\ & & & & \lambda_k \end{matrix}} \end{pmatrix} \in \mathbb{C}^{n \times n},$$

where the λ_i are not necessarily distinct.

The boxes appearing in the matrix $J(\Phi)$ are called the **Jordan boxes**

$$J_{n_i}(\lambda_i) = \begin{pmatrix} \lambda_i & 1 & & & \\ & \lambda_i & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda_i & 1 \\ & & & & \lambda_i \end{pmatrix} \in \mathbb{C}^{n_i \times n_i}$$

of size n_i for the eigenvalue λ_i. We can write $J(\Phi)$ more concisely as

$$J(\Phi) = J_{n_1}(\lambda_1) \oplus J_{n_2}(\lambda_2) \oplus \ldots \oplus J_{n_k}(\lambda_k).$$

The matrix $J(\Phi)$ is the sum

$$J(\Phi) = D + N$$

of the diagonal matrix D with the λ_i as entries and the nilpotent matrix

$$N = J_{n_1}(0) \oplus J_{n_2}(0) \oplus \ldots \oplus J_{n_k}(0).$$

Knowing $J(\Phi)$ is thus equivalent to knowing D and N.

We now investigate how to determine a **Jordan basis** B in which Φ is represented by its Jordan canonical form $J(\Phi)$.

1. First, find out how D can be determined from Φ. Clearly, D and $J(\Phi)$ (and hence Φ) share the same characteristic polynomial

   $$f_\Phi = \det(X \cdot \mathrm{id}_V - \Phi) = (X - \lambda_1)^{n_1}(X - \lambda_2)^{n_2} \cdots (X - \lambda_k)^{n_k} = f_D,$$

   as the diagonal entries of D are precisely the eigenvalues of Φ (where the Fundamental Theorem of Algebra assures us that f_Φ indeed decomposes into linear factors). The exponent n_i of an eigenvalue λ_i determines how often λ_i appears on the diagonal of D or $J(\Phi)$.

2. As the λ_i in $J(\Phi)$ are not necessarily distinct, Φ might have less than k distinct eigenvalues, say $\lambda_1, \ldots, \lambda_m$ with $m \leq k$. If an eigenvalue λ appears with multiplicity α on the diagonal of $J(\Phi)$ or D, then D has an eigenspace $V_\lambda \subset V$ of dimension α.

3. The Jordan boxes for the same eigenvalue λ can be collected (after re-ordering the basis if necessary) into a **Jordan block**:[6)]

$$\hat{J}_{(m_1,\ldots,m_r)}(\lambda) = \begin{pmatrix} \boxed{\begin{smallmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{smallmatrix}} & & \\ & \ddots & \\ & & \boxed{\begin{smallmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{smallmatrix}} \end{pmatrix} \in \mathbb{C}^{(m_1+\ldots+m_r)\times(m_1+\ldots+m_r)},$$

[6)] The distinction between Jordan boxes and Jordan blocks is not standard in the literature.

or more concisely

$$\hat{J}_{(m_1,\ldots,m_r)}(\lambda) = J_{m_1}(\lambda) \oplus \ldots \oplus J_{m_r}(\lambda) \in \mathbb{C}^{\alpha\times\alpha}$$

with $m_1 + \ldots + m_r = \alpha$. As can be seen from the canonical form $J(\Phi)$, the space V_λ is invariant under Φ and the restriction $\Phi|_{V_\lambda}$ is represented by the Jordan block $\hat{J}_{(m_1,\ldots,m_k)}(\lambda)$ in a suitable basis $B_\lambda \subset B$ of V_λ.

4. If, for every eigenvalue λ_i, we know this basis B_{λ_i} of V_{λ_i}, we obtain the desired basis B of V as their union

$$B = B_{\lambda_1} \cup \ldots \cup B_{\lambda_m}.$$

5. In order to determine the basis B_λ for a given eigenvalue λ, we consider the endomorphism

$$\Phi - \lambda \cdot \mathrm{id}_V.$$

The restriction $(\Phi - \lambda \cdot \mathrm{id}_V)|_{V_\lambda}$ is represented by the Jordan block

$$\hat{J}_{(m_1,\ldots,m_k)}(0) = \hat{J}_{(m_1,\ldots,m_k)}(\lambda) - \lambda I_\alpha$$

and is thus nilpotent of a degree $\leq \alpha$. We obtain

$$V_\lambda = \ker(\Phi - \lambda \cdot \mathrm{id}_V)^\alpha.$$

This does not yet determine the basis B_λ, but we have reduced the problem of determining the Jordan canonical form to the case of nilpotent endomorphisms. This case will be studied in Section 2.5.

For a matrix $A \in \mathbb{C}^{n\times n}$ we define its **Jordan canonical form** $J(A)$ as the Jordan canonical form of the endomorphism $\Phi_A(x) = Ax$.

2.4 The Primary Decomposition

In this section, we will initially consider vector spaces V of finite dimension over an arbitrary scalar field $\mathbb{K}$.

Theorem 2.20 *Let $\Phi \in \mathrm{End}(V)$, and let $g, h \in \mathbb{K}[X]$ be coprime and $f = gh$, such that $f(\Phi) = 0$ holds. Set $U = \ker g(\Phi)$ and $W = \ker h(\Phi)$. Then:*

(a) $V = U \oplus W$.

(b) $U = \mathrm{im}\, h(\Phi)$ *and* $W = \mathrm{im}\, g(\Phi)$.

(c) *U and W are Φ-invariant.*

PROOF: As g and h are coprime, we can determine polynomials $r, s \in \mathbb{K}[X]$ by means of the Extended Euclidean Algorithm, such that

$$1 = rg + sh$$

holds. Plugging Φ into this expression, we obtain

$$\begin{aligned} \mathrm{id}_V &= r(\Phi) \circ g(\Phi) + s(\Phi) \circ h(\Phi) \\ &= g(\Phi) \circ r(\Phi) + h(\Phi) \circ s(\Phi). \end{aligned} \tag{$*$}$$

(a) By assumption $0 = f(\Phi) \circ r(\Phi) = (hg)(\Phi) \circ r(\Phi) = h(\Phi) \circ (gr)(\Phi)$ and analogously $0 = g(\Phi) \circ (hs)(\Phi)$. By plugging $x \in V$ into $(*)$ we find

$$x = \underbrace{g(\Phi)\big(r(\Phi)(x)\big)}_{\in \ker h(\Phi)} + \underbrace{h(\Phi)\big(s(\Phi)(x)\big)}_{\in \ker g(\Phi)},$$

so $V = U + W$. If $x \in U \cap W$, that is, $g(\Phi)(x) = 0 = h(\Phi)(x)$, then plugging this into $(*)$ yields $x = 0$, so that $V = U \oplus W$.

(b) If $x \in U$, then $(*)$ means

$$x = h(\Phi)\big(s(\Phi)(x)\big) \in \operatorname{im} h(\Phi).$$

Conversely, for $x = h(\Phi)(y)$ the following holds:

$$g(\Phi)(x) = g(\Phi)\big(h(\Phi(y))\big) = \big((gh)(\Phi)\big)(y) = f(\Phi)(y) = 0,$$

that is $x \in U$. Hence $\operatorname{im} h(\Phi) = U$. Analogously $\operatorname{im} g(\Phi) = W$ holds.

(c) By (b), $\Phi(U) = \Phi\big(h(\Phi)(V)\big) = h(\Phi)\big(\Phi(V)\big) \subset h(\Phi)(V) = U$ and analogously $\Phi(W) \subset W$. ◇

The unique prime factorisation (Theorem 1.36) allows to decompose a polynomial $f \in \mathbb{K}[X]$ into a product of powers of irreducible normalised polynomials p_i,

$$f = p_1^{\alpha_1} \cdots p_m^{\alpha_m}.$$

Corollary 2.21 *Let $\Phi \in \mathrm{End}(V)$ and $f \in \mathbb{K}[X]$. Moreover, let $f = q_1 \cdots q_m$ be a factorisation with mutually coprime $q_i \in \mathbb{K}[X]$. Then*

$$\ker f(\Phi) = \ker q_1(\Phi) \oplus \ldots \oplus \ker q_m(\Phi). \tag{2.3}$$

PROOF: Clearly, $\ker f(\Phi)$ is a Φ-invariant subspace of V and $f(\Phi)|_{\ker f(\Phi)} = 0$ holds. By Theorem 2.20 (applied to the vector space $\ker f(\Phi)$) it follows that

$$\ker f(\Phi) = \ker q_1(\Phi) \oplus \ker(q_2 \cdots q_m)(\Phi).$$

Then it follows by induction over n that

$$\ker(q_2 \cdots q_m)(\Phi) = \ker q_2(\Phi) \oplus \ldots \oplus \ker q_m(\Phi),$$

and hence the assertion holds. ◇

Theorem 2.22 *Let V be a $\mathbb{K}$-vector space of dimension n and $\Phi \in \mathrm{End}(V)$. Further, let $f_\Phi = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ be the prime factorisation of the characteristic polynomial of Φ. Then*

$$V = V_1 \oplus \ldots \oplus V_m \tag{2.4}$$

with $V_i = \ker p_i^{\alpha_i}(\Phi)$ is a decomposition of V into Φ-invariant subspaces.

PROOF: The Cayley-Hamilton Theorem implies $V = \ker f_\Phi(\Phi) = \ker 0$. Thus the theorem follows from Corollary 2.21, applied to $f = f_\Phi$ and $q_i = p_i^{\alpha_i}$. ◇

The decomposition (2.4) of V into Φ-invariant subspaces coarsens the prime factorisation of f_Φ and is thus called the **primary decomposition** of V with respect to Φ.

Corollary 2.23 *Let $\Phi \in \mathrm{End}(V)$. Every prime factor of the characteristic polynomial f_Φ of Φ is also a prime factor of the minimal polynomial h_Φ of Φ.*

PROOF: If $V = V_1 \oplus \ldots \oplus V_m$ is the primary decomposition of V with respect to Φ, then $p_i^{\alpha_i}(\Phi|_{V_i}) = 0$ by definition of V_i. Hence the minimal polynomial $h_i = h_{\Phi|_{V_i}}$ of $\Phi|_{V_i}$ divides $p_i^{\alpha_i}$, and in particular we have $h_i = p_i^{k_i}$ for some $k_i \le \alpha_i$. But $h_\Phi(\Phi|_{V_i}) = 0$ holds as well, hence h_i is a divisor of h_Φ. ◇

The proof of Corollary 2.23 implies $p_i^{k_i}(\Phi|_{V_i}) = 0$, where k_i is the exponent of p_i in the minimal polynomial. This also means $p_i^r(\Phi|_{V_i}) \neq 0$ for $r < k_i$. We can therefore conclude:

Corollary 2.24 *The statement of Theorem 2.22 remains true if f_Φ is replaced by the minimal polynomial h_Φ. In particular, $V_i = \ker p_i^{k_i}(\Phi)$.*

Remark 2.25 If $B_1, \ldots, B_m$ are bases of the invariant subspaces $V_1, \ldots, V_m$ and $B = B_1 \cup \ldots \cup B_m$ a basis of V, then

$$\varrho_B^B(\Phi) = \begin{pmatrix} \varrho_{B_1}^{B_1}(\Phi|_{V_1}) & & & \\ & \varrho_{B_2}^{B_2}(\Phi|_{V_2}) & & \\ & & \ddots & \\ & & & \varrho_{B_m}^{B_m}(\Phi|_{V_m}) \end{pmatrix}.$$

In the following, we study the primary decomposition in the special case $\mathbb{K} = \mathbb{C}$. By Corollary 1.41 the irreducible polynomials in $\mathbb{C}[X]$ are the polynomials $X - \lambda$ of degree 1. The prime factorisation of the characteristic polynomial of Φ is therefore a product of linear factors $p_i = X - \lambda_i$,

$$f_\Phi = (X - \lambda_1)^{\alpha_1} \cdots (X - \lambda_m)^{\alpha_m},$$

where the λ_i are the distinct eigenvalues of Φ with **algebraic multiplicity** α_i. By Corollary 2.23, the minimal polynomial is a product of the same linear factors,

$$h_\Phi = (X - \lambda_1)^{k_1} \cdots (X - \lambda_m)^{k_m}$$

with $0 < k_i \leq \alpha_i$ for $i = 1, \ldots, m$. The Φ-invariant subspaces in the primary decomposition (2.4) are thus the subspaces

$$V_i = \ker p_i^{k_i}(\Phi) = \ker(\Phi - \lambda_i \cdot \mathrm{id}_V)^{k_i}.$$

So every space V_i is determined by a certain eigenvalue λ_i. If $k_i = 1$, then V_i even coincides with the eigenspace $E_{\lambda_i} = \ker(X - \lambda_i \cdot \mathrm{id}_V)$. We define accordingly:

Definition 2.26 Let V be $\mathbb{C}$-vector space of dimension n and $\Phi \in \mathrm{End}(V)$. If λ is an eigenvalue of Φ and k the exponent of $X - \lambda$ in the minimal polynomial of Φ, then

$$V_\lambda = \ker(\Phi - \lambda \cdot \mathrm{id}_V)^k \tag{2.5}$$

is called the **generalised eigenspace** of Φ for the eigenvalue λ.

In the complex case, Theorem 2.22 takes the following form:

Theorem 2.27 *Let V be a $\mathbb{C}$-vector space of dimension n and $\Phi \in \mathrm{End}(V)$. Further, let $\lambda_1, \ldots, \lambda_m$ be the distinct eigenvalues of Φ. Then*

$$V = V_{\lambda_1} \oplus \ldots \oplus V_{\lambda_m} \tag{2.6}$$

where V_{λ_i} is the generalised eigenspace for the eigenvalue λ_i.

Lemma 2.28 *For $i = 1, \ldots, m$ it holds that:*

(a) $E_{\lambda_i} \subseteq V_{\lambda_i}$.

(b) $\Phi|_{V_{\lambda_i}} - \lambda_i \cdot \mathrm{id}_{V_{\lambda_i}}$ *is nilpotent of degree k_i.*

(c) $\dim V_{\lambda_i} = \alpha_i$.

PROOF:

(a) Follows directly from the definition.

(b) The minimal polynomial of $\Phi|_{V_{\lambda_i}}$ is $h_i = (X - \lambda_i)^{k_i}$. The claim holds, because $h_i(\Phi|_{V_{\lambda_i}}) = 0$ and h_i is the polynomial of lowest degree with this property.

(c) As $\Phi|_{V_{\lambda_i}} - \lambda_i \cdot \mathrm{id}_{V_{\lambda_i}}$ is nilpotent by (b), its characteristic polynomial is $\det(X \cdot \mathrm{id}_{V_{\lambda_i}} - \Phi|_{V_{\lambda_i}} + \lambda_i \cdot \mathrm{id}_{V_{\lambda_i}}) = X^{\dim V_{\lambda_i}}$ by Theorem 2.12. Hence

$$f_i = \det(X \cdot \mathrm{id}_{V_{\lambda_i}} - \Phi|_{V_{\lambda_i}}) = (X - \lambda_i)^{\dim V_{\lambda_i}}$$

is the characteristic polynomial of $\Phi|_{V_{\lambda_i}}$. Morever, $f_\Phi = f_1 \cdots f_i \cdots f_m$ and the linear factor $X - \lambda_i$ with exponent α_i in f_Φ appears in f_i and in none of the f_j with $j \neq i$, so that $\dim V_{\lambda_i} = \alpha_i$. ◇

Remark 2.29 If $B_{\lambda_1}, \ldots, B_{\lambda_m}$ are arbitrary bases of the generalised eigenspaces $V_{\lambda_1}, \ldots, V_{\lambda_m}$, and $A_1, \ldots, A_m$ the matrices representing the respective $\Phi|_{V_{\lambda_i}}$ in the bases B_{λ_i}, then

$$A = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_m \end{pmatrix} = A_1 \oplus A_2 \oplus \ldots \oplus A_m \tag{2.7}$$

is the matrix representation of Φ with respect to the basis $B = B_{\lambda_1} \cup \ldots \cup B_{\lambda_m}$. This matrix can be seen as a first step towards the Jordan canonical form. Here, the blocks A_i correspond to the Jordan blocks $\hat{J}(\lambda_i)$. In order to actually obtain $A_i = \hat{J}(\lambda_i)$, we have to choose special bases B_{λ_i}. To find these bases, we will study the restriction $\Phi|_{V_{\lambda_i}}$ for every eigenvalue λ_i. As the matrix representation A_i of $\Phi|_{V_{\lambda_i}}$ corresponds uniquely to a matrix representation $A_i - \lambda_i I_{\alpha_i}$ of the nilpotent endomorphism $\Phi|_{V_{\lambda_i}} - \lambda_i \cdot \mathrm{id}_{V_{\lambda_i}}$, we can study this nilpotent map instead. For if $A_i - \lambda_i I_{\alpha_i} = \hat{J}(0)$ is a Jordan block, then $A_i = \hat{J}(0) + \lambda_i I_{\alpha_i} = \hat{J}(\lambda_i)$ is a Jordan block as well. The advantage of this approach is that we only have to study nilpotent endomorphisms.

2.5 The Canonical Form of Nilpotent Endomorphisms

In this section we will prove that every nilpotent endomorphism Φ of a finite-dimensional $\mathbb{K}$-vector space V has a matrix representation A of the form

$$A = \hat{J}_{(m_1,\ldots,m_r)}(0).$$

Throughout this section, we assume Φ to be k-step nilpotent (that is, $\Phi^k = 0$ and $\Phi^{k-1} \neq 0$).

Definition 2.30 An element $x \in V$ is of **degree j** (with $j \geq 1$), if

$$\Phi^j(x) = 0 \quad \text{and} \quad \Phi^{j-1}(x) \neq 0.$$

As Φ is nilpotent, its only eigenvalue is 0. Clearly the eigenvectors of Φ with eigenvalue 0 are elements of degree 1. As $\Phi^{k-1} \neq 0$, there exist elements of degree k (but none of higher degrees, as $\Phi^k = 0$).

Lemma 2.31 *Let $\Phi \in \mathrm{End}(V)$ be nilpotent and x an element of degree j. Then the elements*

$$\Phi^{j-1}(x), \ldots, \Phi(x), x$$

are linearly independent.

PROOF: Let

$$0 = \lambda_0 x + \lambda_1 \Phi(x) + \ldots + \lambda_{j-1} \Phi^{j-1}(x) \qquad (*)$$

with $\lambda_0, \ldots, \lambda_{j-1} \in \mathbb{K}$. Apply Φ^{j-1} to this:

$$0 = \Phi(0) = \lambda_0 \Phi^{j-1}(x) + \lambda_1 \underbrace{\Phi^j(x)}_{=0} + \ldots + \lambda_{j-1} \underbrace{\Phi^{2j-2}(x)}_{=0} = \lambda_0 \underbrace{\Phi^{j-1}(x)}_{\neq 0}.$$

Hence $\lambda_0 = 0$ and $(*)$ becomes

$$0 = \lambda_1 \Phi(x) + \ldots + \lambda_{j-1} \Phi^{j-1}(x).$$

Now apply Φ^{j-2} to this to obtain $\lambda_1 = 0$. Repeat in this manner, until we obtain

$$\lambda_0 = \lambda_1 = \ldots = \lambda_{j-1} = 0.$$

This means

$$x, \Phi(x), \ldots, \Phi^{j-1}(x)$$

are linearly independent. ◇

This immediately implies:

Corollary 2.32 *If $x \in V$ is an element of degree j, then*

$$B_x = \{\Phi^{j-1}(x), \ldots, \Phi(x), x\} \qquad (2.8)$$

is a basis of the Φ-invariant subspace

$$V_x = \mathrm{span}\{\Phi^{j-1}(x), \ldots, \Phi(x), x\}. \qquad (2.9)$$

The matrix representing $\Phi|_{V_x}$ with respect to B_x is

$$J_j(0) = \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix} \in \mathbb{K}^{j\times j}. \tag{2.10}$$

We call x a **generator** of V_x.

Example 2.33 (Nilpotent canonical forms)

(a) Let $\Phi \in \mathrm{End}(\mathbb{R}^4)$ be given by

$$\Phi(x) = \left(\begin{array}{c|ccc} 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) \cdot x.$$

The matrix is

$$\hat{J}_{(1,3)}(0) = J_1(0) \oplus J_3(0)$$

and this already is the Jordan canonical form of Φ. The fourth canonical basis vector e_4 is a generator of degree 3, the vectors e_1 and e_2 are eigenvectors, and thus generators of degree 1. Moreover, $V_{e_1} = \mathrm{span}\{e_1\}$ and

$$V_{e_4} = \mathrm{span}\{e_4, e_3, e_2\} \supset V_{e_3} = \mathrm{span}\{e_3, e_2\} \supset V_{e_2} = \mathrm{span}\{e_2\}.$$

(b) If Φ is given by

$$\Phi(x) = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) \cdot x,$$

then there are no generators of degree 3 or 4, as Φ is 2-step nilpotent. Here also the matrix is already the Jordan canonical form

$$\hat{J}_{(2,2)}(0) = J_2(0) \oplus J_2(0).$$

Generators of degree 2 are e_2 and e_4. Here,

$$V_{e_2} = \mathrm{span}\{e_2, e_1\} \supset V_{e_1} = \mathrm{span}\{e_1\},$$
$$V_{e_4} = \mathrm{span}\{e_4, e_3\} \supset V_{e_3} = \mathrm{span}\{e_3\}.$$

(c) If Φ is given by

$$\Phi(x) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \cdot x,$$

then Φ is 4-step nilpotent and the matrix is already the Jordan canonical form. A generator of degree 4 is e_4. We have

$$\begin{aligned} \mathbb{R}^4 = V_{e_4} &= \operatorname{span}\{e_4, e_3, e_2, e_1\} \\ \supset V_{e_3} &= \operatorname{span}\{e_3, e_2, e_1\} \\ \supset V_{e_2} &= \operatorname{span}\{e_2, e_1\} \\ \supset V_{e_1} &= \operatorname{span}\{e_1\}. \qquad \heartsuit \end{aligned}$$

Next, we will prove that V has a basis B which is the union of bases $B_{x_1}, \ldots, B_{x_r}$ of type (2.8). Then the matrix representation $\varrho_B^B(\Phi)$ takes the desired form:

$$\hat{J}_{(m_1,\ldots,m_r)}(0) = \begin{pmatrix} J_{m_1}(0) & & \\ & \ddots & \\ & & J_{m_r}(0) \end{pmatrix}.$$

In the following we describe the construction of this decomposition for a given Φ and how the basis B is determined. We write

$$K^j = \ker \Phi^j \tag{2.11}$$

for short. Because of nilpotency,

$$\{0\} = K^0 \subset K^1 \subset K^2 \subset \ldots \subset K^{k-1} \subset K^k = V \tag{2.12}$$

and for all j

$$\Phi(K^j) \subset K^{j-1}. \tag{2.13}$$

The elements of degree j are precisely the elements contained in the set $K^j \setminus K^{j-1}$. Choose a vector subspaces $W_k \subset V$ such that

$$V = W_k \oplus K^{k-1}.$$

Then W_k consists of elements of degree k. Now we can also choose a subspace W_{k-1} in K^{k-1} such that

$$K^{k-1} = W_{k-1} \oplus K^{k-2}$$

and W_{k-1} consists of elements of degree $k-1$. By proceeding in this manner, we obtain a decomposition of V of the following form

$$\begin{aligned} V &= W_k \oplus K^{k-1} \\ &= W_k \oplus W_{k-1} \oplus K^{k-2} \\ &\vdots \\ &= W_k \oplus W_{k-1} \oplus \ldots \oplus W_2 \oplus K^1 \\ &= W_k \oplus W_{k-1} \oplus \ldots \oplus W_2 \oplus W_1. \end{aligned}$$

By means of this decomposition we can construct the desired basis of V:

Lemma 2.34 *If W is a vector subspace of V with $W \cap K^j = \{0\}$ for some $j > 0$, then $\Phi|_W$ is injective.*

PROOF: For $j > 0$ we have $\ker \Phi = K^1 \subset K^j$. Then $\ker \Phi|_W = \{0\}$ follows from the assumption, which means $\Phi|_W$ is injective. ◇

For $j = 1, \ldots, k$ set

$$d_j = \dim W_j.$$

Let $b_1^{[k]}, \ldots, b_{d_k}^{[k]}$ be a basis of W_k. As $\Phi|_{W_k}$ is injective by Lemma 2.34, the elements

$$\begin{gathered} \Phi^{k-1}(b_1^{[k]}), \ldots, \Phi(b_1^{[k]}), b_1^{[k]}, \\ \Phi^{k-1}(b_2^{[k]}), \ldots, \Phi(b_2^{[k]}), b_2^{[k]}, \\ \vdots \\ \Phi^{k-1}(b_{d_k}^{[k]}), \ldots, \Phi(b_{d_k}^{[k]}), b_{d_k}^{[k]} \end{gathered}$$

are linearly independent. Moreover, $\Phi^l(b_i^{[k]}) \in W_{k-l}$, and in particular

$$\Phi(b_1^{[k]}), \ldots, \Phi(b_{d_k}^{[k]})$$

are linearly independent in W_{k-1}. If these elements do not already constitute a basis of W_{k-1}, we can complete them to a basis of W_{k-1} by choosing suitable elements

$$b_1^{[k-1]}, \ldots, b_{s_{k-1}}^{[k-1]},$$

where $s_{k-1} = d_{k-1} - d_k$. It follows from Lemma 2.34, that

$$\Phi^{k-2}(b_i^{[k-1]}), \ldots, \Phi(b_i^{[k-1]}), b_i^{[k-1]}, \quad i = 1, \ldots, s_{k-1}$$

are linearly independent. Proceed in this manner until a basis for V has been constructed according to the following pattern:

$$\begin{array}{r|llllllllll}
W_k & b_1^{[k]} & \cdots & b_{s_k}^{[k]} & & & & & & & \\
W_{k-1} & \Phi(b_1^{[k]}) & \cdots & \Phi(b_{s_k}^{[k]}) & b_1^{[k-1]} & \cdots & b_{s_{k-1}}^{[k-1]} & & & & \\
\vdots & \vdots & & \vdots & \vdots & & \vdots & \ddots & & & \\
W_1 & \Phi^{k-1}(b_1^{[k]}) & \cdots & \Phi^{k-1}(b_{s_k}^{[k]}) & \Phi^{k-2}(b_1^{[k-1]}) & \cdots & \Phi^{k-2}(b_{s_{k-1}}^{[k-1]}) & \cdots & b_1^{[1]} & \cdots & b_{s_1}^{[1]}
\end{array}$$

Here,

$$s_k = d_k \quad \text{und} \quad s_i = d_i - s_{i+1} - s_{i+2} - \ldots - s_k. \tag{2.14}$$

To obtain a **Jordan basis** B for Φ, we order these basis vectors first from bottom to top and then from left to right:

$$\begin{aligned}
B &= \{\Phi^{k-1}(b_1^{[k]}), \ldots, b_1^{[k]}, \ldots, \Phi^{k-1}(b_{s_k}^{[k]}), \ldots, b_{s_k}^{[k]},\ \Phi^{k-2}(b_1^{[k-1]}), \ldots, b_1^{[k-1]},\ \ldots,\ b_1^{[1]}, \ldots, b_{s_1}^{[1]}\} \\
&= B_{b_1^{[k]}} \cup \ldots \cup B_{b_{s_k}^{[k]}} \cup B_{b_1^{[k-1]}} \cup \ldots \cup B_{b_1^{[1]}} \cup \ldots \cup B_{b_{s_1}^{[1]}}.
\end{aligned}$$

Theorem 2.35 *The matrix representation $\varrho_B^B(\Phi)$ of Φ is the Jordan canonical form $J(\Phi)$:*

$$\begin{pmatrix}
J_k(0) & & & & & & & & \\
& \overset{s_k}{\ddots} & & & & & & & \\
& & J_k(0) & & & & & & \\
& & & J_{k-1}(0) & & & & & \\
& & & & \overset{s_{k-1}}{\ddots} & & & & \\
& & & & & J_{k-1}(0) & & & \\
& & & & & & \ddots & & \\
& & & & & & & 0 & \\
& & & & & & & & \overset{s_1}{\ddots} \\
& & & & & & & & & 0
\end{pmatrix} \tag{2.15}$$

This canonical form is unique up to the order of the Jordan boxes.

PROOF: That $\varrho_B^B(\Phi) = J(\Phi)$ holds is an immediate consequence of the preceding construction. Uniqueness (up to order) follows from the fact that the numbers $s_k, \ldots, s_1$ given by (2.14) are uniquely determined by the dimensions of the kernels K^i (as $d_i = \dim W_i = \dim K^j - \dim K^{j-1}$). These kernels are uniquely determined by Φ. $\diamond$

Remark 2.36 As $K^1 = W_1$ is the eigenspace E_0 of Φ for the eigenvalue 0,

$$\begin{aligned}\dim E_0 &= s_k + s_{k-1} + \ldots + s_1 \\ &= \text{number of Jordan boxes in } J(\Phi).\end{aligned}$$

Furthermore, $\Phi^{k-1} \neq 0$, so that at least one Jordan box $J_k(0)$ of size k must appear in $J(\Phi)$. But as $\Phi^k = 0$, there cannot be any larger Jordan box. We can characterise this via the minimal polynomial $h_\Phi = X^k$:

$$\text{size of the largest Jordan box} = k = \deg h_\Phi.$$

As a Corollary of Theorem 2.35 we immediately obtain the corresponding result for nilpotent matrices:

Theorem 2.37 *Every nilpotent matrix $A \in \mathbb{K}^{n\times n}$ is conjugate to a matrix of the form (2.15). The conjugacy class of A is uniquely determined by the numbers $(s_k, s_{k-1}, \ldots, s_1)$. In particular, there are only finitely many conjugacy classes of nilpotent matrices in $\mathbb{K}^{n\times n}$.*

2.6 The Jordan Canonical Form

Now, the moment has come to combine the results of Sections 2.4 and 2.5.

Let V be a $\mathbb{C}$-vector space of dimension n and $\Phi \in \mathrm{End}(V)$. Moreover, let $\lambda_1, \ldots, \lambda_m$ be the distinct eigenvalues of Φ, let $V_{\lambda_1}, \ldots, V_{\lambda_m}$ be their respective generalised eigenspaces and let $\alpha_1, \ldots, \alpha_m$ be their algebraic multiplicities (in particular, $\alpha_i = \dim V_{\lambda_i}$).

By Ψ_j denote the nilpotent endomorphisms (Lemma 2.28)

$$\Psi_j = \Phi|_{V_{\lambda_j}} - \lambda_j \cdot \mathrm{id}_{V_{\lambda_j}}.$$

Theorem 2.38 (Jordan canonical form) *There exists a basis B of V, such that the matrix representation $\varrho_B^B(\Phi)$ of Φ has the following form:*

$$J(\Phi) = \begin{pmatrix} \lambda_1 I_{\alpha_1} + J(\Psi_1) & & \\ & \ddots & \\ & & \lambda_m I_{\alpha_m} + J(\Psi_m) \end{pmatrix} \tag{2.16}$$

This canonical form is unique up to the respective orders of the λ_i and the Jordan boxes within the $J(\Psi_i)$.

PROOF: By Theorem 2.22, the primary decomposition $V = V_{\lambda_1} \oplus \ldots \oplus V_{\lambda_m}$ is uniquely determined (up to order) by the characteristic polynomial's prime factorisation. This decomposition is Φ-invariant, so it is sufficient to consider the restrictions of Φ to the V_{λ_i}. For these,

$$\Phi|_{V_{\lambda_i}} = \lambda_i \cdot \mathrm{id}_{V_{\lambda_i}} + \Psi_i$$

holds. We choose a Jordan basis B_i for this nilpotent endomorphism of V_{λ_i} as in Theorem 2.35. As $\lambda_i \cdot \mathrm{id}_{V_{\lambda_i}}$ is represented by $\lambda_i I_{\alpha_i}$ in any basis, it follows that $\Phi|_{V_{\lambda_i}}$ is represented by the matrix

$$J(\Phi|_{V_{\lambda_i}}) = \lambda_i I_{\alpha_i} + J(\Psi_i)$$

with respect to the basis B_i. By Theorem 2.35, this matrix is unique (up to the order of the Jordan boxes). Then Φ then has the matrix representation (2.16) with respect to the basis $B = B_1 \cup \ldots \cup B_m$ of V. ◇

The basis B in Theorem 2.38 is called a **Jordan basis** of V for Φ.

Remark 2.39 Considering Remark 2.36, we find

$$\begin{aligned}
\dim V_{\lambda_i} &= \text{algebraic multiplicity } \alpha_i = \text{size of the Jordan block for the eigenvalue } \lambda_i, \\
\dim E_{\lambda_i} &= \text{number of Jordan boxes in } J(\Phi) \text{ for the eigenvalue } \lambda_i, \\
\text{exponent } k_i \text{ of } X - \lambda_i \text{ in } h_\Phi &= \text{size of the largest Jordan box for the eigenvalue } \lambda_i.
\end{aligned}$$

We rephrase Theorem 2.38 for complex matrices:

Corollary 2.40 *Every matrix $A \in \mathbb{C}^{n\times n}$ is conjugate to a Jordan canonical form (2.16). The conjugacy class of A is uniquely determined by its Jordan canonical form.*

There are infinitely many possibilites for the eigenvalues of a complex matrix, but for a given eigenvalue, it follows by reduction to the nilpotent case (Theorem 2.37) that there are only finitely many possibilities for the Jordan canonical form of the restriction $\Phi|_{V_{\lambda_i}}$. We thus obtain the following corollary:

Corollary 2.41 *There are infinitely many conjugacy classes of matrices in $\mathbb{C}^{n\times n}$. However, there are only finitely many conjugacy classes of matrices in $\mathbb{C}^{n\times n}$ with the same characteristic polynomial.*

An exhaustive study of conjugacy classes of matrices over arbitrary fields can be found in Sections 11.6 and 11.7 of Brieskorn [2].

Remark 2.42 Diagonal matrices are a special case of Jordan canonical forms. Here, all Jordan boxes are of size 1, and the generalised eigenspaces coincide with the eigenspaces.

Algorithm 2.43 To compute a Jordan basis for Φ, proceed as follows:

(i) Determine the characteristic polynomial f_Φ and its zeros $\lambda_1, \ldots, \lambda_m$, the eigenvalues of Φ.

(ii) For $i = 1, \ldots, m$ execute the following steps:

(ii.a) Determine the smalles number k_i, such that

$$\ker(\Phi - \lambda_i \cdot \mathrm{id}_V)^{k_i} = \ker(\Phi - \lambda_i \cdot \mathrm{id}_V)^{k_i+1}.$$

Then also $\ker(\Phi - \lambda_i \cdot \mathrm{id}_V)^{k_i} = \ker(\Phi - \lambda_i \cdot \mathrm{id}_V)^n = V_{\lambda_i}$ holds. The number k_i is the exponent of $X - \lambda_i$ in the minimal polynomial h_Φ.

If the kernels here are determined via the Gauß Algorithm, for one obtains, for $s = 1, \ldots, k_i$, a basis $B_i^{[s]}$ of $\ker(\Phi - \lambda_i \cdot \mathrm{id}_V)^s$ consisting of elements of degree $\leq s$. In particular, $B_i^{[k_i]}$ is a basis of V_{λ_i} (which in general will not be a Jordan basis). This facilitates the next step.

(ii.b) To begin, let L_i be an empty list of basis vectors.

For $s = k_i, \ldots, 1$ execute the following steps:

As long as there exists a $b \in V_{\lambda_i}$ of degree s which is not contained in the span of the elements so far contained in L_i, compute

$$(\Phi - \lambda_i \cdot \mathrm{id}_V)^j(b), \quad j = s-1, \ldots, 0$$

and add these elements in this order to the list L_i. Otherwise, proceed with degree $s-1$.

In the end, the list L_i contains a Jordan basis of V_{λ_i} for $\Phi|_{V_{\lambda_i}}$.

(iii) Combine the elements of the lists $L_1, \ldots, L_m$ from step (ii) to a basis B, so that B is a Jordan basis for Φ. Obtain the Jordan canonical form as $J(\Phi) = \varrho_B^B(\Phi)$.

If one is only interested in determining $J(\Phi)$ (without the basis), step (ii.b) can be omitted and in step (ii.a) one can determine the number of Jordan boxes of a given size for the eigenvalue λ_i via the differences in the dimensions of the kernels $\ker(\Phi - \lambda_i \cdot \mathrm{id}_V)^j$, $j = 1, \ldots, k_i$.

We now give two examples of matrices A and B which have the same eigenvalues, the same characteristic polynomial and the same minimal polynomial, but nevertheless have distinct Jordan canonical forms.

Example 2.44 Let

$$A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 3 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} \in \mathbb{C}^{4\times 4}.$$

- The characteristic polynomial of A is

  $$f_A = \det(XI_4 - A) = (X-2)^4.$$

  So A has the sole eigenvalue 2 of algebraic multiplicity 4.

- By means of the Gauß Algorithm determine $\ker(A-2\cdot I_4)^j$ for $j = 1, 2, \ldots$ and observe

  $$\ker(A - 2\cdot I_4) \neq \mathbb{C}^4, \quad \ker(A - 2\cdot I_4)^2 = \mathbb{C}^4.$$

  Hence the minimal polynomial is $h_A = (X-2)^2$.

- Choose a vector $b_1^{[2]} \in \mathbb{C}^4 \setminus \ker(A - 2\cdot I_4)$, say $b_1^{[2]} = e_1$. As the first two vectors of the Jordan basis we choose

  $$(A - 2\cdot I_4)\cdot b_1^{[2]} = \begin{pmatrix} -1 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \quad b_1^{[2]} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

  As $\dim\ker(A - 2\cdot I_4)^2 - \dim\ker(A - 2\cdot I_4) = 4 - 3 = 1$, there do not exist any further linearly independent vectors of degree 2.

- Complete the Jordan basis with the linearly independent vectors $b_1^{[1]} = e_3$ and $b_2^{[1]} = e_4$ from $\ker(A - 2\cdot I_4)$. Our Jordan basis for A is thus:

  $$\left\{ \begin{pmatrix} -1 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}.$$

- The Jordan canonical form of A is

  $$J(A) = \left(\begin{array}{cc|cc} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ \hline 0 & 0 & 2 & 0 \\ \hline 0 & 0 & 0 & 2 \end{array}\right). \qquad \heartsuit$$

Example 2.45 Let

$$B = \begin{pmatrix} 9 & -7 & 0 & 2 \\ 7 & -5 & 0 & 2 \\ 4 & -4 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix} \in \mathbb{C}^{4\times 4}.$$

- The characteristic polynomial of B is

  $$f_B = \det(XI_4 - B) = (X-2)^4.$$

  So B has the sole eigenvalue 2 of algebraic multiplicity 4.

- By means of the Gauß Algorithm determine $\ker(B-2\cdot I_4)^j$ for $j = 1, 2, \ldots$ and observe

  $$\ker(B - 2\cdot I_4) \neq \mathbb{C}^4, \quad \ker(B - 2\cdot I_4)^2 = \mathbb{C}^4.$$

  Hence the minimal polynomial is $h_B = (X-2)^2$.

- Choose a vector $b_1^{[2]} \in \mathbb{C}^4 \setminus \ker(B - 2\cdot I_4)$, say $b_1^{[2]} = e_1$. As the first two vectors of the Jordan basis we choose

  $$(B - 2\cdot I_4)\cdot b_1^{[2]} = \begin{pmatrix} 7 \\ 7 \\ 4 \\ 0 \end{pmatrix}, \quad b_1^{[2]} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

  We have $\dim\ker(B - 2\cdot I_4)^2 - \dim\ker(B - 2\cdot I_4) = 4 - 2 = 2$, so we can choose another vector of degree 2 linearly independent to the ones above.

- The vector $b_2^{[2]} = e_4$ is in $\mathbb{C}^4 \setminus \ker(B - 2\cdot I_4)$ as well and clearly linearly independent of the two vectors in the previous step. We complete our Jordan basis by the vectors

  $$(B - 2\cdot I_4)\cdot b_2^{[2]} = \begin{pmatrix} 2 \\ 2 \\ 1 \\ 0 \end{pmatrix}, \quad b_2^{[2]} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

- Hence our Jordan basis for B is:

  $$\left\{ \begin{pmatrix} 7 \\ 7 \\ 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}.$$

- The Jordan canonical form of B is

$$J(B) = \left(\begin{array}{cc|cc} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ \hline 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{array}\right). \qquad \heartsuit$$

Finally, we want to study an example of a Jordan canonical form for a matrix with two different eigenvalues.[7)]

Example 2.46 Let

$$A = \begin{pmatrix} 2 & 0 & -2 & 0 & -1 \\ 0 & 3 & 0 & 0 & 0 \\ -1 & -1 & 1 & 0 & -1 \\ 2 & -2 & 0 & 3 & 2 \\ -1 & 2 & 2 & 0 & 2 \end{pmatrix} \in \mathbb{C}^{5\times 5}.$$

- The characteristic polynomial of A is

$$f_A = \det(XI_5 - A) = (X-1)^2(X-3)^3.$$

  So A has the two eigenvalues $\lambda_1 = 1$ and $\lambda_2 = 3$.

- Firstly, compute a Jordan basis for the generalised eigenspace V_1.

$$A - 1 \cdot I_5 = \begin{pmatrix} 1 & 0 & -2 & 0 & -1 \\ 0 & 2 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & -1 \\ 2 & -2 & 0 & 2 & 2 \\ -1 & 2 & 2 & 0 & 1 \end{pmatrix}, \quad \text{rank } 4.$$

  This means the eigenspace is of dimension $\dim E_1 = 1$, and by recalling Remark 2.39 we already know that $\dim V_1 = \alpha_1 = 2$. To determine a Jordan basis, we need to find a vector in $\ker(A - 1 \cdot I_5)^2 \setminus \ker(A - 1 \cdot I_5)$:

$$(A - 1 \cdot I_5)^2 = \begin{pmatrix} 4 & 0 & -4 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & -4 & 0 & 0 & 0 \\ 4 & -4 & 0 & 4 & 4 \\ -4 & 4 & 4 & 0 & 0 \end{pmatrix}, \quad \text{rank } 3,$$

[7)] To avoid "death by notation" in the following example, we slightly deviate from the previous notation for Jordan basis vectors and simply list them in order of appearence as $b_1(\lambda), b_2(\lambda), \ldots$ for any given eigenvalue λ of A.

so

$$\ker(A - 1 \cdot I_5)^2 = \operatorname{span}\left\{ \begin{pmatrix} -1 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ -1 \\ 0 \\ 1 \end{pmatrix} \right\}.$$

Set

$$b_2(1) = \begin{pmatrix} -1 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix} \in \ker(A - 1 \cdot I_5)^2 \setminus \ker(A - 1 \cdot I_5)$$

and

$$b_1(1) = (A - 1 \cdot I_5) \cdot b_2(1) = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ -1 \end{pmatrix}.$$

We now have a Jordan basis for V_1,

$$B_1 = \{b_1(1), b_2(1)\} = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix} \right\}.$$

- Next, we determine a Jordan basis for the generalised eigenspace V_3.

$$A - 3 \cdot I_5 = \begin{pmatrix} -1 & 0 & -2 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & -2 & 0 & -1 \\ 2 & -2 & 0 & 0 & 2 \\ -1 & 2 & 2 & 0 & -1 \end{pmatrix}, \quad \text{rank } 3.$$

Again, the eigenspace is only of dimension $\dim E_3 = 1$, and the dimension of V_3 is now $\dim V_3 = \alpha_3 = 3$. Determine $\ker(A - 3 \cdot I_5)^3$ first:

$$(A - 3 \cdot I_5)^2 = \begin{pmatrix} 4 & 0 & 4 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 4 & 0 & 4 \\ -4 & 4 & 0 & 0 & -4 \\ 0 & -4 & -4 & 0 & 0 \end{pmatrix}, \quad \text{rank } 2,$$

$$(A - 3 \cdot I_5)^3 = \begin{pmatrix} -12 & 4 & -8 & 0 & -12 \\ 0 & 0 & 0 & 0 & 0 \\ -12 & 4 & -8 & 0 & -12 \\ 8 & -8 & 0 & 0 & 8 \\ 4 & 4 & 8 & 0 & 4 \end{pmatrix}, \quad \text{rank } 2.$$

As the rank did not change in the last step, it holds that

$$V_3 = \ker(A - 3 \cdot I_5)^2 = \ker(A - 3 \cdot I_5)^3,$$

and a basis of V_3 is given by

$$\ker(A - 3 \cdot I_5)^2 = \operatorname{span}\left\{ \begin{pmatrix} -1 \\ -1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}.$$

Set

$$b_2(3) = \begin{pmatrix} -1 \\ -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \in \ker(A - 3 \cdot I_5)^2 \setminus \ker(A - 3 \cdot I_5),$$

and

$$b_1(3) = (A - 3 \cdot I_5) \cdot b_2(3) = \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

As $\dim V_3 = 3$, one basis vector is still missing. Choose a second eigenvector linearly independent of $b_1(3)$:

$$b_3(3) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \in \ker(A - 3 \cdot I_5)$$

So a Jordan basis of V_3 is given by

$$B_3 = \{b_1(3), b_2(3), b_3(3)\} = \left\{ \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \right\}.$$

- Finally, combine the bases B_1 and B_3 to obtain a Jordan basis of $\mathbb{C}^5$ for A:

$$B = B_1 \cup B_3 = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \right\}.$$

The matrix for the base change from the Jordan basis B to the canonical basis of $\mathbb{C}^5$ is given by

$$S = \begin{pmatrix} 1 & -1 & -1 & -1 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 1 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ -1 & 0 & 1 & 0 & 0 \end{pmatrix},$$

and the Jordan canonical form of A is

$$J(A) = S^{-1} \cdot A \cdot S = \left(\begin{array}{cc|ccc} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 3 & 1 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{array}\right) = \hat{J}_{(2)}(1) \oplus \hat{J}_{(2,1)}(3). \quad \heartsuit$$

2.7 The Jordan Decomposition

For an endomorphism Φ of an n-dimensional $\mathbb{C}$-vector space V we already noted in Section 2.3 that its Jordan canonical form decomposes as a sum

$$J(\Phi) = D + N,$$

where D is a diagonal matrix with the eigenvalues of Φ on the diagonal, and N is a nilpotent upper triangular matrix. As $J(\Phi)$ represents Φ in a Jordan basis, the matrices D and N represent a diagonalisable endomorphism Φ_d and a nilpotent endomorphism Φ_n in the same Jordan basis, respectively. In this section, we will study these endomorphisms.

Lemma 2.47 *Let $\Phi_\mathrm{n}, \Psi_\mathrm{n} \in \mathrm{End}(V)$ be nilpotent endomorphisms, and assume that $\Phi_\mathrm{n} \circ \Psi_\mathrm{n} = \Psi_\mathrm{n} \circ \Phi_\mathrm{n}$ holds. Then $\lambda\Phi_\mathrm{n} + \mu\Psi_\mathrm{n}$ is also nilpotent for any $\lambda, \mu \in \mathbb{C}$.*

PROOF: Let m be the maximum of the degrees of nilpotency of Φ_n and Ψ_n. Because Φ_n and Ψ_n commute, we can make use of the binomial formula to evaluate

the following expression:

$$(\lambda\Phi_{\mathrm{n}} + \mu\Psi_{\mathrm{n}})^{2m} = \sum_{j=1}^{2m} \binom{2m}{j} \lambda^{2m-j}\mu^j \Phi_{\mathrm{n}}^{2m-j} \circ \Psi^j.$$

In each summand, one of the powers Φ_{n}^{2m-j} or Ψ_{n}^{j} has exponent $\geq m$ and thus equals 0. So

$$(\lambda\Phi_{\mathrm{n}} + \mu\Psi_{\mathrm{n}})^{2m} = 0$$

and $\lambda\Phi_{\mathrm{n}} + \mu\Psi_{\mathrm{n}}$ is nilpotent of degree $\leq 2m$. ◇

Lemma 2.48 *Let $\Phi_{\mathrm{d}}, \Psi_{\mathrm{d}} \in \mathrm{End}(V)$ be diagonalisable endomorphisms, and assume that $\Phi_{\mathrm{d}} \circ \Psi_{\mathrm{d}} = \Psi_{\mathrm{d}} \circ \Phi_{\mathrm{d}}$ holds. Then Φ_{d} and Ψ_{d} are simultaneously diagonalisable (meaning there exists a basis B of V such that both are represented by diagonal matrices in this basis B). In particular, $\lambda\Phi_{\mathrm{d}} + \mu\Psi_{\mathrm{d}}$ is diagonalisable for any $\lambda, \mu \in \mathbb{C}$.*

PROOF: The proof is by induction on $n = \dim V$. For $n = 1$, all endomorphisms are diagonalisable.

So now assume $n > 1$. Let

$$V = E_{\lambda_1}(\Phi_{\mathrm{d}}) \oplus \ldots \oplus E_{\lambda_k}(\Phi_{\mathrm{d}})$$

be the eigenspace decomposition for Φ_{d}. Because Φ_{d} and Ψ_{d} commute, we find for every eigenvector $v_i \in E_{\lambda_i}(\Phi_{\mathrm{d}})$ that

$$\Phi_{\mathrm{d}}(\Psi_{\mathrm{d}}(v_i)) = \Psi_{\mathrm{d}}(\Phi_{\mathrm{d}}(v_i)) = \lambda_i \cdot \Psi_{\mathrm{d}}(v_i),$$

that is, $\Psi_{\mathrm{d}}(v_i)$ is again an eigenvector for the eigenvalue λ_i. So the eigenspaces $E_{\lambda_i}(\Phi_{\mathrm{d}})$ are Ψ_{d}-invariant. If $\dim E_{\lambda_i}(\Phi_{\mathrm{d}}) = n$, then $\Phi_{\mathrm{d}} = \lambda_i \cdot \mathrm{id}_V$, so that Φ_{d} is represented by a diagonal matrix in any basis B of V. Choose B such that Ψ_{d} is represented by a diagonal matrix, and the claim follows. If $\dim E_{\lambda_i}(\Phi_{\mathrm{d}}) < n$, then by the induction hypthesis, the restrictions of $\Phi_{\mathrm{d}}|_{E_{\lambda_i}(\Phi_{\mathrm{d}})}$ and $\Psi_{\mathrm{d}}|_{E_{\lambda_i}(\Phi_{\mathrm{d}})}$ are represented by diagonal matrices in some basis B_i of $E_{\lambda_i}(\Phi_{\mathrm{d}})$. Then the union $B = B_1 \cup \ldots \cup B_k$ is a basis of V such that Φ_{d} and Ψ_{d} are both represented by diagonal matrices in B.

For the last statement note that any linear combination of diagonal matrices is again a diagonal matrix, so $\lambda\Phi_{\mathrm{d}} + \mu\Psi_{\mathrm{d}}$ is diagonalisable. ◇

In the following, let V be an n-dimensional $\mathbb{C}$-vector space.

Theorem 2.49 (Jordan decomposition) *For an endomorphism $\Phi \in \mathrm{End}(V)$ there exist polynomials $p_\mathrm{d}, p_\mathrm{n} \in \mathbb{C}[X]$ such that $p_\mathrm{d}(\Phi) = \Phi_\mathrm{d}$ is a diagonalisable endomorphism, $p_\mathrm{n}(\Phi) = \Phi_\mathrm{n}$ is a nilpotent endomorphism, $\Phi_\mathrm{d} \circ \Phi_\mathrm{n} = \Phi_\mathrm{n} \circ \Phi_\mathrm{d}$, and*

$$\Phi = \Phi_\mathrm{d} + \Phi_\mathrm{n} \tag{2.17}$$

holds. Moreover, Φ_d and Φ_n are uniquely determined by these properties.

PROOF: To construct the polynomial p_d, consider the following system of congruences in the ring $\mathbb{C}[X]$:

$$\begin{aligned} p_\mathrm{d} &\equiv \lambda_1 \bmod (X-\lambda_1)^{\alpha_1}, \\ &\vdots \\ p_\mathrm{d} &\equiv \lambda_k \bmod (X-\lambda_k)^{\alpha_k}, \end{aligned}$$

where $\lambda_1, \ldots, \lambda_k$ are the distinct eigenvalues of Φ with algebraic multiplicities $\alpha_1, \ldots, \alpha_k$. The polynomials $(X-\lambda_i)^{\alpha_i}$ are coprime for distinct λ_i, so this system of congruences has a solution according to the Chinese Remainder Theorem 1.57. By construction, such a solution p_d satisfies

$$p_\mathrm{d} = \lambda_j + q_j \cdot (X-\lambda_j)^{\alpha_j}$$

for a suitable polynomial $q_j \in \mathbb{C}[X]$, and hence

$$p_\mathrm{d}(\Phi)(v_j) = \lambda_j \cdot v_j + q_j(\Phi)(v_j)(\Phi - \lambda_j \cdot \mathrm{id}_V)^{\alpha_j}(v_j)$$

for every v_j in the generalised eigenspace V_{λ_j} of Φ. Recall from the definition of V_{λ_j} that $(\Phi - \lambda_j \cdot \mathrm{id}_V)^{\alpha_j}(v_j) = 0$, so that

$$p_\mathrm{d}(\Phi)(v_j) = \lambda_j \cdot v_j$$

for all j. In other words, $V_{\lambda_j} = E_{\lambda_j}(p_\mathrm{d}(\Phi))$, so that

$$V = E_{\lambda_1}(\Phi_\mathrm{d}) \oplus \ldots \oplus E_{\lambda_k}(\Phi_\mathrm{d})$$

is decomposition into eigenspaces of $\Phi_\mathrm{d} = p_\mathrm{d}(\Phi)$, so Φ_d is diagonalisable.

Now set

$$p_\mathrm{n} = X - p_\mathrm{d},$$

and $p_\mathrm{n}(\Phi) = \Phi - \Phi_\mathrm{d} = \Phi_\mathrm{n}$. Clearly, $\Phi = \Phi_\mathrm{d} + \Phi_\mathrm{n}$ holds. Since powers of Φ commute,

$$\Phi_\mathrm{d} \circ \Phi_\mathrm{n} = p_\mathrm{d}(\Phi) \circ p_\mathrm{n}(\Phi) = p_\mathrm{n}(\Phi) \circ p_\mathrm{d}(\Phi) = \Phi_\mathrm{n} \circ \Phi_\mathrm{d}.$$

We show that Φ_n is nilpotent: By construction of Φ_n, the generalised eigenspaces V_{λ_i} of Φ are Φ_n-invariant, and Φ_n restricted to V_{λ_i} is

$$\Phi_\mathrm{n}|_{V_{\lambda_i}} = \Phi|_{V_{\lambda_i}} - \Phi_\mathrm{d}|_{V_{\lambda_i}} = \Phi|_{V_{\lambda_i}} - \lambda_i \cdot \mathrm{id}_{V_{\lambda_i}}.$$

Recall that this means $(\Phi_\mathrm{n}|_{V_{\lambda_i}})^{\alpha_j} = 0$, and since V is the direct sum of the V_{λ_i} it follows that $\Phi_\mathrm{n}^{\max\{\alpha_1,\ldots,\alpha_k\}} = 0$ and Φ_n is nilpotent.

It remains to prove the uniqueness of Φ_d and Φ_n. So let Ψ_d and Ψ_n be two endomorphisms satisfying the conditions of Theorem 2.49. Then

$$\Phi_\mathrm{d} + \Phi_\mathrm{n} = \Phi = \Psi_\mathrm{d} + \Psi_\mathrm{n},$$

or

$$\Phi_\mathrm{d} - \Psi_\mathrm{d} = \Psi_\mathrm{n} - \Phi_\mathrm{n}.$$

By Lemma 2.47, $\Psi_\mathrm{n} - \Phi_\mathrm{n}$ is nilpotent and by Lemma 2.48, $\Phi_\mathrm{d} - \Psi_\mathrm{d}$ is diagonalisable. So the two can only coincide if both equal 0. This means $\Phi_\mathrm{d} = \Psi_\mathrm{d}$ and $\Phi_\mathrm{n} = \Psi_\mathrm{n}$, proving the uniqueness. ◇

The following corollary is the matrix version of Theorem 2.49:

Corollary 2.50 *For $A \in \mathbb{C}^{n\times n}$ there exist polynomials $p_\mathrm{d}, p_\mathrm{n} \in \mathbb{C}[X]$ such that $p_\mathrm{d}(A) = A_\mathrm{d}$ is diagonalisable, $p_\mathrm{n}(A) = A_\mathrm{n}$ is nilpotent, $A_\mathrm{d}A_\mathrm{n} = A_\mathrm{n}A_\mathrm{d}$, and*

$$A = A_\mathrm{d} + A_\mathrm{n} \tag{2.18}$$

holds. Moreover, A_d and A_n are uniquely determined by these properties.

The proof of Theorem 2.49 shows that to compute the Jordan decomposition, one needs to know the eigenvalues of Φ (or A, respectively) and an algorithm to solve a system of simultaneous congruences as given in Section 1.5. Computing a Jordan basis also gives the Jordan decomposition, but it does not yield the polynomials p_d and p_n.

Example 2.51 Consider the matrix

$$A = \begin{pmatrix} 2 & 0 & -2 & 0 & -1 \\ 0 & 3 & 0 & 0 & 0 \\ -1 & -1 & 1 & 0 & -1 \\ 2 & -2 & 0 & 3 & 2 \\ -1 & 2 & 2 & 0 & 2 \end{pmatrix} \in \mathbb{C}^{5\times 5}.$$

From Example 2.46 we know that A has the eigenvalues $\lambda_1 = 1$ with multiplicity $\alpha_1 = 2$ and $\lambda_2 = 3$ with multiplicity $\alpha_2 = 3$.

We find the polynomial p_{d} as solution to the simultaneous congruences

$$p_{\mathrm{d}} \equiv 1 \bmod (X-1)^2,$$
$$p_{\mathrm{d}} \equiv 3 \bmod (X-3)^3.$$

The solution computed via Algorithm 1.59 is

$$p_{\mathrm{d}} = \frac{3}{8}X^4 - \frac{7}{2}X^3 + \frac{45}{4}X^2 - \frac{27}{2}X + \frac{51}{8}.$$

Then

$$p_{\mathrm{n}} = -\frac{3}{8}X^4 + \frac{7}{2}X^3 - \frac{45}{4}X^2 + \frac{29}{2}X - \frac{51}{8},$$

and

$$p_{\mathrm{d}}(A) = \begin{pmatrix} 3 & -2 & -2 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & -2 & 1 & 0 & 0 \\ 2 & -2 & 0 & 3 & 2 \\ -2 & 4 & 2 & 0 & 1 \end{pmatrix}, \quad p_{\mathrm{n}}(A) = \begin{pmatrix} -1 & 2 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 1 \end{pmatrix}$$

is the Jordan decomposition of A. ♡

For invertible Φ, there exists also a multiplicative version of the Jordan decomposition.

Definition 2.52 An endomorphism $\Phi \in \mathrm{End}(V)$ is called **unipotent** if the endomorphism $\Phi - \mathrm{id}_V$ is nilpotent. Accordingly, a matrix $A \in \mathbb{K}^{n\times n}$ is called unipotent if $A - I_n$ is nilpotent.

Theorem 2.53 (Multiplicative Jordan decomposition) *For an automorphism Φ of V there exists a diagonalisable automorphism Φ_{d} and a unipotent automorphism Φ_{u} such that*

$$\Phi = \Phi_{\mathrm{d}} \circ \Phi_{\mathrm{u}} \tag{2.19}$$

and $\Phi_{\mathrm{d}} \circ \Phi_{\mathrm{u}} = \Phi_{\mathrm{u}} \circ \Phi_{\mathrm{d}}$. Moreover, Φ_{d} and Φ_{u} are uniquely determined by these properties.

PROOF: Let Φ_{d}, Φ_{n} be as in Theorem 2.49. As Φ is invertible, all its eigenvalues are different from 0, and as Φ_{d} has the same eigenvalues as Φ, it is also invertible. So we can write

$$\Phi = \Phi_{\mathrm{d}} + \Phi_{\mathrm{n}} = \Phi_{\mathrm{d}} \circ (\mathrm{id}_V + \Phi_{\mathrm{d}}^{-1} \circ \Phi_{\mathrm{n}}).$$

Set $\Phi_u = \mathrm{id}_V + \Phi_d^{-1} \circ \Phi_n$. Proving that Φ_u is unipotent now amounts to proving that $\Phi_d^{-1} \circ \Phi_n$ is nilpotent. Let m be the degree of nilpotency of Φ_n. As Φ_d and Φ_n commute,

$$(\Phi_d^{-1} \circ \Phi_n)^m = (\Phi_d^{-1})^m \circ \Phi_n^m = 0$$

and therefore Φ_u is unipotent.

To see the uniqueness, observe that from any pair Φ_d, Φ_u satisfying the properties in the theorem the Jordan decomposition $\Phi = \Phi_d + \Phi_n$ can be reconstructed by setting $\Phi_n = \Phi_d \circ (\Phi_u - \mathrm{id}_V)$. Thus uniqueness of the pair Φ_d, Φ_u follows from the uniqueness of Φ_d, Φ_n. ◇

Corollary 2.54 *For a matrix $A \in \mathbf{GL}_n(\mathbb{C})$ there exists a diagonalisable matrix $A_d \in \mathbf{GL}_n(\mathbb{C})$ and a unipotent matrix $A_u \in \mathbf{GL}_n(\mathbb{C})$ such that*

$$A = A_d \cdot A_u \tag{2.20}$$

and $A_d \cdot A_u = A_u \cdot A_d$. Moreover, A_d and A_u are uniquely determined by these properties.

So far we studied the Jordan canonical form for a matrix A or an endomorphism Φ defined over the field $\mathbb{C}$. This was necessary because we needed the primary decomposition into generalised eigenspaces in Theorem 2.27 to derive the Jordan canonical form. Naturally, one wants to know in how far these results hold if A or Φ is defined over some subfield $\mathbb{K}$ of $\mathbb{C}$, such as $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{R}$.

By going through the arguments leading up to Theorem 2.27, one finds that this primary decomposition also exists for a $\mathbb{K}$-vector space provided all eigenvalues of A or Φ are elements of $\mathbb{K}$. So in this case, Theorem 2.38 and Corollary 2.40 hold for Φ and A, respectively. But if the eigenvalues.....

2.8 The Real Canonical Form

NOT YET WRITTEN

2.9 The General Canonical Form

NOT YET WRITTEN

Part II
Applications: Codes and Chiphers

The philosophers have only interpreted the world in various ways;
the point, however, is to change it.
– KARL MARX

3 Cryptography

Alice wants to send a secret message `m` to Bob. However, she cannot be sure that the channel on which `m` is to be sent is safe from eavesdropping. Therefore, she has to devise a method to encrypt her message in such a way that only Bob can decrypt and read it. The art of constructing and investigating such methods is known as **cryptography**. More precisely, one studies the following situation: Given is a set $\mathcal{M}$ of "plaintext" messages which are to be mapped to a set of "ciphertexts" $\mathcal{C}$ by means of an encryption function

$$\text{enc} : \mathcal{M} \to \mathcal{C}.$$

The code $\mathcal{C}$ is supposed to unreadable for anyone without the proper authorisation. A legitimate recipient of a message on the other hand should be able to use a decryption function

$$\text{dec} : \mathcal{C} \to \mathcal{M}$$

to obtain the original plaintext from the ciphertext. That is,

$$\text{dec} \circ \text{enc} = \text{id}_{\mathcal{M}}$$

holds. One possibility to achieve this is for Alice and Bob to use procedure enc and dec which they keep as a secret among themselves. However, the problems with this approach are obvious: Once the methods become known via betrayel or negligence, they become worthless. Moreover, for each additional participant in the communication, a new method would have to be devised. It is therefore the philosophy of **public key cryptography** to employ publically known algorithms whose security relies on an additional parameter, the **key**. Every party involved has its own key. The key consists of two components, the **public key** for encryption and the **secret key** for decryption.

Most algorithms in public key cryptography exploit the algebraic properties of the integer numbers (or other integral domains) in some ingenious way. In this

section, we want to explore some simple cryptographic procedures which can be easily understood based on the knowledge acquired in the previous chapters. To begin, we study some properties of finite groups and the units in $\mathbb{Z}/n\mathbb{Z}$.

In this section we follow the convention that data which are to be kept secret are set in typewriter font $\mathtt{m}, \mathtt{k}, \ldots$.

3.1 Lagrange's Theorem

PUT THIS IN A SEPARATE CHAPTER

Definition 3.1 Let G be a group and $g \in G$. The **order of G** is

$$\operatorname{ord}(G) = |G|.$$

The **order of g** is

$$\operatorname{ord}(g) = \operatorname{ord}(\langle g \rangle),$$

that is, the order of the cyclic subgroup $\langle g \rangle = \{1, g, g^2, g^3, \ldots\}$ generated by g.

Theorem 3.2 (Lagrange) *If G is a finite group and H a subgroup of G, then*

$$\operatorname{ord}(H) \mid \operatorname{ord}(G).$$

In particular, $\operatorname{ord}(g) \mid \operatorname{ord}(G)$ *for all $g \in G$.*

PROOF: For every $g \in G$ it holds that $|H| = |gH|$, as $H \to gH$, $h \mapsto gh$ is a bijection.

For $g_1, g_2 \in G$ either $g_1 H = g_2 H$ holds, or $g_1 H \cap g_2 H = \emptyset$: If there exists $a \in g_1 H \cap g_2 H$, then $g_1 h_1 = a = g_2 h_2$ for suitable $h_1, h_2 \in H$. This means $g_1 = g_2 h_2 h_1^{-1}$. Then every element $g_1 h \in g_1 H$ can be written as

$$g_1 h = g_2 (h_2 h_1^{-1} h) \in g_2 H.$$

Hence $g_1 H \subset g_2 H$ and analogously $g_2 H \subset g_1 H$, so that $g_1 H = g_2 H$.

As every element $g \in G$ is contained in some gH, it follows that G is the disjoint union of certain finite subsets $g_1 H, \ldots, g_k H$. Hence

$$|G| = \Big|\bigcup_{j=1}^{k} g_j H\Big| = \sum_{j=1}^{k} |g_j H| = k|H|,$$

that is, $|H|$ divides $|G|$. ◇

Lemma 3.3 *Let G be an abelian group and $g, h \in G$. Moreover, let* $\operatorname{ord}(g) = m$, $\operatorname{ord}(h) = n$ *and* $\gcd(m, n) = 1$. *Then* $\operatorname{ord}(gh) = mn$.

PROOF: Assume $r = \operatorname{ord}(gh)$. As G is abelian,

$$(gh)^{mn} = (g^m)^n (h^n)^m = 1 \cdot 1 = 1,$$

that is, $r \leq mn$. By Corollary 1.30 there exist $s, t \in \mathbb{Z}$ such that $sm + tn = 1$. This means

$$g^r = (g^{sm+tn})^r = (\underbrace{g^m}_{=1})^{sr} (g^n)^{tr} = (g^n)^{tr} = (g^n h^n)^{tr} = ((gh)^r)^{tn} = 1.$$

So m divides r, and in the same way one shows that n divides r. Now $\gcd(m, n) = 1$ and the uniqueness of prime factorisation imply that mn is a divisor of r, in particular $mn \leq r$. Hence $mn = r$. ◇

Lemma 3.4 *Let G be a finite abelian group and $g \in G$ an element of maximal order $m = \operatorname{ord}(g)$. Then the order* $\operatorname{ord}(h)$ *of any $h \in G$ divides m.*

PROOF: Let $n = \operatorname{ord}(h)$. Assume $n \nmid m$. Then there exists a prime factor p appearing in the factorisation of n with a larger exponent than in the factorisation of m, say

$$m = p^r a, \quad n = p^s b$$

with $r < s$ and $p \nmid a, b$. This means $\operatorname{ord}(g^{p^r}) = a$ and $\operatorname{ord}(h^b) = p^s$. As $\gcd(p^s, a) = 1$, Lemma 3.3 gives $\operatorname{ord}(g^{p^r} h^b) = p^s a$. But $p^s a > p^r a = m$, so that $g^{p^r} h^b$ has a higher order than g, contradicting our choice of g. ◇

3.2 Units in $\mathbb{Z}/n\mathbb{Z}$

Theorem 3.5 *The group of units in $\mathbb{Z}/n\mathbb{Z}$ is*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{k} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(k, n) = 1\}. \tag{3.1}$$

PROOF: If k and n are coprime, then by Lemma 1.30 ther exist elements $s, t \in \mathbb{Z}$ such that $sk + tn = 1$. This means

$$sk \equiv 1 \bmod n.$$

Hence $\overline{k} = \overline{s}^{-1}$ is a unit.

Conversely, if $sk \equiv 1 \bmod n$ for some suitable $s \in \mathbb{Z}$, then $sk = 1 + mn$ for some $m \in \mathbb{Z}$. If d divides k and n, say $ad = k$ and $bd = n$, then $sad = 1 + mbd$. This is equivalent to

$$1 = (sa - mb)d.$$

Hence $d \in \mathbb{Z}^\times = \{-1, 1\}$ and as a consequence k, n are coprime. ◇

Definition 3.6 The function

$$\varphi : \mathbb{N} \to \mathbb{N}, \quad n \mapsto |(\mathbb{Z}/n\mathbb{Z})^\times| \tag{3.2}$$

is called **Euler's totient function** (or **Euler's φ function**).

By Theorem 3.5, $\varphi(n)$ is the number of integers $0 < k < n$ coprime to n.

Theorem 3.7 (Euler) *Let $n \in \mathbb{N}$, $n \geq 2$. For every number a coprime to n,*

$$a^{\varphi(n)} \equiv 1 \bmod n. \tag{3.3}$$

PROOF: If $\gcd(a, n) = 1$, then $\overline{a}$ is a unit in $\mathbb{Z}/n\mathbb{Z}$. We have $\operatorname{ord}((\mathbb{Z}/n\mathbb{Z})^\times) = \varphi(n)$ and therefore there exists a $k \in \mathbb{N}$ with $k \cdot \operatorname{ord}(\overline{a}) = \varphi(n)$ by Lagrange's Theorem. This means

$$\overline{a}^{\varphi(n)} = (\overline{a}^{\operatorname{ord}(\overline{a})})^k = 1^k = 1,$$

which is equivalent to (3.3). ◇

A special case of Euler's Theorem is known as *Fermat's Theorem*.

Theorem 3.8 (Fermat) *Let p be a prime number. Then for all $a \in \mathbb{Z}$ which are not multiples of p,*

$$a^{p-1} \equiv 1 \bmod p. \tag{3.4}$$

Remark 3.9 Fermat's Theorem allows us to test if q is *not* a prime number. For if (3.4) is not satisfied for any $0 < a < q$, then q is not prime. However, it is not valid to make the converse conclusion that q is prime if (3.4) holds for all $0 < a < q$. There are numbers satisfying this without being prime numbers, called **Carmichael numbers**. The three smallest Carmichael numbers are 561, 1105 and 1729. In Forster [5] the properties of Carmichael numbers and some effective primality tests are discussed.

Theorem 3.10 below is of fundamental importance in cryptography.

Theorem 3.10 *If p is prime, then $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.*

PROOF: As p is prime, $\mathbb{Z}/p\mathbb{Z}$ is a field and $(\mathbb{Z}/p\mathbb{Z})^\times$ has $p-1$ elements.

Let g be an element of maximal order $m \leq p-1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Then g is a zero of the polynomial $X^m - 1$. As a consequence of Lemma 3.4,

$$a^m = 1$$

holds for all $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, so that all the other $p-1$ elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ are zeros of $X^m - 1$ as well. By Theorem 1.39,

$$m = \deg(X^m - 1) \geq p - 1$$

holds. Therefore, $m = p - 1$ and $\langle g \rangle = (\mathbb{Z}/p\mathbb{Z})^\times$. ◇

3.3 Diffie-Hellman Key Exchange

Alice and Bob wish to exchange a common key $\mathtt{k}$ via an unsafe channel. To this end, they need to exchange a "partial key" via this channel from which $\mathtt{k}$ can be generated. They can proceed as follows:

Algorithm 3.11 (Diffie-Hellman protocol) Let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$, where p is some large prime number.

(i) Alice picks a secret random number $\mathtt{a}$ and sends $g^{\mathtt{a}}$ to Bob.

(ii) Bob picks a secret random number $\mathtt{b}$ and sends $g^{\mathtt{b}}$ to Alice.

(iii) Alice receives $g^{\mathtt{b}}$ and computes $\mathtt{k} = (g^{\mathtt{b}})^{\mathtt{a}}$.

(iv) Bob receives $g^{\mathtt{a}}$ and computes $\mathtt{k} = (g^{\mathtt{a}})^{\mathtt{b}}$.

So Alice and Bob generated the common key $\mathtt{k}$, which was not transmitted via the unsafe channel.

Remark 3.12 The security of the method relies on the difficulty of computing the discrete logarithm in $(\mathbb{Z}/p\mathbb{Z})^\times$ (for this, a very large p is to be chosen). An attacker could use the discrete logarithm to obtain $\mathtt{a}$ and $\mathtt{b}$ from the intercepted partial keys $g^{\mathtt{a}}$ and $g^{\mathtt{b}}$, and then compute $\mathtt{k}$. An algorithm to compute discrete logarithms in cyclic groups is introduced in §8 of Forster [5].

Remark 3.13 In principle, the Diffie-Hellman protocol works with any finite cyclic group, such as elliptic curves (Forster [5], §20).

3.4 ElGamal Encryption

An idea similar to the Diffi-Hellman protocol is the basis of ElGamal's encryption method. For simplicity we assume that the set of plaintexts is $\mathcal{M} = (\mathbb{Z}/p\mathbb{Z})^\times$ and the set of ciphertexts is $\mathcal{C} = (\mathbb{Z}/p\mathbb{Z})^\times$ as well.

Algorithm 3.14 (ElGamal encryption) Alice wants to send a secret message $\mathtt{m}$ to Bob. Let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$, where p is a large prime number.

(i) Bob picks a secret random number $\mathtt{b}$ (the secret key) and computes $x = g^{\mathtt{b}}$ (the public key).

(ii) Alice picks a secret random number $\mathtt{a}$ satisfying $\gcd(\mathtt{a}, p-1) = 1$.

(iii) Alice computes $y = g^{\mathtt{a}}$ and $z = x^{\mathtt{a}}\mathtt{m}$, and sends (y, z) to Bob.

(iv) Bob can use his secret key $\mathtt{b}$ to decrypt the message:

$$z(y^{\mathtt{b}})^{-1} = z((g^{\mathtt{a}})^{\mathtt{b}})^{-1} = z(g^{\mathtt{ab}})^{-1} = x^{\mathtt{a}}\mathtt{m}(x^{\mathtt{a}})^{-1} = \mathtt{m}.$$

Again, the security of the method relies on the difficulty of computing discrete logarithms. The condition $\gcd(\mathtt{a}, p-1) = 1$ is not required for the method to work. However, if $\mathtt{a}$ and $p-1$ had a large common divisor the computation of the discrete logarithm of $g^{\mathtt{a}}$ would become significantly easier.

3.5 RSA Encryption

The RSA algorithm is named after its inventors Rivest, Shamir and Adleman.

Exercise 3.15 For prime numbers $p, q \in \mathbb{N}$, $\varphi(pq) = (p-1)(q-1)$ holds.

Algorithm 3.16 (RSA encryption) Alice will eine Nachricht $\mathtt{m}$ an Bob schicken.

(i) Bob picks two secret large prime numbers $\mathtt{p}, \mathtt{q}$ and publishes $n = \mathtt{pq}$.

(ii) Bob picks a number e coprime to $\varphi(n)$ (the public key). By means of the Extended Euclidean Algorithm he determines a number $\mathtt{d}$ (the secret key) satisfying $e\mathtt{d} \equiv 1 \bmod \varphi(n)$.

(iii) Alice can encrypt a message $\mathtt{m} \in \mathbb{Z}/n\mathbb{Z}$ by means of the public data as follows:

$$\mathrm{enc} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad \mathtt{m} \mapsto \mathtt{m}^e.$$

She then sends this encrypted message $\mathtt{m}^e$ to Bob.

(iv) Bob can decrypt the ciphertext $\mathtt{m}^e$ by means of his secret key $\mathtt{d}$:

$$\mathrm{dec} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto x^{\mathtt{d}}.$$

Then $\mathrm{dec}(\mathtt{m}^e) = \mathtt{m}^{e\mathtt{d}} = \mathtt{m}$.

PROOF: We need to show that the statement in step (iv) is true.

Let $x \in \mathbb{Z}/n\mathbb{Z}$. According to the Chinese Remainder Theorem there exists an isomorphism

$$\Psi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/\mathtt{p}\mathbb{Z} \times \mathbb{Z}/\mathtt{q}\mathbb{Z}.$$

Now let $(x_1, x_2) = \Psi(x)$. If $x_1 = 0$, then trivially $x_1^{e\mathtt{d}} = x_1$. If $x_1 \neq 0$, then x_1 is a unit in $\mathbb{Z}/\mathtt{p}\mathbb{Z}$. By Exercise 3.15, $\varphi(n) = (\mathtt{p}-1)(\mathtt{q}-1)$, and hence also $e\mathtt{d} \equiv 1 \bmod \mathtt{p}-1$ and $e\mathtt{d} \equiv 1 \bmod \mathtt{q}-1$. Moreover, $\varphi(\mathtt{p}) = \mathtt{p}-1$, so that it follows from Euler's Theorem that

$$x_1^{e\mathtt{d}} = x_1^{1+k\varphi(\mathtt{p})} = x_1.$$

Analogously, $x_2^{e\mathtt{d}} = x_2$. This means

$$(x_1, x_2)^{e\mathtt{d}} = (x_1^{e\mathtt{d}}, x_2^{e\mathtt{d}}) = (x_1, x_2),$$

and hence

$$x^{e\mathtt{d}} = \Psi^{-1}((x_1, x_2)^{e\mathtt{d}}) = \Psi^{-1}(x_1, x_2) = x.$$

This proves $\mathrm{dec} \circ \mathrm{enc} = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$. ◇

One might wonder why the proof takes a detour using the Chinese Remainder Theorem rather then applying Euler's Theorem directly to conclude that

$$x^{e\mathtt{d}} = x^{1+k\varphi(n)} = x$$

holds. But this argument is only valid for those x coprime to n. So we relocated the problem to the rings $\mathbb{Z}/\mathtt{p}\mathbb{Z}$ and $\mathbb{Z}/\mathtt{q}\mathbb{Z}$, where, as $\mathtt{p}$ and $\mathtt{q}$ are prime, we can be sure that Euler's Theorem is applicable to all $x_i \neq 0$.

Remark 3.17 The security of the RSA algorithms relies on the difficulty of determining the secret key $\mathtt{d}$. For this, one would have to know $\varphi(n)$ and then determine the inverse of e modulo $\varphi(n)$. But in order to find $\varphi(n)$, one needs to compute the prime factorisation $\mathtt{pq}$ of n. In general, this is very hard to compute.

Part III
Geometry in Vector Spaces

So far we have studied the algebraic properties of vector spaces and their linear maps. If we endow a vector space V with an additional structure known as an *inner product*, then V obtains geometric properties. More precisely, we can then define angles, distances and lengths in V. As so often, we draw inspiration from an elementary special case, which here is the *canonical inner product* in $\mathbb{R}^2$. By prescinding its algebraic properties from its particular definition we are lead to an abstract definition for inner products in arbitrary real or complex vector spaces.

4 Vector Spaces with Inner Products

4.1 The Canonical Inner Product

The **canonical inner product** of two vectors

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \; y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{R}^n$$

is defined as

$$\langle x|y\rangle = x^\top \cdot y = x_1 y_1 + \ldots + x_n y_n \tag{4.1}$$

The output is a real number, which explains why it also called a *scalar product*.

For simplicity, we restrict to the case $n = 2$. To begin, we note some algebraic properties of the canonical inner product:

Remark 4.1 For $x, y \in \mathbb{R}^2$,

$$\langle x|y\rangle = x_1 y_1 + x_2 y_2 = y_1 x_1 + y_2 x_2 = \langle y|x\rangle. \tag{4.2}$$

So the inner product is *symmetric*.

Remark 4.2 For all $x, y, z \in \mathbb{R}^2$ and every number $\alpha \in \mathbb{R}$,

$$\begin{aligned} \langle x|y+z\rangle &= x_1(y_1+z_1) + x_2(y_2+z_2) \\ &= x_1 y_1 + x_1 z_1 + x_2 y_2 + x_2 z_2 \\ &= (x_1 y_1 + x_2 y_2) + (x_1 z_1 + x_2 z_2) \\ &= \langle x|y\rangle + \langle x|z\rangle \end{aligned}$$

and

$$\begin{aligned}\langle x|\alpha y\rangle &= x_1(\alpha y_1) + x_2(\alpha y_2)\\ &= \alpha(x_1 y_1) + \alpha(x_2 y_2)\\ &= \alpha(x_1 y_1 + x_2 y_2)\\ &= \alpha\langle x|y\rangle.\end{aligned}$$

This means $\langle x|\cdot\rangle$ for a fixed x is a linear function:

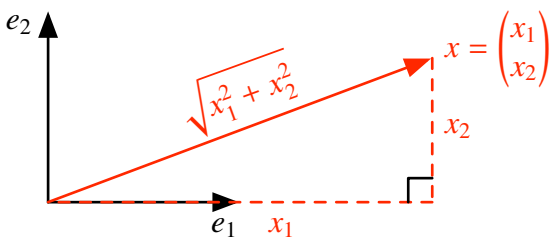
$$\langle x|\alpha y + z\rangle = \alpha\langle x|y\rangle + \langle x|z\rangle. \tag{4.3}$$

It follows from the symmetry (4.2), that $\langle\cdot|x\rangle$ for fixed x is a linear function as well. This property we call the *bilinearity* of the inner product.

Let us now turn our attention to the geometric properties: Plug $x = y$ into (4.1) to obtain

$$\langle x|x\rangle = x_1^2 + x_2^2.$$

The figure below explains how this is interpreted geometrically:



In this figure the e_1-axis and the e_2-axis are perpendicular, so we obtain a right-angled triangle whose sides are given by x, the e_1-component of x and the e_2-component of x. The hypthenuse is the line segement from the origin to x. In this situation, Pythagoras' Theorem gives us

$$x_1^2 + x_2^2 = (\text{length of the vector } x)^2.$$

So the inner product allows us to determine the length

$$\sqrt{\langle x|x\rangle} = \sqrt{x_1^2 + x_2^2} \tag{4.4}$$

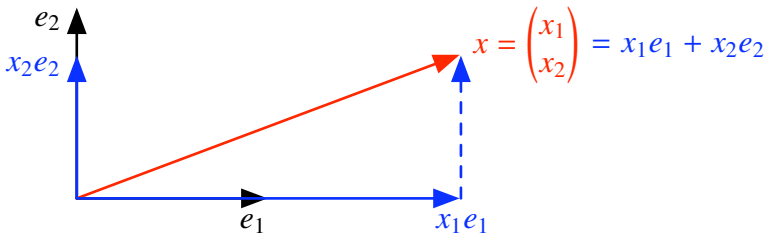
of a vector x. We note in particular:

Remark 4.3 Every vector $x \neq 0$ has a positive length. However, the vector 0 has length 0. This means

$$\langle x|x\rangle \geq 0, \quad \text{with "} = 0\text{" only if } x = 0. \tag{4.5}$$

We will get to know this property as *positive definite* later on.

Auch das Skalarprodukt zweier verschiedener Vektoren $x, y \in \mathbb{R}^2$ lässt sich geometrisch deuten. Dazu betrachten wir die Spezialfälle $y = e_1$ und $y = e_2$ mit jeweils beliebigem x. Im folgenden Bild sehen wir, wie x sich aus einem Vielfachen von e_1 und einem Vielfachen von e_2 zusammensetzt.



Dabei ist der Betrag der jeweiligen e_i-Komponente der $i$te Koeffizient x_i ($i = 1, 2$). Im Fall $y = e_1$ gilt

$$\langle x|y\rangle = \langle x|e_1\rangle = x_1 \cdot 1 + x_2 \cdot 0 = x_1,$$

und im Fall $y = e_2$ gilt

$$\langle x|y\rangle = \langle x|e_2\rangle = x_1 \cdot 0 + x_2 \cdot 1 = x_2.$$

Das Skalarprodukt $\langle x|e_i\rangle$ berechnet also den Betrag der senkrechten Projektion von x auf die e_i-Achse. Lax formuliert gibt $\langle x|e_i\rangle$ an, welchen Beitrag der $i$te Einheitsvektor zum Vektor x leistet. Dies liefert eine Zerlegung von x in orthogonale Komponenten:

$$x = x_1e_1 + x_2e_2 = \langle x|e_1\rangle e_1 + \langle x|e_2\rangle e_2.$$

Ist nun y ein beliebiger Vektor der Länge 1, so kann man in einem geeigneten Koordinatensystem annehmen, dass $y = e_1$ gilt. Wir stellen somit fest:

Remark 4.4 Für einen Vektor y der Länge 1 gibt das Skalarprodukt $\langle x|y\rangle$ die Länge der senkrechten Projektion von x auf die y-Achse an. Sind y_1, y_2 zwei senkrecht aufeinanderstehende Vektoren der Länge 1 (z.B. $y_i = e_i$), so lässt sich x mittels des Skalarproduktes in seine orthogonalen Komponenten bzgl. der Basis $\{y_1, y_2\}$ zerlegen:

$$x = \langle x|y_1\rangle y_1 + \langle x|y_2\rangle y_2.$$

Diese letzte Eigenschaft erlaubt uns, die Darstellung von x in einer geeigneten Basis allein durch das Berechnen von Skalarprodukten zu ermitteln. Besonders interessant ist dies im Falle unendlicher Dimension, in dem man eine solche Darstellung nicht durch das Lösen linearer Gleichungssysteme erhalten kann.

In den folgenden Abschnitten 4.2 und 4.3 gelangen wir über die Eigenschaften (4.3), (4.2) und (4.5) zu einer abstrakten Definition von Skalarprodukten. Zunächst werden wir dazu den Begriff der Bilinearität von einem sehr allgemeinen Standpunkt aus untersuchen.

4.2 Bilinearformen

In diesem Abschnitt sei $\mathbb{K}$ ein Körper und V ein $\mathbb{K}$-Vektorraum.

Definition 4.5 Eine Abbildung $s : V \times V \to \mathbb{K}$ heißt **Bilinearform**, falls für alle $x, y, z \in V$ und alle $\lambda \in \mathbb{K}$ gilt:

$$\begin{aligned} s(x + y, z) &= s(x, z) + s(y, z), \\ s(x, y + z) &= s(x, y) + s(x, z), \\ s(\lambda x, y) &= \lambda s(x, y), \\ s(x, \lambda y) &= \lambda s(x, y). \end{aligned}$$

Es bezeichne $\mathrm{Bil}(V)$ die Menge der Bilinearformen auf V.

Remark 4.6 Dass s eine Bilinearform ist, ist äquivalent dazu, dass für jedes $x \in V$ die Funktionen $s(x, \cdot) : V \to \mathbb{K}$ und $s(\cdot, x) : V \to \mathbb{K}$ Linearformen sind. $\mathrm{Bil}(V)$ ist mit der üblichen Addition und Skalarmultiplikation von Funktionen ein $\mathbb{K}$-Vektorraum.

Definition 4.7 Es sei $s : V \times V \to \mathbb{K}$ eine Bilinearform.

(a) s heißt **symmetrisch**, falls $s(x, y) = s(y, x)$ gilt für alle $x, y \in V$.

(b) s heißt **schiefsymmetrisch**, falls $s(x, y) = -s(y, x)$ gilt für alle $x, y \in V$.

(c) s heißt **alternierend**, falls $s(x, x) = 0$ gilt für alle $x \in V$.

Es bezeichne $\mathrm{Sym}(V)$ die Menge der symmetrischen Bilinearformen auf V.

Exercise 4.8 Jede alterniernde Bilinearform s ist schiefsymmetrisch. Falls die Charakteristik von $\mathbb{K}$ nicht 2 ist, ist s genau dann alternierend, wenn s schiefsymmetrisch ist.

Example 4.9 (Bilinearformen)

(a) Das Standardskalarprodukt $s = \langle\cdot|\cdot\rangle$ im $\mathbb{R}^n$ ist eine symmetrische Bilinearform (vgl. Abschnitt 4.1).

(b) Auf $\mathbb{K}^2$ ist durch
$$s(x, y) = \det(x\ y)$$
eine alternierende Bilinearform gegeben.

(c) Auf dem Vektorraum $\mathrm{C}([a, b])$ der stetigen reellwertigen Funktionen auf dem Intervall $[a, b]$ ist durch
$$s(f, g) = \int_a^b f(t)g(t)\,\mathrm{d}t$$
ist eine symmetrische Bilinearform gegeben.

(d) Jede Matrix $A \in \mathbb{K}^{n\times n}$ definiert auf $\mathbb{K}^n$ eine Bilinearform durch die Vorschrift
$$s_A(x, y) = x^\top \cdot A \cdot y.$$

In der Tat können alle Bilinearformen von Vektorräumen endlicher Dimension in der Form von Beispiel 4.9 (d) dargestellt werden:

Lemma 4.10 *Es sei* $\dim V = n$ *und* $B = \{b_1, \ldots, b_n\}$ *eine Basis von* V*. Weiter sei* $s : V \times V \to \mathbb{K}$ *eine Bilinearform. Wir setzen* $s_{ij} = s(b_i, b_j)$ *und definieren die Matrix*
$$S_B(s) = \begin{pmatrix} s_{11} & \cdots & s_{1n} \\ \vdots & \ddots & \vdots \\ s_{n1} & \cdots & s_{nn} \end{pmatrix} \in \mathbb{K}^{n\times n}. \tag{4.6}$$
Dann gilt
$$s(x, y) = \Theta_B(x)^\top \cdot S_B(s) \cdot \Theta_B(y). \tag{4.7}$$

PROOF: Beide Seiten der Gleichung (4.6) sind bilinear. Es genügt also, die Gleichheit für Basisvektoren $x = b_i$, $y = b_j$ zu zeigen. Es gilt
$$\Theta_B(b_i) = e_i.$$
Also ist
$$\Theta_B(b_i)^\top \cdot S_B(s) \cdot \Theta_B(b_j) = e_i^\top \cdot S_B(s) \cdot e_j = s_{ij} = s(b_i, b_j),$$
wie behauptet. ◇

Exercise 4.11 Für gegebene Basis B ist die Abbildung

$$S_B : \mathrm{Bil}(V) \to \mathbb{K}^{n\times n}, \quad s \mapsto S_B(s)$$

bijektiv und sogar ein Isomorphismus von $\mathbb{K}$-Vektorräumen.

Example 4.12 (Matrizen von Bilinearformen) Es sei B die Standardbasis von $\mathbb{K}^n$.

(a) Für das Standardskalarprodukt im $\mathbb{R}^n$ gilt $\langle e_i | e_j \rangle = \delta_{ij}$. Also ist

$$S_B(\langle \cdot | \cdot \rangle) = I_n.$$

(b) In Beispiel 4.9 (b) gilt

$$s(e_1, e_1) = 0 = s(e_2, e_2), \quad s(e_1, e_2) = 1, \quad s(e_2, e_1) = -1.$$

Also ist

$$S_B(s) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Lemma 4.13 *Es sei* $\dim V = n$ *und* B *eine beliebige Basis von* V*. Weiter sei* s *eine Bilinearform auf* V *und* $S = S_B(s)$*.*

(a) *s ist genau dann symmetrisch, wenn S eine symmetrische Matrix ist (d.h. $S = S^\top$).*

(b) *s ist genau dann schiefsymmetrisch, wenn S eine schiefsymmetrische Matrix ist (d.h. $S = -S^\top$).*

PROOF:

(a) s symmetrisch genau dann, wenn $s_{ij} = s_{ji}$ gilt in (4.6). Dies ist äquivalent zu $S = S^\top$.

(b) s schiefsymmetrisch genau dann, wenn $s_{ij} = -s_{ji}$ gilt in (4.6). Dies ist äquivalent zu $S = -S^\top$. ◇

Sind für eine Bilinearform s die Matrizen $S_B(s)$ und $S_C(s)$ für zwei Basen B, C von V gegeben, so können wir ähnlich wie bei den Abbildungsmatrizen von Endmorphismen $S_C(s)$ bestimmen, wenn wir $S_B(s)$ kennen.

Theorem 4.14 *Es sei* $\dim V = n$ *und es seien* B, C *Basen von* V. *Für jede Bilinearform* $s : V \times V \to \mathbb{K}$ *gilt*

$$S_C(s) = (M_B^C)^\top \cdot S_B(s) \cdot M_B^C. \tag{4.8}$$

Hier bezeichnet $M_B^C = M_B^C(\mathrm{id}_V)$ *die Übergangsmatrix für den Basiswechsel von der Basis* C *zur Basis* B.

PROOF: Für alle $x \in V$ gilt $\Theta_C(x) = M_C^B \cdot \Theta_B(x)$.

Also gilt nach (4.7) für alle $x, y \in V$:

$$\begin{aligned} \Theta_B(x)^\top \cdot S_B(s) \cdot \Theta_B(y) = s(x,y) &= \Theta_C(x)^\top \cdot S_C(s) \cdot \Theta_C(y) \\ &= (M_C^B \cdot \Theta_B(x))^\top \cdot S_C(s) \cdot (M_C^B \cdot \Theta_B(y)) \\ &= \Theta_B(x)^\top \cdot (M_C^B)^\top \cdot S_C(s) \cdot M_C^B \cdot \Theta_B(y). \end{aligned}$$

Wegen der Eindeutigkeit von $S_B(s)$ folgt $S_B(s) = (M_C^B)^\top \cdot S_C(s) \cdot M_C^B$. ◇

Remark 4.15 Man beachte, dass im Allgemeinen

$$(M_C^B)^\top \neq (M_C^B)^{-1} = M_B^C$$

gilt! Der Basiswechsel für Bilinearformen ist also anders zu berechnen als der Basiswechsel für lineare Abbildungen (in der Tat ist jener leichter zu berechnen, da man M_C^B lediglich transponieren und nicht invertieren muss).

Definition 4.16 Eine Bilinearform $s \in \mathrm{Sym}(V)$ heißt **ausgeartet**, falls $x_0 \in V$, $x_0 \neq 0$, existiert, so dass gilt

$$s(x_0, x) = 0 \quad \text{für alle } x \in V. \tag{4.9}$$

Andernfalls heißt s **nicht ausgeartet**.

Exercise 4.17 Es sei $\dim V < \infty$. Es ist $s \in \mathrm{Sym}(V)$ genau dann nicht ausgeartet, wenn für alle $x \in V$ die Abbildungen

$$\begin{aligned} s_{1,x} &: V \to V^\star, \quad x \mapsto s(x, \cdot), \\ s_{2,x} &: V \to V^\star, \quad x \mapsto s(\cdot, x) \end{aligned}$$

Isomorphismen sind.

Example 4.18 In Beispiel 4.9 sind alle Bilinearformen nicht ausgeartet. Ein nichttriviales Beispiel für eine ausgeartete Bilinearform auf $\mathbb{R}^2$ ist

$$s(x,y) = x^\top \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot y.$$

Definition 4.19 Es sei $s \in \mathrm{Sym}(V)$. Die Menge

$$\mathrm{Rad}\, s = \{x_0 \in V \mid s(x_0, x) = 0 \text{ für alle } x \in V\} \tag{4.10}$$

heißt das **Radikal** (oder der **Kern**) von s.

Remark 4.20 Offensichtlich ist $s \in \mathrm{Sym}(V)$ genau dann nicht ausgeartet, wenn $\mathrm{Rad}\, s = \{0\}$ gilt.

Lemma 4.21 *Ist $S_B(s)$ eine Matrix für $s \in \mathrm{Sym}(V)$, so gilt*

$$\Theta_B(\mathrm{Rad}\, s) = \ker S_B(s).$$

PROOF: Ist $x_0 \in \mathrm{Rad}\, s$, so gilt $e_i^\top \cdot S_B(s) \cdot \Theta_B(x_0) = 0$ für alle Einheitsvektoren e_i. Also ist $S_B(s) \cdot \Theta_B(x_0) = 0$.
Gilt umgekehrt $S_B(s) \cdot v = 0$ für ein $v \in \mathbb{K}^n$, so ist $s(x, \Theta_B^{-1}(v)) = \Theta_B(x)^\top \cdot S_B(s) \cdot v = 0$ für alle $x \in V$. Also ist $\Theta_B^{-1}(v) \in \mathrm{Rad}\, s$. ◇

Corollary 4.22 *$s \in \mathrm{Sym}(V)$ ist genau dann nicht ausgeartet, wenn $S_B(s) \in \mathbf{GL}_n(\mathbb{K})$.*

4.3 Euklidische Vektorräume

Um zu einer abstrakten Definition von Skalarprodukten zu gelangen, ergänzen wir den Begriff der Bilinearform nun um die den Eigenschaften (4.2) und (4.5) enstprechenden Begriffe.

Definition 4.23 Es sei V ein $\mathbb{R}$-Vektorraum. Eine Bilinearform $s \in \mathrm{Sym}(V)$ heißt **positiv definit**, falls für alle $x \in V$, $x \neq 0$, gilt

$$s(x, x) > 0.$$

Ein **Skalarprodukt** $\langle \cdot | \cdot \rangle$ auf V ist eine positiv definite symmetrische Bilinearform.

Definition 4.24 Ein **euklidischer Vektorraum** $(V, \langle \cdot | \cdot \rangle)$ ist ein $\mathbb{R}$-Vektorraum V zusammen mit einem Skalarprodukt $\langle \cdot | \cdot \rangle : V \times V \to \mathbb{R}$.

Remark 4.25

(a) Beachte, dass wegen der Bilinearität stets $s(0, 0) = 0$ gilt.

(b) Wir beschränken uns bei der Definition von Skalarprodukten auf $\mathbb{R}$-Vektorräume, da die positive Definitheit nur Sinn ergibt, wenn der zugrundeliegende Skalarkörper geordnet ist.[8)]

(c) Neben der Schreibweise $\langle x|y\rangle$ ist auch die Schreibweise $\langle x, y\rangle$ in der Mathematik weit verbreitet. Gelegentlich wird das Standardskalarprodukt im $\mathbb{R}^n$ mit einem Punkt geschrieben: $x \cdot y$.

(d) Die Schreibweise $\langle x|y\rangle$ wurde von Dirac als **Bra-Ket-Notation** (von engl. *bracket*) in der Quantenphysik eingeführt. Dirac interpretiert dabei einen Vektor $y \in V$ als *Ket-Vektor* $|y\rangle$ und bezeichnet die Linearform $x \mapsto \langle x|\cdot\rangle$ aus $V^\star$ als *Bra-Vektor* $\langle x|$. Das Anwenden der Linearform $\langle x|$ auf den Vektor $|y\rangle$ liefert dann gerade den Wert des Skalarprodukts $\langle x|y\rangle$.

Example 4.26 (Euklidische Vektorräume)

(a) Der $\mathbb{R}^n$ mit dem Standardskalarprodukt ist ein euklidischer Vektorraum (dass das Standardskalarprodukt ein Skalarprodukt im Sinne von Definition 4.23 ist, ergibt sich sofort aus den Überlegungen in Abschnitt 4.1).

(b) Im $\mathbb{R}^n$ ist für jede Matrix $A \in \mathbb{R}^{n\times n}$ durch $s_A(x, y) = x^\top \cdot A \cdot y$ eine Bilinearform gegeben. Wir überlegen, welche Eigenschaften die Matrix A besitzen muss, damit s_A ein Skalarprodukt ist: Zunächst muss A nach Hilfssatz 4.13 eine symmetrische Matrix sein. Positive Definitheit bedeutet

$$s_A(x, x) = x^\top \cdot A \cdot x > 0$$

für alle $x \in \mathbb{R}^n$, $x \neq 0$. ♡

Die Beobachtung im letzten Beispiel veranlasst uns zu folgender Definition:

Definition 4.27 Eine symmetrische Matrix $S \in \mathbb{R}^{n\times n}$ heißt **positiv definit**, falls für alle $x \in \mathbb{R}^n$, $x \neq 0$, gilt:

$$x^\top \cdot S \cdot x > 0. \tag{4.11}$$

Die Bedingung (4.11) direkt nachzuprüfen ist in der Regel sehr schwer. In Abschnitt **??** lernen wir einige Kriterien kennen, mit denen man eine symmetrische Matrix leicht auf positive Definitheit prüfen kann.

Lemma 4.28 *Es sei $(V, \langle\cdot|\cdot\rangle)$ ein euklidischer Vektorraum.*

[8)] In Abschnitt 4.5 werden wir ausnutzen, dass $\mathbb{R}$ ein Teilkörper von $\mathbb{C}$ ist, um auch in komplexen Vektorräumen Skalarprodukte zu definieren.

(a) $\langle\cdot|\cdot\rangle$ *ist nicht ausgeartet.*

(b) *Ist* $\dim V < \infty$ *mit Basis* B*, so ist die Matrix* $S = S_B(\langle\cdot|\cdot\rangle)$ *symmetrisch, positiv definit und invertierbar.*

(c) *Alle Eigenwerte der Matrix* S *aus (b) sind positiv.*

PROOF:

(a) Wegen der positiven Definitheit ist $\mathrm{Rad}\langle\cdot|\cdot\rangle = \{0\}$.

(b) Ergibt sich aus Hilfssatz 4.13, Beispiel 4.26 (b) und Teil (a) zusammen mit Folgerung 4.22.

(c) Sei λ Eigenwert von S mit Eigenvektor $x \in \mathbb{R}^n$. Dann gilt

$$0 < x^\top \cdot S \cdot x = x^\top \cdot (\lambda \cdot x) = \lambda \cdot \underbrace{x^\top \cdot x}_{>0}.$$

Das bedeutet $\lambda > 0$. ◇

Zum Ende dieses Abschnitts betrachten wir noch ein Standardbeispiel eines Skalarprodukts in Funktionsvektorräumen von unendlicher Dimension.

Example 4.29 Der Vektorraum $\mathrm{C}([a,b])$ der stetigen Funktionen auf dem Intervall $[a,b]$ ist ein euklidischer Vektorraum mit dem Skalarprodukt

$$\langle f|g\rangle = \int_a^b f(t)g(t)\mathrm{d}t. \tag{4.12}$$

Aus Beispiel 4.9 (c) wissen wir bereits, dass dies eine symmetrische Bilinearform ist. Sie ist auch positiv definit: Es ist $\int_a^b f(t)^2\mathrm{d}t \geq 0$ für alle $f \in \mathrm{C}([a,b])$, da $f(t)^2 \geq 0$ ist für alle $t \in [a,b]$. Falls $f \neq 0$ ist, so ist $f(t_0)^2 > 0$ an einer Stelle $t_0 \in (a,b)$. Aus der Definition der Stetigkeit folgt, dass $f(t)^2 > 0$ in einer geeigneten Umgebung $[t_0-\delta, t_0+\delta]$ von t_0 gilt (mit $\delta > 0$). Dann gilt aber

$$\langle f|f\rangle = \int_a^b f(t)^2\mathrm{d}t \geq \int_{t_0-\delta}^{t_0+\delta} f(t)^2\mathrm{d}t \geq 2\delta \min\{f(t)^2 \mid t \in [t_0-\delta, t_0+\delta]\} > 0.$$

Somit ist $\langle\cdot|\cdot\rangle$ in der Tat ein Skalarprodukt.

Wir wollen nun noch heuristisch verstehen, wieso man (4.12) als die Entsprechung des Standardskalarprodukts im $\mathbb{R}^n$ auf Funktionsvektorräumen auffassen kann: Ein Element $x \in \mathbb{R}^n$ ist durch seine Koeffizienten $x_1, \ldots, x_n$ festgelegt. Eine andere Sichtweise auf x ist es, x als Funktion $x : \{1, \ldots, n\} \to \mathbb{R}$ aufzufassen,

die der Zahl i gerade den Wert des Koeffizienten x_i zuweist: $x(i) = x_i$. Das Standardskalarprodukt zweier Vektoren $x, y \in \mathbb{R}^n$ ist dann

$$\langle x|y\rangle = \sum_{i=1}^{n} x(i)y(i),$$

die Summe über das Produkt der Funktionswerte von x und y, ausgewertet an allen Elementen von $\{1, \ldots, n\}$. Betrachten wir nun anstelle der endlichen Menge $\{1, \ldots, n\}$ das Intervall$[a, b]$ und die Funktionen darauf, so entspricht der endlichen Summe $\sum_{i=1}^{n}$ wegen der Überabzählbarkeit von $[a, b]$ das Integral $\int_a^b$. Auf diese Weise führt uns das Standardskalarprodukt auf (4.12). ♡

4.4 Normen, Winkel und Orthogonalität

Normen verallgemeinern den elementargeometrischen Längenbegriff:

Definition 4.30 Es sei V ein $\mathbb{R}$-Vektorraum. Eine Funktion $\|\cdot\| : V \to \mathbb{R}$ heißt **Norm**, wenn sie folgende Eigenschaften besitzt:

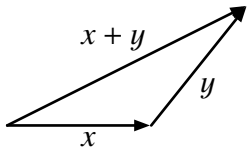
(i) $\|x\| > 0$ für alle $x \in V\backslash\{0\}$ und $\|0\| = 0$.

(ii) $\|\lambda \cdot x\| = |\lambda| \cdot \|x\|$ für alle $x \in V$ und $\lambda \in \mathbb{R}$.

(iii) $\|\cdot\|$ erfüllt die **Dreiecksungleichung** für alle $x, y \in V$:

$$\|x + y\| \leq \|x\| + \|y\|. \tag{4.13}$$

Die Dreiecksungleichung bedeutet, dass die Summe zweier Seitenlängen eines Dreiecks mindestens so groß ist wie die Länge der längsten Seite des Dreiecks.



Die positive Definitheit eines Skalarprodukts erlaubt es, in Analogie zu (4.4) einen Längenbegriff für euklidische Vektorräume einzuführen.

Theorem 4.31 *Es sei $(V, \langle\cdot|\cdot\rangle)$ ein euklidischer Vektorraum. Dann ist durch*

$$\|x\| = \sqrt{\langle x|x\rangle} \tag{4.14}$$

eine Norm auf V definiert.

PROOF: Die Eigenschaft (i) folgt aus der positiven Definitheit des Skalarprodukts. Die Eigenschaft (ii) folgt aus der Bilinearität:

$$\|\lambda \cdot x\| = \sqrt{\langle \lambda x | \lambda x \rangle} = \sqrt{\lambda^2 \langle x|x\rangle} = \sqrt{\lambda^2} \cdot \sqrt{\langle x|x\rangle} = |\lambda| \cdot \|x\|.$$

Für Eigenschaft (iii) verwenden wir die Cauchy-Schwarz-Ungleichung (4.16), die im Anschluss bewiesen wird:

$$\begin{aligned} \langle x+y|x+y\rangle &= \langle x|x\rangle + 2\langle x|y\rangle + \langle y|y\rangle \\ &\le \langle x|x\rangle + 2\|x\| \cdot \|y\| + \langle y|y\rangle \\ &= (\|x\| + \|y\|)^2. \end{aligned}$$

Wurzelziehen erhält $\le$, und somit folgt die Dreiecksungleichung. ◇

Theorem 4.32 (Cauchy-Schwarz-Ungleichung) *Es sei $(V, \langle\cdot|\cdot\rangle)$ ein euklidischer Vektorraum. Für alle $x, y \in V$ gilt:*

$$\langle x|y\rangle^2 \le \langle x|x\rangle \cdot \langle y|y\rangle. \tag{4.15}$$

Gleichheit gilt genau dann, wenn x und y linear abhängig sind.

PROOF: Falls $x = 0$ oder $y = 0$ ist nichts zu zeigen. Also nehmen wir $x \neq 0$ und $y \neq 0$ an. Es gilt

$$0 \le \Big\langle \frac{x}{\|x\|} \pm \frac{y}{\|y\|} \Big| \frac{x}{\|x\|} \pm \frac{y}{\|y\|} \Big\rangle = \underbrace{\frac{\langle x|x\rangle}{\|x\|^2}}_{=1} + \underbrace{\frac{\langle y|y\rangle}{\|y\|^2}}_{=1} \pm 2\frac{\langle x|y\rangle}{\|x\| \cdot \|y\|} = 2 \pm 2\frac{\langle x|y\rangle}{\|x\| \cdot \|y\|}. \tag{$*$}$$

Daraus folgt

$$\mp \frac{\langle x|y\rangle}{\|x\| \cdot \|y\|} \le 1 \quad \text{bzw.} \quad \mp \langle x|y\rangle \le \|x\| \cdot \|y\|.$$

Quadrieren ergibt (4.15).

Sind x, y linear abhängig, so gilt $y = \lambda x$ für ein $\lambda \in \mathbb{R}$. Dann ist

$$\langle x|y\rangle^2 = \lambda^2 \langle x|x\rangle^2 = \lambda^2 \langle x|x\rangle\langle x|x\rangle = \langle x|x\rangle \cdot \langle \lambda x|\lambda x\rangle = \langle x|x\rangle \cdot \langle y|y\rangle.$$

Umgekehrt nehmen wir nun an, es gelte Gleichheit in (4.15), also auch $\langle x|y\rangle = \|x\| \cdot \|y\|$. Einsetzen in $(*)$ ergibt

$$0 \le \Big\langle \frac{x}{\|x\|} - \frac{y}{\|y\|} \Big| \frac{x}{\|x\|} - \frac{y}{\|y\|} \Big\rangle = 2 - 2 = 0.$$

Aus der positiven Definitheit folgt $0 = \frac{x}{\|x\|} - \frac{y}{\|y\|}$ bzw. $x = \frac{\|x\|}{\|y\|} y$. ◇

Die Cauchy-Schwarz-Ungleichung wird auch in der folgenden Form angegeben:

$$\langle x|y\rangle \le \|x\| \cdot \|y\|. \tag{4.16}$$

Remark 4.33 Es gibt Normen, die nicht von der Form (4.14) sind, also nicht zu einem Skalarprodukt gehören. Ein Beispiel hierfür ist die **Maximumsnorm** auf dem $\mathbb{R}^n$, gegeben durch

$$\|x\|_{\max} = \max\{x_1, \ldots, x_n \mid x_i \text{ Koeffizienten von } x\}.$$

Es lässt sich zeigen, dass eine Norm $\|\cdot\|$ genau dann zu einem Skalarprodukt gehört, wenn alle $x, y \in V$ die **Parallelogrammgleichung** erfüllen:

$$\|x + y\|^2 + \|x - y\|^2 = 2\|x\|^2 + 2\|y\|^2.$$

Siehe dazu Werner [13], Satz V.1.7. In diesem Fall lässt sich das Skalarprodukt durch die Norm ausdrücken. Dies nennen wir **Polarisierung**:

$$\langle x|y\rangle = \frac{1}{2}(\|x + y\|^2 - \|x\|^2 - \|y\|^2). \tag{4.17}$$

Exercise 4.34 Es sei $S \in \mathbb{R}^{n\times n}$ eine symmetrische positiv definite Matrix mit Einträgen s_{ij}. Dann gilt:

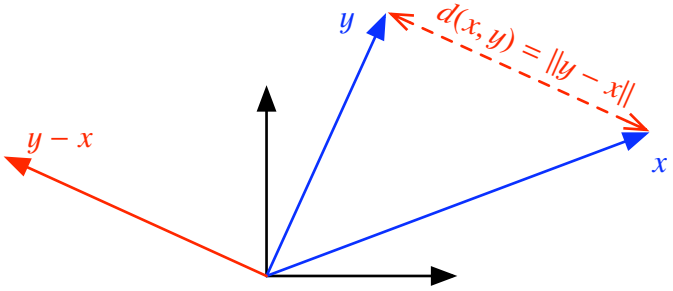
(a) Es ist $s_{ik}^2 < s_{ii}s_{kk}$ für $i \neq k$.

(b) Es existiert ein k mit $\max_{i,j} |s_{ij}| = s_{kk}$ (d.h. der betragsgrößte Matrixeintrag liegt auf der Diagonalen).

Können wir Längen bestimmen, so können wir auch Abstände bestimmen. Dazu definieren wir den Abstand zweier Vektoren x, y als die Länge des Verbindungsvektors von x zu y.

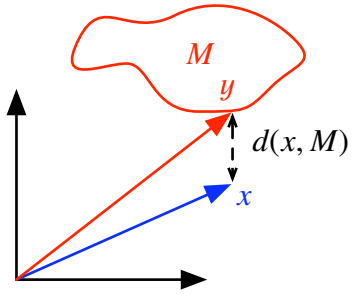
Definition 4.35 Es sei $(V, \langle\cdot|\cdot\rangle)$ ein euklidischer Vektorraum, M eine Teilmenge von V und $x, y \in V$. Der **Abstand $d(x, y)$ von x zu y** ist

$$d(x, y) = \|y - x\| \tag{4.18}$$



und der **Abstand $d(x, M)$ von x zu M** ist

$$d(x, M) = \inf\{d(x, y) \mid y \in M\}. \tag{4.19}$$



Exercise 4.36 Es sei $V = \mathbb{R}^n$ und $\langle\cdot|\cdot\rangle$ das Standardskalarprodukt. Ist $M \subset \mathbb{R}^n$ abgeschlossen, so ist das Infimum in (4.19) ein Minimum. Insbesondere gilt dies, wenn M ein Untervektorraum von V ist.

Exercise 4.37 Es seien $x, y, z \in V$. Aus den Eigenschaften der Norm schließt man für den Abstand:

(i) $d(x, y) > 0$ falls $x \neq y$ und $d(x, y) = 0$ falls $x = y$.

(ii) $d(x, y) = d(y, x)$.

(iii) $d(x, z) \leq d(x, y) + d(y, z)$.

Example 4.38 In einem euklidischen Vektorraum $(V, \langle\cdot|\cdot\rangle)$ nennen wir die Menge aller Vektoren mit Abstand r von einem Punkt $x_0 \in V$ die **Sphäre** vom Radius r mit Mittelpunkt x_0, geschrieben

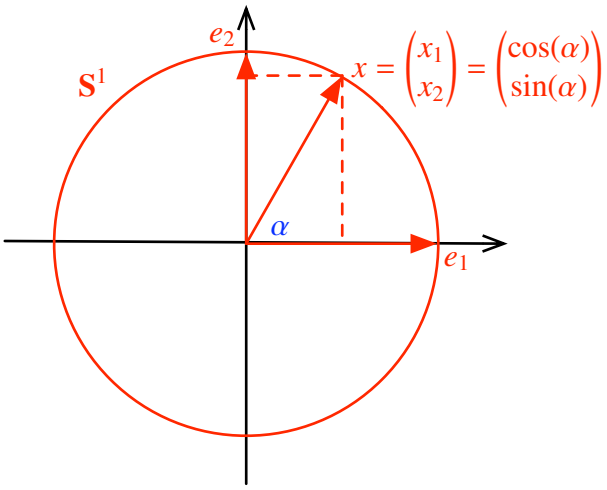
$$\mathbf{S}_r(x_0) = \{x \in V \mid d(x, x_0) = r\}. \tag{4.20}$$

Die Sphäre $\mathbf{S}_1(0)$ heißt **Einheitssphäre** und ihre Elemente **Einheitsvektoren** (oder **normierte Vektoren**). Im Fall $V = \mathbb{R}^n$ mit Standardskalarprodukt $\langle\cdot|\cdot\rangle$ nennen wir $\mathbf{S}_r(0)$ die ***n* − 1-Sphäre**[9] vom Radius r, geschrieben

$$\mathbf{S}_r^{n-1} = \{x \in \mathbb{R}^n \mid \|x\| = r\}. \tag{4.21}$$

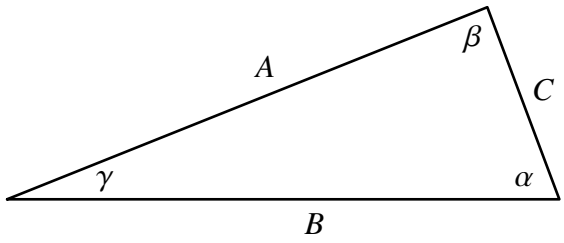
Für die Einheitssphäre im $\mathbb{R}^n$ schreiben wir $\mathbf{S}^{n-1} = \mathbf{S}_1^{n-1}$.

[9] Dass man hier $n - 1$ statt n wählt liegt daran, dass die Punkte auf $\mathbf{S}_r^{n-1}$ bereits durch $n - 1$ Polarkoordinaten eindeutig festgelegt sind. In diesem Sinne ist $\mathbf{S}_r^{n-1}$ ein "$n - 1$-dimensionales" Gebilde.



Ein Skalarprodukt auf V ermöglicht es nicht nur, Längen in V zu definieren, sondern auch Winkel. In diesem Sinne enthält ein Skalarprodukt mehr Information als eine Norm.

Betrachten wir zunächst wieder die vertraute Situation im $\mathbb{R}^2$. Gegeben sei ein Dreieck mit Seitenlängen A, B, C und entsprechenden Innenwinkeln α, β, γ.



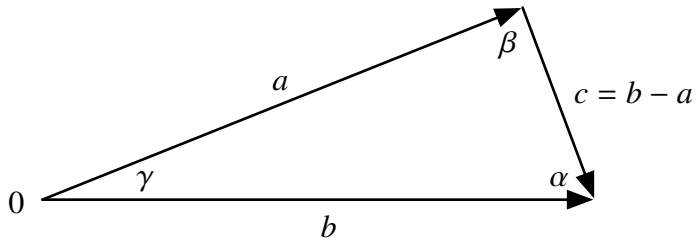
Mit Hilfe des elementargeometrischen **Cosinussatzes**

$$A^2 + B^2 - 2AB\cos(\gamma) = C^2. \tag{4.22}$$

können wir den Winkel γ in Abhängigkeit von den Seitenlängen angeben:

$$\cos(\gamma) = \frac{A^2 + B^2 - C^2}{2AB}. \tag{4.23}$$

Wir können also Winkel allein durch Längen ausdrücken. Die Längen wiederum können wir durch die Norm $\|\cdot\|$ des Standardskalarprodukts des $\mathbb{R}^2$ ausdrücken. Dazu nehmen wir an, der Eckpunkt des Dreiecks beim Winkel γ sei der Ursprung, und wir wählen Vektoren $a, b \in \mathbb{R}^2$ und $c = b - a$ wie im folgenden Bild:



Insbesondere gilt dann $\|a\| = A$, $\|b\| = B$, $\|c\| = C$, und γ ist der von den Vektoren a, b eingeschlossene Winkel $\sphericalangle(a, b)$. Setzen wir dies in (4.23) ein, so ergibt sich wegen $\langle c|c\rangle = \langle b-a|b-a\rangle = \langle b|b\rangle - 2\langle a|b\rangle + \langle a|a\rangle$:

$$\cos(\gamma) = \frac{\langle a|a\rangle + \langle b|b\rangle - \langle b-a|b-a\rangle}{2\|a\| \cdot \|b\|} = \frac{\langle a|b\rangle}{\|a\| \cdot \|b\|}. \tag{4.24}$$

Da wir in jedem abstrakten euklidischen Vektorraum über die Norm einen Längenbegriff haben, können wir (4.24) als definierende Gleichung für den Cosinus des Winkels nehmen (die Cauchy-Schwarz-Ungleichung (4.16) gewährleistet dabei, dass $|\cos(\gamma)| \leq 1$ gilt):

Definition 4.39 Es sei $(V, \langle\cdot|\cdot\rangle)$ ein euklidischer Vektorraum und $x, y \in V$, $x \neq 0$, $y \neq 0$. Der von x und y eingeschlossene **Winkel** ist die eindeutig bestimmte Zahl $\sphericalangle(x, y) \in [0, \pi]$ mit

$$\cos(\sphericalangle(x, y)) = \frac{\langle x|y\rangle}{\|x\| \cdot \|y\|}. \tag{4.25}$$

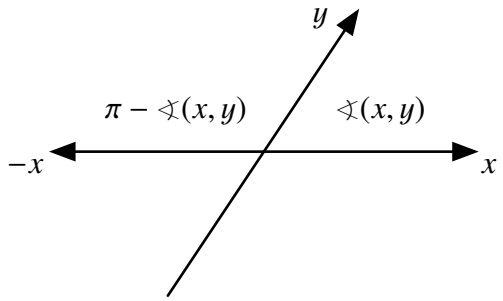
Exercise 4.40 Für alle $x, y \in V\backslash\{0\}$ und $\lambda, \mu \in \mathbb{R}^\times$ gilt:

(a) $\sphericalangle(x, y) = \sphericalangle(y, x)$.

(b) $\sphericalangle(\lambda x, \mu y) = \begin{cases} \sphericalangle(x, y), & \lambda\mu > 0 \\ \pi - \sphericalangle(x, y), & \lambda\mu < 0 \end{cases}$.

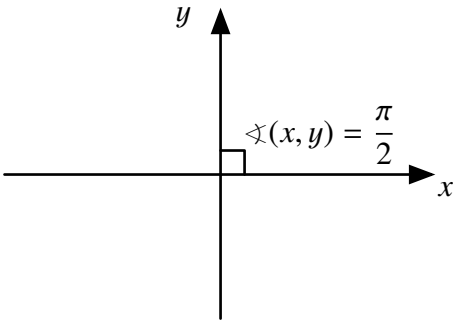
(c) $\sphericalangle(x, y) = 0$ genau dann, wenn $y = \alpha x$ für ein $\alpha > 0$.

(d) $\sphericalangle(x, y) = \pi$ genau dann, wenn $y = \alpha x$ für ein $\alpha < 0$.



Wie in Abschnitt 4.1 erläutert, lässt sich das Skalarprodukt $\langle x|y\rangle$ (und somit der Winkel) als Maß der Komponente in x-Richtung von y auffassen.

Definition 4.41 Es sei $(V, \langle\cdot|\cdot\rangle)$ ein euklidischer Vektorraum. Zwei Vektoren $x, y \in V$ heißen **orthogonal** (oder **senkrecht**), falls $\langle x|y\rangle = 0$ gilt, geschrieben $x \perp y$. Zwei Teilmengen $M_1, M_2 \subset V$ heißen **orthogonal**, $M_1 \perp M_2$, falls $x_1 \perp x_2$ gilt für alle $x_1 \in M_1$, $x_2 \in M_2$.



$x \perp y$ bedeutet zugleich $\cos(\sphericalangle(x, y)) = 0$, was wiederum $\sphericalangle(x, y) = \frac{\pi}{2}$ bedeutet. Dies deckt sich mit unserer Anschauung, dass zwei Vektoren senkrecht aufeinander stehen, wenn sie den Winkel $\frac{\pi}{2}$ $(= 90°)$ einschließen.

Example 4.42 (Orthogonale Vektoren)

(a) In jedem euklidischen Vektorraum gilt $0 \perp x$ für alle x.

(b) Im $\mathbb{R}^3$ mit Standardskalarprodukt sind die beiden Vektoren

$$x = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \; y = \begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix}$$

orthogonal. Es gilt nämlich

$$\langle x|y\rangle = x^\top \cdot y = 1 \cdot (-2) + 2 \cdot 1 + 3 \cdot 0 = -2 + 2 = 0.$$

(c) Im $\mathbb{R}^n$ mit Standardskalarprodukt sind je zwei verschiedene Elemente e_i, e_j der Standardbasis orthogonal.

(d) Im Vektorraum $C([0, 2\pi])$ mit Skalarprodukt (4.12) sind für $m, n \in \mathbb{N}$ die Funktionen $\cos(mt)$ und $\sin(nt)$ orthogonal, d.h. es gilt

$$\langle \cos(m\cdot)|\sin(n\cdot)\rangle = \int_0^{2\pi} \cos(mt)\sin(nt)\mathrm{d}t = 0.$$

In Kapitel **??** werden wir Systeme von orthogonalen Vektoren untersuchen.

Theorem 4.43 (Pythagoras) *Für Elemente x, y eines euklidischen Vektorraumes gilt $x \perp y$ genau dann, wenn*

$$\|x\|^2 + \|y\|^2 = \|x + y\|^2. \tag{4.26}$$

PROOF: Es ist

$$\begin{aligned}\|x + y\|^2 &= \langle x + y|x + y\rangle \\ &= \langle x|x\rangle + \langle x|y\rangle + \langle y|x\rangle + \langle y|y\rangle \\ &= \|x\|^2 + 2\langle x|y\rangle + \|y\|^2.\end{aligned}$$

Also gilt (4.26) genau dann, wenn $\langle x|y\rangle = 0$, d.h. $x \perp y$. ◇

Aus der Motivation für die Definition des Winkels ergibt sich direkt, dass auch der folgende Satz gilt:

Theorem 4.44 (Cosinussatz) *Für Elemente x, y eines euklidischen Vektorraumes gilt*

$$\|x - y\|^2 = \|x\|^2 + \|y\|^2 - 2\|x\| \cdot \|y\| \cos(\sphericalangle(x, y)). \tag{4.27}$$

4.5 Unitäre Vektorräume

Wir wollen nun den Ansatz, einen Vektorraum V vermöge eines Skalarprodukts mit einer geometrischen Struktur auszustatten, auch auf $\mathbb{C}$-Vektorräume übertragen. Dafür können wir jedoch nicht die Definition des Skalarprodukts unverändert übernehmen: Ist etwa $V = \mathbb{C}^2$ und betrachten wir das "Standardskalarprodukt"

$$x^\top \cdot y = x_1 y_1 + x_2 y_2$$

für $x, y \in \mathbb{C}^2$, so ist dies zwar symmetrisch und bilinear, aber aufgrund möglicher imaginärer Einträge kann die positive Definitheit verletzt werden. Für

$$x = \begin{pmatrix} 1 \\ \mathrm{i} \end{pmatrix} \in \mathbb{C}^2$$

ist beispielsweise

$$x^\top \cdot x = x_1^2 + x_2^2 = 1^2 + \mathrm{i}^2 = 0.$$

Durch eine kleine Modifikation kann man aber positive Definitheit erreichen. Dazu definiert man das *Standardskalarprodukt* auf $\mathbb{C}^2$ durch

$$\langle x|y\rangle = x^\top \cdot \overline{y} = x_1\overline{y}_1 + x_2\overline{y}_2.$$

Da $\zeta\overline{\zeta} = |\zeta|^2 \in \mathbb{R}$ für alle komplexen Zahlen $\zeta \in \mathbb{C}$, ist dies positiv definit:

$$\langle x|x\rangle = x^\top \cdot \overline{x} = x_1\overline{x}_1 + x_2\overline{x}_2 = |x_1|^2 + |x_2|^2 \geq 0$$

und "$= 0$" nur dann, wenn $x = 0$. Allerdings ist $\langle\cdot|\cdot\rangle$ nur noch im ersten Argument linear, im zweiten Argument gilt

$$\langle x|y + \lambda z\rangle = \langle x|y\rangle + \overline{\lambda}\langle x|z\rangle.$$

Dies bezeichnen wir als *sesquilinear* ("$1\frac{1}{2}$fach linear"). Auch die Symmetrie ist verlorengegangen. Es gilt stattdessen

$$\langle x|y\rangle = x_1\overline{y}_1 + x_2\overline{y}_2 = \overline{y_1\overline{x}_1 + y_2\overline{x}_2} = \overline{\langle y|x\rangle}.$$

Definition 4.45 Es sei V ein $\mathbb{C}$-Vektorraum. Eine Abbildung $s : V \times V \to \mathbb{C}$ heißt **sesquilinear**[10], falls für alle $x, y, z \in V$ und $\lambda \in \mathbb{C}$ gilt:

$$\begin{aligned} s(x + y, z) &= s(x, z) + s(y, z), \\ s(\lambda x, y) &= \lambda s(x, y), \\ s(x, y + z) &= s(x, y) + s(x, z), \\ s(x, \lambda y) &= \overline{\lambda} s(x, y). \end{aligned}$$

Eine Sesquilinearform s heißt **hermitesch**, falls für alle $x, y \in V$ gilt:

$$s(x, y) = \overline{s(y, x)}.$$

[10] Sesquilinearformen spielen in der theoretischen Physik eine große Rolle. Dort wird Sesquilinearität überlicherweise jedoch so definiert, dass s im *zweiten* Argument linear ist und im ersten Argument $s(\lambda x, y) = \overline{\lambda} s(x, y)$ gilt.

Definition 4.46 Es sei V ein $\mathbb{C}$-Vektorraum. Eine hermitesche Sesquilinearform $s : V \times V \to \mathbb{C}$ heißt **positiv definit**, falls für alle $x \in V$, $x \neq 0$, gilt

$$s(x, x) > 0.$$

Ein **unitäres Skalarprodukt** $\langle \cdot | \cdot \rangle$ ist eine positiv definite hermitesche Sesquilinearform.

Definition 4.47 Ein **unitärer Vektorraum** $(V, \langle \cdot | \cdot \rangle)$ ist ein $\mathbb{C}$-Vektorraum V zusammen mit einem unitären Skalarprodukt $\langle \cdot | \cdot \rangle$.

Example 4.48 (Unitäre Vektorräume) Die Beispiele können als "Komplexifizierung" der enstprechenden euklidischen Beispiele aufgefasst werden:

(a) $\mathbb{C}^n$ ist ein unitärer Vektorraum mit dem (unitären) Standardskalarprodukt

$$\langle x | y \rangle = x^\top \cdot \overline{y} = x_1 \overline{y}_1 + \ldots + x_n \overline{y}_n. \tag{4.28}$$

(b) Der Vektorraum $\mathrm{C}([a, b], \mathbb{C})$ der stetigen $\mathbb{C}$-wertigen Funktionen auf dem Intervall $[a, b]$ ist unitär mit dem Skalarprodukt

$$\langle f | g \rangle = \int_a^b f(t)\overline{g(t)}\mathrm{d}t. \tag{4.29}$$

Die Resultate über euklidische Vektorräumen lassen sich auf unitäre Vektorräume übertragen, wenn man ihre Beweise so anpasst, dass sie die Sesquilinearität berücksichtigen, und gelegentlich einen Ausdruck z^2 durch $|z|^2$ ersetzt. Wir führen sie daher ohne ausführliche Begründungen auf.

Theorem 4.49 *Es sei $(V, \langle \cdot | \cdot \rangle)$ ein unitärer Vektorraum der Dimension n. Weiter sei $B = \{b_1, \ldots, b_n\}$ eine Basis von V und $S \in \mathbb{C}^{n \times n}$ die Matrix mit Einträgen*

$$s_{ij} = \langle b_i | b_j \rangle.$$

Dann gilt für alle $x, y \in V$:

$$\langle x | y \rangle = \Theta_B(x)^\top \cdot S \cdot \overline{\Theta_B(y)}. \tag{4.30}$$

Desweiteren gilt $S \in \mathbf{GL}_n(\mathbb{C})$ und

$$\overline{S}^\top = S. \tag{4.31}$$

Matrizen mit der Eigenschaft (4.31) heißen **hermitesch**.

Remark 4.50 Jede hermitesche Matrix $S \in \mathbf{GL}_n(\mathbb{C})$ definiert ein unitäres Skalarprodukt auf $\mathbb{C}^n$ durch

$$\langle x|y\rangle = x^\top \cdot S \cdot \overline{y}.$$

Remark 4.51 Eine reelle symmetrische Matrix $S \in \mathbf{GL}_n(\mathbb{R})$ ist insbesondere hermitesch, da $S = S^\top = \overline{S}^\top$ gilt.

Theorem 4.52 *Es sei $(V, \langle\cdot|\cdot\rangle)$ ein unitärer Vektorraum. Dann ist durch*

$$\|x\| = \sqrt{\langle x|x\rangle} \tag{4.32}$$

eine Norm auf V definiert.

Durch die Norm können wir Abstände in V wie in Definition 4.35 definieren.
Die Cauchy-Schwarz-Ungleichung gilt, wenn $\langle x|y\rangle^2$ durch $|\langle x|y\rangle|^2$ ersetzt wird:

Theorem 4.53 (Cauchy-Schwarz-Ungleichung) *Es sei $(V, \langle\cdot|\cdot\rangle)$ ein unitärer Vektorraum. Für alle $x, y \in V$ gilt:*

$$|\langle x|y\rangle|^2 \leq \langle x|x\rangle \cdot \langle y|y\rangle. \tag{4.33}$$

Gleichheit gilt genau dann, wenn x und y linear abhängig sind.

Orthogonalität $x \perp y$ wird wieder durch $\langle x|y\rangle = 0$ definiert.

Theorem 4.54 (Pythagoras) *Es seien x, y Elemente eines unitären Vektorraumes. Gilt $x \perp y$, so folgt*

$$\|x\|^2 + \|y\|^2 = \|x + y\|^2. \tag{4.34}$$

Im Folgenden sprechen wir von einem **Vektorraum mit Skalarprodukt**, wenn V entweder ein euklidischer oder unitärer Vektorraum ist.

Part IV
Appendix

A The Geometry of Complex Numbers

The field $\mathbb{C}$ of **complex numbers** consists of the numbers

$$z = x + \mathrm{i}y$$

where $x, y \in \mathbb{R}$ and $\mathrm{i} = \sqrt{-1}$.

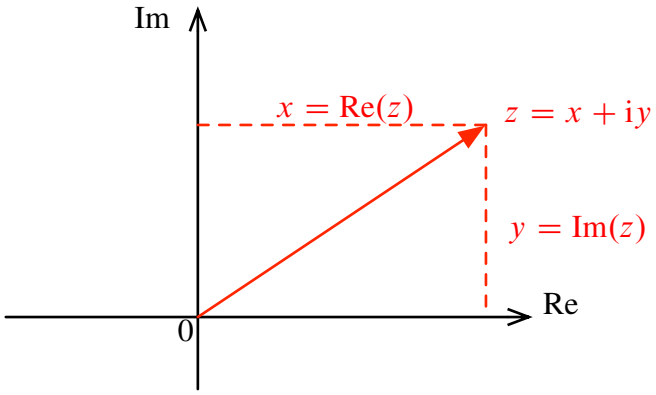
Exercise A.1 Restricting the multiplication in $\mathbb{C}$ to the real numbers $\mathbb{R} \subset \mathbb{C}$ makes $\mathbb{C}$ into an $\mathbb{R}$-vector space of dimension 2.

A.1 The Complex Plane

Via the map

$$x + \mathrm{i}y \mapsto \begin{pmatrix} x \\ y \end{pmatrix}$$

$\mathbb{C}$ is identified with the plane $\mathbb{R}^2$, which is called the **complex plane** in this context.



The x-axis represents the real numbers, the y-axis the purely imaginary numbers. The number 1 corresponds to the first unit vector $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$, the number i corresponds to the second unit vector $\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$.

In this representation, the **absolute value** (or **modulus**) of a complex number

$$|z| = \sqrt{\mathrm{Re}(z)^2 + \mathrm{Im}(z)^2}$$

corresponds to the Euclidean length $\sqrt{x^2 + y^2}$ of the vector $\binom{x}{y}$.

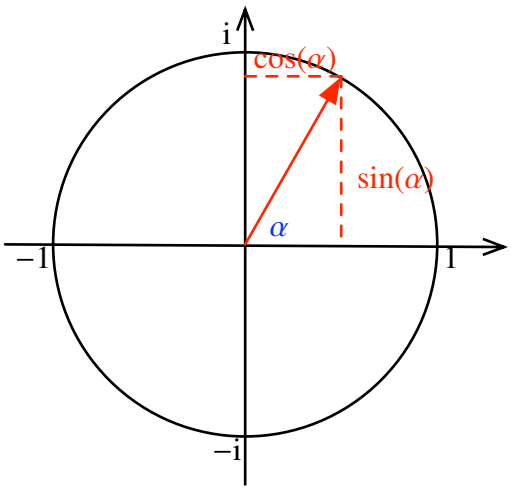
A.2 Complex Addition

The addition of two complex numbers $z_1 = x_1 + \mathrm{i}y_1$, $z_2 = x_2 + \mathrm{i}y_2$ corresponds to the addition of the associated vectors in the plane,

$$z_1 + z_2 = x_1 + \mathrm{i}y_1 + x_2 + \mathrm{i}y_2 = (x_1 + x_2) + \mathrm{i}(y_1 + y_2).$$

A.3 Complex Multiplication

Let $u \in \mathbb{C}$ be a complex number with absolute value $|u| = 1$. Then u lies on the unit circle of the complex plane. The **polar angle** (or **argument**) α of u is the angle enclosed by the real axis and the line segment connecting u to 0.



As indicated in the figure above, u has real and imaginary part

$$\mathrm{Re}(u) = \cos(\alpha), \quad \mathrm{Im}(u) = \sin(\alpha).$$

This means

$$u = \cos(\alpha) + \mathrm{i}\sin(\alpha). \tag{A.1}$$

If we substitute the respective power series for cosine and sine, we obtain the formal equation

$$u = \mathrm{e}^{\mathrm{i}\alpha}. \tag{A.2}$$

Indeed, the same rules as for the real exponential function apply:

$$\mathrm{e}^0 = 1, \quad \mathrm{e}^{\mathrm{i}\alpha}\mathrm{e}^{\mathrm{i}\beta} = \mathrm{e}^{\mathrm{i}(\alpha+\beta)}.$$

We now wish to interprete the multiplication by $u = \mathrm{e}^{\mathrm{i}\alpha}$ geometrically in $\mathbb{R}^2$: For any $z = x + \mathrm{i}y \in \mathbb{C}$ we have

$$\begin{aligned}\mathrm{e}^{\mathrm{i}\alpha} \cdot z &= (\cos(\alpha) + \mathrm{i}\sin(\alpha)) \cdot (x + \mathrm{i}y) \\ &= (\cos(\alpha)x + \mathrm{i}\sin(\alpha)x + \mathrm{i}\cos(\alpha)y - \sin(\alpha)y) \\ &= (\cos(\alpha)x - \sin(\alpha)y) + \mathrm{i}(\sin(\alpha)x + \cos(\alpha)y).\end{aligned}$$

In coordinates of $\mathbb{R}^2$, this corresponds to the map

$$\begin{pmatrix}\cos(\alpha)x - \sin(\alpha)y \\ \sin(\alpha)x + \cos(\alpha)y\end{pmatrix} = \begin{pmatrix}\cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha)\end{pmatrix} \cdot \begin{pmatrix}x \\ y\end{pmatrix}$$

So the multiplication by $\mathrm{e}^{\mathrm{i}\alpha}$ corresponds to a counterclockwise rotation by the angle α, given by the rotation matrix

$$\begin{pmatrix}\cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha)\end{pmatrix}.$$

Exercise A.2 The set

$$\mathbf{S}^1 = \{u \in \mathbb{C} \mid |u| = 1\}$$

with the complex multiplication is a group isomorphic to the special orthogonal group $\mathbf{SO}_2$.

Now let $w \in \mathbb{C}$ arbitrary. As $w = |w| \cdot \frac{w}{|w|}$, we can write w as the product of a real number $r = |w|$ and a complex number $u = \frac{w}{|w|}$ on the unit circle. By (A.2), we can write w as

$$w = r \cdot \mathrm{e}^{\mathrm{i}\alpha}. \tag{A.3}$$

This is the representation of w in **polar coordinates** (r, α). Multiplication of $z = x + \mathrm{i}y \in \mathbb{C}$ by $r \in \mathbb{R}$, $r > 0$, yields

$$r \cdot z = rx + \mathrm{i}ry,$$

so $|r \cdot z| = r \cdot |z|$. This corresponds to a dilation of $\binom{x}{y}$ by the factor r,

$$\begin{pmatrix}r & 0 \\ 0 & r\end{pmatrix} \cdot \begin{pmatrix}x \\ y\end{pmatrix} = \begin{pmatrix}rx \\ ry\end{pmatrix}.$$

So multiplication by an arbitrary number $w = r \cdot e^{i\alpha} \in \mathbb{C}$ is the combination of a rotation by the angle α and a dilation by the factor $r = |w|$:

$$\begin{pmatrix} r\cos(\alpha)x - r\sin(\alpha)y \\ r\sin(\alpha)x + r\cos(\alpha)y \end{pmatrix} = \underbrace{\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}}_{\text{dilation}} \cdot \underbrace{\begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}}_{\text{rotation}} \cdot \begin{pmatrix} x \\ y \end{pmatrix}.$$

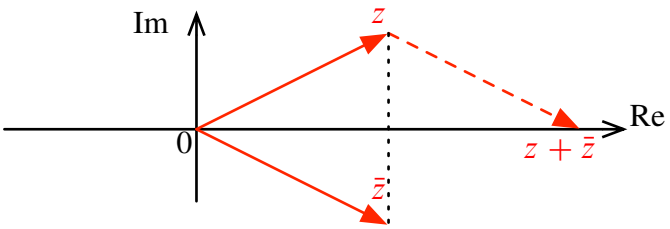
A.4 Complex Conjugation

Complex conjugation is the map

$$\mathbb{C} \to \mathbb{C}, \quad z = x + iy \mapsto \overline{z} = x - iy.$$

In the complex plane, this corresponds to a reflection on the real axis:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ -y \end{pmatrix}.$$



As the figure indicates, $z + \overline{z} \in \mathbb{R}$ and $\frac{1}{2}(z + \overline{z}) = \mathrm{Re}(z)$ is the projection of z onto the real axis. Similarly one sees that $\frac{1}{2}(z - \overline{z}) = i \cdot \mathrm{Im}(z)$ is the projection of z onto the imaginary axis.

The absolute value $|z|$ can be expressed by means the complex conjugation:

$$z \cdot \overline{z} = (x + iy) \cdot (x - iy) = x^2 + y^2 = |z|^2.$$

This provides us with an elegant expression for the inverse of z:

$$z^{-1} = \frac{\overline{z}}{|z|^2}.$$

A.5 Roots of Unity

Let $n \in \mathbb{N}$ and

$$\mathbf{\Omega}_n = \{\omega \in \mathbb{C} \mid \omega^n = 1\}. \tag{A.4}$$

The elements of $\mathbf{\Omega}_n$ are called the ***n*th roots of unity**. They are the zeros of the polynomial $X^n - 1$.

Theorem A.3 *$\mathbf{\Omega}_n$ is a finite subgroup of $\mathbf{S}^1$ of order $|\mathbf{\Omega}_n| = n$. In particular, $|\omega| = 1$ for all $\omega \in \mathbf{\Omega}_n$. Moreover, $\mathbf{\Omega}_n$ is cyclic.*

PROOF: As $1 = |\omega^n| = |\omega|^n$ and $|\omega|$ is a positive real number, it follows that $|\omega| = 1$. So $\mathbf{\Omega}_n \subset \mathbf{S}^1$.

Clearly, $1 \in \mathbf{\Omega}_n$, and for $\omega, \omega_1, \omega_2 \in \mathbf{\Omega}_n$:

$$(\omega^{-1})^n = \frac{1}{\omega^n} = \frac{1}{1} = 1, \quad (\omega_1\omega_2)^n = \omega_1^n\omega_2^n = 1 \cdot 1 = 1,$$

so $\mathbf{\Omega}_n$ is a subgroup of $\mathbf{S}^1$.

Now let

$$\omega_0 = \mathrm{e}^{\frac{2\pi\mathrm{i}}{n}}.$$

Using (A.1) one checks that for all $1 \leq k < n$:

$$\omega_0^k = \mathrm{e}^{2\pi\mathrm{i}\frac{k}{n}} \neq 1 \tag{$*$}$$

and

$$(\omega_0^k)^n = (\omega_0^n)^k = 1,$$

so $\omega_0^k \in \mathbf{\Omega}_n$. The n elements

$$1, \omega_0, \omega_0^2, \ldots, \omega_0^{n-1}$$

are all distinct, for if $\omega_0^p = \omega_0^q$ for some $0 \leq p < q < n$, then $1 \leq q - p < n$ and

$$1 = \omega_0^q(\omega_0^q)^{-1} = \omega_0^q(\omega_0^p)^{-1} = \omega_0^{q-p},$$

which contradicts $(*)$. So $\mathbf{\Omega}_n$ contains at least n elements, but as the $\omega \in \mathbf{\Omega}_n$ are the roots of the polynomial $X^n - 1$, there are at most n elements in $\mathbf{\Omega}_n$. It follows that $|\mathbf{\Omega}_n| = n$ and $\mathbf{\Omega}_n$ is cyclic with generator ω_0. ◇

A generator of $\mathbf{\Omega}_n$ is called a **primitive *n*th root of unity**.

The proof of Theorem A.3 shows that for a given n,

$$\omega_0 = \mathrm{e}^{\frac{2\pi\mathrm{i}}{n}}$$

is a primitive nth root of unity and

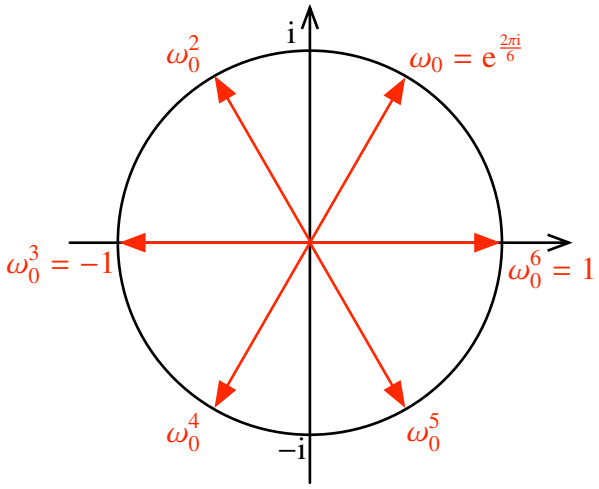
$$\mathbf{\Omega}_n = \langle\omega_0\rangle = \{1, \mathrm{e}^{2\pi\mathrm{i}\frac{1}{n}}, \mathrm{e}^{2\pi\mathrm{i}\frac{2}{n}}, \ldots, \mathrm{e}^{2\pi\mathrm{i}\frac{(n-1)}{n}}\}.$$

Example A.4 (Roots of unity)

(a) $\mathbf{\Omega}_2 = \{1, -1\}$. A primitive root of unity is -1.

(b) $\mathbf{\Omega}_4 = \{1, \mathrm{i}, -1, -\mathrm{i}\}$. The primitive roots of unity are i and $-\mathrm{i}$.

(c) The following figure shows $\mathbf{\Omega}_6$.



One can also see the group $\mathbf{\Omega}_3 \subset \mathbf{\Omega}_6$, generated by ω_0^2. ♡

Exercise A.5 If ω_0 is a primitive $2m$th root of unity, then ω_0^2 is a primitive mth root of unity.

Exercise A.6 $\mathrm{e}^{2\pi\mathrm{i}\frac{k}{n}} \in \mathbf{\Omega}_n$ is a primitive root of unity if and only if $\gcd(k, n) = 1$. As a consequence, there exist precisely $\varphi(n)$ primitive roots of unity in $\mathbf{\Omega}_n$.

Exercise A.7 With the formula for the finite geometric series one shows

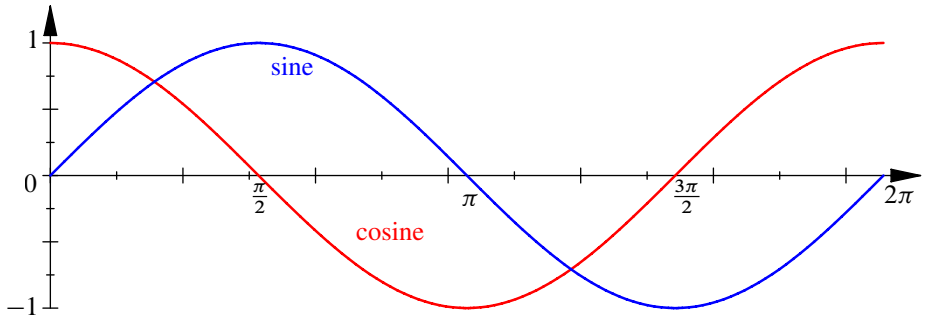
$$0 = 1 + \omega_0^k + \omega_0^{2k} + \ldots + \omega_0^{(n-1)k}$$

for a primitive nth root of unity ω_0 and $0 < k < n$.

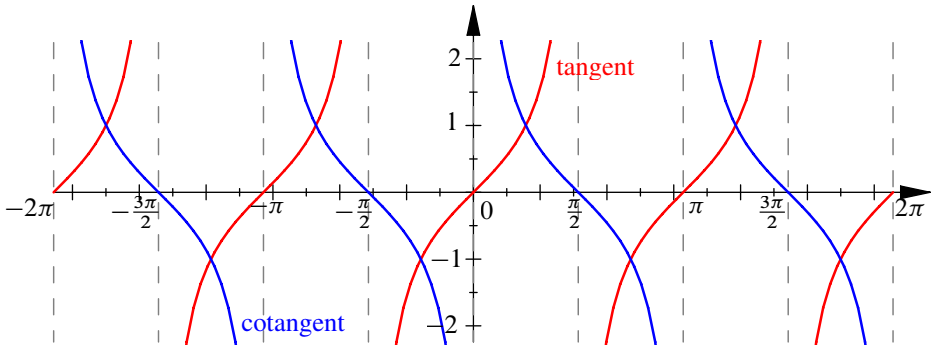
B Trigonometric Functions

B.1 Graphs

The graphs of the sine and cosine functions on the interval $[0, 2\pi]$:



The graphs of the tangent and cotangent functions on the interval $[-2\pi, 2\pi]$:



B.2 Table

α	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$	2π
$\sin(\alpha)$	0	$\frac{1}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{\sqrt{3}}{2}$	1	0	-1	0
$\cos(\alpha)$	1	$\frac{\sqrt{3}}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{1}{2}$	0	-1	0	1
$\tan(\alpha)$	0	$\frac{\sqrt{3}}{3}$	1	$\sqrt{3}$		0		0

B.3 Trigonometric Identities

Pythagoras' Theorem:

$$\sin(x)^2 + \cos(x)^2 = 1$$

Tangent and cotangent:

$$\tan(x) = \frac{\sin(x)}{\cos(x)}, \qquad \cot(x) = \frac{\cos(x)}{\sin(x)}$$

Angle sums:

$$\begin{aligned}
\sin(x \pm y) &= \sin(x)\cos(y) \pm \cos(x)\sin(y) \\
\cos(x \pm y) &= \cos(x)\cos(y) \mp \sin(x)\sin(y) \\
\tan(x \pm y) &= \frac{\tan(x) \pm \tan(y)}{1 \mp \tan(x)\tan(y)} \\
\cot(x \pm y) &= \frac{-1 \pm \cot(x)\cot(y)}{\cot(x) \pm \cot(y)} \\
\sin(2x) &= 2\sin(x)\cos(x) \\
\cos(2x) &= \cos(x)^2 - \sin(x)^2 \\
&= 2\cos(x)^2 - 1 \\
&= 1 - 2\sin(x)^2 \\
\tan(2x) &= \frac{2\tan(x)}{1 - \tan(x)^2} \\
\cot(2x) &= \frac{\cot(x)^2 - 1}{2\cot(x)} \\
\sin(x) + \sin(y) &= 2\sin\Big(\frac{x+y}{2}\Big)\cos\Big(\frac{x-y}{2}\Big) \\
\sin(x) - \sin(y) &= 2\cos\Big(\frac{x+y}{2}\Big)\sin\Big(\frac{x-y}{2}\Big) \\
\cos(x) + \cos(y) &= 2\cos\Big(\frac{x+y}{2}\Big)\cos\Big(\frac{x-y}{2}\Big) \\
\cos(x) - \cos(y) &= -2\sin\Big(\frac{x+y}{2}\Big)\sin\Big(\frac{x-y}{2}\Big) \\
\sin(x)\sin(y) &= \frac{\sin(x+y) - \cos(x-y)}{2} \\
\sin(x)\cos(y) &= \frac{\sin(x+y) + \sin(x-y)}{2} \\
\cos(x)\cos(y) &= \frac{\cos(x+y) + \cos(x-y)}{2}
\end{aligned}$$

Periodicity:

$$\begin{aligned}
\sin(-x) &= -\sin(x) \\
\sin\left(x \pm \frac{\pi}{2}\right) &= \pm\cos(x) \\
\sin(x \pm \pi) &= -\sin(x) \\
\cos(-x) &= \cos(x) \\
\cos\left(x \pm \frac{\pi}{2}\right) &= \mp\sin(x) \\
\cos(x \pm \pi) &= -\cos(x)
\end{aligned}$$

Complex:

$$\begin{aligned}
\mathrm{e}^{\mathrm{i}x} &= \cos(x) + \mathrm{i}\sin(x) \\
\sin(x) &= \frac{\mathrm{e}^{\mathrm{i}x} - \mathrm{e}^{-\mathrm{i}x}}{2\mathrm{i}} \\
\cos(x) &= \frac{\mathrm{e}^{\mathrm{i}x} + \mathrm{e}^{-\mathrm{i}x}}{2}
\end{aligned}$$

References

[1] S. BOSCH
Algebra (7. Aufl.)
Springer, 2009

[2] E. BRIESKORN
Lineare Algebra I & II
Vieweg, 1983 & 1985

[3] G. FISCHER
Analytische Geometrie (7. Aufl.)
Vieweg, 2001

[4] G. FISCHER
Lineare Algebra (17. Aufl.)
Vieweg, 2010

[5] O. FORSTER
Algorithmische Zahlentheorie
Vieweg, 1996

[6] C. GASQUET, P. WITOMSKI
Fourier Analysis and Applications
Springer, 1999

[7] B.C. HALL
Lie Groups, Lie Algebras, and Representations
Springer, 2003

[8] D.E. KNUTH
The Art of Computer Programming 2: Seminumerical Algorithms (3. Aufl.)
Addison-Wesley Longman, 1997

[9] T.W. KÖRNER
Fourier Analysis
Cambridge University Press, 1988

[10] J.D. LIPSON
Elements of Algebra and Algebraic Computing
Benjamin Cummings, 1981

[11] H.P. REHM, W. TRINKS
Lineare Algebra und analytische Geometrie
Vorlesungsskript Universität Karlsruhe (TH), 2000

[12] H.R. SCHWARZ
Numerische Mathematik
Teubner, 1997

[13] D. WERNER
Funktionalanalysis (7. Aufl.)
Springer, 2011

[14] H. WEYL
Symmetry
Princeton University Press, 1952

[15] H. ZIESCHANG
Lineare Algebra und Geometrie
Teubner, 1997

Index